Service Practice Statement for Non eIDAS Certificate Services

Statement of NETLOCK Ltd. regarding the detailed requirements of procedure and operation applied in relation to the provision of enchryption, authentication, codesign and DV SSL (non-eIDAS) certification services and related certificate status services

[TRANSLATION OF THE SAME TITLED HUNGARIAN-LANGUAGE OFFICIAL DOCUMENT]

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

Document name in Hungarian:	Szolgáltatási Szabályzat Nem eIDAS Tanúsítványszolgáltatásokra
Document name in English:	Service Practice Statement for Non eIDAS Certificate Services
Document short name:	SPS-C-EN
Version:	20231004
Object identifier (OID):	1.3.6.1.4.1.3555.1.1.17.0.231103
Date of approval:	04/10/2023
Date of publication:	04/10/2023
Valid from:	03/11/2023
No. of pages:	166 pages including cover
Approved by:	**Frecska Ábel** CEO, NETLOCK Ltd.

© COPYRIGHT NETLOCK KFT., 2023. - ALL RIGHTS RESERVED

The present document is a translation of the original same titled Hungarian language Service Practice Statement. It is published with the same OID as the original hungarian document (see Hungarian and English title and OID on cover).

The present English version is not the official Service Practice Statement for qualified certificate services of NETLOCK. The official Practice Statement registered by the Supervisory Body is the Hungarian version.

In case of any difference between the Hungarian and the English version, the Hungarian version shall be applied.

TRANSLATION

TABLE OF CONTENT

TABLE OF CONTENT 3
1. INTRODUCTION 10
1.1 OVERVIEW 10
1.1.1. Standards and requirements 11
1.1.2. The Service Provider 11
1.2 DOCUMENT NAME AND IDENTIFICATION 12
1.2.1. Certificate policies 13
1.2.2. Revisions of the Document 14
1.3 PKI PARTICIPANTS 16
1.3.1. Certification Authorities 16
1.3.2. Registration Authorities 17
1.3.3. Subscribers, End-Users, and Applicants 18
1.3.4. Relying Party 18
1.3.5. Other participants 18
1.4 CERTIFICATE USAGE 19
1.4.1. Proper use of certificates 19
1.4.2. Prohibited use of certificates 20
1.5 REGULATION ADMINISTRATION 20
1.5.1. The organization that carries out the administration of the document 20
1.5.2. Contact person of the document 20
1.5.3. The organization resplsible for the compliance of the present practice statement with the certificate policy 21
1.5.4. Adoption of the Practice Statement 21
1.6 TERMS & ABBREVIATIONS 22
1.6.1. Definitions 22
1.6.2. Abbreviations 31
2. PUBLICATION AND CERTIFICATE REPOSITORY 34
2.1 REPOSITORIES 34
2.1.1. Publication of certification information 34
2.1.2. Publication of Terms and Conditions 35
2.1.3. Declarations 36
2.2 TIME OR FREQUENCY OF PUBLICATION 36
2.3 ACCESS CONTROLS ON REPOSITORIES 37
3. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS 38
3.1 NAMING 38
3.1.1. Types of names 40
3.1.2. Need for names to be meaningful 40
3.1.3. Pseudonyms 42
3.1.4. Rules for interpreting various name forms 43

TRANSLATION

3.1.5. Uniqueness of names 44
3.1.6. Recognition, authentication, and role of trademarks 44

3.2 Initial identity validation 45
3.2.1. Method to prove possession of private key 47
3.2.2. Authentication of organization identity 47
3.2.3. Authentication of individual identity 50
3.2.4. Non-verified subscriber information 52
3.2.5. Control of eligibilities and delegation 52
3.2.6. Criteria for interoperation 55

3.3 Identification and authentication for managing certificates 55
3.3.1. Identification and certification in the case of a valid certificate 56
3.3.2. Identification and certification in the case of an invalid certificate 56

3.4 Identification and authentication for status change request 57

4. CERTIFICATE LIFECYCLE REQUIREMENTS 58

4.1 Certificate enrolment 58
4.1.1. Who can submit a certificate application 59
4.1.2. Enrolment process and responsibilities 60

4.2 Certificate application processing 64
4.2.1. Performing identification and authentication functions 65
4.2.2. Approval or rejection of certificate applications 67
4.2.3. Time to process certificate applications 69

4.3 Certificate issuance 69
4.3.1. SP actions during certificate issuance 71
4.3.2. Notification by the SP of issuance of certificate 71

4.4 Certificate acceptance 71
4.4.1. Conduct constituting certificate acceptance 72
4.4.2. Publication of the certificate by the SP 72
4.4.3. Notification of certificate issuance by the SP to other entities 72

4.5 Key pair and certificate usage 73
4.5.1. Subscriber private key and certificate usage 73
4.5.2. Relying party public key and certificate usage 73

4.6 Certificate renewal 74
4.6.1. Circumstance for certificate renewal 74
4.6.2. Who may request renewal 75
4.6.3. Processing certificate renewal requests 75
4.6.4. Notification of new certificate issuance to subscriber 77
4.6.5. Conduct constituting acceptance of a renewal certificate 77
4.6.6. Publication of the renewal certificate by the SP 77
4.6.7. Notification of certificate issuance by the SP to other entities 78

4.7 Re-key 78
4.7.1. Circumstance for certificate re-key 78
4.7.2. Who may request certification of a new public key 78
4.7.3. Processing certificate re-keying requests 79
4.7.4. Notification of new certificate issuance to subscriber 79

TRANSLATION

4.7.5. Conduct constituting acceptance of a re-keyed certificate 79
4.7.6. Publication of the re-keyed certificate by the SP 79
4.7.7. Notification of certificate issuance by the SP to other entities 79

4.8 CERTIFICATE MODIFICATION 79

4.8.1. Circumstance for certificate modification 80
4.8.2. Who may request certificate modification 80
4.8.3. Processing certificate modification requests 80
4.8.4. Notification of new certificate issuance to subscriber 80
4.8.5. Conduct constituting acceptance of modified certificate 80
4.8.6. Publication of the modified certificate by the SP 81
4.8.7. Notification of certificate issuance by the SP to other entities 81

4.9 CERTIFICATE STATUS CHANGE 81

4.9.1. Circumstances for revocation and suspension 81
4.9.2. Who can request status change 83
4.9.3. Procedure for revocation, suspension and activation 84
4.9.4. Revocation request grace period 85
4.9.5. Time within which SP must process the status change request 86
4.9.6. Certificate status checking requirement for relying parties 86
4.9.7. CRL issuance frequency 87
4.9.8. Maximum latency for CRLs 88
4.9.9. On-line status checking availability 88
4.9.10. On-line status checking requirements 88
4.9.11. Other forms of revocation advertisements available 88
4.9.12. Special requirements re-key compromise 89
4.9.13. Limits on suspension period 89

4.10 CERTIFICATE STATUS SERVICES 89

4.10.1. Operational characteristics 90
4.10.2. Service availability 91
4.10.3. Optional features 91

4.11 END OF SUBSCRIPTION 91
4.12 KEY ESCROW AND RECOVERY 92

4.12.1. Key escrow and recovery policy and practices 92
4.12.2. Session key encapsulation and recovery policy and practices 92

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 93

5.1 PHYSICAL CONTROLS 93

5.1.1. Site location and construction 94
5.1.2. Physical access 94
5.1.3. Power and air conditioning 95
5.1.4. Water exposures 96
5.1.5. Fire prevention and protection 96
5.1.6. Media storage 96
5.1.7. Waste disposal 96
5.1.8. Off-site backup 96

5.2 PROCEDURAL CONTROLS 97

5.2.1. Trusted roles 97
5.2.2. Number of persons required per task 98

TRANSLATION

5.2.3. Identification and authentication for each role ... 98
5.2.4. Roles requiring separation of duties ... 99
5.3 PERSONNEL CONTROLS ... 99
5.3.1. Qualifications, experience, and clearance requirements ... 100
5.3.2. Inspection Procedures ... 101
5.3.3. Training requirements ... 101
5.3.4. Retraining frequency and requirements ... 102
5.3.5. Job rotation frequency and sequence ... 102
5.3.6. Sanctions for unauthorized actions ... 102
5.3.7. Independent contractor requirements ... 102
5.3.8. Documentation supplied to personnel ... 102
5.4 AUDIT LOGGING PROCEDURES ... 103
5.4.1. Types of events recorded ... 103
5.4.2. Frequency of processing log ... 104
5.4.3. Retention period for audit log ... 104
5.4.4. Protection of audit log ... 104
5.4.5. Audit log backup procedures ... 105
5.4.6. Audit collection system ... 105
5.4.7. Notification to event-causing subject ... 105
5.4.8. Vulnerability assessments ... 105
5.5 RECORDS ARCHIVAL ... 105
5.5.1. Types of records archived ... 106
5.5.2. Retention period for archive ... 106
5.5.3. Protection of archive ... 107
5.5.4. Archive backup procedures ... 107
5.5.5. Requirements for timestamping of records ... 107
5.5.6. Archive collection system ... 107
5.5.7. Procedures to obtain and verify archive information ... 107
5.5.8. Miscellaneous archiving provisions ... 107
5.6 KEY CHANGEOVER ... 107
5.7 COMPROMISE AND DISASTER RECOVERY ... 108
5.7.1. Incident and compromise handling procedures ... 108
5.7.2. Computing resources, software, and/or data are corrupted ... 109
5.7.3. Entity private key compromise procedures ... 109
5.7.4. Business continuity capabilities after a disaster ... 110
5.8 CA OR RA TERMINATION ... 110
6. TECHNICAL SECURITY CONTROLS ... 113
6.1 KEY PAIR GENERATION AND INSTALLATION ... 113
6.1.1. Key pair generation ... 114
6.1.2. Private key delivery to subscriber ... 115
6.1.3. Public key delivery to certificate issuer ... 115
6.1.4. SP public key delivery to relying parties ... 116
6.1.5. Key sizes ... 116
6.1.6. Public key parameters generation and quality checking ... 116
6.1.7. Key usage purposes (as per X.509 v3 key usage field) ... 117
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS ... 118

TRANSLATION

6.2.1. Cryptographic module standards and controls ... 118
6.2.2. Private key (n out of m) multi-person control ... 121
6.2.3. Private key escrow ... 121
6.2.4. Private key backup ... 121
6.2.5. Private key archival ... 121
6.2.6. Private key transfer into or from a cryptographic module ... 121
6.2.7. Private key storage on cryptographic module ... 122
6.2.8. Method of activating private key ... 122
6.2.9. Method of deactivating private key ... 122
6.2.10. Method of destroying private key ... 122
6.2.11. Cryptographic Module Rating ... 122

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT ... 123
6.3.1. Public key archival ... 123
6.3.2. Certificate operational periods and key pair usage periods ... 123

6.4 ACTIVATION DATA ... 123
6.4.1. Activation data generation and installation ... 124
6.4.2. Activation data protection ... 124
6.4.3. Other aspects of activation data ... 124

6.5 COMPUTER SECURITY CONTROLS ... 124
6.5.1. Specific computer security technical requirements ... 125
6.5.2. Computer security rating ... 125

6.6 LIFE CYCLE TECHNICAL CONTROLS ... 125
6.6.1. System development controls ... 125
6.6.2. Security management controls ... 125
6.6.3. Life cycle technical controls ... 126

6.7 NETWORK SECURITY ... 126
6.8 TIMESTAMPING ... 126

7. CERTIFICATE, CRL, OCSP PROFILES ... 127

7.1 CERTIFICATE PROFILE ... 127
7.1.1. Version number(s) ... 138
7.1.2. Certificate extensions ... 138
7.1.3. Algorithm object identifiers ... 140
7.1.4. Name forms ... 140
7.1.5. Name constraints ... 140
7.1.6. Certificate Policy object identifier ... 141
7.1.7. Usage of Policy Constraints extension ... 141
7.1.8. Policy qualifiers syntax and semantics ... 141
7.1.9. Processing semantics for the critical Certificate Policy extension ... 141

7.2 CRL PROFILE ... 141
7.2.1. Version number(s) ... 141
7.2.2. CRL extensions ... 141

7.3 OCSP PROFILE ... 142
7.3.1. Version number(s) ... 142
7.3.2. OCSP extensions ... 142

TRANSLATION

8. COMPLIANCE AUDIT 144
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 144
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 145
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 145
8.4 TOPICS COVERED BY ASSESSMENT/AUDIT 146
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 146
8.6 COMMUNICATION OF RESULTS 146
9. OTHER BUSINESS AND LEGAL MATTERS 147
9.1 FEES 147
9.1.1. Certificate issuance or renewal fees 148
9.1.2. Certificate access fees 148
9.1.3. Status changes or status information access fees 148
9.1.4. Fees for other services 148
9.1.5. Refund policy 148
9.2 FINANCIAL RESPONSIBILITY 149
9.2.1. Insurance coverage 149
9.2.2. Other assets 150
9.2.3. Insurance or warranty coverage for relying parties 150
9.3 HANDLING OF BUSINESS INFORMATION 150
9.3.1. Scope of confidential information 150
9.3.2. Information not within the scope of confidential information 151
9.3.3. Protection of confidential information 151
9.4 PRIVACY OF PERSONAL INFORMATION 152
9.4.1. Data management 152
9.4.2. Private information 153
9.4.3. Information not deemed private 153
9.4.4. Protection of personal data 154
9.4.5. Usage of private information 154
9.4.6. Data management 154
9.4.7. Other information disclosure circumstances 154
9.5 INTELLECTUAL PROPERTY RIGHTS 154
9.6 REPRESENTATIONS AND WARRANTIES 155
9.6.1. The Certification Authority's responsibilities 156
9.6.2. The RA's responsibilities 156
9.6.3. Client representations and warranties 156
9.6.4. Relying party representations and warranties 157
9.6.5. Representations and warranties of other participants 157
9.7 DISCLAIMERS OF WARRANTIES 158
9.8 LIMITATIONS OF LIABILITY 158
9.9 INDEMNITIES 158
9.10 TERM AND TERMINATION 159
9.10.1. Term 159
9.10.2. Termination 159
9.10.3. Effect of termination 159

TRANSLATION

9.11 Individual notices and communications with participants 159
9.12 Modifications 160
9.12.1. Amendments 161
9.12.2. Notification mechanism and period 161
9.12.3. Circumstances under which OID must be changed 161
9.13 Dispute resolution 162
9.13.1. Dispute resolution provisions 162
9.13.2. Amicable dispute resolution through negotiations 163
9.13.3. Litigious dispute resolution 163
9.14 Governing law 163
9.15 Compliance with applicable law and standards 163
9.16 Miscellaneous provisions 165
9.16.1. Entire agreement 165
9.16.2. Transferral 165
9.16.3. Partial invalidity 165
9.16.4. Enforcement 165
9.16.5. Force Majeure 166
9.17 Miscellaneous provisions 166

TRANSLATION

1. Introduction

The present document is the statement of NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (hereinafter: Service Provider or SP) regarding the detailed requirements of procedure and operation applied in relation to the provision and using of the so-called non-eIDAS certification services (hereinafter: Practice Statement or Statement).

The procedures and the practical rules pertaining thereto, which are recorded in the present practice statement shall only apply to the services enlisted in chapter 1.1 hereof and related to the certificates compliant with the certification policies set out in chapter 1.2.1 Certificate Policies (LCP, NCP, NCP+, DVCP and Codesign) of the document entitled Service Policy for Non-eIDAS Certificate Services (hereinafter: Service Policy).

The certificates compliant with each certificate policies and the short description thereof with the names used in the commercial communication of Service Provider are set out in Chapter 1.2.1 hereof.

For the definitions and abbreviations see chapter 1.6.

1.1 Overview

The present document contains the requirements pertaining to the following services of Service Provider:

- According to LCP, NCP, NCP+ certificate policies:
  - Personal authentication
  - Business authentication
  - Layer authentication
  - Organizational authentication
  - Personel enchryption
  - Business enchryption
  - Layer enchryption
  - Organizational enchryption
  - Codesign (Non-EV) for private persons
  - Codesign (Non-EV) for organizations
- According to DVCP certificate policies:
  - DV SSL
  - DV SSL UCC

Certificate status services related to non-eIDAS certificate services.

TRANSLATION

See Chapter 1.2.1 Certificate policies for the connection between the various certificates and certificate policies.

In addition to details information on the Service Provider's procedural and operational rules, the present Statement also provides Relying Parties with recommendations for checking electronic signatures, seals, including the certificates of these, and for the use of certificates for website authentication and other certificates.

1.1.1. Standards and requirements

The Service Practice Statement was created in line with the structure of the NETLOCK Service Policy for Non-eIDAS Certificate Issuance Service and sets forth the method for meeting the requirements determined therein. The various chapter titles serve only to order the contents according to the given logical order but are not governing in the interpretation of the provisions.

The contents of the Statement makes use of the recommendations of standards ETSI EN 319 401, ETSI EN 319 411, ETSI EN 319 412, and x.509.

In the case of website authentication certificates (DVCP) the NetLock conforms to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and this Guideline, this Guideline take precedence over this document

The laws, standards and requirements used and applied by Service Provider are detailed in Chapter 9.15.

1.1.2. The Service Provider

The entity referred to as the Service Provider in the present Statement is NETLOCK Kft.

Service Provider data:

Company Name:	**NETLOCK Informatics and Network Security Services Limited Liability Company**
Hungarian name:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Short name (EN/HU):	NETLOCK Ltd. / NETLOCK Kft.
Registered seat:	H-1101 Budapest, Expo tér 5-7.
Site (Customer Service)	H-1143 Budapest, Hungária körút 17.
Postal address:	H-1439 Budapest, Pf. 663
Company registration number:	01-09-563961
TAX ID:	12201521-2-42

TRANSLATION

PHONE NUMBER:	(+36 1) 437 6655 | *Application for certificate status change: Press 3*
WEBSITE:	https://netlock.hu/
STATEMENTS AND CLAUSES PUBLISHED:	https://netlock.hu/aktualis-szabalyzatok (official Hungarian versions) https://netlock.hu/aktualis-szabalyzatok/#en (English translation)
CUSTOMER SERVICE E-MAIL:	info@netlock.hu
FOR ORDERS, DOCUMENT COPIES, AND AGREEMENTS:	igenylesek@netlock.hu *or* kerelmek@netlock.hu
NETLOCK POLICY ACCEPTANCE UNIT EMAIL:	szee@netlock.hu
CUSTOMER SERVICE /BUSINESS HOURS:	At the place and within the time interval set out on the website of the Service Provider

This Service Practice Statement contains procedural and operational requirements concerning the rendering of certification services outside of the provisions of eIDAS and non-eIDAS certification services.

Annual voluntary accreditations and other qualifications:

- The certification of the certificate creation service has taken place in accordance with the ETSI EN 319 401, ETSI EN 319 411, and ETSI EN 319 412 standards.
- ISO 9001 standard
- ISO 27001 standard

Also see Chapter 8.

1.2 Document name and identification

For the name of the document and its OID, see the cover sheet (first page with the logo of Service Provider) in the lines of "Document name in Hungarian" and "Document name in English" and also in the "Object identifier (OID)" lines.

On the other pages in the header the OID is displayed, and the English name in the footer.

For the date of the approval, publishing and validity, also see the cover sheet.

The present document is one of the documents issued by Service Provider, which provide for a uniform regulatory framework of the conditions of the services provided by Service Provider. Such documents are the General Terms and Conditions, the Service Agreement, the practice statements, as well as the other agreements made with the Clients and the Partners.

In the present document the entity referred to as the Service Provider shall mean NETLOCK Kft. – see chapter 1.1.2 for its details.

TRANSLATION

1.2.1. Certificate policies

The Service Provider shall indicate the identification of the primary (standard) and secondary (unique) Certificate Policy identifiers defined in Section 1.2.1 of the Service Policy in the "Certificate Policies" field of the End User Certificates (see 7.1 Certificate profile).

The end-user certificate types distributed by the Service Provider and the compliance of the certificate policies (see Chapter 7.1 for the connection between certificate policies and certificate profiles).

About the currently publicly available certificate types – among the following – informations are provided on the SP's website and pricelist.

In case any specific procedure set out in the present practice statement does not apply to the application, issuance and management of all certificate types enlisted above, the different terms and conditions shall be separated herein on the basis of commercial names, and if necessary for the sake of clarity, the ID of the certificate policy shall also be indicated.

Default certificate types

COMMERCIAL NAMES OF NETLOCK CERTIFICATES	CERTIFICATE POLICY ID[1]	DESCRIPTION
PERSONAL ENCRYPTION - SW	LCP/NCP	Encryption certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of decoding files encoded with its public keypair.
BUSINESS ENCRYPTION - SW	LCP/NCP	Encryption certificate with business profile with software key storage and with key generation by the Client, the private key of which is capable of decoding files encoded with its public keypair.
ORGANIZATIONAL ENCRYPTION - SW	LCP/NCP	Encryption certificate with organizational profile with software key storage and with key generation by the Client, the private key of which is capable of decoding files encoded with its public keypair.
PERSONAL AUTHENTICATION - SW	LCP/NCP	Authentication certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
BUSINESS AUTHENTICATION - SW	LCP/NCP	Authentication certificate with business profile with software key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
ORGANIZATIONAL AUTHENTICATION - SW	LCP/NCP	Authentication certificate with organizational profile with software key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
PERSONAL AUTHENTICATION - SCD	LCP/NCP+	Authentication certificate with personal profile with SCD key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
BUSINESS AUTHENTICATION - SCD	LCP/NCP+	Authentication certificate with business profile with SCD key storage and with key generation by the Client, the private key

[1] See at Service Policy 1.2.1

TRANSLATION

		of which is capable of user authenticating in IT systems.
ORGANIZATIONAL AUTHENTICATION - SCD	LCP/NCP+	Authentication certificate with organizational profile with SCD key storage and with key generation by the Client, the private key of which is capable of user authenticating in IT systems.
PERSONAL AUTHENTICATION - SCD (CAMS)	LCP/NCP+	Authentication certificate with personal profile with SCD key storage and with key generation by the SP, the private key of which is capable of user authenticating in IT systems.
BUSINESS AUTHENTICATION - SCD (CAMS)	LCP/NCP+	Authentication certificate with business profile with SCD key storage and with key generation by the SP, the private key of which is capable of user authenticating in IT systems.
ORGANIZATIONAL AUTHENTICATION - SCD (CAMS)	LCP/NCP+	Authentication certificate with organizational profile with SCD key storage and with key generation by the SP, the private key of which is capable of user authenticating in IT systems.
ONLINE SSL	DVCP	Website authentication certificate for the authentication of one domain name, of which subject field contains only the domain name.
PERSONAL CODESIGN - SW	CSBR	Codesign certificate with personal profile with software key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
ORGANIZATIONAL CODESIGN - SW	CSBR	Codesign certificate with organization profile with software key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
PERSONAL CODESIGN - SCD/CAMS	CSBR	Codesign certificate with personal profile with SCD key storage and with key generation by the SP, the private key of which is capable of electronic signing program codes.
ORGANIZATIONAL CODESIGN - SCD/CAMS	CSBR	Codesign certificate with organisational profile with SCD key storage and with key generation by the SP, the private key of which is capable of electronic signing program codes.
PERSONAL CODESIGN - SCD	CSBR	Codesign certificate with personal profile with SCD key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.
ORGANIZATIONAL CODESIGN - SCD	CSBR	Codesign certificate with organizational profile with SCD key storage and with key generation by the Client, the private key of which is capable of electronic signing program codes.

Unique certificate types

In addition to the above certificate types, the Service Provider may issue other types of certificates, based on individual client demand. Uniquely configured certificate types always match a type derived from one of the types above (or other certificate policies defined in Section 1.2.1 of the Service Policy).

1.2.2. Revisions of the Document

OID	VALIDITY	DESCRIPTION OF CHANGE	PREPARED BY
1.3.6.1.4.1.3555.1.49.20191015	17.10.2019 - 05.04.2020	This document is a translation of the original same titled hungarian language Practice Statement that has also the same OID as the present document has (see Hungarian and English title and the OID on cover).	Zoltán Szabó Viktor Varga

TRANSLATION

1.3.6.1.4.1.3555.1.49.20200402	06.04.2020 - 07.09.2021.	New QSCD Client Device (6.2.1)	Éva Varga-Szabó
1.3.6.1.4.1.3555.1.49.20210830	08.09.2021- 02.11.2023.	All previous revisions in the same titled Hungarian document added in English translation.	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.17.0.231103	from 03.11.2023 until it is withdrawn or until a new version comes into force	• 1.1.2: Updating the Service Provider's contact details: removing fax availability (also in 4.1.2; 9.11.). • 1.2.1: Refinement • 2.1.1. Removal of IVCP caused by the IV SLL certificate type revocation • 4.1.2: Certificate Profile chart Refinement • 4.2.2 Clarification of the processing conditions for certificate applications • 5.7.3.c: Clarification of the procedure to be followed in case of compromise caused by an algorithm change; • 6.2.1: Clarification of the status monitoring methodology of SCD devices; SCD register update; • 6.3.2: Clarification of the lifetime of website authentication certificates; • 7.1.2: Correction of the key usage extension chart • 8.1 Implementation of Auditing of external partners and other service providers according to the ISO 27001 standard • 8.4: Clarifying details with configuration check regarding the areas covered by audit,; • 9.12.3: Refinement and alteration of the document ID (OID) procedure; • 9.15: Supplementing compliance standards with the ETSI EN 301 549 standard, • Other structural and formal changes (1.1; 1.1.2; 1.2.1; 2.1.1; 2.1.3; 3.1; 3.1.2;3.1.4; 3.2; 3.2.2; 3.2.3; 3.2.5; 3.3; 4.1; 4.1.2; 4.2.1; 4.2.2; 4.3; 4.3.1; 4.4.3; 4.5.2; 4.6.1; 4.6.3; 4.9; 4.9.3; 4.9.4; 4.9.5; 4.9.6; 4.9.10; 4.10.1; 4.10.2; 5.1.3; 5.1.7; 5.2.2; 5.2.4; 5.3; 5.3.1; 5.3.3; 5.5.1; 5.7.1; 5.7.3; 5.7.4; 5.8; 6; 6.1.1; 6.1.5; 6.1.6; 6.1.7; 6.2.1; 6.2.4; 6.3.1; 6.3.2; 7.1; 7.1.2; 8.; 8.2; 9.1.4; 9.2.1; 9.5; 9.6.3; 9.6.4; 9.7; 9.12.3; 9.13.2; 9.15.)	NETLOCK Compliance

1.3 PKI participants

The community that uses the issued certificates consists of the Service Provider, the Registration and other Cooperating Authorities in a contractual relationship with the Service Provider, certificate Applicants, End-Users, Subscribers, and the Relying Parties.

See also the relevant definitions in Section 1.6.1 Definitions.

1.3.1. Certification Authorities

The Service Provider operates a Certification Authority and more than one CA managed by it.

Service Provider does not associate with any External Certification Authority.

The operation of the Certificate Authority compliant with the requirements covering the Authority set out in the Certificate Policy, the present Practice Statement and other Terms shall be ensured by the proprietary internal rules of operation of the Certification Authority. The Certification Authority employees Certification Administrator. The employees working at the Certification Authority shall carry out their activities in accordance with the requirements set out in the internal rules of operation.

The Service Provider uses the following CAs:

- the Intermediate CA that certifies both end-user and SP certificates, and
- the top-level Root CA

which operate in the form of a hierarchy.

The Service Provider may also authenticate Servers that are linked to Subordinated Services.

The Certification Authority is responsible for issuing certificates. The Certification Authorities employs Certification Administrators who are responsible for executing the (non-automated) tasks related to the issuance, renewal, modification, and status change of certificates on the basis of the identification and data verification performed by the Registration Authority. See Chapter 9.6.1. The Validation Specialists trusted role is filled by the Certification Administrators.

The name and SHA256 hash of the Root CAs of the Service Provider:

NAME OF ROOTCA	HASH
NetLock Arany (Class Gold) Főtanúsítvány	6C:61:DA:C3:A2:DE:F0:31:50:6B:E0:36:D2:A6:FE:40:19:94:FB:D1:3D:F9:C8:D4:66:59:92:74:C4:46:EC:98
NetLock Platina (Class Platinum) Főtanúsítvány	EB:7E:05:AA:58:E7:BD:32:8A:28:2B:F8:86:70:33:F3:C0:35:34:2B:51:6E:E8:5C:01:67:3D:FF:FF:BB:FE:58

Main data of the non-eIDAS intermediary CAs:

TRANSLATION

NAME OF CA	LINK TO CA CERTIFICATE	LINK TO CRL
NETLOCK Trust CA	www.netlock.hu/index.cgi?ca=trust	www.netlock.hu/index.cgi?crl=trust
NETLOCK DVSSL CA	www.netlock.hu/index.cgi?ca=DVCA	www.netlock.hu/index.cgi?crl=DVCA
NETLOCK CodeSign CA	www.netlock.hu/index.cgi?ca=codesignca	http://www.netlock.hu/index.cgi?crl=codesignca

More information and other CAs can be found on the website of the Service Provider[2].

1.3.2. Registration Authorities

The Service Provider operates a Central Registration Authority and cooperates with valamint External Registration Authorities. The Central Registration Authority employs Registration Administrators, Mobile Registration Associates, and works together with Delivery Agents. The External Registration Authorities employ at least one Registration Administrator. The Central Registration Authority of Service Provider operates at the registered office of the Service Provider, which may be attended by the Clients in the hours of servce set out on the website of Service Provider (see 1.1.2) for the validation of their identity and for other registration-related administration.

The External Registration Authorities provide registration services only for the clientele set out in the agreement made with the Service Provider Partner. Service Provider shall provide information on the External Registration Authorities, the contact details and clientele on its website (see 1.1.2).

The Registration Authorities are responsible for identifying the entity(-ies) indicated as the subject of the certificate and involved in the application, checking their data and authorisation to proceed, recording the certificate application and forwarding it to the Certification Authority, coordinating the certificate issuance procedure, documentation, performing additional certificate management and status change requests, and handing over the Client device.

The Service Provider's customer service employees take care of customer service tasks and communicate with Clients. Customer service is a separate group within the Central Registration Authority. The Service Provider publishes their contact information (see 1.1.2) on its website.

The operation of the Registration Authorities compliant with the requirements covering the Authorities set out in the Certificate Policy, the present Practice Statement and other Terms shall be ensured by the proprietary internal rules of operation of the Registration Authority. The employees working at the Registration Authorities shall carry out their activities in accordance with the requirements set out in the internal rules of operation. Service Provider obliges the

[2] https://netlock.hu/tanusitvanykiadok/

TRANSLATION

External Registration Authorities to comply with the applicable requirements in the agreement made with the Partner to the Service Provider.

See Chapter 9.6.2.

1.3.3. Subscribers, End-Users, and Applicants

The Subscriber and the Applicant are the Clients of the Service Provider, with whom the Service Provider enters into contractual relationship.

The person of the End User shall be determined by the Subscriber.

See the respective definitions in Chapter 1.6 of Definitions and Abbreviations.

The Service Provider, any employee, organizational unit or service partner may also become a Client of Service Provider. The same terms and conditions shall apply to such clients as the ones apply to the remaining clients; Service Provider shall not diverge from the requirements and rules of the certificate policy and the present practice statement. In the case of such an application for certificate, Applicant, Subscriber, End User and Recipient shall not participate in the activities of Service Provider made in the course of the processing of such related application (registration, validation of identity, activities related to client devices, approval of application, certificate issuance etc. – for further details see Chapter 4) and shall not exercise any influence thereto.

1.3.4. Relying Party

The Relying Parties are typically not in contractual relationship with the Service Provider, but the present Practice Statement prepared on the basis of the present Certificate Policy may provide them with recomendations in relation to the services they use, which are typically free of charge, mostly certificate status reports. The Service Provider primarily communicates with Relying Parties by way of the certificate repository.

See further the definition of Relying Party in Chapter 1.6.1.

1.3.5. Other participants

Encrypting partners

Creating encrypted message with public key of encryption certificate is available for anyone.

Before encryption the participant who do encryption shall convinced of revocation status of the certificates used.

TRANSLATION

1.4 Certificate usage

Certificate types described in Section 1.2.1. Certificate Policies of the present Practice Statement can be applied according to the rules presented in the following sections.

For the applicability of certificates, see also the Key Use field and the Key Usage of the secondary certificate policy, as well as the other restrictions included in the certificate (which can even be text-based) for the applicability of the certificates in Section 7.1.2 Certificate extensions.

1.4.1. Proper use of certificates

a. End user certificates

The private keys belonging to the end user certificates issued under the present Statement shall be used only for encryption, user authentication or website authentication.

The private key that belongs to the certificates issued in accordance with the NCP+ certification policy is protected by a cryptografic device (SCD) and shall be stored and used in SCD.

The private key that belongs to the certificates issued under the NCP certification policy is stored by software key storage.

In case of certificates issued under the LCP certificate policy there is no similar requirement as to the storage of keys.

The private keys belonging to the end user certificates issued under the Codesign certificate policy shall be used only for signing program codes.

Private keys belonging to SCD-type certificates (see 1.2.1) can only be stored and used on an SCD device (see also 4.5.1).

In the case of the website authentication certificates issued under the DVCP certification policies, there is no similar requirement as to the storage of keys. The website authentication certificates are capable of certifying websites.

b. SP certificates

SP certificates are usable for signing end user certificates exclusively after the publishing of the certificate.

For the use of keys belonging to the certificates, see Section 6.1.7 Key usage purposes. For specific restrictions on each certificate type see also the profiles belonging to the certificate types (see Chapter 7).

TRANSLATION

1.4.2. Prohibited use of certificates

The use of certificates issued by the Service Provider other than the corresponding use of the certificate according to Section 1.4.1 above is prohibited, especially the use of private key pairs of public keys included in End-User Certificates to sign other public key certificates, or their application for any trust service.

The intermediate certificates, and their keys, that certify the service provider root and end user certificates shall not be used for certification of certificates prior to the publication of the service provider certificate and its public key.

1.5 Regulation administration

The issuance and maintenance of the present Service Practice Statement shall be carried out by that organizational unit of the Service Provider, which is responsible for the practice statement. The permanent members of the responsible organizational unit are those employees of the Service Provider, who are designated as such by the management of the Service Provider. The operation of the Unit is regulated by the internal, non-public rules of operation of the Policy Adopting Authority.

1.5.1. The organization that carries out the administration of the document

The name of the organizational unit of the Service Provider that is responsible for the policies (terms) is NETLOCK Policy Adopting Authority. The permanent members of the Policy Adopting Authority are those employees of the Service Provider, who are appointed in writing by the Management of the Service Provider. The operation of the Authority is regulated in the internal, non-public rules of operation of the Policy Adopting Authority.

See Chapter 9.12 for the amendment to the policies of the Service Provider.

1.5.2. Contact person of the document

The responsible contact person of the Policy Adopting Authority shall be the approver of the present document (see the cover page of the document).

Customers, End Users and the Relying Parties may submit their questions and comments related to the present document to the NETLOCK Policy Adopting Authority in e-mail to szee@netlock.hu.

The employees of Service Provider may also submit their comments to the Policy Adopting Authority in other channels, as well, but their comments shall be made in writing in all cases.

TRANSLATION

The contact person shall be responsible for replying to queries sent in e-mail to the Policy Adopting Authority (see Chapter 1.5.1) and for implementing other measures, if necessary, on the basis of the comment.

In the case of any question or comment related to the present document and submitted to the Policy Adopting Authority, the contact person shall designate the member of the Authority who shall process the query. In the case of a complicated query, the contact person shall convene the meeting of the Policy Adopting Authority.

In the course of processing the query the Authority or the member shall identify the section(s) of the document affected by the query, then shall respond to the sender in e-mail upon consulting with the other members of the Authority, and with other employees, if necessary.

In the event the amendment of the present Certificate Policy or any other document becomes necessary on the basis of the query, the Service Provider shall act in accordance with Chapter 9.12 in relation to the amendment.

1.5.3. The organization resplsible for the compliance of the present practice statement with the certificate policy

The compliance of the Practice Statement – which contains the detailed practical requirements of the provisioning and use of the certification service under the Certificate Policy – with the Certificate Policy shall be monitored by the NETLOCK Policy Adopting Authority. The practice statement prepared on the basis of the Certificate Policy may be approved by the Policy Adopting Authority if practice statement is in complete compliance with the the present Certificate Policy. The Certificate Policy or its public draft may be published only upon approval.

1.5.4. Adoption of the Practice Statement

In case the practice statement is needed to be amended, the modified new version shall be drafted, adopted and issued under the uniform (rules of) procedure under Chapter 9.12.1 and in accordance with the rules of operation of the Authority. In case the employee responsible for the adoption of the new version has ensured that the Practice Statement will continue to comply with the requirements of the Certificate Policy, the responsible employee shall approve the practice statement and shall arrange for the publication thereof without any delay, but at least 30 days prior to the effective date of the new version.

TRANSLATION

1.6 Terms & Abbreviations

1.6.1. Definitions

AIA	CAI (Authority Information Access:Certificate Authority Issuers): Included in certificates and points to the download URL of the Issuer certificate
Subordinated service	Non-qualified trust service operated on the basis of the Service Provider's Statements, for which the Service Provider provides a certificate.
Activation data	A code (password or PIN code) generated by the Service Provider or provided by the End-User that is known only to the End-User and is used for bringing the private key into a state ready for use. Unrelated to certificate activation.
Signature	See electronic signature
Signature / Seal Creation device	A Cryptographic device that is not suitable for creating qualified signatures / seals. (See also Chapter 1.6.2 Abbrevations SCD)
Signature service	The following services as defined by eIDAS: ● the creation, checking, and validation of electronic signatures and electronic seals, ● as well as the checking and validation of the related certificates. In the framework of this policy, the provision of these services is understood to mean "cloud-based," by the Service Provider storing the end-user signature and seal keys and signing/sealing (including the affixing of an optional timestamp) the documents uploaded by clients via the web-based service/protocol and checking the above.
Signing Partner	A service partner that provides a signature service to its own clients, as part of which it can participate in the identification of End-Users (in regards to whom it has limited informational and administrative rights), that uses the signature service in an integrated manner with its own services to provide services, and that undertakes to pay fees on behalf of End-Users as a Subscriber.
Subject	See the definition in Article 1 point 43 of the Electronic Administration Act. In the framework of the present Stetement, Subject is taken to mean the Subject and SAN fields and the data included therein, which can refer to a natural person and/or an organization and/or a trademark/product name or the identifier/other name of a device/system or to its pseudonym. See the Applicant, Subscriber, Client, and End-User entities.
Status change	The procedure that results in a change in the certificate's status (valid, suspended) and receives a new value (valid, suspended, revoked).
Archiving service	According to Article 1 point 2 of the Electronic Administration Act: "A service for the long term storage of electronic documents, which also includes the trust service referred to in Article 3 point 16 c) of the eIDAS Regulation."
Recipient	A person receiving one of the end-user's keys or devices (e.g. Client device) and its activation data from the Service Provider (in person, via traditional or electronic means of delivery); a person that can be an Applicant of the given certificate can be a Recipient.
Seal	See electronic seal
Trusted list	A list managed by an authority or software producer, which contains the identifiers (generally the certificates) of the trust services considered reliable. A software handling a

TRANSLATION

	given trust list accepts those signatures, seals, and timestamps for the services that can be traced back to it. It is generally used to refer to the EU trust list, which includes qualified and non-qualified services as defined by eIDAS on recommendation of the supervisory bodies of the various member states. See: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers
Service Policy, Policy	*Szolgáltatási Rend Nem eIDAS Tanúsítványszolgáltatásra* *Service Policy for Non eIDAS Certificate Services* Requirements for non eIDAS certification services and related services of SP.
Supervisory Body	The body designated by the Electronic Administration Act to supervise trust services. Specifically the National Media and Infocommunications Authority.
Trusted role	The executive role generally responsible for the Service Provider's IT system. See Chapter 5.2.1 Trusted roles.
Trusted employee	A person in a trusted role at the Service Provider or at a Service Partner.
Trust service	According to Article 3 point 16 of eIDAS: "an electronic service normally provided for remuneration which consists of: ● the creation, verification, and validation of electronic signatures, electronic seals or electronic timestamps, electronic registered delivery services and certificates related to those services; or ● the creation, verification and validation of certificates for website authentication; or ● the preservation of electronic signatures, seals or certificates related to those services." Under this policy it means the Service Provider's service regarding electronic signatures, electronic seals and website authentication, certificate issuance and lifecycle management, as well as timestamp service.
Security zone:	A (logically or physically) secured area that protects the privacy, integrity, and accessibility of the systems used by the Service Provider.
CAA check	A check where the Service Provider searches the DNS registry for CAA records as per RFC 6844. The certificate cannot be issued if it contains a record that shows that the domain name holder communicates with another Service Provider.
Eakta (container format)	Digital signature container format, which includes the documents, also include their meta data, digital signatures and contra signatures, and timestamp too. as described in the ETSI TS 101 903 (XAdES) specification. See detailed at: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html (hungarian content)
EV certificate Extended Validation Certificate (EVC)	A certificate for website authentication that meets EVCG requirements.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (Article 3 point 10 of eIDAS). Within the framework of the present Practice Statement: Electronic data created by a natural person with the pair to the signature certificate private key issued by the Service Provider, which data is attached to the electronic document that is to be signed (or to other electronic data) and that can be checked with the certificate and the public key included in it. Legal entity equivalent of electronic signature.

TRANSLATION

Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. (eIDAS Article 3 Section25) Within the framework of the present Practice Statement: The seal certificate issued by the Service Provider with its private key pair are electronic data created by a legal person, which is attached to the electronic document (or other electronic data) to be sealed, and which can be verified with the certificate and the public key stored therein. The equivalent to the electronic signature created by a legal person.
Subscriber	The Service Provider's contractual partner that undertakes to pay service fees. The Subscriber's rights and obligations are separately defined in the GTC and the Service Agreement. In the case of certificate creation services, if an organization has also been indicated as the Subject of the certificate or it names only one natural person, it is generally the same as such person(s). In the case of of NLSign services equal to the Signing Partner or the End-User in the case of signature services. See the Client, Applicant and End-User entities, as well as Chapter 1.3.3 Subscribers, End-Users, and Applicants.
Relying Party	A natural or legal person who does not enter into a contractual relationship with the Service Provider but receives one of its certification creation services (generally free of charge) (e.g. checks electronic signatures, seals, or timestamps and thereby checks the validity information of certain certificates or service provider regulations). See Chapter 1.3.4 Relying Parties.
Valid certificate	A certificate that is currently valid and that is presently neither suspended nor revoked (see Certificate Status).
Validity (period)	A period between a start and end date for which the certificate was issued.
Device-based certificate	A certificate where the private key is issued for a Cryptographic device.
Certificate chain	The electronic document or its hash and the series of information that can be linked to each other (thus especially the certificates, information pertaining to certificates, the data used to create the signature or seal, the information pertaining to the current status or revocation of the certificate, and the information pertaining to the validity data of the service provider that issued the certificate and to its revocation) which can be used to establish whether the advanced or qualified electronic signature, seal, or timestamp on the electronic document was valid at the time of affixing the signature, seal, or timestamp. In general, this means a hierarchy of certificates that authenticate each other, all the way to the root certificate.
Advanced electronic signature	An electronic signature that meets the requirements defined by Article 26 of eIDAS.
Advanced electronic seal	An electronic seal that meets the requirements defined by Article 36 of eIDAS.
Certificate Policy	In the framework of the Service Provider's regulations, a standard procedural policy on the basis of which the Service Provider issues and manages certificates. The Service Provider's regulations contain more than one Certificate Policies, which differ in their applicable requirements and procedures.

TRANSLATION

Certification Authority	The Service Provider's organisational unit that performs issuance, publication, revocation, and suspension of certificates and the publication of the Certificate revocation list based on the request of the Registration Authority. See Chapter 1.3.1.
Certification Administrator	The employees in this position approve the issuance of the certificates within the Certification Authority.
Authorized Person	A Relying Party who has access free of charge to specific functions of the service for documents specified by, upon the request of, the Subscriber of the archiving service.
Applicant	In the case of certificate creation services, the natural person proceeding in the certificate issuance, certificate authentication, and status change procedure and that accepts the service agreement on behalf of the Client. The Applicant can be: ● the natural person indicated as the Subject of the certificate (in case of a pseudonym, the pseudonym's applicant); ● in absence of the above, the representative or authorized representative of the organization indicated as the Subject of the certificate; ● in absence of the above, the holder of the domain name, trademark, or product name; if the owner is an organization, the representative or authorized representative of such organization; or the person with control over the domain name. The same as the Subscriber if the Subject of the certificate is indicated as being a natural person (and no organization is indicated). In the case of NLSIGN service it's the same as the End-User. It's the Subscriber's representative/agent in the case of timestamping and archiving services.
Timestamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
Timestamp Server	The Service Provider's technical system that issues timestamps.
Timestamp URL	The virtual token that provides access to the timestamp service and contains the unique identifier of the Subscriber, through which the End User may transmit timestamp requests to Service Provider, and Service Provider may transmit timestamp replies to End User on the basis of the request.
Delivery Agent	The Delivery Agent is a partner of the Service Provider, who carries out the delivery of the client device in relation to the Issuance of the Certificate upon the appointment by the Service Provider at a place and date agreed with the Applicant, if requested by the Applicant. The Delivery Agent may be identical to the Registration Agent, as the case may be.
Public Root Provider	Public Root Provider (Közigazgatási Gyökér Hitelesítés-Szolgáltató) See Article 1.3.5 and http://www.kgyhsz.gov.hu/
Central Registration Authority	The organizational unit operating within the organization of the Service Provider that processes the applications for services, identifies the Applicant and the Subscriber, verifies their right to act and their credentials.
Timestamp service	The Service Provider's service in the framework of which it provides a timestamp for the provided data hash on the basis of the submitted electronic data.
Initial suspension	A special case of Certificate suspension where the Service Provider immediately suspends a certificate after its issuance, thus protecting it from abuse until the time the Certificate and the private key are safely received by the Client.

TRANSLATION

Right of representation	Full or partial right of representation, or any legal relationship that can be understood as such (see Article 82 (9) of the Electronic Administration Act).
CA	The Service Provider's technical system that issues certificates. The Service Provider has an Intermediate CA that issues end-user and certain SP certificates, as well as a Root CA with the highest level in the hierarchy that authenticates these units.
External Certification Authority	A Certification Authority operated by a separate organisation or person independent of the Service Provider (as a Service Partner) based on the Service Provider's requirements.
External Registration Authority	A Registration Authority operated by a separate organisation or person independent of the Service Provider (as a Service Partner) based on the Service Provider's requirements.
Terms and Conditions	Those of the Service Provider's documents that provide information on how the Service Provider meets which requirements pertaining to the provision of its services, as well as on the rights and obligations of the other participants. This includes the Service Provider's excerpt of services, Authentication Policy, Service Practice Statement , GTC, Service Agreement, and the aggregate of any other agreements concluded between them.
Cryptographic device	A secure hardware device that includes the End-User's private key, protects it from being compromised, and uses the key to conduct cryptography actions (e.g. signatures, encryption) on behalf of the End-User. It can be an SCD and QSCD, HSM or other, non-signature targeted device. It can be managed by both the Service Provider or the Client. In the latter case, it is referred to as a "Client device."
Critical services	The Service Provider's services pertaining to certificate and key creation, to providing Clients with devices, and to status changes.
Re-key	The process where the Service Provider issues a new Certificate and a private key to an already registered Client (or to itself) on the basis of an existing certificate. The end-user's public key is changed in the new certificate. See Chapter 4.7.
Key escrow service	A service that ensures the safekeeping of the end-user's private key and its handing over to the end-user (if the end-user's key were to become lost, destroyed, or inoperable for any other reason).
Private key	One of the keys in the pair generated by the Service Provider or the client, which is managed by the end-user. See public key. If the public key is included in a signature or seal certificate, it complies with the definition of electronic signature creation data and data used for the creation of electronic seals as defined by eIDAS.
Qualified Signature / Seal Creation device	A Cryptographic device that is suitable for creating qualified signatures / seals.
Qualified certificate	A certificate issued by a qualified SP and that is in line with Annex I, III, or IV of eIDAS or Directive 1999/93/EC, depending on which was in effect at the time of the issuance of the certificate.
Qualified certificate for website authentication	According to Article 3 point 39 of eIDAS: "A certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV of eIDAS."

TRANSLATION

	A qualified certificate that ensures the visitors to a website with the authentication of the websites indicated in it that there is a real and legitimate organisation behind it.
Mobile Registration Agent	A registration agent, who carries out the identification of the Applicant at a place and time agreed with the Applicant upon the request of the Applicant if a personal meeting is necessary.
NL Sign service	A secure central key storage (managed SCD) and key management service, which makes possible the electronic signature/stamping (and timestamping) of documents uploaded on a web-based interface, as well as the verification of the signature/stamp of the document certified this way. The application for the certificates usable within the framework of the NL Sign service and the submission of the required registration details, and (the commencement of) use of the service after the issuance of the certificate shall take place on the web-based interface of the NL Sign service.
Public key	One of the keys of the pair generated by the Service Provider or the client, which the Service Provider includes in the certificate it creates. See private key.
Permanent Identifier	An identifier, which enables the unique identification of the user of the certificate. The implementation thereof in the certificate shall take place on the basis of RFC 4043. It may be generated by the service provider, or a unique identifier recorded in the official registry. The identifier generated by the service provider is an OID that consists of two parts: the unique identifier of the Service Provider (1.3.6.1.4.1.3555), which is followed by that of the Client. The unique identifier of the Client begins with a 5, which is followed by a number, which may have the following values: ● 1,6,8,10: in the case of personal or business certificates, where the identifier is generated from the data of the natural person. ● 2,7,9,11: in the case of organizational certificates, where the identifier is generated from the data of the organization. If applied, the Permanent Identifier is located in the Subject/SerialNumber field of the certificate.
Registration	An initial identification procedure that the Service Provider performs in the interest of identifying the Applicant and the Subscriber, verifying their right to proceed, and registering their data.
Registration Authority	The Service Provider's authority that conducts the processing of requests for services, the identification of the Applicant and Subscriber, and the checking of their right to proceed and the data to be included in the certificate. The Registration Authority can be both within the Service Provider (as an internal organisational unit) and outside of it (External Registration Authority).
Validation Specialist	Trusted role. See Chapter 5.2.1 Trusted roles.
Registration (validation and revocation) Administrator	The employee of the Service Provider who works in this position within the Registration Authority shall manage the applications for certification and verify the veracity of the data submitted in the application for certificate (lásd see chapter 4.2.1) as well as the processing and implementation of the requests for revocation (4.9)) within any of the Service Provider's Registration Authorities. Registration administrators of Service Provider's external registration authorities perform tasks that is specified by the partnership agreement of operating the unit, to be performed. If these scope of tasks does not cover all of the tasks required to issue certificate, Provider's Central Registration Authority performs the rest as needed. Periodically, tasks

TRANSLATION

	performed by any external RA are posteriorly checked by a validation specialist of the Central Registration Authority based on a randomly selected sample. In case of website authentication certificate, domain validation processes are performed exclusively by Registration Administrators of Central Registration Authority. This provider role is equal the “Validation Specialist” role defined by BRG 1.6.1: the person who performs data validation duties.
SSL certificate	Certificate for website authentication
Statements	The present Practice Statement and the Service Policy collectively.
Organization	Legal person or private entrepreneur or independent attorney in the respect of the subject / subscriber of the certificate.
Software Certificate	A certificate, the private key of which is not issued onto a Cryptographic device.
Service	For the purposes of this Policy, the Service Provider’s enchryption, authentication, codesign and DV SSL (non-eIDAS) certificate services (see Chapter 1.1).
Service Practice Statement, Practice Statement	*Szolgáltatási Szabályzat Nem eIDAS Tanúsítványszolgáltatásokra* *Service Practice Statement for Non eIDAS Certificate Services* The statement of the service provider about the requirements and conditons of the procedural and operational requirements, which is the regulations containing the detailed procedural and other operational rules related to the Service Provider’s activities, based on the Service Policy. Present document.
Service Agreement	The Agreement concluded between the Service Provider and the Client, which contains the terms for the provision and use of the service. Its conclusion is a prerequisite of using the service.
Service Provider	NetLock, which provides trust and non-trust services in accordance with the present Trust Service Policy.
Service Provider’s regulations	The present Service Practice Statement, the Service Policy the GTC, the Service Agreement, and the Service Disclosure, as well as other private regulations.
Service Partner	An independent natural or legal person separate from the Service Provider that participates in the provision of the service on the basis of an agreement concluded with the Service Provider.
SP system	The aggregate of the Service Provider’s systems providing the service.
SP certificate	Those of the Service Provider’s certificates that it uses in the interest of providing the service (e.g. certificates for CAs and Timestamp Servers).
Certificate	The authenticated certification issued by the Service Provider that links the public key to the Subject and certifies the veracity of the data published in the Certificate.
Certificate Activation	The status change procedure that restores the validity of a suspended certificate. Following its activation, a certificate is also retroactively valid for the time of the suspension as if the suspension had not taken place.

TRANSLATION

Certificate Status	The valid/revoked/suspended status of the certificate registered by the Service Provider during the validity of the certificate, about which it informs its Clients and the Relying Parties by way of the Certificate Revocation List and the Certificate Status service.
Online Certificate Status Service (OCSP)	A service that provides real-time information on the status of a given certificate to Relying Parties. See also: Certificate Revocation List.
Certificate Suspension	The status change procedure in which the Service Provider temporarily terminates the validity of a still valid Certificate before the end of its originally planned expiration. Certificate suspension is a temporary state; suspended Certificates can be revoked or the Certificate can be revalidated within its original period of validity. If suspension is revoked, the Certificate becomes retroactively valid as if the suspension had never taken place.
Certificate enrolment	The process by which the Applicant enrols for a certificate, i.e. it provides the data required for preparing the certificate and certifies those to the Service Provider and then certifies its request with the signing of the Service Agreement by the Applicant and - if different than the Applicant - the Subscriber for the certificate being applied for, thus authorizing the Service Provider to issue the requested certificate.
Certificate Management Procedure	A procedure that results in the issuance of a new certificate based on the data of an existing certificate and the data of an earlier client registration (see Chapter 3.3 Authentication and certification in the course of certificate management procedure and Chapter 4 Lifecycle requirements).
Certificate creation service	Those of the Service Provider's services within the framework of which it creates a new certificate. This can be based either on an existing certificate (subsequent issuance with a certificate management procedure) or without any such precedent (original issuance).
Certificate renewal	The process by which the Service Provider issues a new Certificate for the same public key with the same Subject but for a new validity period. See Chapter 4.6.
Certificate modification	The process by which the Service Provider issues a Certificate to a previously registered Applicant on the basis of a Certificate issued previously, with the public key included in the latter, but with modified Subject or Service Provider data. See Chapter 4.8.
Certificate repository	The Service Provider's records containing issued certificates, through which the public certificates issued by the Service Provider and the Certificate Revocation List can be queried.
Certificate type	Differentiation between the various certificates issued by the Service Provider according to certain features, generally on the purpose of use. See Chapter 1.2.1 of the Service Agreement.
Certificate Revocation	The status change procedure in which the Service Provider terminates the validity of a Certificate before the end of its originally planned expiration. Certificate Revocation is irreversible and results in a permanent status change; a revoked certificate loses its validity at the time of its revocation and can never again be validated.
Certificate Revocation List (CRL)	An authentic list of the certificates that are temporarily or permanently invalid published regularly and following status changes by the Service Provider in the Certificate Repository. Accepting and using the certificates included in the list is not recommended. A type of certificate status service as defined by Article 17 of Decree 24/2016 of the Minister of the Interior.
Test Certificate	A Certificate issued by the Service Provider for testing purposes, the contents of which is the same as a specific certificate but its certificate policy field and the name of the Subject indicate that it is a test. Such certificates cannot be used to undertake commitments, result

TRANSLATION

	in no legal effects, and can only be approved for testing purposes. The Service Provider does not assume liability for the data contents or use of such certificates or for the availability of the connected services.
UCC website authentication certificate	A certificate for the certification of websites, which enlists various different domain names (in the SubjectAltName/DNSname record).
Client Menu	An interface accessible on the website of the Service Provider, which is provided for the submission of various applications related to certificates and the related services, and for monitoring the status of the applications in progress, where clients may log in by entering a unique user name and password (following the registration with the client menu). The management of the qualified certificates requires the registration with, and logging in, the qualified client menu, while the management of the non-qualified certificates requires the registration with, and logging in, the enhanced security client menu.
Client Menu Registration	The process, where natural or legal persons create their own Client Menu by submitting their data, as well as the login name and password required for logging in the Client Menu.
Client	The party that concludes a contract with the Service Provider. In the case of certificate creation services, the Applicant and Subscriber of the certificate (in certain cases, these may be identical). In the case of NLSIGN signature services, the Signing Partner and the End-User. See Chapter 1.3.3 Subscribers, End-Users, and Applicants
Client device	A client-managed Cryptographic device. Only the device acquired, checked and delivered to Client by TSP can be used as Client device that shall be listed in the chapter 6.2.1 in present Practice Statement.
Client Registration	Validation of the identity of natural and non-natural persons, validation and recording of their data prior to entering into the first service agreement and issuing the first certificate. See Chapter 3.2 Initial Identity Validation.
End-User	The natural person who disposes over the private key pair to the public key included in the certificate (is the sole user or is responsible for its use). See the Client and Subscriber entities, as well as Chapter 1.3.3 Subscribers, End-Users, and Applicants.
End-User Certificate, End-User Key	Indicates the Subscribers' certificate and key, as opposed to the Service Provider's own certificates and keys.
Certificate for Website Authentication	The certificate according to Article 3 point 38 of eIDAS.
Wildcard Certificate for Website Authentication	A certificate for website authentication that was issued by the Service Provider for the authentication of more than one subdomain (the domain name is indicated in the format *.domain.hu, meaning it includes all the subdomains that belong to domain.hu).

TRANSLATION

1.6.2. Abbreviations

a. The acronyms of referenced legislation

eIDAS	Regulation 910/2014/EU on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Electronic Administration Act	Act on the General Rules of Electronic Administration and Trust Services
Records Act	Act on Keeping Records on the Personal Data and Address of Citizens
Free Movement Act	Act on the Admission and Residence of Persons with the Right of Free Movement and Residence
Third-Country Nationals Act	Act on the Admission and Residence of Third-Country Nationals
Information Act	Act on Informational Self-Determination and Freedom of Information
Regulation No. 24/2016	Regulation No. 24/2016. of the Ministry of Interior on the detailed requirements of trust services and trust service providers.

For the exact name of the laws above in force on the day of the present document entered into effect, see chapter 9.15.

b. Acronyms of technical terms

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CAA	Certification Authority Authorization
CAMS	Card Management System: The name of the system used by the Service Provider for the personalization of the Client Devices
IP	Internet Protocol
IT	Information Technology

TRANSLATION

SP	Service Provider
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy
CPS	Certification Practice Statement / Service Practice Statement
CSBR	Code Signing Baseline Requirements
CRL	Certificate Revocation List
CSP	Certification Service Provider
EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
FQDN	Fully qualified domain name
gTLD	Generic top-level domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
OCSP	Online Certificate Status Protocol
OID	Object Identifier

TRANSLATION

OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAN SubjectAltName	Subject Alternative Name
SCD	Signature / Seal Creation Device
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider
QSCD (previously SSCD)	Qualified Signature / Seal Creation Device
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
URL	Uniform Resource Locator

TRANSLATION

2. PUBLICATION AND CERTIFICATE REPOSITORY

Service Provider shall publish the various information pertaining to the chertificates (certificates, expiry information, policies and other terms).

2.1 Repositories

The Service Provider shall maintain a public certificate repository and systems that communicate certificate revocation information (CRL, OCSP), and shall publish the Terms and conditions related to the certificates that may be issued under the present Practice Statement in downloadable PDF format on its website. (See Chapter 1.1.2)

2.1.1. Publication of certification information

Service Provider shall provide the Clients and Relying Parties with certificate revocation information (CRL, OCSP) via HTTP protocol, with an availability level of at least 99% per annum, and that the length of the service outage shall not exceed 4 hours per occasion.

Service Provider shall make available the public certificate repository on its website, via HTTPS protocol – the public certificate repository shall consist of the subject data of end user certificates of the clients who consented to the publication in the service agreement. The certificates published in the public repository are downloadable by the public. Service Provider maintains websites for the purposes of checking revoked, expired, and valid certificates for website authentication certificates (OVCP AND EVCP) (testing)[3].

The certificate repository's SP certificates, as well as the valid end-user certificates for the publication of which the Client has granted its consent, can be queried on the Service Provider's websites (see Chapter 4.4.2).

The Service Provider applies the following procedure for the publication of the various certificates:

- It publishes CA certificates on its website (Chapter 1.1.2)
- It displays valid end-user certificates in the public certificate repository immediately following their issuance and - if applicable - activation.
- The Service Provider ensures that all of the certificate types it issues can be tested by issuing test certificates (see Chapter 7.1).

[3] The Service Provider publishes the addresses of these websites in its own website (see Technical data).

TRANSLATION

The Service Provider publishes the status information pertaining to certificates with the use of the following methods:

- The status information pertaining to the end-user certificates issued by the Service Provider and to SP certificates are immediately accessible within the certificate status service following the status change.
- The information on certificate status changes are also displayed in certificate revocation lists (CRLs). The CRLs can be queried on the Service Provider's website and are also accessible by applications via http protocol.

When logging into the client menu, the end-user can access information pertaining to its respective certificates and their current status.

The KGyHSz publishes, in accordance with its own regulations, the status information pertaining to its own root certificates and to certificates of service providers that it endorsed; the information is available in accordance with relevant legislation in the certificate repository which, at the time of the publication of this Statement, is found at http://www.kgyhsz.gov.hu/.

Service Provider shall inform its Clients and the Relying Parties on the various terms and conditions applicable to various types of certificates (see Chapter 1.1.2).

2.1.2. Publication of Terms and Conditions

The present Practice Statement and the underlying Certificate Policy shall be published by Service Provider with the contents and in a structure conform with RFC 3647, save for the derogations specific to the Service Provider.

The Service Provider shall, at least before their entry into force, publish the new versions to be implemented of the Certificate Policy, the Practice Statement and the General Terms and Conditions pertaining to the services based on the present Certificate Policy and affected by the subject modification. In addition to the documents in force, those earlier versions thereof shall also be continuously available on the website, on the basis of which any certfificate is still in force

Following the entering into of the service agreement, upon the issuance of the certificate, Service Provider shall provide the Client with the Practice Statement and the Service Agreement attached to the e-mail, which shall be deemed as a durable medium under the laws of Hungary in force.

TRANSLATION

2.1.3. Declarations

a. BRG Declaration

NETLOCK is compliant with the actual version of the document entitled “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, which is published at http://www.cabforum.org website. In case of any diecrepancy, the Baseline document shall prevail in the case of the DVCP certificates.

b. CSBR Declaration

NETLOCK is compliant with the actual version of the document entitled “Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates”, which is published at http://www.cabforum.org website. In case of any diecrepancy, the document shall prevail in the case of the codesigning (CSBR) certificates.

2.2 Time or frequency of publication

Service Provider shall publish on its website the public draft of the new version of the Practice Statement at least before entering into effect, in order to allow its Clients and the Related Parties to get acquainted with it and to make comments to the Service Provider before the draft enters into effect (see Chapters 1.5.2 Contact person of the document and 9.12.1 Amendments).

The Policy Adopting Unit of Service Provider shall revise the Practice Statement and the Certificate Polcy at least once in every year and shall modify them if necessary (see Chapter 9.12).

The publication of new versions regarding the present Statement takes place as set out in Chapter 9.12. See Chapter 9.12 for the publication of new versions of the Service Practice Statement.

The Service Provider’s other policies and contractual terms, as well as their new versions, will be issued as required.

When necessary, the Service Provider shall publish extraordinary information in accordance with the requirements of relevant legislation or, in absence of such, without delay.

The certificates of the Authenticator CAs will be published no later than when commencing the service.

See Chapter 4.9.7 for the frequency of publishing CRLs.

TRANSLATION

2.3 Access controls on repositories

The Terms and Conditions, extraordinary information, certificates, and status information published by the Service Provider are public information. Read access to these is made publically available in accordance with the features of the media used for publication.

The Service Provider's certificate repository is accessible via standard HTTP or HTTPS protocols.

The Service Provider continuously ensures the access of the certificate repository (24/7, every day of the year), with the exception of the time required for scheduled maintenance. As far as possible, the Service Provider will schedule maintenance outside work hours. The certificate repository can only be accessed lawfully through the Service Provider's website, by way of individual manual requests. Other requests (e.g. automated) are only possible with the Service Provider's written consent.

Online services (certificate repository, OCSP) do not have any restrictions on access, but requests can be limited for security reasons if a certain limit is exceeded. The conditions for restrictions will be published on the Service Provider's website.

See Chapter 2.1.1 and 4.9.9 for the availability of services.

TRANSLATION

3. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The Service Provider uses Client identification and data verification steps outlined in the following points for issuing certificates and concluding the service agreement in the framework of certificate creation services.

3.1 Naming

The Issuer and Subject fields of the certificates issued by Service Provider are conform with the name format requirements of the recommendations ITU-T X.509 and RFC 5280.

The Subject (Subject and SAN) fields in the certificates identify the entity which owns the private key associated with the public key contained in the certificate, that is for which the certificate was issued. The Subject fields contain more than one type of identifiers, the contents of which are as follows:

NAME AND ID OF DATA (Standard name, OID, English name)	CONTENT
Subject field	
CN id-at-commonName 2.5.4.3 Name	In case of personal and business certificates, this includes the full name of the natural person Applicant in the form used in the data source.
	In case of a pseudonym certificate, this is the same as the contents of the pseudonym field.
	In case of an organisational certificate, the organisation's full or short name /DBA / Trademark / Product identifier In case of a DBA, its contents can be: A company name including the company type It can include the verified company name's long or short form without the indication of the company type (Kft., Bt., etc.) Domain name Product ID Product name preceded by a company name / DBA / Trademark
	The website name in the name of certificates for website authentication The commonName can only contain an FQDN, which also has to be included in the SAN/DNSName field.
SN Id-at-surname 2.5.4.4 Last name	The last name of the natural person's full name as indicated in the certificate CN field. The delineation between the names is performed in accordance with the MELASZ recommendation.
G id-at-givenName 2.5.4.42 First names	The first name of the natural person's full name as indicated in the certificate CN field. The delineation between the names is performed in accordance with the MELASZ recommendation.
Id-at-pseudonym 2.5.4.65 Pseudonym	In case of pseudonym certificates, the certificate contains the pseudonym selected by the Applicant. The pseudonym is repeated in the commonName field. The pseudonym cannot be misleading and has to be unique at the Service Provider, i.e. the same pseudonym cannot be used for two different users.
id-at-serialNumber	The globally unique serial number of the natural/legal person indicated in the certificate CN field.

TRANSLATION

2.5.4.5 Serial number	
id-at-countryName 2.5.4.6 Country	The country of the Subscriber's seat or home address. The two-letter country code as defined by ISO 3166-1.
L id-at-localityName 2.5.4.7	The city of the Subscriber's seat or home address.
id-at- stateOrProvinceName 2.5.4.8	The county or state of the Subscriber's seat or home address.
id-at-organizationName 2.5.4.10	In the case of business and organisational certificates. The Subscriber organisation's full or short name.
id-at- organizationalUnitName 2.5.4.11	In the case of business and organisational certificates. The name of the organizational unit within the Subscriber organisation The Subscriber has to certify its existence in order to be included in the certificate.
organizationIdentifier 2.5.4.97	In the case of business and organisational certificates The Subscriber's tax identification number as included in the registry, in the semantic format defined by ETSI EN 319 412-1. It can contain, in a bound format, a unique identifier received in an official national or other identification system, as set forth below: 1. If the organisation has a tax number: a VAT prefix followed by the organisation's registered country code, a hyphen, and the organisation's taxpayer identification number, in unchanged format. For Hungarian organisations: the "VATHU-" prefix can be followed by a domestic tax number and the "VATEU-" prefix can be followed by a community tax number, in unchanged format. 2. If the previous point is not applicable, the commercial register code will be used following the prefix "NTRHU-". 3. If the previous points are not applicable, the value "XX:HU" is to be used based on the national registered semantics, where "XX" is the two characters of the national or EU identification schema. 4. If the above points are not applicable, another individual official identification will be used. 5. If none of the mentioned forms of identification are available, the ID of the deed of foundation and the name of the founding document can also be used. For the identification system of other countries, the Service Provider shall use the country codes defined by ISO 3166.
Id-at-title 2.5.4.12 Title	For business certificates The Applicant's position or title within the Subscriber organisation. Optional.
subject/EMAIL	The contents are the same as that of the SubjectAlternateName:emailaddress field.
SAN field	
SAN SubjectAlternateName:DNSName	For certificates for website authentication Contains one or more domain names If the CN also contains a DNS record, it is included here as well.
SAN SubjectAlternateName:emailaddress	The email address certifiably belonging to the entity defined in the CN, as per the requirements of RFC 822. Not used for certificates for website authentication.
SAN SubjectAlternateName:otherIdentifier	The Service Provider's individual identifier (which is equal to the Service Provider's part of the permanent ID).

TRANSLATION

See Chapter 7.1 for the different requirements pertaining to filling out the above Subject fields (Subject and SAN) and Issuer fields according to certificate profile.

3.1.1. Types of names

When creating the Subject fields for certificates, the Service Provider has to follow the X.500 distinguished name requirements in accordance with the RFC 5280 standard. The Service Provider distinguishes between the following name types in the case of end-user certificates, and it links the following profiles to them:

Name type (Subject type)	Certificate profile
Natural person	Personal
Legal person	Organisational
DBA / Trademark / Product identifier and legal person together	Organisational
Natural and legal person together	Business
Pseudonym	Pseudonym
Website	DV certificate for website authentication

See Chapter 7 of the present Statement for a description of the certificate profiles.

3.1.2. Need for names to be meaningful

The *Subject* field of encryption or authentication certificates issued to natural persons have to include the following data:

- commonName (name)
- givenName and surName or pseudonym (first and last name or pseudonym)
- countryName (country code)
- serialNumber (unique identifier of the Subject)

The *Subject* field of encryption or authentication certificates issued to legal persons have to include the following data:

- commonName (name)
- countryName (country code)
- organizationIdentifier (organization Identifier)

TRANSLATION

The *Subject* field of DVCP certificates for website authentication have to include the following data:

- commonName (name);
- countryName (country code).

In case a legal person is specified as the Subject of the, Service Provider shall, in all cases, specify the unique identifier of the organization in the Subject/organizationIdentifier field of the certificate.

In case both a natural and a legal person is specified as the Subject of the certificate (business certificate profile, see Chapter 7.1), the Service Provider shall mandatorily specify the unique identifier of the organization in the Subject/organizationIdentifier of the certificate, unless the applicant of the certificate is an attorney-at-law or a law firm.

The SAN field of the website authentication certificates (DVCP) shall also mandatorily include the domain name set out in the commonName field, as well as the further domain names in the case of a UCC certificate.

Chapter 3.1 contains a detailed description of the Subject field.

The name of the natural and legal person included in the certificate shall be checked by the Service Provider against authentic records or, in absence of such, official identification documents, and shall be included identically to the manner included in those.

If the contents of the *Subject/Serialnumber* field is an official (checked on the basis of a document) national identifier, its obligatory format: <REF>HU-<documentnumber>, where <REF> is replaced by three characters as set forth below:

1. "PAS" for passport numbers (e.g. PASHU-AE123456)
2. “IDC" for ID card and driving licence numbers (e.g. IDCHU-123456AB (ID card) or IDCHU-AB123456 (driving licence))
3. “TIN” for tax identification numbers (e.g. TINHU-1234567890)

In the case of individual identification systems, <REF> is replaced by a series of characters in the format “XX:”, where “XX” is the two-character designation of the national or EU identification schema (e.g. EI:HU-200007292386 or AT:EU-BH16251).

In case the certificate contains more serialnumber values, no formal requirements shall apply to the further serialnumber fields, assuming that those are not filled with the numbers of the above identification documents.

TRANSLATION

The certificate identifier fields (“Subject” and “Issuer”) meet the requirements of the X.500 name format. Additional rules pertaining to the “*Subject*” and “*Issuer*” fields:

- Data are indicated in the certificates without special and control characters.
- By default, names are indicated in certificates as follows: in the same exact format as the name used for personal identification in the official document, including accented letters in their original form in the CN, SN, and G fields, with the use of UTF-8 encoding. The various name units are separated by spaces.
- Abbreviations can be used in the case of names that exceed the maximum number of characters defined in the applicable standards.

The Subject/organizationIdentifier field shall be filled with a unique identifier given within an official national or other identification system in a mandatory format, which is defined by ETSI EN 319 412-1 5.1.4 (it is set out in the form of *REFCO-organization identifier*, where REF shall consist of three and CO shall consist of two characters, as follows).

Rules of filling:

1. In case the organization has VAT number, the field shall be filled on the basis of the VAT number, as follows: in the case of Hungarian VAT number, it shall be filled with the value "VATHU", while it shall be filled with the value “VATEU” in the case of an EU VAT number.
2. If the previous point cannot be applied, the Hungarian company registry number shall be filled with the value "NTRHU".
3. If the previous points cannot be applied, it shall be filled on the basis of the national registered scheme with the "XX:HU" value, where „XX” shall be the double-character sign of the national or EU identification scheme.
4. If the previous points cannot be applied, any other unique official identifier can be applied.
5. If none of the above referred identifiers are available, the field may be filled with the identifier of the deed of foundation and the name of the founding legislation.

In the case of identifier systems of other countries, the country code according to ISO 3166 shall be applied instead of the HU country code.

The Subject fields of test certificates can take the form of any of the certificates issued by the Service Provider; however, the commonName field is always to indicate the fact that it is a test with the words “TEST” or “TESZT”, which can be followed by other name data in a clear manner that can be mistaken with any real person.

3.1.3. Pseudonyms

Service Provider shall also issue pseudonym certificates. The Applicant may only apply for pseudonym certificates on its own behalf. The Applicant shall choose the pseudonym, which the

TRANSLATION

Service Provider will not check; the Subscriber is liable for any problems (e.g. copyright, etc.) in relation to the pseudonym.

The Service Provider shall issue pseudonym certificates in accordance with the pseudonym certificate profile, where the "CN=CommonName" and the "Pseudonym" fields contain the pseudonym in the same format; no legal/natural person can be indicated next to the pseudonym.

In case of using a pseudonym, the Service Provider may only hand over the data pertaining to the Client's true identity to third parties or the authorities if granted the Client's consent, unless required to do so by a final court ruling. The Service Provider is authorised to deny the issuance of a pseudonym certificate that incurs legal difficulties (or is likely to do so) or revoke such certificate at its own discretion.

Pseudonym certificates for website authentication cannot be applied for. (DVCP)

3.1.4. Rules for interpreting various name forms

The certificates issued by the Service Provider do not aim to function as a digital form of identity for the natural or legal persons indicated as the Subject or for their identities to be established solely on the basis of the data included in the certificate.

The business profile certificate (see Chapter 7.1) itself does not support the right of representation. In case Service Provider issues a certificate purported to support full or partial right of representation, or a legal relationship that may be interpreted as such, then Service Provider shall indicate the above by indicating the position verified on the basis of a public database or on the lack thereof, public instrument. The position shall be indicated by Service Provider in the Subject/Title field of the certificate, and shall indicate the following statement in the certificatePolicies/policyQualifier field of the certificate on the basis of Chapter 7.1.8: "Prior to the issuance of the certificate Service Provider verified on the basis of credible information the right of the natural person indicated in the Subject/CN field of the Certificate to represent the organization indicated in the Subject/O field.

The contents of the present Statement provide information to Relying Parties for interpreting the identifiers (see especially Chapter 7.1.5.). If the Relying Parties require help with the interpretation of the identifier or any data included in the certificate, they can also contact the Service Provider directly (see Chapter 1.1.2).

The Service Provider will only provide additional information (besides the information that helps in interpreting certificate data) on the data of the Subject(s) on the basis of an authorisation or of relevant legislation.

TRANSLATION

a. Issuer identifier

The issuer identifier is understood to mean that the Service Provider issued the certificate with the use of a given SP (intermediate/root) certificate.

The SP certificate's *Issuer* field contains the country code of the country (*Country*) and city (*Locality*) in which the certificate issuer has its seat, the name of the organisation (*Organisation*), its organisational unit (*Organisation Unit*), and the name of the CA issuing the given certificate (*Common Name*).

b. Subject identifier

The *Subject* field is understood to mean that the certificate belongs to the natural person / legal person / website (domain name) / DBA / product name / pseudonym with the *Common Name* of the *Organisation unit* within the natural or legal person that has the name of the *Organisation*.

The home address of the natural person or the seat or site of the organisation is defined under the fields *Country* (country), *State* (country/county), and *Locality* (settlement). The certificate does not contain any information that is more accurate as regards location.

3.1.5. Uniqueness of names

The Service Provider clearly distinguishes between certificate Subjects (Subject field) in the case of end-user certificates . In the interest of the above, the Service Provider provides all Clients with a unique subject identifier (OID-based Permanent ID), which it includes in the certificate's Subject/Serialnumber field (see Chapter 7.1). This identifier individually identifies the natural or legal person included in the certificate. A Subject may have more than one identifier, but an identifier may never be issued to another Subject.

In addition to the above, the Service Provider can also indicate another individual identifier in another Subject/Serialnumber field (e.g. personal identification card number, official card ID, etc.).

The Permanent identifier is not applicable in the case of certificates for website authentication (DVCP).

3.1.6. Recognition, authentication, and role of trademarks

The Service Provider may also use a trademark in the certificate on the basis of a DBA, trademark, product name, or product identifier owned/possessed by the Client. These data are included in the certificate in the Subject/CN and/or SubjectAltName/dirname fields. See Chapter 3.2.2 for checking these.

TRANSLATION

The acquisition of a trademark by the Client is not an event that requires the modification of a certificate.

3.2 Initial identity validation

Service Provider shall carry out the client registration prior to the issuance of the end user certificates, with the identity validation and authentication procedures detailed in the subchapters of the present chapter (3.2), provided that Service Provider has not carried out such procedures earlier or the earlier procedures ceased to be valid.

In case of DV website authentication (DVCP) certificates, requirements of present chapter shall be applied, only if the text indicates it separately.

Service Provider shall carry out the following procedures within the framework of the initial identification:

1. identifies the person of the Applicant, by validating the personal data, his right/power to act and his right to use the other data to be recorded in the certificate;
2. identifies the Subscriber if the Subscriber is different from the Applicant, by validating at least the full name and unique identifier of the Subscriber to be recorded in the certificate as well as his right to use the other data to be recorded in the certificate;
3. identifies the person(s) entitled to represent the Subscriber;
4. identifies the person of the attorney in fact of the representative(s) of the Subscriber and validates the power of attorney;
5. validates the Subject-related data to be indicated in the certificate; and
6. validates the possession of the private key counterpart of the public key to be recorded in the certificate, and
7. records the validated data and documents the identification and validation procedures.

For the validations under points 1-5 the Service Provider shall use authentic and valid instruments, documents and/or trusted central registries or databases, which support the veracity and validity of the data submitted by the Applicant and the Subscriber with sufficient confidence, such as:

- the identity of the natural or legal person to be indicated as Subject;
- the right/power of the representative of Applicant and Subscriber to act,
- the right to dispose over the domain (address range) supported by the certificate, or over the IP address to be recorded in the certificate (in the case of website authentication - DVCP - certificate),

TRANSLATION

- the right to pursuit the regulated profession indicated in the certificate (in the case of the application for a certificate indicating a regulated profession) and
- the authentication of the identifiers and documents used for establishing the identity.

In case there is no official instrument, document or reliable data source is available for the verifications, Service Provider shall verify the above on the basis of a declaration recorded in a private document with full probative value.

The procedures can be deemed successful if the data submitted by the Applicant and Subscriber are precisely identical to the data set out in the instruments, documents and/or reliable data sources and/or declarations.

Before the Service Provider starts using any data source as a reliable data source or database, it shall be evaluated as regards reliability, accuracy, and resistance to change and falsification.

During the evaluation, the Service Provider takes the following into account:

1. The date of the provided information,
2. The frequency of updates to the information source,
3. The purpose of the data provider and data collection,
4. The public accessibility of the data,
5. The relative difficulty of falsifying or changing the data.

In case the registry or database contains public data on grounds of statutory provisions, Service Provider shall not carry out the above evaluation and shall deem such database or registry as reliable data source.

In addition to the recorded data, the Service Provider also records the validity certified by the data source if such is interpreted (e.g. validity of an official document). The validity of the issued certificate can exceed the above validity; however, the data source must be valid at the time of signing the service agreement.

Service Provider shall provide its employees who carry out the identification and validation procedures with a detailed rules of operation regarding the means of the entity identification and data validataion procedures, the practical steps to be performed, furthermore such rules shall provide for a detailed description for the execution of the above.

The Applicant and Subscriber of the end-user certificate can be the Service Provider's employee or partner; however, the Service Provider shall proceed in the same manner as in the case of any other Client. Besides the role of Applicant/Subscriber, the Service Provider's employees and partners cannot take any other part in the application and provision of the provided service.

TRANSLATION

3.2.1. Method to prove possession of private key

If the Applicant generates the key pair that serves the basis of the certificate, the Service Provider ensures that all technical procedures are applied that allow it to make certain that the Applicant is actually in possession of the private key paired to the public key to be included in the certificate. This can be certified, among others, with the standardised certificate application created by the Client (e.g. PKCS#10 or SPKAC CSR) or with an application based on a self-signed certificate and its submission to the Service Provider.

The certification of principal possession in this manner is valid until a valid certificate is linked to the private key.

3.2.2. Authentication of organization identity

a. Identifying the Subscriber

In the case of non natural person Subscribers, Service Provider shall use a public register or a public document supporting the incorporation and the following data for the validation of the full name and unique identifier of the Subscriber to be indicated in the certificate, and for establishing the person of the legal representative. In the lack of the above, the validation may be based on another reliable data source or legislation.

Service Provider shall use primarily the following public or reliable databases in relation to the identification of the non natural persons:

- in the case of the business associations under the Civil Code, the information provided by online company information service of OPTEN Ltd. or the online company registry provided by the online company information service of the Company Information and Electronic Company Registration Service set out in Section 1 of the Company Registration Act;
- in the case of the organizations under the Act on NGOs, the National Name Register set out in Section 84 of the Act on NGOs;
- in the case of attorneys-at-law under the Act on Attorneys, the online registry available on the website of the Hungarian Bar Association as set out in Section 116 of the Act on Attorneys;
- in the case of a public education institution under the Act on Public Education, the institution search engine that pertains to the public data of the institution master data register of the public education information system set out in the Government Decree no. a 229/2012, which search engine is available on the website of the Educational Authority;

TRANSLATION

- in the case of government bodies, public bodies, local governments and other state-listed legal entities under the Public Finances Act, the Master Registry available on the website of the Hungarian State Treasury, as specified in the Public Finances Act.
- in the case of the undertakings under the act on private enterpreneurs and individual companies, the online registry of private enterpreneurs operated by the Deputy State Secretariat of the Ministry of Interior for Management of Registers, as set out in the above referred act.

In case the above registries are not accessible, or in the case of any other types of organization, or entities registered outside Hungary, Service Provider shall use other applicable reliable data sources, or if such data sources cannot be accessed, or the cost of access and verification is disproportionately high, the verification shall be based on the public document on the founding or establishing of the organization, or the public document on appointing the respective person, or any other public document supporting the name, unique identifier, as well as the person of the representative of the other non natural person.

In the case of entities registered outside Hungary, the Service Provider shall carry out its verification on the basis of the English or Hungarian translation, attested by a public notary, of the documents supporting the name, unique identifier and the person of the representative of the entity. In case the original language of the document is English, translation is not needed and in this case the facsimile of the original documents attested by a public notary shall serve as the basis of the verification.

Service Provider shall indicate primarily the VAT number as the unique identifier of the non natural persons in the end user certificate; and if the VAT number is not included in the above enlisted registries, Service Provider shall verify the Hungarian VAT number by querying the tax subject in the official registry available on the website of the National Tax and Customs Administration. If there is only EU VAT number, it shall be verified on the website of VIES VAT number validation site of EU. In case the company registration number is used as a unique identifier, it shall be verified by the Service Provider in the above referred company registry.

An attorney-in-fact may also act on behalf of the representative of the non natural person. Service Provider shall verify the power of the attorney-in-act in accordance with Chapter 3.2.3 b.

Service Provider shall verify the other data of the non natural person to be indicated in the certificate on the basis of other reliable data source, other official documents or a power of attorney in the form of a written document. The veracity of the organizational unit of the Subscriber to be indicated in the certificate (Subject/organizationalUnitName) shall be supported by the declaration of the Subscriber regarding the existence of the organizational unit.

TRANSLATION

Authenticity of the organization unit displayed in the certificate is ensured by the statement of the Subscriber in the Service Agreement – in case the verification options above are not available.

Service Provider may require the Applicant and Subscriber to present original documents or copies (see Chapter 4.1).

b. Retention of Subscriber data

The Service Provider stores, in its own system, the following data to be indicated as the subject of the Subscriber's certificate and to be stored in the Service Provider's records (see Chapter 9.4):

- The Subscriber's identification data (full and short name, official address, taxpayer identification number, company registration number, name of its organisational unit);
- The data of the documents used to check these (e.g. document type, identification number, validity) and originals/copies OR electronic seal and the data used to check the seal;
- The right of the Subscriber's representative to represent the Subscriber (see Chapter 3.2.3 for other representative data);
- Signed copies of the service agreement and other statements (e.g. authorisations);
- Queries and the provided responses in various records;
- The data required for contact (e.g. telephone number, e-mail address).

Checking other, non-personal subject data

If the Applicant requests that a name or identifier of an asset, system, or product, a DBA / Trademark, or other unique name is indicated as the Subject of the certificate (independently or with a natural or legal person), the Service Provider shall ascertain that the Client is in rightful possession of the name and identifier and that these are not misleading. The check has to be based on an official document, reliable data source, or discussions with the official body that manages the identifier, if any are available.

Except of the DV website authentication certificates (DVCP), because in this case only domain verification is required.

By applying for and accepting a certificate, the Client declares that the names, trademarks, and other data included therein do not violate the rights of third persons.

TRANSLATION

3.2.3. Authentication of individual identity

a. Checking the Applicant's identity

In case the requested certificate contains the data of a private individual, Service Provider to check the Applicant's (Subject) identity inspects the personal identification documents (or their copies) submitted to it to check their validity and authenticity and the veracity of the data provided by the Applicant.

The Service Provider also uses central registries to check the validity and authenticity of the personal identification document, including the data included therein. In the case of Hungarian natives, this shall be done trough the Central Registry of the Ministry of Internal Affairs. If the Service Provider does not know if such records are available – for example person, who is not Hungarian native -, or the price for access and performing the check is disproportionately high, the Service Provider will record this fact and will decide on the basis of the documents available to it on whether to issue the given certificate to the Applicant.

In this case, if SP will issue the certificate, the way of verification, the documenents and/or datasources used for it must be noticed in protocol and the protocol must be preserve with other verification data.

In case of requesting an LCP and/or DVCP or codesign certificate, personal appearance of the Applicant is not required for checking her/his identity.

In case of requesting NCP and/or NCP+ certificate, personal appearance of the Applicant is required for checking her/his identity. SP provides information on its website about the possibilities of the personal appearance identification.

b. Checking the identity of the Subscriber's representative or agent

If the Subscriber or its representative / agent is different than the Applicant, the service agreement shall also be signed by the Subscriber's representative / agent. A personal appearance is not necessary.

The identity of the Subscriber's representative (or, in case of joint representation, representatives) is established on the basis of the legislation, authentic records, public document certifying registry, instrument of incorporation, or trusted and regularly updated data source defined in Chapter 3.2.2. The Subscriber's agent is determined on the basis of the authorisation signed by the representative(s). The Service Provider shall accept a general power of attorney in private documents or public instruments according to Section 6:16. of the Civil Code, or a power of attorney issued as a simple private document authorizing the application for and management of certificates in accordance with the sample published by the Service Provider on its website.

TRANSLATION

The signature of the Subscriber's representative / agent as included on the service agreement and authorisation is verified on the basis of an authentic specimen signature (e.g. specimen signature drawn up in the presence of an attorney or a public notary, or, in the case of an agent, the signature on the letter of authorisation). See also Chapter 3.2.5 for more information on rights and authorisations.

The authentication of the service agreement and authorisation can be performed by other than the Subscriber, in which case it shall be authenticated with an electronic signature (the electronic signature(s) of the representative(s)); the service agreement can also be authenticated with the Agent's electronic signature

c. Checking other subject data

If titles pertaining to a regulated profession or information pertaining to company registration rights are indicated, the Service Provider shall check the pertinent data (if applicable, based on a professional certificate, authentic information described in Chapter 3.2.2, other trusted sdata sources, or documents, the data of a registry kept by a professional chamber, or other official authentic records).

The Service Provider requires that the Applicant send an email to certify the email address to be included in the certificate (or to be in contact, if not included into the certificate) as follows:

- sending an email to Applicant with random value,
- Applicant can confirm the email address by sending back this email contained the random value;
- validity of the random value is 30 days.

d. Identifying the Receiver

If the Applicant did not personally appear at the Service Provider (or receipt does not take place immediately after personal identification) and the Service Provider wishes to hand over to the Client the Client device containing the private key that the Service Provider generated, the Approved Agent shall identify the Receiver at a personal meeting with the use of photographic personal identification documents.

e. Recording Applicant, Subscriber, representative, and agent data

The Service Provider will record the data to be indicated as the certificate's Subject (based on the data sources used during the course of the above checks) and records this check

The Service Provider stores, in its own system, the following data and documents pertaining to the Applicant and its representative and agent, as well as to the Receiver (see Chapter 9.4):

TRANSLATION

- The data required for unequivocally establishing the identities of the Applicant, Subscriber's representative and agent, and the Receiver, based on authentic documents;
- The Applicant's home address, based on authentic documents;
- The Applicant's data required for contact (e.g. postal address, telephone number, e-mail address).
- A signed copy of the service agreement;
- Public key of the requested certificate;
- The data of responses provided to queries in various records;
- The data of the documents used for identification and verification (e.g. document type, identification number, validity)
- The copies of the documents, certifications, and authorisations submitted during the Application, which were either provided by the Applicant or scanned by the Service Provider.

f. Miscellaneous provisions

The Applicant and the Subscriber have to acknowledge the veracity of the data provided during the identification process by signing the Service Agreement.

The Service Provider does not have to indicate an actual natural or legal person as the Subject of the test certificate (if the contents of the certificate unequivocally indicate that it is a test certificate); the checking of such subject data is therefore obviously not an expectation.

3.2.4. Non-verified subscriber information

Only such subject data are included in a certificate issued by the Service Provider that the Service Provider has verified (as written in Chapter 3.2), or about the authenticity of which the Applicant or Subscriber has provided a written statement beforehand in full knowledge of their liability under criminal law. If the Service Provider is unable to credibly ascertain the veracity and correctness of the data, it can deny the issuance of the certificate (see Chapter 4.2.2).

3.2.5. Control of eligibilities and delegation

If the Subscriber is a legal person, one natural person(s) may proceed at the Service Provider as Applicant. Such natural persons can be the official representative(s) of the legal person or a third person authorised by such person(s). These persons shall be identified in accordance with Chapters 3.2.3 or 3.3, and the Service Provider shall record the results of the check.

TRANSLATION

In the case of authorisations granted for specific periods of time, the fact that the expiration day has not yet been reached and (in case of legal persons) that the principal's right of representation is still valid shall be checked for each use.

If a natural person End-User is also named as the Subject of the certificate in addition to the legal person Subscriber, the Subscriber's representative(s) or agents shall grant their consent for the inclusion of the given legal and natural person's name and other data in the certificate.

If the certificate includes a full or partial right of representation (or a right that can be interpreted as such) (hereinafter jointly: right of representation), the Service Provider is obligated to ascertain the validity of the right of representation and its contents as included in the certificate before issuing the certificate, based on legislation, authentic public records, instruments of incorporation or, in absence of the above, an authorisation; the Service Provider is also obligated to record the results of the check.

Additional controls in the case of website authentication certificate (DVCP)

If the Subject (Subject or SAN field) of the certificate is a domain name, the Service Provider verifies that the Subscriber has the right to use and the control of the domain name. Service Provider uses the following methods for verifying that the Subscriber has the control to use the domain:

1. Constructed email to domain contact (BRG 3.2.2.4.4), wich consists of the following steps:

sending an email to Applicant with a unique randomized link (random access token), to the email address related to the domain or one of the subdomains that is given by the Applicant;

local host of this email address shall be 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'.

Applicant can confirm the email address by clicking on this link.

Validity of the random access token is 30 days. With validation of the domain, the related subdomains are also validated.

2. Agreed-Upon Change to Website (BRG 3.2.2.4.6), wich consists of the following steps:
    - sending an email to Applicant with a unique random value;
    - Applicant places the value in the /.well-known/pki-validation directory on webserver;

TRANSLATION

- Applicant informs TSP about placing the value using the related function of client menu, as result of which TSP system automatically checks the value.

Validity of the random access token is 30 days. With validation of the domain, the related subdomains are also validated.

3. DNS Change (BRG 3.2.2.4.7), wich consists of the following steps:
   - sending an email to Applicant with a unique random value;
   - Applicant places the value in DNS TXT record related to the domain; the value shall be prefixed with “netlock=” label;
   - Applicant informs TSP about placing the value using the related function of client menu, as result of which TSP system automatically checks the value.

Validity of the random access token is 30 days. With validation of the domain, the related subdomains are also validated.

4. DNS CAA Contact Email (BRG 3.2.2.4.13), wich consists of the following steps:
   - sending an email to Applicant with a unique randomized link (random access token), to the email address consisted as “ContactEmail” in the relevant CAA Resource.
   - Applicant can confirm the email address by clicking on this link.

Validity of the random access token is 30 days. With validation of the domain, the related subdomains are also validated. DNS record format shall be as follows: „CAA 0 contactemail user@domain.hu”

5. Email to DNS TXT Contact (BRG 3.2.2.4.14), wich consists of the following steps:
   - sending an email to Applicant with a unique randomized link (random access token), to the consisted contact email address in the relevant DNS TXT record.
   - Applicant can confirm the email address by clicking on this link.

Validity of the random access token is 30 days. With validation of the domain, the related subdomains are also validated.

DNS TXT record format shall be as follows:

- A “validation-contactemail” subdomain shall be made;

TRANSLATION

- DNS TXT record of this subdomain shall contain the contact email address (a single address and only email address is allowed to be consisted in DNS TXT record, according to RFC 6532 3.2).

For the widest possible browser acceptance of website authentication certificates, as well as avoiding possible abuses and verification of the relationship between domains and certificates issued, the Service Provider shall submit the certificates to the so-called "Certificate Transparency" (CT)[4] procedure before issuing them. In doing so, after the identification and verification procedures set out in this Section (3.2) – if successful –, the Service Provider forwards the certificate to the public so-called CT registry – before issuing it – as a pre-certification authenticated in accordance with RFC 6962 recommendation, in which the certificate is recorded as a new entry.

About the publication of the pre-certificate, CT log sends back a signed and timestamped confirmation to the Service Provider. A reference of this confirmation will be placed in a right field of the certificate (see chapter 7.1) directly before the issuance.

Domain validation shall be performed also in case of website-authenticating test certificate.

3.2.6. Criteria for interoperation

During the provision of services, the Service Provider may cooperate with other Service Providers, who will acknowledge the requirements included in the Service Policy as binding upon themselves.

The Service Provider discloses on its website all cross-certified certificates that it is the Subject or issuer of.

3.3 Identification and authentication for managing certificates

In the case of a process resulting in the issuance of a new certificate (see Chapter 4 Certificate lifecycle requirements, in particular, Subchapters 4.6 Certificate renewal, 4.7. Re-key, and 4.8 Certificate modification), Service Provider shall identify and verify the Client or clients and verify the data set out in the application in accordance with the identification procedure set out in Chapter 3.2.

In case Service Provider has already carried out the followings:

[4] For details on the so-called "Certificate Transparency" program visit https://www.certificate-transparency.org

TRANSLATION

- verification of the identity of the Applicant, verification of his personal data and his right/power to act;
- vertification of the identity of the Subscriber and the verification of his identifiers and his right to use the other data to be specified in the certificate;
- verification of the identity of the person or persons entitled to represent the Subscriber;
- verification of the identity and authorization of the agent of the representative or representatives of the Subscriber;
- verification of the data to be specified as the Subject of the certificate and recorded in the registry of Service Provider; and
- verification of the possession of the private key,

then Service Provider shall repeat these procedures in accordance with the rules of initial identity validation set out in Chapter 3.2 only if the earlier validation is obsolete or not reliable, or if the data of the Applicant, Subscriber or Subject recorded earlier have changed, or if a new key pair is generated for the new certificate.

In such a case Service Provider shall repeat only that parts of the procedures, which are required for verifying the changed data or facts.

In case the application contains a new encryption, authentication or codesign public key and/or includes the request for a new Client Device, then the provisions under Chapter 3.2.1 shall be complied with in all cases.

In case of applications for the management of website authentication certificates (DVCP), Service Provider shall repeat the verification of the data and the identification at least in every 27 months.

3.3.1. Identification and certification in the case of a valid certificate

In case the data required to be verified for the issuance of the requested certificate are identical to the data verified prior to the issuance of the certificate issued for the Client at an earlier date, and that earlier certificate is still valid at the time of the application of the new certificate, Service Provider does not carry out the verification of such data.

3.3.2. Identification and certification in the case of an invalid certificate

Service Provider shall not accept the service agreement, authorization (power of attorney) or any other document signed or stamped with an invalid certificate.

TRANSLATION

3.4 Identification and authentication for status change request

The Service Provider provides certificate revocation, suspension, and reactivation services. The Service Provider always identifies the applicant of the status change and ascertains that they have authorisation to perform the given action.

The Applicant's authorisation is checked as per Chapter 4.9.2 and the action is processed as per Chapter 4.9.4. The Service Provider identifies the Applicant of the status change as set forth below for the certificate's Applicant and Subscriber:

CHANNEL	IDENTIFICATION OF THE APPLICANT FOR STATUS CHANGE
CLIENT MENU (Only for suspension requests)	Enter user name and password.
PHONE	Of the personal information recorded in the client menu registration, at least three different pieces of information have to be checked. Identification is considered successful if all three pieces of information provided by the applicant are the same as those recorded in the client menu registration.
EMAIL	If a status change request arrives by email, the identification of the requester is based on the sender email address. If the sender email address is the same which is placed in the certificate of the status change request, the identification is success. If the sender email address is not the same which is placed in the certificate of the status change request, SP tries to connect via phone with the person who entitled to request to change the status of the certificate, to identify her/him via phone (see above) and to confirm or refute the request.

In case of being contacted by the authorities, identification takes place on the basis of the body's official (electronic or traditional) seal or its electronic signature.

TRANSLATION

4. CERTIFICATE LIFECYCLE REQUIREMENTS

The present Chapter 4 describes the actions that manage the lifecycles of the certificate issued by the Service Provider.

The certificate's lifecycle extends from the application for and the issuance of the certificate until its expiration or revocation. During this time, there is a possibility for suspending, activating, or modifying the certificate (if applicable in the case of the given certificate policy (see Chapter 1.2.1) or key use (see Chapter 7.1.2)) or replacing the certificate's keys. The Service Provider ensures that the Relying parties can also apply for certificates for testing (see Chapter 7.1). Of the rules set out in the present Chapter 4, only those rules are applicable to test certificates where explicitly indicated by the text of the Statement.

4.1 Certificate enrolment

The conditions and method laid out in the present Statement can only be used to apply for the services defined in Chapter 1.1. to request certificates written in Chapter 1.2.1

The present Chapter 4.1 describes only the procedures pertaining to original certificate applications. The certificate issuance that takes place in the framework of renewal, modification, or re-key applications is described in the appropriate Chapters (4.6-8).

The certificate application submitted previously to the Service Provider's Central (see Chapter 4.1.2) or External Registration Authority by the Applicant is required for the issuance of all end-user certificates (see Chapter 1.3.2).

The Service Provider provides easy-to-understand information in its regulations and/or on its website (see Chapter 1.1.2) regarding:

- the non-eIDAS nature of the certificates that can be applied for and the legal effects related to their application;
- their use (see Chapter 1.4);
- the business and legal information pertaining to the service (see Chapter 9);
- the conditions for concluding the Service Agreement;
- the rights and obligations of the Parties;
- the parts of the Service Provider's General Terms and Conditions (GTC) that pertain to services related to certificates;
- the security measures necessary in relation to the use of private keys;
- the use of the Client device, if the Applicant acquired such from the Service Provider.

TRANSLATION

Service Provider shall publish its statements and other information documents on its website in non-editable PDF format, and shall publish information by contents displayed directly on its website.

At least after the conclusion of the agreement, the Service Provider shall make available the service agreement, the service policy and the statement via link(s) in e-mail.

4.1.1. Who can submit a certificate application

The following parties can apply for end-user certificates in accordance with the requested profile:

CERTIFICATE PROFILE *(see chapter 7.1.)*	APPLICANT
PERSONAL PROFILE	The natural person indicated as the Subject of the certificate, on behalf of itself.
PSEUDONYM PROFILE	The pseudonym indicated by the natural person as the Subject of the certificate, on behalf of itself.
BUSINESS PROFILE	The natural person indicated as the Subject of the certificate, on behalf of itself, in certification of the fact that the organization also indicated as the subject of the certificate granted its consent for the certificate application. OR According to the preliminary agreement between the Service Provider and the Client, the representative or agent of the organization indicated as the Subject of the certificate, naming the natural person whose data it also wishes to indicate as the Subject of the certificate.
ORGANISATIONAL PROFILE	The representative or agent of the legal person indicated as the Subject of the certificate. OR The representative or agent of the legal person holding the trademark indicated as the Subject of the certificate.
DV WEBSITE AUTHENTICATION PROFILE	The natural person who has the control of the domain.

Any natural person can apply for a certificate for testing purposes (see Chapter 7.1) with any profile on behalf of itself, the organisation it represents, or its device.

The Service Provider manages a risk list of the natural and legal persons for whom it registers a risk related to certificate application, and may also use external data sources for its risk

TRANSLATION

assessment. Based on the risk assessment, the Service Provider can reject the certificate application.

4.1.2. Enrolment process and responsibilities

The certificate enrolment process starts with the application submitted by the Applicant to the Service Provider's Central or External Registration Authority and ends with the issuance of the certificate. During the course of this process, the Applicant is liable for the veracity of the data included in the application and the Service Provider is responsible for checking those and correctly displaying the certificate subject data.

a. Client System Registration and Certificate enrolment

The application for the issuance of encryption, authentication or codesign (LCP, NCP, NCP+) certificate may be initiated following the registration (see below) with the Client Menu available on the Website of the Service Provider, by signing in the Client Menu and selecting the certification application function and submitting the data requested by the system (see below). In the case of the service plans set out in the GTC the Application may be initiated by filling and sending the plan order forms available on the website of Service Provider. In this case the registration with the Client Menu (see below) and the recording of the application in the system of Service Provider (see below) takes place on the basis of the data submitted to Service Provider in the order form.

The application for the issuance of DV website authentication (DVCP) certificate may be initiated on onlinessl.netlock.hu available on the Website of the Service Provider after entering the Applicant's name, email address, username and password. The below i, iii and iv points do not apply to the application for DV website authentication certificates.

The Client can initiate its application for a test certificate (see Chapter 7.1) by sending an email to the Service Provider's Registration Authority (see Chapter 1.1.2). The application, after agreed upon with the Client, can be performed if approved by the Service Provider's Legal Department. Following negotiations with the Service Provider's Internal Auditors, any of the Service Provider's employees can request a test certificate for the purposes of internal testing.

The Service Provider may deviate from the above described means of the certificate application process in the case of a separate agreement made with Client, or with the Partner to the Service Provider, provided that an External Registration Authority is involved in the latter case (e.g. in case of bulk application for certificates or in the case of a special type of certificate).

During the certificate application process, the Service Provider uses the data provided when registering in the client menu and applying for a certificate to prepare, and then send to the Applicant in an electronic format, the service agreement applicable to the issuance of the requested certificate.

TRANSLATION

Registration in the Client menu and the certificate application process, which are required for certificate enrolment, are partially automated processes but also require human intervention. The steps that the Applicant has to take during these processes are discussed in detail in the guidelines available on the Service Provider's website.

i. Data recorded in the course of the registration with the Client Menu

Service Provider recordes the data required for certificate applications and for contacting the Applicant and the Subscriber.

In the course of the registration of Applicant with the personal Client Menu Service Provider records and retains the following data in its IT system:

- name (mandatory);
- identity card number (mandatory)
- country of home address (mandatory);
- city of home address (mandatory);
- postal code, street and house number of home address (optional);
- phone number (mandatory);
- e-mail address(mandatory);
- login name (mandatory);
- password (mandatory);
- password reminder (optional).

In case a certificate is requested for a legal person (in case of organisational or business profile, see Chapter 7.1), the following data shall also be recorded:

- name (mandatory);
- country of registered address (mandatory);
- city of registered address (mandatory);
- postal code, street and house number of registered address (optional);
- phone/fax number (optional);
- e-mail address (mandatory).

ii. Information required and recorded for certificate enrolment

Certificate enrolment can be initiated by submitting the following data (as part of the application or documents) in accordance with the requested certificate profile. Furthermore, the Subscriber's data required for contract conclusion and invoicing are also required, regardless of the certificate profile and the Applicant's name and password.

TRANSLATION

CERTIFICATE PROFILE (see chapter 7.1)	REQUIRED DATA
PERSONAL PROFILE	The data of the natural person indicated as the Subject of the certificate: • number of the personal identification document; • the family and given name(s) included in the personal identification document; • the home address or residence in the official address certification; • e-mail address.
PSEUDONYM PROFILE	• The data of the natural person applying for the certificate, as in the case of the personal profile. • The pseudonym to be used in the certificate.
BUSINESS PROFILE	• The data of the natural person to be indicated as the Subject of the certificate, as in the case of the personal profile (except address). • The data of the legal person to be indicated as the Subejct of the certificate and the data of its representative agent, as in the case of organisational profile.

ORGANISATIONAL PROFILE	The data of the organizasion indicated as the Subject of the certificate:
	• the name indicated in the identification document;
	• the registered address indicated in the identification document;
	• the name of the organizational unit (optional, except for website authentication certificates);
	• e-mail address;
	• taxpayer identification number;
	• the following data of the representative(s) or agent of the organization
	  ○ name
	  ○ e-mail address.

DV WEBSITE AUTHENTICATING PROFILE	The submission of the domain name(s) to be indicated as the Subject of the certificate. Furthermore, Applicant shall also provide a Certificate Signing Request (CSR) file.
⁕ **The scope of the requested data may be extended in certain cases.**	

When applying for a certificate for testing (see Chapter 7.1), the Applicant has to provide the purpose of the testing and the profile of the certificate to be tested.

iii. Submission of documents

In case a public document or any other official document is needed for the identification of any identity set out in any certificate application under Chapter 3, or for the verification of any right or power, or of any data to be included in the certificate, Applicant shall also present these documents to the Service Provider following the submission of the application. Service Provider shall, after recording the application, provide the Applicant with precise information on the documents to be presented. Applicant may send the copies of the documents in advance to the dedicated e-mail address (see Chapter 1.1.2).

iv. Additional conditions for certificate enrolment

1) In addition to the above, the Applicant also has to indicate
   a) the planned use of the certificate,
   b) the type of Subscriber (private person, company, government, or other),

TRANSLATION

c) and also has to submit the service agreement, authenticated as described in Chapter 4.2.1, to the Service Provider.

2) By signing the service agreement, the Client declares the following:
   a) its personal information included in the agreement are true and that it provided those to the Service Provider voluntarily;
   b) it has familiarized itself with, understands, and accepts the General Terms and Conditions, the present Practice Statement applicable to the requested certificate, and the Service Provider's Service Policy, which are available on the Service Provider's website;
   c) prior to the conclusion of the agreement, it has received the information as required by relevant legislation and has understood the limitations pertaining to the certificate (e.g. key use or the undertaking of liability by the Service Provider);
   d) in the case of website authentication certificate, Applicant consents that SP – before the issuance – submits a certified pre-certificate to a public CT log, where the pre-certificate will be recorded (see 3.2.5), and accepts that the issuance is possible exclusively after this submisson.
   e) it authorises the Service Provider to issue the certificate indicated in the service agreement.
3) By signing the service agreement, the Client furthermore certifies the following:
   a) it grants its consent for the handling of the data provided when registering in the client menu and in its Application;
   b) it requests the authentication of the public key set out in the agreement and its registry, storage, and handling in the certificate's public certificate repository (see also Chapter 4.4.2);
   c) it is familiar with the rights and obligations of the contracting parties.
4) If an organization is named as the certificate Subject, its representative or agent declares the following in the service agreement or - if such is attached separately to the service agreement - in the annex to the service agreement:
   a) the certificate enrolment is taking place with its knowledge and consent;
   b) it authorizes the Applicant to apply for the certificate, or
      i. with its suspension, revocation, or activation (4.9),
      ii. renewal (4.6),
      iii. modification (4.8),
      iv. to proceed in the re-key process (4.7);
   c) it undertakes to pay the service fees incurred in relation to the agreement;
   d) it has familiarized itself with, understands, and accepts the GTC, the present Practice Statement applicable to the requested certificate, and the Service

TRANSLATION

Policy, which are available on the Service Provider's website (see Chapter 1.1.2).

b. Responsibilities of Clients

During Application, the Applicant is responsible for exactly providing the data discussed in the present Chapter (4.1.2), for familiarising itself with the information sent by the Service Provider via email, and taking the steps requested by the Service Provider. If the present Statement requires the certification of identity for the issuance of the requested certificate, the Applicant is responsible for such certification as per Chapter 3.

The service agreement has to be signed by the Applicant and the Subscriber, as set out in Chapter 4.2.1. Except the website authentication (DVCP) certificates, where the service agreement is undefined.

4.2 Certificate application processing

The rules of the present Chapter (4.2) apply to applying for new certificates (Chapter 4.1) and to the processing of requests for renewal (Chapter 4.6), modification (Chapter 4.8), and re-keys (Chapter 4.7) - also including the identification-authentication procedure that precedes Certificate issuance, the acceptance or rejection of the issued certificate by the Client, and the duration of processing. The applicable chapters contain any rules that differ from those applied by the Service Provider under this Chapter for processing any requests.

When processing a certificate application, the employees of the Central or External Registration Authority check the personal and organisational data provided when filling out the electronic order form; they also identify the Applicant and his right to proceed and - in case of device order - generate the key pair. The Service Agreement is prepared automatically or with the involvement of the employees of the Registration Authorities, subject to the mean of the application.

In case of the NETLOCK SIGN service, the Central or External Registration Authority is not involved in the generation of the key. The key is generated by the users following the submission of the certificate application, in the protected environment of NETLOCK SIGN.

During the Application, the Service Provider also checks the trueness of the provided email address by requesting confirmation of certificate enrolment from this address and forwarding instructions and information to this address, the performance by and knowledge of which by the Applicant are essential for conducting the certificate enrolment process.

TRANSLATION

If, based on the application or the Service Provider's offer, the private key is generated for a Client device provided by the SP, the Service Provider will generate the key during the processing of the application (see Chapter 6.1), after which it compiles a package containing:

- the Client device and, if required for its use, the Client device reader;
- the information required for the first use of the Client device.

The Service Provider will inform the Client on the completion of the package (Client device, reader, and information) by sending an email to the address provided during the Application. The Receiver can then take over the package at the place and with the method provided in the email.

The rules above are not applicable in case of DV website authentication (DVCP) certificates. Therefore the rules in the subchapter below should be applicable only if the given action does not require human intervention.

4.2.1. Performing identification and authentication functions

If the Applicant has provided all information and data during the certificate application process and has also submitted the copies of all documents required for their certification (which are to be handed over or sent to the Service Provider in accordance with the requested certificate profile as per the present Statement (see Chapter 4.1.2), the Service Provider's Registration Authorities performs the identification and authentication tasks that are to be completed before Certificate issuance.

The Registration Authorities of Service Provider use independent sources to check, in accordance with Chapter 3, the data submitted or acquired during the application and the Applicant's identity and right to proceed. Registration Administrators and Validation Specialists perform the identification and authentication procedure in line with the requirements pertaining to the work processes included in the Registration Authorities' internal regulations. These internal regulations may set forth additional requirements (not discussed in this Statement) for identifying certificate applications that the Service Provider considers to be high-risk and for which supplemental control procedures are required.

See Chapters 3.2 and 3.3 regarding the identification of the Applicant and the Subscriber.

a. Certification of the Service Agreement and submitting it to the Service Provider

The Service Agreement has to be authenticated by the Applicant and, if applicable, the Subscriber prior to every certificate issuance, even if the certificate was issued on the basis of a data check performed earlier.

TRANSLATION

The service agreement includes the Applicant's and Subscriber's statement pertaining to the fact that they have familiarized themselves with their obligations and undertake to keep those.

The service agreement can be authenticated and submitted in hard copy format with a handwritten signature or electronically with an electronic signature and, if applicable, an electronic seal.

The Applicant has to sign the hard copy of the service agreement in the same manner as the handwritten signature on the personal identification document. If the Subscriber is different than the Applicant, it has to sign the hard copy of the authorisation by way of its representative or agent with the same signature used on the submitted specimen signature (see Chapter 3.2.3).

If the service agreement is authenticated electronically, the personal identification data in the certificate used for the signature have to be the same as the personal data of the Applicant / Subscriber indicated in the service agreement or the unequivocal certificate identification data indicated in the authorisation. The Subscriber can also use a seal for authentication. In this case, the organisation identification data indicated in the seal have to be the same as the Subscriber data included in the service agreement.

If the authorisation does not form a part of the service agreement but is a separate document, the method used to sign the agreement and the authorisation may differ, i.e. one can be hard copy-based and the other can be electronic.

The Applicant cannot authorise others to sign the service agreement; however, an authorised person can also sign the service agreement on behalf of the Subscriber.

The person acting as the attorney-in-fact on behalf of the Subscriber may also act as the Applicant, in such a case only Applicant shall sign the Service Agreement on behalf of the Client, whereby Applicant makes his statements both on his behalf and on behalf of the Subscriber. After its approval, Service Provider shall certify the Service Agreement by sealing it with its own electronic stamp, or with the electronic or handwritten signature of the employee of the Registration Authority who is authorized to do so. In the case of electronic signature or seal, the certificate thereof is issued on the basis of the NCP, NCP+ or QCP certification policies. Service Provider shall, after certifying the Service Agreement, send it to Applicant in the form of an electronic copy.

b. CAA verification (DVCP)

In the case of website authentication certificates (DVCP), the Service Provider shall carry out CAA verification.

TRANSLATION

In the course of the CAA verification the Service Provider shall query the CAA record of the domain.

Service Provider deems that the certificate is authorized in the following cases:

- in the case of non wildcard domain, the CAA record issue contains „netlock.hu", „netlock.net" or „netlock.eu";
- in the case of wildcard domain, the CAA record issuewild contains „netlock.hu", „netlock.net" or „netlock.eu".
- the CAA record is unavailable.

In case the CAA record contains issue or issuewild, but it is empty, Service Provider shall refuse the issue of the certificate.

4.2.2. Approval or rejection of certificate applications

The Service Provider certifies receipt of the Application by sending an automatic reply to the email address provided during the Application. The automatic response does not mean that the Service Provider has accepted the Application and merely serves to inform the Client that the Service Provider's Registration Authority has received the Application and it will commence its processing.

The Service Provider's Registration Authorities decide on its acceptance or rejection during the processing of the certificate application. The Registration Authority will accept the certificate application if the identification and authentication steps set out in Chapter 4.2.1 have been successfully completed. i.e.

- the Applicant's person has been successfully identified;
- the data provided as the certificate subject have been checked and found to be true;
- the service agreement has been properly signed (if applicable).

If identification and authentication were successful and the signed service agreement has been accepted, the Registration Agent performing the check approves the certificate application.

The Service Provider will call upon the Applicant to submit missing information if the identification and authentication steps set out in Chapter 4.2.1 are unsuccessful because

- the Service Provider does not have all the data or documents at its disposal to process the Application (see Chapter 4.1.2), *or*
- the available data are not authentic or their authenticity cannot be determined, *or*
- the Applicant's right to apply for the certificate cannot be established.

TRANSLATION

The Service Provider will reject or delete the certificate application if the identification and authentication steps set out in Chapter 4.2.1 are unsuccessful because

- the data provided in the application are false, or
- the Applicant is not authorised to submit the given certificate application,

Additional circumstances that can lead to the rejection or deletion of the certificate application:

- General, business, and legal conditions:
  - the Applicant fails to comply with the Service Provider's request for completion or clarification within the deadline;
  - the service fee has not been paid by the deadline set out in the GTC;
  - the Subscriber has overdue amounts for any services under the present Statement;
  - the authorised party does not receive the Client device within 30 days of being notified;
  - the conditions necessary for issuing the certificate are not met - for any reason - within 30 calendar days from the date of submission of the application
  - final liquidation or settlement proceedings are under way against the organization indicated as the certificate subject;
  - the entity(-ies) indicated as the certificate subject and/or the Applicant's home/registered address are in a country subjected to a technological or economic embargo imposed by Hungary or the European Union.

- Circumstances regarding identification and authentication:
  - the relationship between the entity(-ies) indicated as the certificate subject and the Applicant/Subscriber is not clear;
  - the Applicant's right to apply for the certificate is not clear;
  - doubts arise regarding the originality, trueness, or validity of the data provided in the certificate application;
  - doubts arise regarding the originality, trueness, or validity of the documents submitted in their original or copies thereof to certify the data provided in the certificate application;
  - the Applicant and/or Subscriber do not grant consent for reproducing and/or storing reproductions of the documents presented for the purposes of verifying the data provided in the certificate application;

TRANSLATION

- the subject of the certificate application is the issuance of a certificate containing the data of an organisation without legal personality or an association;
- other conditions violating the Service Provider's regulations.

The Applicant will be notified of rejected applications and of the reason therefor.

The Service Provider will not issue certificates (DVCP) for certain domain endings (which are defined in its internal regulations) and internal domain names; it automatically rejects applications containing such domain names.

4.2.3. Time to process certificate applications

The certificate application will be considered processed once the certificate has been issued or rejected by the Service Provider.

The Service Provider will process the certificate application within 14 days of having received the documents required for certificate application. The Service Provider will generally issue the certificate within an additional 3-5 workdays if the conditions for issuing the certificate have been met.

In case of a request for missing information, the duration of the request for missing information is not part of the deadline for processing the certificate application.

4.3 Certificate issuance

The rules of the present Chapter (4.3) apply to applying for new certificates (Chapter 4.1) and to the processing of requests for renewal (Chapter 4.6), modification (Chapter 4.8), and re-keys (Chapter 4.7) - also including the Service Provider's activities conducted during certificate issuance and informing the End-User on certificate issuance. The applicable chapters contain any rules that differ from those applied by the Service Provider under this Chapter for certificate issuance conducted on the basis of modification, renewal, or re-key requests.

The time of certificate issuance is the time when the Service Provider makes the signed certificate available in the Client Menu; the start of the certificate's validity can differ from this time.

a. The issuance of end-user certificates

A condition for issuing an end-user certificate is the submission by the Applicant of a certificate application (as defined in Chapter 4.1) to the Service Provider. The Service Provider will only issue the certificate if the application has been processed as set out in Chapter 4.2.

TRANSLATION

A certificate application approved by the Service Provider's Registration Authority is submitted to the Service Provider's Central or External Certification Authority, that takes the steps necessary for the issuance of the certificate. The Service Provider can only issue the certificate with the data provided during the application process. Website authentication (DVCP) certificates are issued by automatic system without human interaction, after domain control check and payment.

Payment is due before certificate issuance in the manner defined in the GTC. The Service Provider can also agree with the Subscriber differently, in which case the Service Provider can create and issue the certificate before the payment of the service fee and can also set a deadline by which the Subscriber has to pay the service fee.

The End-User can start using the keys after the issuance of the certificate, as set forth below:

CERTIFICATE	KEYS AND THE USE OF THE CERTIFICATE
SOFTWARE-BASED CERTIFICATE	In the case of a software-based certificate, the Applicant generates the key itself on its own computer. Following its issuance, the End-User has to install the certificate on its computer as shown by the instructions available on the Service Provider's website. The keys and the certificate can then be used.
DEVICE-BASED CERTIFICATE	The Service Provider will only hand over the ordered Client device to an authorised Receiver. Following its issuance, the End-User has to upload the certificate to the device as shown by the instructions available on the Service Provider's website. The keys and the certificate can then be used. If the keys included in the certificate were generated by the Service Provider during the course of the application, the certificate can only be issued if the Service Provider has ascertained that the authorised Receiver has received the Client device. However, the Service Provider may, based on a preliminary agreement concluded with the Applicant, issue the certificate and upload it to the device in a suspended state before handing it over. In this case, the End-User shall activate the certificate without delay, but no later than by the deadline set out in Chapter 4.9.13. The keys and the certificate can then be used.
DV SSL	In the case of an SSL certificate, the Applicant generates the key pair itself on the server to be authenticated. The keys and the certificate can then be used after the certificate has been installed on the server.

b. The issuance of SP certificates

SP certificates are issued in the manner defined in the Service Provider's Security Regulations and with the control of at least two trusted employees; records shall also be drawn up. The Service Provider publishes SP certificates in the manner and by the deadline set out in Chapter 2.2.

TRANSLATION

4.3.1. SP actions during certificate issuance

a. End-user certificates

Based on the data provided during the application, the Service Provider creates the certificate in its IT system and, after the service agreement has been signed and approved, certifies it with its SP certificate. The certificate will then be made available to the End-User in the client menu and, the NETLOCK sign system. Unless the Applicant requests otherwise, the certificate will then also be available in the public certificate repository (see Chapter 4.4.2). During these activities (i.e. issuance), the Service Provider ensures that the entire process is secure, thus preventing the certificates from being falsified.

Unless the Service Provider and Subscriber agree beforehand, the certificate can only be issued following the payment of the service fee; the Service Provider will therefore prepare, based on the invoicing data provided during the application, the hard copy or electronic invoice or the proforma invoice required for payment of the service fee and will mail it to the invoicing/email address provided in the application (see the GTC) before issuing the certificate. In some cases fees are payable online by credit card – in case of DV website authentication certificates it is exclusively.

b. SP certificates

Simultaneously to making the certificate available, the Service Provider also publishes a brief description of the purpose of the SP CA certificate. The certificates may be downloaded from the public certificate repository of Service Provider. During these activities (i.e. issuance), the Service Provider ensures that the entire process is secure, thus preventing the certificates from being falsified.

4.3.2. Notification by the SP of issuance of certificate

The Service Provider notifies the End-User on the issuance of the certificate - no later than the day the certificate becomes valid - by sending an email to the address in the certificate.

The Service Provider provides information on the download and installation or activation of the certificate via email.

4.4 Certificate acceptance

The rules of the present Chapter (4.4) apply to applying for new certificates (Chapter 4.1) and to the certificates issued on the basis of requests for renewal (Chapter 4.6), modification (Chapter 4.8), and re-keys (Chapter 4.7). The applicable chapters contain any rules that differ from those applied by the Service Provider under this Chapter for certificate issuance conducted on the basis of modification, renewal, or re-key requests.

TRANSLATION

4.4.1. Conduct constituting certificate acceptance

Before downloading or activating the certificate or starting to use the private key, the Client is obligated to check the veracity of the data in the certificate. The End-User can view the certificate data by logging into the Client Menu. If it discovers any irregularities or deviations, it cannot start using the certificate or private key and is to notify the Service Provider's Customer Service immediately about its objection; it shall then take the steps necessary for revoking/suspending the certificate (see Chapter 4.9).

The Client has to check whether the private key and the certificate are connected by executing the task for which the key is intended and by verifying the action with a certificate.

In case of device-based certificates, the Service Provider will consider the certificate, the connected public key, and the private key paired to be accepted if the Client does not raise any objections at the Service Provider within 5 workdays of the receipt of the Client device or does not initiate its revocation or suspension. In other cases, the Service Provider will consider the end-user certificate to be accepted by the Client 5 workdays after certificate issuance.

4.4.2. Publication of the certificate by the SP

Following the issuance of the end-user certificate, the Service Provider will publish it in the public certificate repository unless the certificate's Applicant has requested otherwise. The Applicant can submit such requests to the Service Provider's Registration Authorities by email during the processing of the certificate application.

4.4.3. Notification of certificate issuance by the SP to other entities

a. End-user certificates

The Service Provider does not notify any other actors on certificate issuance besides those set out in Chapter 4.3.2.

b. SP certificates

The Service Provider publishes information on the issuance of SP certificates on its website (see Chapter 1.1.2).

TRANSLATION

4.5 Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The Certificate and the private key paired to the public key included in the Certificate can be used for the purposes defined in the “Key Usage” and “ExtendedKeyUsage” fields, in line with Chapters 7.1 and 1.4.

Other requirements for the use of the certificate:

- If the private key was generated for a cryptographic device, the End-User can only activate and use the private key on the device for which it was generated (see more in chapter 1.4.1).
- If the private key was generated for an SCD, the End-User can only activate and use the private key on the SCD for which it was generated (see more in chapter 1.4.1).
- If the key was generated for a cryptographic device, the End-User can only activate and use the private key on the device over which it has control.
- The private key has to be under the sole control of the End-User.
- The use of expired, revoked, or suspended certificates or related keys is not permitted.
- If the End-User makes a copy of the private key, it has to handle the copy with the same level of diligence as the original copy.
- The End-User is obligated to inform the Service Provider immediately if any of the following events transpire prior to the expiration of the certificate, and shall immediately terminate the use of the private key:
    - the loss or theft of the private key, or if the private key becomes compromised
    - the loss of sole control over the private key, e.g. due to the activating data becoming compromised
    - the inaccuracy of or a change to the data included in the certificate.
- If the SP key used to sign the end-user certificate becomes compromised, the End-User is obligated to immediately terminate the use of the private key and the certificate.
- See Chapter 6.2.10 if the certificate expires or is revoked.

4.5.2. Relying party public key and certificate usage

When using the certificate, the Relying Party’s circumspect procedure is a requisite for maintaining the security level guaranteed by the Service Provider: the Relying Party shall proceed in line with the Service Provider’s regulations, with especial regard to the following:

TRANSLATION

- it is to only accept public keys in case of use that is in line with the Certificate's "KeyUsage" and "ExtendedKeyUsage" fields (see Chapter 7.1.);
- it is to check certificate validity and status (see Chapter 4.9.6.);
- it is to take into account all restrictions that are included in the certificate or the regulations referred to by the certificate (see Chapters 1.4 and 6.1.7.);
- it shall only use trusted software for using keys and certificates.

If the Relying Party does not proceed in line with the Service Provider's regulations, the Service Provider does not assume liability for the resulting damages.

4.6 Certificate renewal

The Client may request the certificate provided by the SP to be renewed before the expiration of its validity. During the course of renewal, the Service Provider generates a new certificate with the public key in the certificate to be renewed and based on the Subject data.

In case of renewal, the Client cannot request that the Subject data be modified; however, the certificate's other data can change (e.g. certificate serial number and validity, Service Provider data, CRL/OCSP information).

The Service Provider can initiate the renewal of end-user certificates at any time at its own discretion.

End-user certificates can be renewed more than once; the Service Provider is authorised to reject requests for renewal.

4.6.1. Circumstance for certificate renewal

The Client can request that its certificate be renewed if the following conditions are met:

- the certificate is valid;
- the validity of the certificate will expire in no more than 30 days;
- the public key used in the certificate can still be considered to be cryptographically secure and is expected to remain such during the validity of the renewed certificate;
- the private key paired to the public key included in the certificate has not been compromised.

No more than 30 days before the expiration of the certificate, the Service Provider sends an email to the address included in the certificate, in which it informs the Client on the approaching expiration date and the process for certificate renewal / applying for a new certificate.

TRANSLATION

An application for certificate renewal can be submitted following the instructions available on the Service Provider's website or, based on a previous agreement, by other means in writing.

The Service Provider can initiate the renewal of an end-user certificate at its own discretion if the following conditions are met:

- the certificate is valid;
- the certificate is to be revoked before the expiration of its original validity due to an external circumstance (e.g. a change in legislation or a supervisory decision) and the renewal can ensure that the certificate will meet the new conditions;
- the public key used in the certificate can still be considered to be cryptographically secure and is expected to remain such during the validity of the renewed certificate.

Renewal of the Service Provider certificates is subject to a valid certificate to be renewed.

4.6.2. Who may request renewal

Renewals of end-user certificates can be requested by the Service Provider or the Applicant or Subscriber of the certificate that is to be renewed.

4.6.3. Processing certificate renewal requests

The Service Provider certifies the receipt of the application for certificate renewal by sending an automatic reply to the email address included in the certificate. The automatic response does not mean that the Service Provider has accepted the Application and merely serves to inform the Applicant that one of the Service Provider's Registration Authorities has received the application and it will commence its processing.

The certificate renewal process is partially an automated process, but it also requires human intervention. During the application for renewal, the Service Provider sends instructions and information to the email address in the certificate, the performance by and knowledge of which by the Applicant are essential for conducting the certificate renewal process. The steps that the Applicant has to take during the renewal process are discussed in detail in the guidelines available on the Service Provider's website.

During the renewal application process, the Applicant has to provide its invoicing data and the data required for preparing the new service agreement. The Service Provider sends the service agreement to the Applicant in an electronic format.

a. Identification and authentication

In case of an application for certificate renewal, the identification of the Applicant and the signing and forwarding to the Service Provider of the service agreement necessary for the

TRANSLATION

issuance of the renewed certificate take place as set out in Chapter 4.2.1., with the following exceptions.

Validation of the data placed in the renewed certificate is based on the original certificate. In this case SP does not check the datas in any authentic datasource or official document, because the datas in the original certificate – if the certificate is still valid – can be considered authentic.

During renewal, the Applicant declares the following by signing the service agreement (if applicable):

- the data checked when the original certificate was issued has remained unchanged;
- the documents that certified the veracity of its data at the time are still valid;
- it is not aware of the certificate private key having been compromised.

b. Approval or rejection of renewal applications

The Service Provider decides on the acceptance or rejection of a renewal application during its processing. The Service Provider will accept the certificate application if the identification and authentication steps set out in Chapter 4.6.3.1 have been successfully completed.

The renewal application will be considered complete and authentic once the service agreement has been signed. The Service Provider will not sign the service agreement, but will indicate its acceptance by issuing the renewed certificate.

The trusted employee of the Service Provider's Registration Authorities will check whether the renewal application is complete and the service agreement is correct and authentic. If the data provided when applying for a renewal are incomplete and/or the service agreement is incorrect, unsuitably authenticated, or its authentication cannot be established, the Service Provider's Registration Authority will call upon the Applicant to submit missing information.

The Service Provider can reject the request for renewal if the following conditions are met:

- the missing information requested by the Service Provider is not provided by the expiration of the certificate that is to be renewed;
- during the course of processing the application, the Service Provider finds out that the data checked when the original certificate was issued have since become invalid, in which case the Service Provider will revoke the certificate to be renewed (see Chapter 4.9);
- during the course of processing the application, the Service Provider finds out that the private key of the certificate to be renewed has become compromised, in which case the Service Provider will immediately implement measures to revoke the certificate;

TRANSLATION

- any conditions that can result in the rejection of a certificate application and are also applicable to renewal;
- the Client owes overdue payments for an invoice issued for any of the Service Provider's services;
- the certificate to be renewed cannot be unequivocally identified.

The Service Provider can reject the renewal of the certificate with other reasons set out in writing (e.g. supervisory decision).

If the renewal request is rejected, the Client can maintain the continuity of the services by applying for a new certificate.

c. Time to process renewal applications

The Service Provider processes certificate renewal requests with the time set out in Chapter 4.2.3. In case of a request for missing information, the duration of the request for missing information is not part of the deadline for processing the renewal application.

d. Issuance of the renewed certificate

If the applicable conditions are met, the Service Provider will issue the renewed certificate 2-10 workdays before the expiration of the original certificate, unless agreed upon otherwise by the Service Provider and the Client.

The Service Provider does not assume liability if the renewed certificate is not issued before the expiration of the original certificate and the continuity of the service is interrupted if such was caused by the Client's omission or delay.

See also Chapter 4.3.

4.6.4. Notification of new certificate issuance to subscriber

The Service Provider will notify the Client on the issuance of the renewed certificate in the manner set out in Chapter 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal certificate

The provisions of Chapter 4.4.1 are applicable to the acceptance of the renewed certificate.

4.6.6. Publication of the renewal certificate by the SP

The provisions of Chapter 4.4.2 are applicable to the publication of the renewed certificate.

TRANSLATION

4.6.7. Notification of certificate issuance by the SP to other entities

The provisions of Chapter 4.4.3 are applicable to notifying other actors.

4.7 Re-key

The Client is provided with the possibility of requesting the replacement of the public key and its private key pair before the expiration of the validity of its certificate provided by the SP. During the course of the re-key, the Client will generate a new key pair on behalf of itself or the Service Provider will generate one for it, after which the Service Provider will create a new certificate (including the new public key) with the use of the subject data included in the certificate on which the re-key is based. The Client has to destroy the private key belonging to the revoked certificate (see Chapter 6.2.10).

In case of a re-key, the Client cannot request that any data besides the key be modified; however, the certificate's other data can change (e.g. serial number, Service Provider data, CRL/OCSP information).

The Client can request the re-key in writing; information on the method for submitting the application is found on the Service Provider's website. In addition to the written request, the Applicant also has to initiate a new certificate application (as set out in Chapter 4.1.2) in order to start the re-key process.

The Service Provider may initiate the re-key of end-user certificates at its own discretion at any time. The Service Provider will inform the Client of re-keys performed at its own discretion by sending an email to the address in the certificate.

Re-keys are possible for both valid and revoked (e.g. due to a compromised key) certificates.

4.7.1. Circumstance for certificate re-key

The Client can initiate the replacement of the key pair belonging to the certificate within the validity of the certificate.

The Service Provider can initiate the replacement of the keys of an end-user certificate if the key pair can no longer be considered to be cryptographically secure or it is forced to do so by an external circumstance (e.g. a change in legislation or a supervisory decision).

The Service Provider will send a notification to the email address provided in the certificate regarding the end-user certificate re-key it initiates.

4.7.2. Who may request certification of a new public key

The provisions of Chapter 4.6.2 are applicable to re-key applications.

TRANSLATION

4.7.3. Processing certificate re-keying requests

The provisions of Chapter 4.6.3 are applicable to processing requests for certificate modification, with the deviation that the valid status of the certificate and the non-compromised private key is not a prerequisite.

4.7.4. Notification of new certificate issuance to subscriber

The provisions of Chapter 4.3.2 are applicable to notifying the Client.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

The provisions of Chapter 4.4.1 are applicable to the acceptance of the certificate.

4.7.6. Publication of the re-keyed certificate by the SP

The provisions of Chapter 4.4.2 are applicable to the publication of the certificate.

4.7.7. Notification of certificate issuance by the SP to other entities

The provisions of Chapter 4.4.3 are applicable to notifying other actors.

4.8 Certificate modification

The Client has to request the modification of its certificate provided by the SP within its validity if its subject data change within its validity.

During the course of certificate modification, the Service Provider creates a new certificate with the public key in the certificate to be modified and with the subject data modified according to the application. If the certificate on which the modification request is based contains invalid data because of a change in such data, the Service Provider will revoke the certificate during the modification process (see Chapter 4.9).

If the modification request takes place in the 30-day period prior to the expiration of the validity of the certificate for which the application is submitted, the modification is considered to also be a request for renewal (see Chapter 4.6). In this case, Chapter 4.6 is governing regarding the validity period of the new certificate.

In case of a modification, the certificate's other data can also change (e.g. certificate serial number and validity, Service Provider data, CRL/OCSP information) in addition to the requested change in subject data.

The Service Provider may also initiate the modification of end-user certificates at its own discretion at any time. The Service Provider will inform the Client of the above by sending an

TRANSLATION

email to the address in the certificate. In this case, the Service Provider will determine the validity period of the new certificate.

An application for certificate modification can be submitted by the Client following the instructions available on the Service Provider's website or, based on a previous agreement, by other means that take place in writing.

End-user certificates can be modified more than once; the Service Provider is authorised to reject requests for modification.

4.8.1. Circumstance for certificate modification

The provisions of Chapter 4.6.1 are applicable to the circumstances of certificate modification, with the difference that the modification request can be initiated at any time within the certificate's validity period.

4.8.2. Who may request certificate modification

The provisions of Chapter 4.6.2 are applicable to Applicants of certificate modification.

4.8.3. Processing certificate modification requests

The provisions of Chapter 4.6.3 are applicable to processing requests for certificate modification, with the following deviations:

- the Service Provider's Central or External Registration Authority will check the changed subject data as defined in Chapter 4.2.1;
- the statement on the fact that the subject data remained unchanged and the validity of the documents presented at the time of the original check does not pertain to the changed data;
- the Service Provider will not reject the application due to the invalidity of the data certified at the time of issuing the original certificate.

4.8.4. Notification of new certificate issuance to subscriber

The Service Provider will notify the Client on the issuance of the modified certificate in the manner set out in Chapter 4.3.2.

4.8.5. Conduct constituting acceptance of modified certificate

The provisions of Chapter 4.4.1 are applicable to the acceptance of the renewed certificate.

TRANSLATION

4.8.6. Publication of the modified certificate by the SP

The provisions of Chapter 4.4.2 are applicable to the publication of the modified certificate.

4.8.7. Notification of certificate issuance by the SP to other entities

The provisions of Chapter 4.4.3 are applicable to notifying other actors.

4.9 Certificate status change

The Client may request the status of its certification to be changed before the expiration of its validity. The request for status change can include the suspension, activation, or revocation of the certificate (see *Chapter 1.6.1 Definitions* of the *Service Policy*).

In case of a status change request, the Service Provider will change the status of the certificate subject to the request on the basis of the application, as set forth below:

- only active certificates can be suspended;
- only suspended certificates can be activated;
- valid and suspended certificates can be revoked.

A suspension is for a fixed term, within which time the Client is to revoke or reactivate the certificate; otherwise, the Service Provider will revoke the certificate at the end of the period. A suspended certificate will once again become valid after activation, and will then also be considered valid for the term of the suspension. The revocation permanently invalidates a certificate from the moment of its revocation (or its preceding suspension).

The revocation or suspension can pertain to both end-user certificates and SP certificates.

The subscriber and activation is not applicable in the case of certificates for website authentication certificates (DVCP).

4.9.1. Circumstances for revocation and suspension

The Service Provider will evaluate the request for the revocation/suspension no later than within 24 hours of its receipt by taking into account the following circumstances; based on the evaluation, it will revoke or suspend the end-user certificate or will reject the application for revocation/suspension. The following circumstances may serve as basis of the revocation or suspension of the end user certificates. In the following cases Service Provider shall revoke or suspend the certificate not later than within 24 hours from the receipt of the Request:

Compliant request submitted by Client (Status Change request of Client);

TRANSLATION

- Client notifies Service Provider that the original certificate request was not authorized and does not authorize it subsequently;
- Non-compliance of any obligation of the Client;
- Notification by any third party regarding a lost and found client device;
- any other circumstance set out in the GTC;
- compromising of the private key that belongs to the public key of the certifcate;
- compromising of the service provider private key used for certifying the certificate;
- renewal, modification or key replacement of the certificate;
- unauthorized use of name or data,
- data incorrectly recorded in the certificate, incorrectness, change, misleading nature of the data;
- the Client failed to request the activation of the certificate within the time period of suspension;
- use of the certificate in bad faith;
- a related final, binding and executable resolution of any court or authority;
- the technical properties of the certificate expose any of the parties to a level of risk that exceeds an acceptable level on the basis of the significant professional recommendations (e.g. the key length is shorter than recommended);
- breach or termination of the service agreement;
- the certificate has not been issued in compliance with the applicable policies;
- the Service Provider becomes aware that the Client is not entitled to use any of the names (e.g. FQDN) indicated in the certificate;
- the Service Provider becomes aware of the termination of the right of representation indicated in the certificate;
- the provision of the expiry information services pertaining to the certificate is terminated;
- termination of the service, unless if the Service Provider had early arranged for the continuation of the provision of the CRL and OCSP services related to the certificates issued by the Service Provider;
- required by the law.

Possible grounds for suspension of the certificates:

- initial suspension following the issue of the certificate in order to increase the security of the shipment;
- a strong presumption of any circumstance that serves as ground for the revocation of the certificate.

TRANSLATION

Suspension is not applicable in the case of certificates for website authentication certificates (DVCP).

The Service Provider shall make arrangements within at least seven days for the revocation of the service provider certificates in the following cases:

- the compliant, written request of the Certification Authority (in the case of outsourced issuer);
- the Certification Authority notifies the servie provider that the original issuer certificate request was not certified and does not certify or authorize it subsequently (in the case of outsourced issuer);
- compromising of the private key that belongs to the public key of the certifcate;
- compromising of the service provider private key used for certifying the certificate;
- use of the certificate in bad faith;
- data incorrectly recorded in the certificate, incorrectness, change, misleading nature of the data;
- the provision of the expiry information services pertaining to the certificate is terminated;
- the technical properties of the certificate expose any of the parties to a level of risk that exceeds an acceptable level on the basis of the significant professional recommendations (e.g. the key length is shorter than recommended);
- a related final, binding and executable resolution of any court or authority;
- termination of the service;
- required by the law.

4.9.2. Who can request status change

The Service Provider, courts, the Supervisory Body, other authorities, and, in the case of end-user certificates, Applicants and Subscribers can request the suspension, revocation, or activation of certificates. In case of regulated professions the Chamber of the profession can also request the suspension and revocation of the certificate if Client is no longer authorised to exercise a regulated profession.

In case of notification by a third-party of an abuse of the Service the Service Provider will investigate the circumstances and to decide on the suspension of the certificate.

Client can activate the certificate, only if the requesting of the suspension was requested by Applicant or Subscriber and the circumstances of the suspension have already eliminated. If SP suspended the certificate at its own discretion, after the circumstances of the suspension have eliminated, SP shall activate the certificate forthwith.

TRANSLATION

4.9.3. Procedure for revocation, suspension and activation

a. Procedure for revocation and suspension

The revocation or suspension procedure is a process that starts with the receipt of the status change request for revocation or suspension by the Service Provider or with the Service Provider's decision or instruction and ends with the revocation or suspension of the certificate or, in case of an unsuitable application, with the rejection of the application.

The Service Provider evaluates requests for revocation and suspension without delay and before other requests.

Revocation, suspension, and activation can be requested by the authorised parties (see Chapter 4.9.2) by email or phone. The request for revocation, suspension, or activation has to contain at least the following data:

- the certificate serial number,
- the name of the (natural or legal) person requesting the revocation / suspension,
- the contact information of the person requesting the revocation / suspension,
- the time of the revocation / suspension (if not immediate).
-

Suspension can be claimed in client menu, in which case the suspension will be automatically made.

If the key is compromised or lost, the Service Provider conducts a re-key procedure (see Chapter 4.7). The Service Provider can also handle client requests for revocation by issuing a suspension for the time of processing the request.

The use of the private key belonging to the suspended certificate shall also be suspended for the term of the suspension. The private key belonging to the revoked certificate has to be destroyed immediately after revocation, if this is possible (see Chapter 6.2.10).

The following rules of liability are applicable to the damages arising from the accepting the certificate as a result of certificate status changes:

- Until the request for revocation or suspension is received by the Service Provider, the Client is liable for any resulting damages.
- Following the receipt of the revocation or suspension request by the Service Provider, the Service Provider is liable for any resulting damages until the time the changed status of the certificate is published.

TRANSLATION

- If the Service Provider has already published the invalid status of the certificate (revoked or suspended), the Service Provider does not assume any liability for any Relying Parties still considering the certificate to be valid.

See chapters 9.6 and 9.8.

b. Procedure for certificate activation

Those persons can request that the suspended certificate be (re-)activated who are authorised to request the certificate's suspension or revocation. The application can take place in the manner set out in Chapter 4.9.3.1 with the condition that the activation of the certificate cannot be initiated in the Client Menu. If the certificate is not activated during the term of suspension set out under Chapter 4.9.13, the certificate will be automatically revoked after the expiration of the term of suspension.

4.9.4. Revocation request grace period

Before executing status change requests, the Service Provider checks them according to the following:

1. The identification of the Applicant: see the contents of Chapter 3.4
2. The right of the Applicant: see the contents of Chapter 4.9.2
3. The veracity of the application: see the contents of Chapter 4.9.3.1

The executability of the status change request:

- For revocation requests: if the certificate is valid or suspended.
- For suspension requests: if the certificate is valid.
- For activation requests: the certificate is suspended and the circumstances that led to the suspension are no longer applicable.

Once the Service Provider's Central or External Registration Authority has ascertained that the Applicant has authorisation and the application if complete and authentic, it will suspend/revoke the certificate without delay.

If the above requirements are not met, the Service Provider rejects the application; otherwise, it has to take measures without delay to revoke, suspend, or activate the certificate without any further consideration. The Service Provider can also handle the application for revocation by temporarily suspending the certificate in the interest of clarifying the circumstances that led to the revocation.

The Service Provider will inform the certificate's Applicant and the Subscriber via email about all executed and rejected applications for suspension, revocation, and certificate activation.

TRANSLATION

The Service Provider publishes certificate status changes in the framework of its certificate status services (see Chapters 4.9.7-10 and 4.10).

4.9.5. Time within which SP must process the status change request

The deadlines for processing revocation/suspension/activation requests are as follows depending on the channel used for the application:

CHANNEL	PROCESSING DEADLINE	MAXIMUM PROCESSING DURATION
CLIENT MENU (only suspension)	Requests are processed continuously, 24/7.	Maximum of 24 hours
PHONE (See Chapter 1.1.2)	Requests are processed continuously, 24/7.	maximum of 24 hours
EMAIL (See Chapter 1.1.2)	Requests are processed during working time. The receiving time of the requests is the time of the first human respons for the request.	maximum 24 hours from the first human respons

If the Service Provider is unable to ascertain the legality of the revocation, suspension, or activation request (or the authorisation of the requesting party) within the above time frame, it will consider the request to have been submitted by an unauthorised person until proven otherwise and will close the revocation, suspension, or activation process as having been unsuccessful.

Following the implementation of status change requests, the Service Provider validates the change:

- immediately in the Online Certificate Status Service (OCSP);
- a new revocation list will be issued no later than 1 hour following the change;
- in the public certificate repository no later than 1 hour following the change.

4.9.6. Certificate status checking requirement for relying parties

When accepting and using the information included in the Certificate, the Relying Parties have to proceed with suitable diligence, taking into account the requirements of Chapters 1.4 and 4.5 and the contents of the table in Chapter 7.1 that presents the relationships between certificate profiles, certificate policies, and uses. It is thus especially recommended to check:

TRANSLATION

- the validity of the end-user certificate;
- the validity period of the intermediate CA's certificate (SP certificate) used to authenticate the end-user certificate;
- the validity period of the top-level Root CA's certificate (SP certificate) used to authenticate the intermediate CA's certificate;
- the certificate status of the end-user and SP certificates by querying the CRL or OCSP-based certificate status information referred to in the certificates.

The certificate can be considered to be valid if the time of the verification is within the certificate's validity period at which time the certificate was in a valid status, and these conditions are also true for all certificates in the certificate chain.

To determine the past validity of expired certificates, the respective revocation list or OCSP response valid at the given point in time is required (e.g. these can be integrated into an electronic signature or seal at the time of authentication).

The validity of website authentication certificates (DVCP) has to be established for the moment the website was authenticated.

The Relying Parties can receive information on the current status of various certificates with the use of certificate status services (see Chapter 4.10). Only the currently valid certificates can be queried in the public certificate repository available on the Service Provider's website - and only if the Applicant of the queried certificate has granted its consent for disclosing the various data in the certificate. Suspended and revoked or expired certificates are not accessible via the public certificate repository.

4.9.7. CRL issuance frequency

Certificate Revocation Lists (CRLs) primarily include those revoked and suspended certificates that were still valid at the time the list was issued; however, the Service Provider may also issue CRLs that include all of the revoked and currently suspended certificates that the Service Provider issued, regardless of the time of their issuance. Suspended certificates will be removed from the list after being reactivated. The Service Provider certifies CRLs with its own electronic signature.

Generally 4, but no more than 24, hours elapse between the issuance of CRLs pertaining to two consecutively issued end-user certificates; CRLs may not be valid for more than 24 hours. New CRLs pertaining to SP certificates are generally issued every 24 hours, but no less frequently than every 12 months (in case of cross-certified certificates by maximum 31 days); CRLs may not be valid for more than 12 months. A CRL is issued with the above frequency even if no

TRANSLATION

certificate revocations, suspensions, or activations have taken place since the last issuance. CRLs always include the latest time by which the subsequent list has to be issued.

4.9.8. Maximum latency for CRLs

The Service Provider will publish the certificate revocation list (CRL) no later than one hour following the approval of the status change request.

4.9.9. On-line status checking availability

The Service Provider also provides an Online Certificate Status Service (OCSP) for verifying certificate status, as set out in Chapter 4.10.

4.9.10. On-line status checking requirements

The Service Provider supports Online Certificate Status Protocol (OCSP) requests received with the 'GET' and 'POST' parameters defined by RFC 2560 or RFC5019 for querying certificate status information. See: Chapter 4.10.

All Relying Parties are authorised to perform OCSP requests. The Service Provider always serves requests with the proper parameters, by taking into account the provisions laid down in Chapter 6.5. Requests are processed and OCSP replies are sent automatically. The Service Provider authenticates OCSP replies with its own SP certificate dedicated to this purpose (OCSP responder certificate). The Relying Party that checks the validity of the certificate with the use of the OCSP service also has to check the signature of the OCSP reply.

When the certificate in question is valid, the OCSP reply issued by the Service Provider contains "good" status information if

- the OCSP request pertains to a certificate issued by the Service Provider;
- the OCSP request pertains to the availability of the OCSP indicated in the certificate.

4.9.11. Other forms of revocation advertisements available

The Relying parties can also use the public certificate repository to collect certificate status information: if they do not find a specific certificate issued by the Service Provider here, it is to be considered as not valid.

If the Service Provider terminates the use of its root certificate, it is to publish this fact on its website.

TRANSLATION

4.9.12. Special requirements re-key compromise

The Service Provider will always notify the Client(s) by sending an email to the address in the end-user certificate if it gains knowledge of a threat of the end-user key(s) becoming compromised or the possibility of any of the circumstances set out in Chapter 4.9.1.

In the case of the assumed or proven key compromise, it will perform the steps of the revocation procedure (Chapter 4.9.1.1). A compromised private key can never be used again; if possible, steps are to be taken to have it destroyed and it is to be provided the same supervision and protection until its destruction as given a valid private key (see Chapter 6.2.10).

The Client is obligated to take all steps to prevent or mitigate damages, including notifying any Relying Parties affected by the private key having been compromised.

If the SP's intermediate CA private key is compromised or threat arises of such, the steps of the revoking the certificate shall be performed (Chapter 4.9.1.2).

If the TSP's root CA private key is compromised or threat arises of such, TSP shall destroy the root CA certificate and the related keys immediately, then informs Clients and Relying parties via its webpage and if it is possible via email. Furthermore TSP also informs that browser developers whose root program includes the TSP's root certificate.

4.9.13. Limits on suspension period

A certificate can be suspended until the suspicion of the circumstances that led to its revocation is confirmed or rebuked, but for no more than 30 calendar days. The Service Provider has to provide for the revocation or activation of the certificate as soon as possible. The start of the suspended status is to be calculated from the time the suspension request is approved, i.e. the request defined under Chapter 4.9.3.1, which time is indicated in the CRL. If the suspicion of the circumstances leading to its revocation is not confuted during this period, the Service Provider will automatically revoke the certificate.

Suspension is not applicable in the case of certificates for website authentication certificates (DVCP).

4.10 Certificate status services

The Service Provider provides Relying Parties with the services required for checking the status (valid, suspended, revoked) of certificates issued on the basis of the present Statement.

TRANSLATION

4.10.1. Operational characteristics

The CRL and Online Certificate Status Service pertaining to the various certificates are available at the URLs indicated in the certificate's crlDistributionPoints and authorityInfoAccess:OCSP certificate extension fields (see Chapter 7.1.2). These records can be used to verify certificates within their periods of validity. Following the time indicated in the certificate's "notAfter" field

- the certificate will not be included in the CRL even if the certificate has been previously revoked/suspended.
- the Service Provider provides the last certificate status within the certificate's validity period as a response to OCSP requests.

After the validity period of certificates the status information can be checked in former CRLs, available (by individual request) at the Service Provider.

During the management of certificate status services, the Service Provider shall proceed according to the following:

- it ensures the continuous, 24/7 online availability of certificate status information (at the URLs indicated in the certificate's applicable fields and on the Service Provider's website);
- the time data indicated in the CRL and OCSP responses will be synchronized at least once a day with the Coordinated Universal Time (UTC);
- it uses a PKI-based signature to ensure the integrity and authenticity of certificate status information;
- it ensures that information on revocation is included amongst the respective certificate status information for at least the certificate's original validity period;
- the revocation information pertaining to expired certificates is accessible amongst the archived CRLs issued during the validity of the certificate;
- it offers a CRL and OCSP for the purposes of verifying certificate status;
- it ensures that the CRL and OCSP services harmonize with each other: the information on a certificate status change has to be available in both of these services and has to be the same;
- it ensures that certificate revocation information is publicly and internationally accessible;
- it ensures that the revoked and suspended certificate statuses are differentiated amongst the certificate status indications;
- it ensures that suspended certificates are removed from the Certificate Revocation List (CRL) after activation;
- in the case of certificate suspension or revocation due to a key being compromised, the Service Provider issues an extraordinary CRL after registering the status change; in

TRANSLATION

case of revocation or suspension for any other reason, the status change will be published no later than in the next planned revocation list.

In the case of web site authetnitcation certificates (DVCP) the Service Provider will keep the size of the CRL under 7 MB (if possible) in the interest of providing for a fast download.

4.10.2. Service availability

The Service Provider continuously (24/7) provides as part of its certificate services, the availability of requests for revoking and suspending end-user certificates and of CRLs; as set forth below.

In regard to the availability of

- certificate status services;
- the other Terms and Conditions applicable to the use of certificates issued by the Service Provider; and
- services related to status change

and also taking into account the contents of Chapter 4.9, the Service Provider ensures the following:

- 99% availability on an annual level;
- the duration of any single service disruption will not exceed 3 hours.

For the Web site authentication certificates (DVCP) the response time of CRL and OCSP services will be no more than 10 seconds under normal loads.

Service Provider provides the activation of the end user certificates on business days during the hours of service published on its website (see Chapter 1.1.2).

SP ensures the CRLs issued by it to be available on the original URL for 2 years after CRL is issued. Availability (URL) of CRLs that are older than 2 years may change.

SP ensures the CRLs issued by CodeSign CA contain the revoked certificates until 10 years after the relevant certificate's original expiry date.

4.10.3. Optional features

The Service Provider will not apply any more requirements for the certificate status service.

4.11 End of subscription

Service Provider provides information on the termination of the service agreement in the GTC.

TRANSLATION

See the relevant Chapter of the GTC.

4.12 Key escrow and recovery

SP privides key escrow and recovery services for encryption certificates.

In other cases Service Provider shall not store or save the private keys of the end user certificates in any way whatsoever, and therefore Service Provider cannot restore such keys in case these keys are stolen or damaged while in possession of the end user.

4.12.1. Key escrow and recovery policy and practices

In the case of the private keys of end-user certificates, the Service Provider does not provide any key deposit, or key recovery services.

The same level of security requirements apply to copies of end-user private keys made by the Client as to the original private key (see Chapter 6.2). The number of copies of a private key should not exceed the amount necessary for maintaining the service. Client is allowed to make a backup of her/his own private key, exclusively if she/he can provide the compliance storage and protection of it.

The Service Provider also saves and stores its own SP private keys.

4.12.2. Session key encapsulation and recovery policy and practices

The Service Provider does not store or recover symmetric keys.

TRANSLATION

5. Facility, management, and operational controls

In the interest of decreasing risks, the Service Provider stores the hardware, software, and other devices required for the services it provides in two different locations physically separate from each other: in a primary location and a secondary location. The requirements applicable to the two locations are the same; any deviations are indicated at the applicable points.

The configuration of the Service Provider's systems is regularly checked in order to filter out any changes that are in violation of the security requirements.

The devices of the Certificate and Registration Authorities are handled exclusively by authorised and suitably trained personnel whose knowledge is checked.

Backups are made of the Authorities' files (see Chapter 6.5). The Service Provider retains the backups for the time set out in Chapter 5.5.2.

The Service Provider examines the physical, procedural, and personal requirements by regularly assessing risks. The Service Provider keeps an inventory of assets which include the devices (and information assets) that it uses.

The Service Provider's private Security Regulations include the requirements pertaining to information security rules.

The Service Provider reviews the Security Regulations and asset inventory regularly or immediately following any significant changes to ensure they remain continuously applicable, suitable, and effective.

5.1 Physical controls

The aim of physical controls is to prevent unauthorised access, damages, and unlawful entry to the Service Provider's confidential information and physical premises (server rooms). The Service Provider uses a suitable system of authorisations to limit physical access; these authorisations are regularly reviewed.

The Service Provider ensures that the loss of and damages to values are avoided, that values are not compromised, and that operating activities are not disturbed by applying the measures set out in the Service Provider's Security Regulations.

Services that process critical or sensitive information are performed and modules that use cryptographic modules are used and stored in secure locations. The provided protection is proportionate to the risks determined by the Service Provider in the risk assessment.

TRANSLATION

5.1.1. Site location and construction

The Service Provider performs the services subject to the greatest risks in a secure, protected computer room located on its site. Physical access, the supervision and checking of entry, the power supply, air conditioning, protection against leaks and flooding, fire prevention and fire protection, the storage of data media, the accessibility of the telecommunications network, electromagnetic radiation, etc. are all controlled on the basis of the same factors of protection. Access by unauthorised persons to the computer room is made difficult, but the security personnel can quickly gain access in case of a breach. The security zone does not have any windows; with the exception of the door, the only way access can be gained is by demolishing the reinforced walls. The room is equipped with redundant climate control, automatic fire fighting, and intrusion alarm systems. All equipment is hooked up to a multiply redundant electricity supply.

The Service Provider's secondary location is a server safe in a protected secure computer room, the security level of which is the same as that of the on-site location.

The Service Provider's Central Registration Administrators perform key generation, the preparatory actions pertaining to key storage devices, certificate issuance, and the management of status changes in a separate server room specially designed for this purpose. The protected server room was designed expressly for this purpose.

5.1.2. Physical access

The relevant internal operational documents contain the exact parameters of the security zones and the list of persons who are authorised to enter. Persons other than the employees who fill trusted roles can only enter the security zone with separate authorisation and if accompanied. Access to the computer room takes place with a personalized electronic card; all access is logged both physically and electronically. Within the computer room, the SP systems are installed in a separate area where access is only granted after biometric identification. Round-the-clock video surveillance is provided for the room that provides access to the security zone as well as for the computer room itself.

The access system to the secondary location does not use biometric identification; however, security guards provide round the clock protection to protect homogeneity and the security of the secondary location. Access to the server room is granted to authorised employees with their key cards; entry and exit is continuously logged. Round-the-clock video surveillance is provided for the server room.

In the framework of critical services, the Service Provider's risk assessment deals with the regulation of physical access, protection against natural catastrophes, the factors of protection against lightning and fire safety, the faults of support equipment (especially electricity and

TRANSLATION

climate control equipment), the collapse of the building, leaky water pipelines, protection against groundwater, protection against theft and breaking and entering, and restoration after catastrophes.

The Service Provider stores SP certificates separately from its normal operations and access to those is granted only to trusted employees.

5.1.3. Power and air conditioning

The uninterrupted power supply of the Service Provider's protected computers is especially important in order to ensure continuous operation, in the interest of which the Service Provider uses (has used) the following:

- uninterruptible power supply,
- selective short circuit protection,
- protection against electrical anomalies, lightning, and overvoltage.

The system providing the uninterruptible power supply is structured as follows:

- diesel generator,
- local battery-based uninterruptible power supply,
- redundant circuit selector.

The following operational procedure is followed:

- if the network power supply is interrupted or decreased, the system switches to the backup power supply,
- the system meanwhile starts the generator,
- when the network power supply is again usable (for 5 minutes continuously), the system returns to its use.

A selective short circuit protection was used in the computer room to develop several systems that operate independently of each other and thereby support continuous operations. The distribution network was designed to ensure that if any group of equipment is short circuited, power will be cut off from that group while the other equipment groups that are operating flawlessly can remain operational.

In the server room, the computer rooms have an air conditioning system independent of the rest of the building. A suitable filtration system is used to ensure the cleanliness of the air inducted into the protected computer room, which filters out various pollutants and also provides the staff with the air they require. The humidity and temperature of the air is continuously monitored. The air conditioning systems provide for the cooling that the IT systems require. Continuous operation is also supported by a second (backup) climate control

TRANSLATION

system which will turn on if necessary. The location of the climate control systems ensures that their maintenance does not cause any disturbances to the computer room's operations.

5.1.4. Water exposures

The Service Provider's service locations are protected from leaks and floods. The use of a raised floor increases security in the protected computer room.

5.1.5. Fire prevention and protection

The Service Provider's service locations are operated in line with fire safety requirements. The locations are equipped with fire and smoke detectors as well as manual and automatic fire extinguishers. The location of manual fire extinguishers and escape routes are indicated in high visibility locations.

5.1.6. Media storage

A security zone and a rented bank safe is used to ensure the safe storage of the Service Provider's data media. The Service Provider has several backups of critical data. The Service Provider continuously ensures and takes the necessary steps to prevent the deprecation of its data media.

The Service Provider disposes of data media that contain sensitive data in the manner set forth in the Security Regulations, if such are no longer necessary. The Service Provider permanently deletes the contents of disposed tools or irreparably destroys them.

5.1.7. Waste disposal

The Service Provider shall proceed according to the following regarding physical destruction:

- paper-based documents are shredded,
- floppy disks are shredded (after removal from their housing),
- other magnetic data media are demagnetized and then crushed,
- other data media are crushed.

5.1.8. Off-site backup

In the interest of providing for the continuity of business and of avoiding data loss, the Service Provider makes backups and ensures that the entirety of the IT system can be restored if necessary. Backups are protected from unauthorised access, modification, deletion, and destruction. Preparation for extraordinary situations includes the application and testing of plans for specific situations.

TRANSLATION

The Service Provider provides for the secure storage of the data by using write-only media, saving backups in a remote location, or concurrently storing those in more than one place.

5.2 Procedural controls

The Service Provider ensures that its systems operate securely, in accordance with applicable rules, and with a minimal risk of error. In the interest of the above, it employs a suitable number of staff with appropriate skills, technical knowledge, and experience.

In the case of non-qualified services, the Service Provider operates an internal management and control policy, including the connected responsibility system, that is up to date and meets the requirements of relevant legislation and standards. The control activities of independent system controllers also ensure that the system operates suitably.

The Service Provider has a quality assurance and information security management system in place that is continuously monitored by an external, independent system controller.

The Service Provider classifies the managed data created during the provision of non-qualified services into a security class on the basis of the risk assessment defined by relevant legislation and in the Practice Statement; it furthermore ensures that they are suitably recorded, checked, and protected, and that the required responsibility system is used.

5.2.1. Trusted roles

Only those persons can fill trusted roles (see Chapter 5.2.1 of the Trust Service Policy) at the Service Provider for whom it certifies with technical experience, education, and vocational qualifications that they are protected from corruption and have the necessary expertise.

The role that is generally responsible for the IT system is filled by a person who has a vocational higher education degree[5] and at least three years of experience in IT security.

The Service Provider employs the person fulfilling a trusted role in the framework of employment; moreover, the person in the trusted role is free of all interests that can negatively affect the reliability or security of the service. The Service Provider ensures that the person dealing with the provision of services has the required and suitably up-to-date skills and experience. The Service Provider ensures that all trusted roles are fulfilled.

[5] A vocational higher education degree means a university degree in mathematics or physics, or a college or university degree in an engineering major of a technical science.

TRANSLATION

The Service Provider keeps a current registry on trusted roles; in case of any changes, it reports the change without delay to the Supervisory Body.

5.2.2. Number of persons required per task

The following activities are performed by the Service Provider in the physical presence of at least two designated trusted employees with direct authorisation, in a physically protected environment:

- generating of SP key pairs;
- issuing intermediate CA certificates;
- saving and restoring SP private keys;
- destroying SP private keys.
- saving and restoring end-user private keys used in NLSIGN service.

5.2.3. Identification and authentication for each role

All of the Service Provider's employees in trusted roles can only access the secure zone after proper identification and authentication, which in addition to which further identification is also required for access to IT systems. Access to the secure zone and the system is not possible without successful identification and authentication, thus no activities critical to security can be performed without these steps.

The Service Provider personally identifies all users of its IT systems and all actors of administrative processes, with the exception of users with read-only authorisation for public data services. Only authorised persons can access the Service Provider's IT systems. The Service Provider provides for the administration of access by System Administrators, System Operators, and Independent System Controllers, including the management and ad hoc modification of user accounts or the termination of access.

Access to the various applications is restricted. The system can differentiate between the various trusted roles, thus especially access by System Administrators and System Controllers.

Staff is identified and authenticated before they are allowed to use applications critical to services, and they can be held accountable for such activities.

The Service Provider records the permission levels for the various trusted roles in the Human Resources Policy.

TRANSLATION

5.2.4. Roles requiring separation of duties

In these systems, the Service Provider applies security measures and defines permission levels that minimize unauthorised or unintentional modifications and decrease the possibility of violations.

In the interest of separating roles

- the security officer does not perform the tasks of the independent system controller and the manager generally responsible for the IT system;
- the independent system controller does not perform the tasks of the manager generally responsible for the IT system;
- the security officer does not perform the tasks of the system administrator; and
- the independent system controller does not perform the tasks of the validation specialist and the system administrator.

The Service Provider uses a strict control policy to ensure that registration tasks are separated, i.e. the data required for the issuance of certificates should not be validated by the same trusted employee who approves the issuance of the certificate. Inspection procedures can be audited.

The Service Provider's Security Regulations contain the detailed rules on conflicts of interest.

5.3 Personnel controls

The purpose of security measures pertaining to personnel is to decrease the risk of human error, theft, fraud, and abuse.

In the interest of the above, the Service Provider deals with personnel security even during the hiring process, and then ensures personnel security with checks performed during the term of employment.

The Service Provider has a detailed and exact Personnel Policy. The Service Provider documents the temporary and permanent roles and responsibilities defined in the Personnel Policy in job descriptions, which include:

- the information management performed by each role and the classification of risks based on their effects on the various authentication processes,
- technical and experience requirements,
- a description of the activities regarding the position and the tasks of the given employee, the scope and extent of responsibilities, and the name of the related positions.

TRANSLATION

The Service Provider's employees may not fill trusted roles until the time the checks regarding the persons and the required statements have been implemented and until they have participated in the required trainings and gained the necessary experience.

The Service Provider's executives, managers, and employees in trusted roles are independent of all business, financial, and other influences that could influence the trust shown towards the services offered by the Service Provider.

5.3.1. Qualifications, experience, and clearance requirements

The Service Provider employs staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards.

All persons designated to fill a trusted role at the Registration Authority undergo an initial check (to verify their reliability and technical suitability). During this basic security check, the inspectors check the data provided in the curriculum vitae (details, references, professional advancement, etc.). During the course of the above:

- the data pertaining to education are compared to the certificates and degrees to be submitted by the candidate,
- the statements made regarding practical experience are verified with personal references, based on publications, and by other means.

Service Provider shall ensure that the Registration Administrators and Validation Specialists shall have sufficient knowledge for performing their activities in compliance with the practice statement, to this end Service Provider shall provide the Registration Administrators and Validation Specialists with trainings in the following subject matters:

- basic PKI knowledge;
- principles and procedues of authentication and certification set out in the Certificate Policy and the Practice Statement;
- phishing and other techniques threatening the reliability of the authentication and certification procedure.

Service Provider shall maintain a registry of the trainings.

TRANSLATION

The Registration Administrators and Validation Specialists shall not carry out their activities without the knowledge set out above, and therefore Service Provider requires the Registration Administrators and Validation Specialists to successfully pass the related examination.

The Registration Administrators and Validation Specialists are familiar with current official documents and other equivalent documents as well as with their types and characteristics, and they are also capable of verifying the validity of the submitted documents.

All employees who fulfil trusted roles have to undergo periodical security checks in addition to the basic security check.

Persons qualified as a “high security risk” at the basic or any periodical security checks cannot fill a trusted role. Trusted roles may only be filled by people who have no criminal records, which shall be certified during the hiring process with a Certificate of Good Conduct that is no older than 3 months.

Employees who are employed in trusted roles are succumbed to periodical security checks every year (see Chapter 5.2.1).

Following their appointment, Validation Specialists participate in basic training that provides them with the theoretical and practical knowledge required for their position; they are to take an exam at the end of the training. The main purpose of this form of training is to become familiar with and understand the uniform security policy applicable to the service in the interest of correctly applying the current procedures based on those. The Personnel Policy contains more information.

Employees can fill trusted roles after gaining suitable experience.

5.3.2. Inspection Procedures

During the hiring procedure, the Service Provider checks the identity of the persons during their physical appearance or by checking their photographic personal identification documents. In addition to the above, the Service Provider also takes into consideration the information pertaining to previous employers, relevant education, and professional references.

Employees in trusted roles cannot receive access to the Service Provider’s systems before these checks have been performed.

5.3.3. Training requirements

Employees in trusted roles have to have the knowhow required for performing their tasks. In the interest of ensuring this knowhow, employees in trusted roles have to take an exam to

TRANSLATION

certify their knowledge. They cannot access the SP systems until passing this exam. The exam and the training extend to the following, depending on the type of trusted role:

- PKI basic knowledge;
- Authentication and control rules and procedures;
- Security and data protection rules;
- General threats to information authentication processes (including data fishing and other social engineering tactics);
- the requirements of the Practice Statement and other regulations;
- The legal consequences of certain acts;
- The unique features of the Service Provider's IT system and the method for its management.

5.3.4. Retraining frequency and requirements

The Service Provider defines its training and retraining practices in the annual retraining plan.

If any significant changes take place in the trust services, all employees undergo a modular retraining with the necessary structure and level in addition to being provided the required documentation.

5.3.5. Job rotation frequency and sequence

The Service Provider's Personnel Policy defines the applicable rules.

5.3.6. Sanctions for unauthorized actions

The Service Provider regulates the sanctions applied for the unauthorised use of the Service Provider's system and for any errors, omissions, or damages caused during the provision of the service in the employment contracts of the persons filling trusted roles.

5.3.7. Independent contractor requirements

The same security rules apply to any contractors used by the Service Provider in other than employment relationships as to its employees.

5.3.8. Documentation supplied to personnel

The Service Provider continuously ensures that the current regulations and documentations necessary for persons participating in the provision of services are available to them.

TRANSLATION

5.4 Audit logging procedures

In the interest of retaining the actions involving certificates and the preparation of Client devices and the data used during these processes, the Service Provider's authentication system performs a wide array of logging activities that meet the requirements of legislation and applicable standards and requirements. The log file includes the exact time of the record, the calendar date of the logged event, the type of event, the data required for traceability and reconstructing the event, the name of the user or other person that caused the event, and whether the action was successful or not. The Service Provider synchronizes the time indicated in its logs with a frequency that ensures that the difference between its own time and the current time does not exceed 1 second. Any deviations that exceed this amount will also be logged.

The Service Provider's other system also perform logging. The characteristics of these logs depend on the given application. The log elements are created separately in the various modules. Since the system consists of several components, the log files are not created in one location; however, they are processed in one central location.

The Service Provider protects all records in the log file from changes and unauthorised access. The log is handled in a manner that excludes the possibility of its destruction, the deletion or modification of its records, and modifying the order of records in any way. The Service Provider regularly backs up the log file and ensures that log data are continuously evaluated and controlled. The Service Provider documents the method of accessing logged information and the time for which it must be stored.

At an operative level, the operational descriptions of the various systems regulate the handling of log data.

5.4.1. Types of events recorded

The system used by the Service Provider logs all the events and errors required by relevant legislation that are critical from the aspect of services. Log files are recorded automatically or manually. In addition to the log files, the Service Provider also uses records to record various events.

The Service Provider sets forth in detail in the Security Regulations the exact data/events that it records in relation to each event.

Logged events are recorded in the log file as dated entries. The Service Provider protects all log entries from modification, unauthorised access, destruction, deletion, or any changes to the order of entries by using electronic signatures, saving, and backups.

TRANSLATION

Searches for event type and/or user can be performed in the log files. The log entries are in text format.

5.4.2. Frequency of processing log

The Service Provider's log entries are reviewed on a daily basis by Independent System Controllers who have the required expertise and authorisation. Evaluation takes place both manually and with the use of software tools.

During the course of the evaluation, the evaluator analyses the error messages generated by the systems, the significant changes to the traffic data, the trends that differ from the usual, and suspicious activities. The evaluator or the software tool records the fact and results of the evaluation as well as any necessary measures.

The Service Provider's network protection systems are also equipped with an automatic alarm function, which goes off if any unauthorised access is detected. In the case of such alarms, the log entries are immediately reviewed. The Service Provider may also review the log data if any irregularities are found, if complaints are received, or if otherwise contacted.

5.4.3. Retention period for audit log

Log files are stored at the place of their creation and are also archived (see Chapter 5.5.2); the related certificates are stored for a period of 10 years after their expiration (one year in the case of other services) or until the final closing of any legal disputes that are incurred and reported in relation to those. Log files are accessible to Independent System Controllers.

5.4.4. Protection of audit log

The log entries of the Service Provider's authentication system are stored with the Service Provider's electronic signature and in a manner that excludes the possibility of undetected deletion or insertion.

Backups protect log files from accidental and intentional damages. In the case of log entries containing personal information, the Service Provider ensures that the data storage is confidential. Only those persons are authorised to access the log files who require access for their roles (generally the Independent System Controllers). The Service Provider checks access in a secure manner.

TRANSLATION

5.4.5. Audit log backup procedures

Log files are regularly saved in the manner defined in Chapters 5.1.6 and 5.1.8. If the log entry is created in only one location, the Service Provider ensures that a backup will be created within 24 (twenty four) hours.

5.4.6. Audit collection system

The applications automatically collect and store log entries in the log files. The Service Provider collects the saved media on a daily basis. The Service Provider's own employees transport the media to the place of storage.

5.4.7. Notification to event-causing subject

The persons, units, and applications that cause a log entry are not notified by the Service Provider; however, it may include them in inspecting the event. If the parties that caused the event are in a contractual relationship with the Service Provider or if otherwise required by relevant legislation, they are obligated to cooperate with the Service Provider.

5.4.8. Vulnerability assessments

During the course of processing log entries, the Service Provider performs assessments regarding vulnerability. In addition to the processing performed on a daily basis, the Service Provider's experts also review extraordinary events every month, on the basis of which they assess vulnerabilities. Based on these assessments, the Service Provider takes steps to improve the security of the system.

Every year, the Service Provider performs a risk assessment, with the help of which it identifies, evaluates, and classifies into risk classes the foreseeable external and internal threats that could lead to the unauthorised access, disclosure, modification, destruction, or other abuse of the certificate management processes. The risk assessment also extends to expected damages if such threat were to become real. In addition to the above, the risk assessment also includes a description of the processes and security measures that the Service Provider takes to prevent these threats.

5.5 Records archival

The Service Provider retains the data pertaining to the service in the manner and for the time defined in this Chapter. Together with the retention, the Service Provider also provides a tool with which the contents of the issued certificate can be determined.

The Service Provider protects all entries in archived data files from unauthorised modification, deletion, destruction, and access. Archived data files stored electronically are affixed with at

TRANSLATION

least advanced electronic signatures or seals and with timestamps. The Service Providers ensures that for the time that it stores the data, they remain authentic and accessible and interpretable to authorised persons.

5.5.1. Types of records archived

The Service Provider has to retain the data related to the certificates it issues - thus especially related to their creation and issuance and including personal information. In accordance with the above, the following are archived:

- the data provided by the Applicant and the Subscriber during certificate enrolment (see Chapter 4.1.2.1);
- the electronic or hard-copy documents, or copies thereof, that came into the possession of the Service Provider during the course of the identification and authentication processes (see Chapter 4.2.1);
- the ID of the Registration Administrator who accepted the application (see Chapter 4.2.2);
- the name of the Registration Authority that performed identification and authentication;
- the information disclosed during the certificate status change procedure (see Chapter 4.9.3);
- the information logged in accordance with the present Statement (see Chapter 5.4).

The Service Provider archives electronic data in an electronic format. The Service Provider archives documents available in hard copy format either in the form of an electronic copy or in their original hard copy format.

5.5.2. Retention period for archive

The Service Provider archives the electronic and hard copy information and personal data pertaining to certificates for at least ten years following the expiration of the certificate as defined by the certificate, or until the legal dispute regarding the certificate, regarding the public key in the certificate is closed in a final ruling. For the same periods as set forth above, the Service Provider also ensures that tools are available that can be used to determine the contents of the issued certificates.

TRANSLATION

5.5.3. Protection of archive

To protect electronic documents and data, the Service Provider applies the requirements set out in Chapter 5.4.4 regarding both documents received in electronic format and the electronic copies that the Service Provider itself makes.

The Service Provider stores the documents available in hard copy format within the security zone defined in Chapter 5.1, thus ensuring that only Registration Administrators, Certification Administrators, and Validation Specialists can access those.

5.5.4. Archive backup procedures

The provisions pertaining to saving log files set out in Chapter 5.4.5 are applicable to archive backups.

5.5.5. Requirements for timestamping of records

The Service Provider affixes the data to be archived with timestamps or time data in the manner defined in Chapter 5.4.1.

5.5.6. Archive collection system

The Partner to the Service Provider shall store confidential the data and documents requested from the Clients by the External Registration Authorities and shall forward them to the Service Provider at the intervals and in the form set out in the agreement.

5.5.7. Procedures to obtain and verify archive information

Access to the archive can be requested by submitting a request to the Service Provider's customer service. Access is provided for Clients to the data that pertain to them; other persons are provided access as laid out in Chapter 2.4.1. The Service Provider always checks authorisation and logs access.

5.5.8. Miscellaneous archiving provisions

The Security Regulations contain the detailed provisions applicable to archiving.

5.6 Key changeover

The Service Provider replaces its own key that it uses if the SP certificate expires or the keys that it uses become deprecated. In addition to the above, the Service Provider can also decide to replace keys at its own discretion.

TRANSLATION

In the case of a new certificate generated with a new key, the Service Provider aligns its profile and data with current regulations and best practices.

5.7 Compromise and disaster recovery

In order to identify the threats that affect the services and to manage any possible risks, the Service Provider uses a risk management assessment and also has a Business Continuity Disaster Recovery Plan (ÜFKT), which applies to the management of extraordinary situations, the prevention as soon as possible of emergencies, and to the provision of continuous operations.

5.7.1. Incident and compromise handling procedures

In accordance with the contents of applicable regulations, the Service Provider continuously monitors the system activities pertaining to logging on to IT systems, to IT system users, and to requests for the provision of services. The Security Regulations contain the exact factors for these checks.

If the Service Provider detects a critical vulnerability in its IT systems, it will perform one of the following measures within 48 hours of detecting such vulnerability.

i. Repairs the critical security hole.
ii. If a critical security hole cannot be repaired within 48 hours, the Service Provider will prepare and implement an action plan to mitigate the vulnerability, the primary task of which is the following:

b. repairs the most critical security holes in accordance with the CVSS6 (starting with the highest score);
c. repairs the security holes of the systems that do not have supplemental protection mechanisms and which are subjected to the threat of unauthorised access and to becoming compromised if the vulnerability is not decreased.

i. The Service Provider documents the facts because of which the vulnerability does not have to be repaired, which can include the following:

a. the Service Provider disagrees with the vulnerability scoring defined by the CVSS;

[6] Common Vulnerability Scoring System v3.0 (https://www.first.org/cvss/specification-document)

TRANSLATION

b. the vulnerability was misidentified;
c. the vulnerability cannot be exploited due to the subscriber protection mechanism;

or

The ÜFKT applied by the Service Provider also includes the disaster recovery plan. The ÜFKT contains procedures that describe the fastest method for restoring reliable services as soon as possible. The Service Provider regularly performs checks (at least annually) to test whether the security regulations are executed correctly regarding the technical and personnel aspects.

The Service Provider uses backups to ensure that it can restore the entirety of its IT system if necessary. The Service Provider protects the backups from modification and access by unauthorised persons.

5.7.2. Computing resources, software, and/or data are corrupted

The Service Provider has equipment and systems with advanced security to minimize the chance of hardware and software errors or data corruption. The ability to restore the Service Provider's services is guaranteed by its background agreements and its own reserve equipment, which are capable of substituting any of the critical equipment within the time undertaken in Chapter 5.7.4. The Service Provider's regular backups (see Chapter 5.5) and transaction logging (see Chapter 5.4) ensure that data can be restored if any data storage equipment becomes faulty. In the worst case scenario, this system is capable of restoring the data of the previous day.

The ÜFKT contains event reporting requirements for the cases in which any of its equipment become faulty and for irregular operations (some are automated and some are the responsibility of the managing personnel). The reports are evaluated by a professional staff, who minimize any damages and service downtime by executing response procedures.

The ÜFKT contains the detailed rules pertaining to faults experienced by critical system components.

The system elements that provide certificate status information shall have priority in the course of the restore.

5.7.3. Entity private key compromise procedures

a. End-user key compromise

See the contents of Chapter 4.9.12 for the end-user key becoming compromised.

TRANSLATION

b. SP key compromise

If the SP key is compromised, the Service Provider informs its Clients, contractual partners and the Relying Parties. It indicates that the certificates issued with the affected Service Provider keys and the certificate status information are no longer valid. The Service Provider will revoke the certificate that contains the private key that has become compromised.

The ÜFKT contains the additional requirements applicable if the SP private key is compromised and the procedure to be followed. In case of a disaster, the Service Provider will take the necessary steps in order to avoid the reoccurrence of the disaster.

c. Change in algorithm

If any of the algorithms used by the Service Provider or any related parameters do not meet the requirements applicable during any period of the planned term of use or are not suitable for intended use for the entire period of the planned term of use (regarding both end-user and SP certificates), the Service Provider informs its Clients, contractual partners and the Relying Parties, and also takes the steps necessary to revoke the affected certificates.

5.7.4. Business continuity capabilities after a disaster

The Service Provider has a business continuity plan in place that it puts into effect in case of a catastrophe. In case of a catastrophe (including if any of the SP private keys or other authenticating data are compromised or if any critical elements of the SP systems become faulty), the Service Provider's normal operations will be reinstated, and it will also be ensured that the errors do not happen again.

The aim of the Service Provider is to restart all services as soon as possible after averting the error and restoring integrity. The recovery of the reliable operation of certificate status services receives priority over the recovery of all other services and activities.

After a natural or other disaster or if the Service Provider's equipment becomes faulty, the Service Provider undertakes to start the provision of the following services within 24 hours:

- status change services,
- OCSP services.

The Service Provider undertakes to start all other services within 5 workdays.

5.8 CA or RA termination

If the Service Provider terminates its activities in a planned manner or for an extended period of time, it will perform the following before cessation of its activities:

TRANSLATION

- Service Provider shall use all reasonable efforts in order that a suitable service provider takes over its registries and its obligations of service provision until the termination of the provision of the service at the latest.
- Service Provider shall, at least 60 days prior to the termination of the provision of the service, publish a notification on its website and send e-mail notification for its clients having an e-mail address of the above termination.
- Service Provider shall destroy its own private keys and shall revoke the certificates related thereto, and shall publish the related information on its website.
- Then Service Provider shall continue to provide the revocation information, if possible.
- In case of all services terminate:
- Service Provider ensures that status information (of end-user and SP certificates) published and handled by SP to be available on the original URL until the termination (then availability of status information shall be ensured by the provider that takes over the services); *and*
- On the day of termination Service Provider destroys the root CA certificate and its private key, and publishes a press release about these.

After the revocation of the certificates, Service Provider shall continue to meet its obligation of publication until the termination of its activities.

- The Service Provider revokes the as-yet unrevoked certificates it issued at least 20 days before the termination of its activity.
- In case of all services terminate, Service Provider informs the browser developers whose root program includes the SP's root certificate 20 days before the planned time of termination of the root CA certificate.
- The Service Provider will revoke all management rights and authorisations derived from agreements concluded with any companies in a contractual relationship with the Service Provider and participating in certificate issuance or with the Registration Authority; the Service Provider will also call upon all Registration Authorities to hand over the data they store.
- In the interest of retaining the registration information and event log archives, the Service Provider will create a full backup including a timestamp. The backup includes the data of previous changes related to certificates, to their status or possible suspension, and to revocation, the Practice Statement pertaining to the issuance of the certificates, public key, and the registry of revoked certificates. The Service Provider protects the saved data files from unauthorised modification and ensures that unauthorised access is excluded; it furthermore provides for the accessibility and interpretability of the data by authorised persons for the retention period.

TRANSLATION

- The Service Provider will not issue new certificates after announcing its termination.

TRANSLATION

6. TECHNICAL SECURITY CONTROLS

The Service Provider uses an IT system that consists of reliable and checked products that have been evaluated as regards security technology.

The key management provisions differentiate between the following keys:

SP private keys:

- private key used to sign end-user certificates and CRL and OCSP responses,
- private key used to sign other certificates and CRL and OCSP responses,
- infrastructure and control keys,
- authorisation response signature key
- other Service Provider private keys (for archiving and timestamp services)

SP public keys:

- the public key pairs to SP private keys.

End-user private keys:

- the private key of an end-user that it created itself,
- the private key of an end-user created on its behalf by the Service Provider.

End-user public keys:

- the public key pair to end-user private keys.

6.1 Key pair generation and installation

In the case of according to secondary certificate policy displayed in the certificate refers to SCD keystorage (see at Service Policy chapter 1.2.1 Cerificate Policy) key is generated in a chriptographic device listed in chapter 6.2.1.

If the cryptographic device or client private key is handled by a third party, the Service Provider shall ensure throughout the lifetime of the certificate that this party complies with the necessary conditions (e.g., supervisory records).

If the client's private key is moved between devices, then the Service Provider shall manage the resulting safety risks with appropriate measures.

If the device's certification relevant to the service ceases to be valid, the Service Provider shall withdraw the certificates issued to that device.

TRANSLATION

6.1.1. Key pair generation

Regardless of who generated the key pair, the Service Provider checks whether the public key had been previously issued to another Client.

a. SP key generation

The Service Provider generates SP key pairs in a physically protected server room in the presence of at least two trusted employees and with the exclusion of the presence of any other persons; a report is drawn up of the process. The list of persons who fill trusted roles and are authorised to generate keys is included in the Service Provider's Security Policy.

The Service Provider uses the cryptographic hardware modules detailed in Chapter 6.2.1 of this Statement for the generation and storage of SP keys. The Service Provider generates all of the SP key pairs. With the exception of the saving described in Chapter 6.2.4, the generated private keys remain on the cryptographic hardware modules for their entire lifecycles and are not transferred anywhere before being destroyed. If it becomes necessary to destroy the SP private key for any reason, such destruction takes place under the control of two persons as required by the device's certificate.

Prior to the expiration of SP keys, the Service Provider will generate the new CA keys and issue the new SP certificates in a manner that ensures that the transition is as smooth as possible for the Client and the replacement of the certificate does not cause any disturbances for the Clients and the Relying Parties.

A qualified auditor also observes the generation by the Service Provider of Root CA keys in order to check compliance with the above requirements and the integrity and confidentiality of the key pair. The auditor issues a certificate stating that:

- The SP has documented its Root CA key generation and protection procedures in its regulations;
- The key generation procedure is suitably in-depth;
- The SP has put effective control measures in place to ensure that key generation is implemented at a security level that is in line with relevant requirements;
- All procedures of the key generation procedure have been executed.

The key generation scenario contains the detailed rules pertaining to the generation of SP keys.

b. End-user key generation by SP

The Service Provider uses algorithms for the generation of end-user keys for authentication, encryption and codesigning purposes meeting the requirements of the standards applicable at

TRANSLATION

the time of issuance and the Supervisory Body's decision. The Service Provider rejects all requests for certificate issuance that do not meet these requirements.

End-user keys are generated only by persons who fill trusted roles and either in an automated manner or in the Service Provider's protected server room. If the key pair is used on a Client device, the Service Provider will create it directly on the device and will not store or save it by any other means, with the exception of the cases outlined in Chapter 4.12 Key escrow and recovery.

The Service Provider ensures that its end-user private key and the activating data are inaccessible to others.

See Chapter 6.1.2 Private key delivery to subscriber.

The Service Provider does not generates private keys for web authentication certificates (DVCP).

c. End-user key generation by itself

For the end-user may also generate the end-user key pair. When using a Client device or, it must notify the Service Provider. End user shall apply one of the following methods for private key generation:

end user applies the so-called Trusted Platform Module according to ISO/IEC 11889 to generate, store and document the private key in operation system;
or

end user generates, stores and documents the private key in a HSM certified according to at least FIPS 140 Level 2, Common Criteria EAL 4 or equvalent method;
or

end user generates, stores and documents the private key in other hardware device about which Client ensures that the device will be connected to the computer exclusively for the period of signing process.

See also Chapter 6.1.3 Public key delivery to certificate issuer.

6.1.2. Private key delivery to subscriber

If the Service Provider generated the end-user key pair, it will deliver it together with the carrier Client device to the End-User in a secure manner, by way of the Receiver.

6.1.3. Public key delivery to certificate issuer

If the key is generated by the End-User, the successfully registered Applicant delivers the public key to the Registration Authority, which first checks whether the Applicant truly has the private

TRANSLATION

key that is paired to the public key sent by the Applicant and then forwards it to the CA, again using a secure channel.

If the Service Provider generates the key pair for the end-user certificate, there is no need to deliver the public key.

6.1.4. SP public key delivery to relying parties

The Service Provider's SP certificates are available on the Service Provider's website (Chapter 1.1.2). The availability of SP certificates is also indicated in the AIA:CAIssuer field of end-user certificates as standard.

The Service Provider's public keys (including timestamp keys) are accessible as part of its SP certificates.

6.1.5. Key sizes

The key pairs used by the Service Provider (for both TSO and end-user certificates) meet the requirements of the applicable standards and the Supervisory Body's decision. The algorithms used by the Service Provider:

Hash algorithm IDs:

- SHA-256 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-256 (1) }
- SHA-384 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-384(2)}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-512(3)}

IDs and key sizes of cryptographic algorithms:

- RSA OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) PKCS-1 (1) RSA Encryption (1) } – Minimum 2048 bit key length
- DSA OID ::= { iso(1) member-body(2) us(840) X9-57 (10040) x9algorithm (4) id-dsa (1) }

The Service Provider may not use the algorithms defined herein past the time indicated in the Supervisory Body's Algorithm Decision.

6.1.6. Public key parameters generation and quality checking

The system used by the Service Provider checks two different aspects of the compliance of key generation parameters:

TRANSLATION

- the compliance of random number generation used for the parameters (whether the generation is statistically random enough),
- the fulfilment of the conditions and relationships pertaining to parameters.

The basis for checking the compliance of random number generation is whether all cryptographic hardware modules used in the system are capable of statistically testing the consistency and independence of the bit sequence it generates. The modules enable the calling of the tests by way of a standard interface.

Besides the testing instruction that can be called with the use of the external interface, the hardware modules also continuously test their own random number generation and stop if they find any faults.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

a. Root CA key

The key issued by the Root CA can be used only for the following purposes:

- Signing Root CA certificates (self-signed certificate)
- Signing certificates pertaining to the authentication of subordinated services
- Signing and cross-certifying Intermediate CA certificates
- Signing internal SP certificates (e.g. OCSP)
- For testing, if the signature of the Root CA is required for live use

b. Intermediate CA key

The key issued by the Intermediate CA can be used only for the following purposes:

- Signing end-user certificates
- Signing internal SP certificates (e.g. OCSP, CRL)
- For testing, if the signature of the Intermediate CA is required for live use

c. End-user certificate keys

The various types of end-user certificates can be used for the following purposes:

- Encryption (encryption certificate)
- User authentication (authentication certificate)
- Signing program code (codesign certificate)
- Website authentication and creating encrypted communication (website authentication certificate)

in accordance with the integrated X509v3 bits.

TRANSLATION

See Chapter 7.1.2 Certificate extensions for the corresponding values of the key usage fields.

6.2 Private key protection and cryptographic module engineering controls

The Service Provider implements physical and logical protection that prohibits unauthorised certificate issuance.

The Service Provider stores its private keys in a secure manner that prevents access and use by unauthorised persons. The Service Provider stores the SP private keys used for the creation of certificates, for the authentication of certificate status services, and for other purposes in a physically protected environment and uses those only for the purposes defined for the given key.

6.2.1. Cryptographic module standards and controls

The Service Provider proceeds as set forth below in regard to the creation, saving, storage and destruction of SP keys:

- keys are created, stored, saved, restored, and destroyed in a physically secure environment under the control of two persons (the joint presence of two employees filling trusted roles) (see Chapter 6.1.1.1),
- in accordance with applicable standards, CA keys are generated, stored, and used on ISO/IEC 19790 or FIP PUB 140-2 level 3 equivalent hardware cryptographic devices with at least EAL4 certificates with the ISO/IEC 15408 or equivalent security requirements (see Chapter 6.1.1.2 and Chapter 6.2.7 Private key storage on cryptographic module),
- keys can only be used by the authorised persons for functions in line with the purpose of their creation,
- before using their own SP keys, the Service Provider's systems make sure that the certificates belonging to these keys are valid,
- the Service Provider's certificate, CRL and OCSP signing keys are different from the keys used for all other functions,
- the Service Provider's keys are updated with an out-of-band technique,
- when exporting a key stored in a secure cryptographic module from a module, the Service Provider ensures that the key is protected,
- the systems that process information sensitive from the aspect of cryptography (private or secret keys) outside of a cryptographic device are protected by the Service Provider from becoming compromised by electromagnetic radiation (see Chapter 5.1.3).

TRANSLATION

The Service Provider handles and operates the cryptographic devices used to provide qualified services separately from those used for non-qualified services and other activities, which latter devices can thereby not influence the reliable operation of the products that are used to provide the qualified service.

The Service Provider keeps a record of its products that are directly used to provide trust services, in which they are classified according to security.

Before the service provider uses its products that implement trust services used to provide a service for any other purposes besides its own provision of services, it ascertains that the product does not contain any data linked to a trust service and that such data cannot be recovered. The Service Provider logs this examination and the measures taken on its basis.

The key storage, key generation and signature creation devices used and provided by the Service Provider could be the followings (end-user and Provider private keys are allowed to be generated exclusively in these devices):

DEVICES	HARDWARE AND FIRMWARE SPECIFICATIONS	THE SPECIFICATION OF THE SOFTWARE USED DIRECTLY FOR KEY MANAGEMENT

SP KEY DEVICE	• Luna® PCI- E Cryptographic Module and Luna® PCI Cryptographic Module for Luna® SA (Hardware Versions: VBD-05-0100, VBD 05-0101 és VBD-05-0103, Firmware Version: 6.10.7, 6.10.9 and 6.11.2)
	• SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM (Hardware Versions: VBD-05-0100, VBD-05-0101, VBD-05-0102 and VBD-05-0103; Firmware Versions: 6.24.6 and 6.24.7)
	• ProtectServer Internal Express 2 (PSI-E2)
	  ◦ Harware Versions: VBD-05-0200,
	  ◦ Firmware Versions: 5.01.02 and 5.01.03)
		• Luna cryptographic module drivers
		• SafeNet drivers
		  ◦ ProtectServer Internal Express 2 (PSI-E2) drivers

QSCD CLIENT DEVICE (can be used as SCD device too)	• SafeNet eToken (Smartcard or USB token), Version 9.1, Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller with IDSign applet embedding • IAS Classic v3 application on Java Card platform with P5CC081V1A chip, according to MultiApp ID V2.1 open standard, MPH117 v2.2 with filter (also known as: Gemalto ID 340) • Bit4id Crypto Java Card (J-SIGN v1.8.9) Version EEPROM: 1.8.9, Version ROM: 1.6.0 • Bit4id Crypto Java Card (J-SIGN3 v1.1.4) Software: 1.1.4, Hardware: 6.2.1 • IAS Classic V4.4.2 with MOC Server 1.1 on MultiApp V4.0.1 (also known as: Gemalto IDPrime 940A)	• Drivers for Bit4ID/Oberthur/Gemalto tools •
SCD CLIENT DEVICE	• IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4, applet IDOneClassIC v1.0 embedded, P5CT072VOP-en, • IDOneClassIC Card (ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1 platforms: P5CT072VOP, P5CC072VOP and P5CD072VOP) secure signature creation tool • ProtectServer Internal Express 2 (PSI-E2) Hardware version VBD-05, firmware version: 5.00.02)	• Oberthur device drivers • NLSIGN system • ProtectServer Internal Express 2 (PSI-E2) drivers

Certificates of Conformity on the above devices and other information can be downloaded on the Service Provider's website (see 1.1.2).

The Service Provider continuously monitors the validity of the certificates for the devices it has applied and any newer restrictions pertaining to their application. In the interest of the above, it has implemented internal administrative policies to keep records of the validity of the certificates and to track the changes in the validity of certifications performed within the European Union. These policies require checking the status of these certifications at least monthly. Furthermore, the Service Provider also communicates with the manufacturers and distributors of the devices affected by the certification to be informed as soon as possible about the changes of the certifications, and to be able to fulfill its related Service Provider's duties.

Service Provider can employ other key handling and cryptographic devices for its own use and as Client devices also, if they possess the certification required for the intended usage.

Information about devices that are currently available for end-user certificates are published on TSP website (see 1.1.2).

6.2.2. Private key (n out of m) multi-person control

The Service Provider's Security Regulations contain the detailed rules on the multi-person control of private keys.

6.2.3. Private key escrow

See Chapter 4.12.

6.2.4. Private key backup

Saving takes place in a ciphered format. When saving, the private key is copied from the cryptographic hardware module that generated the private key (in accordance with the type of the cryptographic hardware module) to smart cards in several parts (see Chapter 6.2.2) and in a protected manner; otherwise, it ends up in the backup HSM module. The saved copies are provided the same type and strength of protection as the original copy of the hardware module that generated the key. An algorithm and key size is used for encryption that ensures protection for its entire remaining validity. The copies of the SP private key not being used are protected with a level of security equal to the productive key.

The Service Provider saves the following SP private keys:

- the Root CA's authenticator private key,
- the Intermediate CA's authenticator private keys.

See Chapter 4.12.1 regarding the saving of end-user private keys.

6.2.5. Private key archival

The Service Provider archives neither SP private keys nor end-user private keys.

6.2.6. Private key transfer into or from a cryptographic module

The transfer into a cryptographic module of SP private keys is implemented by the Service Provider in a physically protected environment with the joint participation of at least two trusted employees and with the exclusion of the presence of any other persons.

See the contents of Chapter 6.2.4.

TRANSLATION

6.2.7. Private key storage on cryptographic module

In the case of the SP private keys stored on cryptographic devices, the Service Provider ensures that the keys cannot be accessible outside the device (with the exception of the saving set out in Chapter 6.2.4). In the case of cryptographic devices, the Service Provider provides protection against forgery even during transport and storage.

See the contents of Chapter 6.2.1.

6.2.8. Method of activating private key

The activation of SP private keys is implemented by the Service Provider in a physically protected environment with the joint participation of at least two trusted employees and with the exclusion of the presence of any other persons. The Service Provider's Security Regulations sets forth the details of the method for activating SP keys.

The end-user private keys generated by the Service Provider and the Client devices can only be activated with the use of activation data.

6.2.9. Method of deactivating private key

The Service Provider's Security Regulations set forth the details of the method for deactivating SP keys.

6.2.10. Method of destroying private key

The Service Provider destroys the SP keys in a manner that ensures that the signing keys cannot be restored. During the course of destruction, the Service Provider uses secure deletion processes that actually overwrite all instances of the key on all storage devices on which copies of the key could have occurred.

If a SP device is destroyed, the Service Provider ensures that the private keys stored on it are also destroyed.

The end-user has to irrecoverably destroy the private keys of end-user signature / seal / website authentication certificates if the certificate has been revoked or its validity expires and no new certificate is issued with the use of the public key paired to the private key.

6.2.11. Cryptographic Module Rating

See the contents of Chapter 6.2.1.

TRANSLATION

6.3 Other aspects of key pair management

The Service Provider uses the SP keys in the manner and for the validity period indicated in the certificate.

6.3.1. Public key archival

The Registration Authority archives all certificates created by the Service Provider for the following period:

- SP certificates: for 10 years starting from the end of their term of validity,
- end-user certificates: for the time following their expiration as required by relevant legislation (see Chapter 5.5.2).

6.3.2. Certificate operational periods and key pair usage periods

Type	Certificate lifetime	Key pair usage period
Encryption, authentication and code signing end-user certificates	maximum of 2 years	The Service Provider does not set a limit for the lifetime of the key but can require the generation of a new key at any time.
Website authentication end-user certificates	maximum of 1 year (365 days)	The Service Provider does not set a limit for the lifetime of the key but can require the generation of a new key at any time.
SP certificate	maximum of 20 years	Equal to the validity of the certificate.
Test Certificate	maximum of 2 years	The Service Provider does not set a limit for the lifetime of the key but can require the generation of a new key at any time

The certificate's validity is indicated in the certificate. The validity of the certificate commences at the time of its issuance or thereafter.

6.4 Activation data

The issues related to the activation data are set out in the following chapters.

TRANSLATION

The installation and restoration of the service key pair on the cryptographic device shall only be carried out under the dual (or higher) control of employees employed in trust position.

The Service Provider shall provide the change of the activation data of the Client Device (SCD) in possession of the current activation data. Service Provider shall, under no circumstances, store the end user activation data.

6.4.1. Activation data generation and installation

The Applicant provides the activation data as part of the key generation or, if a Client device provided by the Service Provider is being used, it is generated by the Service Provider.

The Service Provider generates the activation data belonging to the Client device in a secure manner and independently of the device. The Service Provider provides the Receiver with the activation data in a sealed envelope. The End-User can activate its Certificate (see Chapter 4.9.3.2 if the Service Provider has uploaded it to the Client device in a suspended state) or upload it to the Client device (see Chapter 4.3 if the Service Provider only generated the private key for the Client device and is making the certificate available in the Client Menu) after receiving the device and the envelope. It is recommended that the activation data be changed when the Client device is first used.

The activation data can be changed in possession of the current activation data.

6.4.2. Activation data protection

The Service Provider only records the activation data for the Client devices so it can hand it over to the person utilising the service; the Service Provider does not retain a copy.

6.4.3. Other aspects of activation data

The End-User has to ensure that the private keys it is provided are activated and deactivated in a secure manner.

6.5 Computer security controls

Only authorised persons can access the Service Provider’s systems. The Service Provider protects the boundaries of internal zones with firewalls and takes the steps necessary to ensure that sensitive data cannot be recovered when data media are reused.

The Security Policies applied by the Service Provider ensure that data can only be added and the measures related to changing certificate status (suspension, revocation, activation) can only be accessed by authorised persons.

TRANSLATION

The Service Provider uses monitoring and alarm equipment to filter out unauthorised access.

6.5.1. Specific computer security technical requirements

The Service Provider uses multi-factor authentication for all users authorised to issue Certificates in the manner set out in the Security Regulations.

6.5.2. Computer security rating

The Service Provider's Risk Management Regulations for internal use contain the applicable provisions.

6.6 Life cycle technical controls

6.6.1. System development controls

In the case of the systems developed by the Service Provider, the risks are assessed and analysed from a security aspect.

In the case of the software that it developed, the Service Provider applies a change management procedure for issuance, modification, and urgent software repairs. If possible, the change management procedure is completed before placing into operation. Urgent repairs can be an exception to the above, in the case of which the documentation can also be prepared afterwards if placing the software repair into operation at a later time would threaten the Service Provider's operations or would result in serious financial or moral damages.

The Service Provider's Software Development and IT Change Management Regulations for internal use contain part of the applicable provisions.

6.6.2. Security management controls

The Service Provider uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them. The Service Provider devotes special attention to security even during purchases: the suppliers of its systems of key importance are suppliers evaluated in accordance with the Purchasing Regulations and the purchased equipment are also evaluated equipment. The manufacturers of the equipment are organisations with numerous references and a reliable background. These rules ensure that if necessary, the Service Provider receives the necessary support for its equipment and that any warranty and guarantee claims can be validated against the supplier if any faults occur. The majority of used and integrated equipment are readily available through commercial distribution, meaning they can be replaced with relative ease from several different sources.

TRANSLATION

The Service Provider protects its IT systems and information from viruses, malware, and unauthorised software. The Service Provider applies procedures that ensure that security fixes can be applied within a reasonable amount of time (6 months). The Service Provider will not apply security fixes if they contain additional security holes or cause instability.

Only authorised persons can make entries and changes to the Service Provider's data. The authenticity of the data can be verified. The data pertaining to Clients are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained.

6.6.3. Life cycle technical controls

The Service Provider continuously monitors capacity utilisation and prepares forecasts in the interest of ensuring that enough storage space and processing capacities will be available in the future as well.

6.7 Network security

The Service Provider classifies the systems it uses for the provision of services into various security zones. Following the above classification, the Service Provider ensures that the communication between the various zones is secure. During the provision of its services, the Service Provider removes or blocks all connections and ports that are not required by the service.

The Service Provider provides a separate network for service systems. The productive systems are separated from development, test, and other systems. The Service Provider developed redundant network connections for all cases that require high availability external access.

In the interest of continuously maintaining security, the Service Provider regularly (every quarter or as soon as possible if any significant network changes take place) performs vulnerability testing.

In addition to the vulnerability testing, the Service Provider annually (or as soon as possible in case of any significant changes in infrastructure) also performs intrusion tests.

Further provisions regarding network security are part of the Service Policy.

6.8 Timestamping

Within the framework of provision qualified certificate issue service, Service Provider shall use timestamps issued by qualified trust provider if timestamping is needed.

Service Provider shall, at least once a day, synchronize the time source of its systems to UTC time source.

TRANSLATION

7. CERTIFICATE, CRL, OCSP PROFILES

The Service Provider primarily uses certificate profiles to regulate certificate contents and functions. The Subject(s) of the certificate determine the subject data to be included in the certificates; the purpose of use determines the use of the certificate by way of the X509 extensions.

7.1 Certificate profile

The Service Provider uses different certificate profiles in accordance with the certificate's Subject and use. The various certificate profiles have the data that meet MELASZ eIDAS profile recommendations[7], which is to be interpreted as follows.

End-user certificates contain the following data (irrespective of profile):

Name	Contents
Version	3 (0x2)
Serial Number	contains at least a 64 bit random number
CA signature algorithm (SignatureAlgorithm)	sha256withRSA
Issuer	The Issuer data of the certificate's issuer, corresponding to the Subject data in the CA certificate
Validity	The validity of the certificate (from - to)
The certificate signature	The result of the signature performed with the certificate issuer's CA key

[7] http://www.melasz.hu/lang-en/a-melasz-hirei/1291-melasz-ready-ajanlas-eidas-kompatibilis-tanusitvany-profilokra

TRANSLATION

Certificate Policy	The identifier(s) of the policy(-ies) applicable to the given end-user certificate Primarily standard and, if applicable, secondary identifiers See at Chapter 1.2.1)

Personal certificate profile Subject fields:

Personal certificates are issued to natural person End-Users; thus only a natural person is indicated as the certificate subject, who is identified in the certificate with the use of his/her actual name. The following profile applies to encryption, authentication and codesign certificates.

Field name	Definition
Subject fields	
commonName (CN)	The End-User's full name as registered in authentic records or, if such is unavailable, the name on the certificate used as identification.
surname (SN)	The surname part of the name indicated in the commonName field, in the breakdown provided by the MELASZ profile recommendation.
givenName (G)	The first name part of the name indicated in the commonName field, in the breakdown provided by the MELASZ profile recommendation.
emailAddress (E)	The End-User's own e-mail address.
serialNumber (CNSN) (1.)	The permanent identifier created by the Service Provider (the Service Provider's + the client's identifier).
serialNumber (2.) Optional	A unique identifier with the contents required by the client or a group of clients.

TRANSLATION

countryName (C)	The End-User's country of residence[8]; the two-letter country code as defined by ISO 3166-1.
localityName (L)	The locality of the End-User's residence.
Subject Alternative Name fields	
email	The same as field E.
othername	SP's OID based service ID: 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5

Conditions:

- With the exception of the serialNumber field, there can be only be one of each field.

Fields not included above:

- Pseudonym
- An organisation cannot be used as the Subject of a personal certificate, and the appropriate fields are therefore not included (CN/organizationName, CN/organizationalUnitName, CN/ organizationIdentifier, and CN/title).

Pseudonym certificate profile Subject fields:

Personal certificates are issued to natural person End-Users who are identified by a selected name in the certificate. The person's true name (which the Service Provider knows) and the connected organisation are not included in the certificate. The following profile applies to encryption and authentication certificates.

Field name	Definition
Subject fields	
commonName (CN)	The pseudonym selected by the Applicant (unique at the Service Provider)

[8] based on an address card or, in lack of such, other official document

TRANSLATION

pseudonym (P)	The pseudonym selected by the Applicant. Equivalent to the contents of the commonName field.
serialNumber (CNSN)	The permanent identifier created by the Service Provider (the Service Provider's + the client's pseudonym identifier – see Chapter 1.6.1). 1.3.6.1.4.1.3555.5.x.*ClientPseudID* The value of this field is unique as regards the PSEUDONYM and cannot be the same as the identifier of the pseudonym certificate.
countryName (C)	The Applicant's country of residence; the two-letter country code as defined by ISO 3166-1.
Subject Alternative Name fields	
othername	SP's OID based service ID 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5

Conditions:

- There can be only be one of each field.

Fields not included above:

- title, organizationName, organizationalUnitName, organizationIdentifier, localityName, surname, givenName, emailAddress, SAN/Email

Business certificate profile Subject fields:

Business certificates are issued to natural person End-Users, in addition to whom an organisation can also be named as the subject of the certificate (who will be the certificate's Subscriber). The natural person applies for the certificate with the consent of the organisation, and the certificate can then be used in its representation (which in this case does not necessarily mean legal representation). The relationship between the organisation and the

TRANSLATION

person can be of any type (e.g. employee, member, contractual)[9], which is not examined at the time of issuing the certificate; however, the organisation does have to certify the fact of belonging to it (and, if the Title is provided, its contents). The following profile applies to encryption and authentication certificates.

Field name	Definition
Subject fields	
commonName (CN)	Same as the personal profile.
surname (SN)	Same as the personal profile.
givenName (G)	Same as the personal profile.
serialNumber (1.) (CNSN)	Same as the personal profile.
serialNumber (2.) Optional	Same as the personal profile.
emailAddress (E)	Same as the personal profile.
organizationName (O)	Same as the organisational profile.
organizationalUnitName (OU) Optional	Same as the organisational profile.

[9] As defined by the Electronic Administration Act: “natural person certificate subject: the natural person included in the certificate, regardless of whether the right to represent a non-natural person or a relationship thereto is also certified in the certificate;”

TRANSLATION

organizationIdentifier Optional	Same as the organisational profile.
title (T) Optional	The role or position of the certificate subject in the organisation. This field can contain only verified data. Certain titles can only be used in exceptional cases: (e.g. “Attorney” can only be used for persons authorised for attorney certificates and “CEO” and “Managing Director” can only be used for the persons verified by the business association’s registration documents).
countryName (C)	Same as the organisational profile.
localityName (L)	Same as the organisational profile.
Subject Alternative Name fields	
email	Same as the personal profile.
othername	Same as the personal profile.
dirname Optional	In special cases, the End-User name with a different manner of writing than that indicated in the CommonName field.

Conditions:

- With the exception of the serialNumber field, there can be only be one of each field.

Fields not included above:

- Pseudonym

Organisational certificate profile Subject fields:

Organisational certificates are issued to legal person Subscribers; thus only this legal person can be indicated as the certificate subject. The profile applies to encryption, authentication and codesign certificates.

TRANSLATION

Field name	Definition
Subject fields	
commonName (CN)	The Subscriber's full or short name, OR A certified DBA name / Trademark / Product name and the related identifier, which is both unique and used exclusively by the legal person.
organizationName (O)	The Subscriber's full or short name
organizationalUnitName (OU) Optional	The name of the Subscriber's organizational unit within the organisation identified in the organizationName field.
countryName (C)	The country of the Subscriber's official seat (the two-letter country code as defined by ISO 3166-1).
localityName (L)	The name of the locality of the Subscriber
serialNumber (CNSN) (1.)	The permanent identifier created by the Service Provider (the Service Provider's + the client's identifier). 1.3.6.1.4.1.3555.5.1.*ClientID*
organizationIdentifier	The Subscriber's registered identifier (see Chapter 3.1 Naming).
emailAddress (E)	Subscriber's e-mail address.
Subject Alternative Name fields	
email	The same as field E.
othername	NetLock's OID based service ID: 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5
dirname Optional	The following, as used by the organisation and certified by a statement: DBA name or Trademark

TRANSLATION

	or Product name and related identifier.

Conditions:

- With the exception of the serialNumber field, there can be only one of each field.
- Pseudonyms cannot be used in organizational certificates.

Fields not included above:

- Title, Pseudonym, organizationIdentifier, surname, givenName

The interpretation of the data contents included in the certificate:

- The certificate belongs to the organisation called O, as indicated in the certificate (within which, if indicated, the OU organizational unit).

DV website authentication certificate profile Subject fields:

The DV SSL certificate is a website authentication certificate that has a Subject of one domain name.

Field name	Definition
Subject fields	
commonName (CN) Optional	If the field is present, it can contain one domain name from among those included in the SAN/dNSName. Only an existing domain name rightfully used by the Applicant can be used. Pseudonyms are not allowed. The indicated domain name can be a wildcard.
Subject Alternative Name fields	
DNSname	The domain names of the websites authenticated by the certificate. Only existing domains name rightfully used by the Applicant can be used. They can contain wildcards.

Conditions: -

Fields not included above:

TRANSLATION

- givenname, surname, organization, country, locality, title, pseudonym, organizationalUnitName, organizationIdentifier

SP Root CA certificate profile:

Field name	Contents	
Certificate Serial Number	The certificate's unique identifier (non-sequential, with at least 64 bits of entropy)	
public key	see minimum algorithms table	
Validity	The validity of the certificate (from - to)	
subject:commonName (CN)	Root CA name	
subject:countryName (C)	HU	
subject:localityName (L)	Budapest	
subject:organizationalUnitName	Certificate CAs (Certification Services)	
subject:organizationName (O)	NetLock Kft.	
Signature	the Root CA's own signature	
Extensions		Critical
basicConstraints	CA:TRUE	Yes
keyusage	keyCertSign, cRLSign	Yes
Subject Key identifier	subject key hash	No

TRANSLATION

Requirements: the self-signed subject and issuer parts of the root authenticator certificate are the same

Fields not included above: certificatePolicy, extendedKeyusage

SP Intermediate CA certificate profile

Field name	Contents	
Certificate Serial Number	The certificate's unique identifier (non-sequential, with at least 64 bits of entropy)	
public key	see minimum algorithms table	
Validity	The validity of the certificate (from - to)	
subject:commonName (CN)	Intermediate CA name	
subject:countryName (C)	HU	
subject:localityName (L)	Budapest	
subject:organizationalUnitName	Certificate CAs (Certification Services) or not included	
subject:organizationName (O)	NetLock Kft. or NetLock Ltd.	
Signature	Root CA signature	
Extensions		Critical
basicConstraints	CA:TRUE	Yes
keyusage	keyCertSign, cRLSign	Yes

TRANSLATION

ExtendedKey Usage	CA relevant EKU, that shall not be 'anyExtendedKeyUsage' and shall not contain in parallel 'id-kp-serverAuth' and 'id-kp-emailProtection' value in same certificate.	No
Subject Key identifier	subject key hash	No
AIA:Ca issuers	The availability of the certificate of the root CA that issued the certificate, in an http URL format	No
AIA:OCSP	The availability of the OCSP service of the root CA that issued the certificate, in an http URL format	No
CDP	The availability of the CRL service of the root CA that issued the certificate, in an http URL format	No
Authority Key Identifier	The hash of the Root CA's issuing key	No

Conditions: -

Fields not included above: certificatePolicy, extendedKeyusage

The connection of the various certificate profiles with certificate policies and certificate types:

The table defines the profiles and certificate policies that the various certificate types are available with.

Profile	Certificate policies	Certificate types
Personal	LCP	Encryption, authentication

TRANSLATION

Pseudonym	LCP	Encryption, authentication
Business	LCP	Encryption, authentication
Organisational	LCP	Encryption, authentication
Website authentication	DVCP	Website authentication
Service Provider	-	Service Provider

The Service Provider can create additional special profiles within the certificate profiles listed above (e.g. business profiles that meet the requirements of certain professions).

7.1.1. Version number(s)

The Service Provider issues certificates in accordance with the X.509v3 specifications.

7.1.2. Certificate extensions

The Service Provider uses the certificate extensions defined in the X.509v3 specifications by indicating the critical fields. All end-user certificates include the following certificate extensions:

Extension	Critical	Contents
basicConstraints	yes	CA:FALSE
subjectKeyIdentifier	no	The Subject's own key ID
Subject Alternative Name	no	Other names of the Subject. See the Subject fields of the various certificate profiles for how this is to be filled out.
authorityKeyIdentifier	no	The certificate issuing CA's key ID

TRANSLATION

crlDistributionPoints	no	The availability of the CRL
Authority Information Access:CAIssuers	no	The availability of the SP certificate
authorityInfoAccess:OCSP	no	The availability of the OCSP
Certificate Policies	no	The identifier of the Certificate policies that was used for issuing of the certificate (see the Chapter Certificate policies). If more than one HRs are identified, the field is included more than once. No policy constraints are used. Of the policy qualifiers, only the User Notice field is filled out, the contents of which is a brief textual description, indication, or supplementation with restricting information of the policy valid for the certificate, in a format that is legible for humans.
Keyusage	yes	The permitted possibilities for using the private key paired to the public key included in the certificate (see below for filling out).
extendedKey Usage	no	The use possibilities of the private key extending keyusage (see below for filling out).
SCT	no	X509 v3 extension accordance with Google Certificate Transparency Policy[10].

[10] Lásd https://github.com/chromium/ct-policy

TRANSLATION

Filling out end-user key use extensions, according to certificate types:

Cert type / Key use	Encryption certificates	Authentication certificates	DV Certificate for Website Authentication	Codesigning certificates
Keyusage	keyEncipherment	digitalSignature	keyEncipherment, digitalSignature	codeSigning
extendedKey Usage	documentSigning, emailProtection	clientAuth	serverAuth, clientAuth	(in case of test certificate: lifetimeSigning)

The End-User can use the private key only for the purposes indicated here (the parentheses include the certificate's applicable use):

- nonRepudiation: ensuring non-repudiation (Verification of user)
- digitalSignature: Electronic signature (Verification of integrity and authenticity)
- keyAgreement: Key agreement
- KeyEncipherment: Key encryption (Key decryption)
- clientAuth: Client identification (Client authentication)
- serverAuth: Server identification (Server authentication)
- emailProtection: Also usable in case of signing and enchrypting certificates
- lifetimeSigning: Regardless of using timestamp in signature or not, the signed code is valid only as long as the related certificate is valid.

7.1.3. Algorithm object identifiers

The Service Provider indicates in the certificate the name and parameters of the algorithm used for the authentication of the certificate. Refer to Chapter 6.1.5 for the possible values.

7.1.4. Name forms

The provisions of Chapter 3.1 are governing as regards Subject names forms.

The value in the certificate's CA ("Issuer") field is the same as the "Subject" value in the issuing CA certificate.

7.1.5. Name constraints

The Service Provider indicates any name constraints in the "nameConstraints" field.

TRANSLATION

7.1.6. Certificate Policy object identifier

In the certificates issued on the basis of the Certificate Policy, the Service Provider indicates the Certificate Policy OID.

7.1.7. Usage of Policy Constraints extension

The Service Provider sets no requirements.

7.1.8. Policy qualifiers syntax and semantics

The Service Provider can include brief information regarding the usage of the Certificate in the Certificate Policies extension's Policy Qualifier field. The field also includes the online address (URL) at which the Practice Statement is available.

7.1.9. Processing semantics for the critical Certificate Policy extension

The Service Provider sets no specific requirements.

7.2 CRL profile

7.2.1. Version number(s)

The Service Provider issues CRLs in line with the x509 and RFC5280 standards with the frequency and contents defined in the Policy.

7.2.2. CRL extensions

The CRL does not contain any fields marked as critical. The Service Provider provides CRLs with serial numbering increasing at a rate of one.

The certificate's CRL profile:

Field	Contents
Version	V2
Issuer	The Issuer data of the certificate issuer that issued the CRL
Last update	Date of last update

TRANSLATION

Next update	Date of next update
Signature	Electronic signature of the issuer
CRL entry	The serial number of the invalidated certificate, the date, time, and reason of invalidity in a format in line with RFC 5280.
CRL entry extension	

7.3 OCSP profile

7.3.1. Version number(s)

During the course of the OCSP service, the Service Provider supports the certificate status questions and responses created on the basis of version V1 of the RFC 6960 standard.

7.3.2. OCSP extensions

The OCSP responder certificate includes the NoCheck extension, meaning the OCSP responders do not have to be checked by the client.

The certificate profile of the OCSP responder:

Field name	Contents	Critical
basicConstraints	CA:FALSE	Yes
Certificate Serial Number	The certificate's unique identifier (non-sequential, with at least 64 bits of entropy)	No
extendedKeyusage	OCSPSigning	No
keyusage	digital signature	Yes
private and public key	see minimum algorithms table	No

TRANSLATION

Validity	The validity of the certificate (from - to)	No
Subject Key identifier	subject key hash	No
Authority Key identifier	CA key hash	No
OCSPNocheck	empty	No

Conditions: -

Fields not included above: certificatePolicy

TRANSLATION

8. COMPLIANCE AUDIT

SP shall provide its services compliance with:

- applicable regulation og EU and Hungary,
- rules of present Practice Statement
- standard ETSI 319 411-1

Before commencing the provision of its services, the Service Provider had an external, independent conformity assessment body evaluate those on the basis of applicable standards and legislation.

During the investigation for external conformity assessment of the Service Provider, the following must be observed:

- all non-eIDAS services of the Service Provider to be assessed should be taken into account;
- it must be ensured that all service provider activities in the subject of the investigation are covered by the investigation;
- the investigation shall be based on relevant standards, publicly available specifications and/or relevant legal requirements.
  - ETSI 319411-1
  - ETSI 319412
  - ETSI 319403
  - ETSI 319401

8.1 Frequency or circumstances of assessment

The Service Provider continuously monitors compliance with the terms of this Service Practice Statement and keeps strict control of the quality of its services by performing self-checks. In order to achieve this goal, the Service Provider holds an internal audit once a year.

While it provides certification service, the Service Provider checks compliance with the relevant standards by carrying out internal audits and external conformity assessments at least annually.

The Service Provider strictly controls the quality of website certification service for the website verifier (DVCP). To this end, at least 3% of the website authentication certificates issued by them since the previous self-check must be verified by random samples.

NETLOCK Ltd. regulates external partners and service providers and checks their contractual obligations in accordance with the ISO 27001 standard.

TRANSLATION

8.2 Identity/qualifications of assessor

Internal audits are performed by an experienced professional who has the suitable legal and technical know-how, a higher education degree, and at least 5 years of experience in regulation, IT system audits, or trust services.

External conformity assessments are performed by a legal person that has suitable authorisation granted by a national accreditation organisation of an EU Member State.

During the course of external conformity assessments, the Service Provider cooperates with a natural or legal person, or a group of natural persons, who or that

- is/are capable of performing an audit as regards the standards set forth in Chapter 8;
- meet the requirements set out in Chapter 8.3;
- has/have suitable experience regarding PKIs, IT, IT security solutions, technologies, and audits,
- in the case of audits/evaluations performed on the basis of ETSI standards, has/have
    - the accreditation defined by ETSI EN 319 403, *or*
    - equivalent accreditation as defined by a national standard, *or*
    - accreditation to perform an ISO 27001 assessment with the ISO 27006 methodology provided by the National Accreditation Authority in accordance with ISO 17021;
- in the case of WebTrust audits, has/have the license to perform WebTrust audits;
- whose activities are governed by legislation or a professional code of ethics;
- has/have insurance of at least USD one million to cover any omissions or errors in the assessor's activities.

8.3 Assessor's relationship to assessed entity

The trust employees filling the role of Independent System Controller who perform internal conformity assessment at the Service Provider are independent of the Service Provider's organizational units responsible for services.

The auditors who perform external conformity assessment are independent from:

- the owners, managers, and operations of the audited Service Provider;
- the audited organisation, i.e. neither the auditor nor any direct relation is in an employment relationship with the Service Provider;
- the results of the activities performed during the assessment, which do not affect their relationship.

TRANSLATION

8.4 Topics covered by assessment/audit

The following topics are covered by assessments/audits:

- compliance with applicable law;
- compliance with technical standards;
- compliance with the Service Policy(-ies) and Practice Statement(s);
- compliance of applied processes;
- compliance of physical security;
- compliance of staff;
- compliance of IT security;
- adherence to data protection privacy policy
- occasional configuration monitoring of the Trust Services according to security requirements.

8.5 Actions taken as a result of deficiency

The Service Provider summarizes the results of external and internal conformity assessments in a report that includes the system components and processes that were audited. The document includes the evidence used during the audit and the assessor's findings. The report furthermore contains the deficiencies and derogations uncovered by the audit and the deadlines set for their repair. The uncovered deficiencies are classified into the following categories in accordance with their severity:

- "Slight" deviation, for which the documents certifying the corrective measures have to be presented during the subsequent assessment.
- "Severe" deviation, for which the documents certifying the implemented corrective measure have to be presented during the current assessment.

The Service Provider is obligated to provide a written response to the deviations recorded by the independent assessor and to present as of the next assessment the measures taken to correct those.

8.6 Communication of results

The Service Provider will not disclose the detailed assessment report drawn up on the assessment or audit. However, it will disclose the issued certificate within three months of the assessment.

TRANSLATION

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The Subscriber is obligated to pay in advance the value of the periodic services and the other services made use of in addition or during applying for those (e.g. optional services), as well as other fees determined by the Service Provider (e.g. administration fee), in the manner set out in the GTC and according to the price list made available on the Service Provider website or in the individual client offer.

In the price list published on its website and in its offers, the Service Provider determines especially, but not exclusively, the following fees for the services set out in the present Statement and the related optional service fees.

Periodic Services:

- Certificate service (see Chapter 9.1.1 fejezet);
- Service pack(see Chapter 9.1.4.2);
- services not detailed in the present practice statement (see Chapter 9.1.4.2);

Optional services related to certificate issuance:

- Mobile registration service;
- Delivery of Client device with an approved agent;
- Identification via a Registration Agent;
- Post payment);
- Management of Client requests for amendments to the Service Agreement;
- Unlocking a blocked Client device;
- Replacing a Client device;
- Other administrative fees.

The Service Provider publishes on its website the exact definitions and conditions of the various optional services. The Service Provider may suspend the provision of optional services and can also introduce other optional services in addition to those listed above, about which it will publish information on its website.

The fees for applying for services and for the optional services provided with those are payable to the Subscriber together with the fee of the given service.

The Service Provider can also sell the services as part of service packages, in which case the service fee is included in the service package fee. The conditions of packages and the other rules pertaining to the Service Provider are laid out in the GTC.

TRANSLATION

9.1.1. Certificate issuance or renewal fees

The Certificate creation service fee includes the issuance of the certificate (as part of an initial, renewal, modification, or re-key process), its publication during the entire term of validity (in the certificate repository or in the CRL), the provision of related services (e.g. certificate status), and storage during the entire retaining period.

9.1.2. Certificate access fees

The Service Provider does not charge for queries from the certificate repository if they take place in accordance with the applicable rules of Chapter 2.4, if the interface maintained by the Service Provider for the purpose on its website is used, and if certificates are queried one at a time with the manual entry of the data required for viewing certificates.

The Service Provider only provides for other uses of the certificate repository (e.g. large number of automated queries) on the basis of a separate agreement and with the conditions and for the service fee set forth therein.

9.1.3. Status changes or status information access fees

The Service Provider does not charge for certificate status changes (see Chapter 9.1.3).

The Service Provider only provides for uses of the certificate status service other than that set out in Chapter 2.4 (e.g. frequent or a large number of OCSP queries) on the basis of a separate agreement and with the conditions and for the service fee set forth therein.

9.1.4. Fees for other services

Fees for service packs

The fees of the service packs under the GTC include the fees of the timestamps that can be used during the term, and the fees of the client devices.

Fees for other services not detailed in this Statement

The Service Provider may also charge a fee for the services not detailed in this Statement if those are published on its website in accordance with the GTC or it concludes an agreement with the Subscriber for the provision of such service.

9.1.5. Refund policy

If the service agreement is terminated for a proven serious breach of contract on behalf of the Service Provider as defined in the GTC or due to an amendment of the GTC, or the Service Provider terminates the given service during the term of the agreement (and it is not taken over

TRANSLATION

by another service provider), the Service Provider will pay a fee commensurate to the provided services to the Client as compensation. If the service agreement is terminated or rescinded within 14 days of its conclusion, the Service Provider will refund the entire service fee.

In other cases, e.g. the service agreement is terminated (before its expiration), or the service was not used, the Client device was not taken over, or the service packages pertaining to the contractual term are not used up, the Service Provider will not refund any part of the paid service fees to the Subscriber. The fees of these services were set with the express assumption that a certain proportion of Clients would only make use of a part of the quotas.

9.2 Financial responsibility

The Service Provider restricts its financial liability as set forth below:

In respect of the various services and certificate types, it sets different values for assumptions of liability in the Price list which can be validated per insurance event (which took place as a result of one or more reasons but are linked in time). If more than one Client or several different agreements and the related certificates, timestamps, or files are affected in a given insurance event, the rate of compensation is determined for the individual Clients and agreements (certificates) in a manner that ensures that the highest value of assumption of liability is not exceeded by the total amount of compensation and the value of such assumption for the given service or certificate type is limited in all cases.

The Service Provider provides information on the value of assumed liability on its website.

These amounts were defined for the full price amounts included in the Services price list. If the Client receives the services at a discounted rate, the amount of compensation will be defined commensurately to the provided discounts and will be proportionate to those.

9.2.1. Insurance coverage

Service Provider has liability insurance in order to cover the costs for indemnifying Clients and Relying Parties and any other incurred costs. The liability insurance covers the Service Provider's indemnification liabilities incurred during the provisions of all services set out in this Statement.

The liability insurance shall, in addition, cover the followings:

- the damages caused to service clients in connection with the breach of the service agreement,
- the non-contractual damages caused to service clients and third parties,

The Service Provider must ensure that the insurance contract they signed explicitly lists that the contract covers the above.

TRANSLATION

In case of certificates issued accordance with DVCP (see 1.2.1) Service Provider has adequate level of liability insurance, that is corresponding with the DV specifications.

9.2.2. Other assets

The Service Provider has cover for the costs related to the performance of the requirements for terminating the service. A HUF 25,000,000 bank guarantee is in place for the fulfilment of the obligations.

9.2.3. Insurance or warranty coverage for relying parties

The Service Provider is liable for the damages caused to third parties that it does not have a contractual relationship with in accordance with the general rules of the Civil Code.

9.3 Handling of business information

The Service Provider stores and handles the confidential information that comes into its possession by taking into account the provisions of relevant legislation and in accordance with Chapter 5 and the Service Provider's private Data Management Regulations.

When the obligation of storage expires, the Service Provider irrevocably deletes the confidential information, unless provided otherwise by the Client.

9.3.1. Scope of confidential information

The Service Provider considers all data pertaining to any Clients and not included in Chapter 9.3.2 to be confidential information. The following are especially confidential information:

- the Client personal information that is not included in the certificate;
- registration data (e.g. audio and video recordings, document copies);
- the audio recordings recorded at customer service;
- private keys and their activation data;
- certificate enrolment data;
- service agreements;
- private regulations;
- the log data created in connection with the services;
- all data that would threaten the security of services if disclosed;
- all data that, if disclosed, could lead to third parties learning of the above data.

The Service Provider handles confidential information in the manner set out in Chapter 9.3.3.

TRANSLATION

9.3.2. Information not within the scope of confidential information

The Service Provider does not consider the following information to be confidential:

- the certificate data required for certificate status services;
- all data included in the certificate (see Chapter 7.1), unless provided otherwise by the Applicant during the application;
- other anonymized data that can no longer be linked to the owner of the information or to any persons about which conclusions can be drawn on the basis of the information.

The Service Provide may disclose information not considered confidential, may share such with its partners, and is not liable for their becoming public knowledge.

9.3.3. Protection of confidential information

In addition to the requirements set forth by law and the present Practice Statement, the Service Provider takes all measures, including the method defined in the Data Management Regulations, for the secure handling of the confidential information as defined in Chapter 9.3.1.

The Service Provider stores in an electronic format any data that it was provided in an electronic format; any information provided to it in hard copy format can be stored and managed in both hard copy form and/or electronic format.

The Service Provider retains personal information, protects their security, and prevents data loss, damages, and the incorrect or unauthorised use in the manner laid out in Chapter 5.5 and by taking into account the IT security requirements of Chapter 6.5.

The Service Provider grants access to the confidential information that comes into its possession only to those of the employees defined in Chapter 5.2.1 for whom the information is required (e.g. Registration Administrators).

Service Provider shall disclose confidential information only in the following cases and means:

- Creating the devices necessary for the use of the service;
- Invoicing;
- Enforcement of claims against the Client.

The Service Provider may only disclose confidential data in the following cases:

- In case Service Provider terminates of all of its services, the Service Provider shall, following the termination of the activities related to service provision, provide the statutorily specified recipient service provider with access to the registries related to the services, and shall hand over all data related to the revoked certificates (including personal data).

TRANSLATION

- Service Provider shall, without any delay, provide the investigative authority and/or national security services with the requested data upon request, for the purpose of detection or prevention of criminal offenses that may be linked to the services of Service Provider or in the interest of national security, upon the fulfilment of the criteria set out in separate legislation, including the handover of personal and other information verified and recorded in the course of the authentication-certification procedures (see Chapter 3). Service Provider shall draw up minutes of the fact of disclosure, but Service Provider shall not notify the affected Client or Clients of the disclosure, pursuant to the applicable legislation.
- In the case of civil litigious or non-litiguous proceedings that affect the validity of the certificate issued by Service Provider, Service Provider is entitled to disclose, upon request, the personal and other data verified and recorded in the course of the authentication-certification procedures prior to the issue of the certificate (see Chapter 3) to the counterparty to the proceedings or to the representative therof, or may disclose such data to the court that contacted the Service Provider with such request.

Service Provider shall have no right to refuse the disclosure of data in the above statutority regulated cases. In the course of the disclosure, Service Provider shall maintain the confidentiality of the data, as well as their complete, true and correct form. The actual management of the Service Provider shall appoint the employee responsible for the performance of the mandatory disclosures and for recording the minutes.

9.4 Privacy of personal information

With the exceptions set out in Chapter 9.3.2, the Service Provider considers Client personal information to be confidential information as defined by Chapter 9.3.1 and handles those in line with the provisions of Chapter 9.4.1 and by providing them suitable protection (Chapter 9.3.3).

9.4.1. Data management

The Service Provider handles Client personal data in line with the provisions of:

- this Statement and the Service Policy,
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information,
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and

TRANSLATION

- the Service Provider's Data Management Regulations.

Service Provider shall prevent the unauthorized access to any data it has been provided with.

Provider shall, in accordance with the regulations in force, retain the information related to the certificates – including information connected to the creation of the certificates – and the related personal data for 10 years from the expiry of the certificate, and for the final and binding resolution of the legal dispute arising in connection with the electronic signature/seal or the electronic document furnished therewith, and shall, until the elapse of the same deadline, provide a device with which the contents of the issued certificate can be established.

Service Provider shall, in all cases, publish the status information of the certificates, and upon the written consent/request of the Client, Service Provider shall publish the Subject data of the certificate, as well as the certificate itself in its public certificate repository.

Service Provider shall have a data processing policy in place, which shall be comprised of detailed provisions on the processing of confidential information and personal data. Service Provider shall, on its website (see Chapter 1.1.2) inform its Clients in a Privacy Notice on the data processing practice laid down by the data processing policy

The Service Provider is registered by the Nemzeti Adatvédelmi és Információszabadság Hatóság [The Hungarian National Authority for Data Protection and Freedom of Information] (NAIH) as a data controller. ; data processing registration number of Service Provider: NAIH-50145/2017

9.4.2. Private information

The Service Provider considers all data in its possession to be private information

- on the basis of which the natural person can be identified, with especial regard to the name of the person or his/her identifier registered by the authorities, and
- which can be linked to a natural person, or
- from which conclusions can be drawn regarding the natural person, and
- which is not listed under Chapter 9.4.3.

The Service Provider requests the Client to provide only the personal information that is indispensable and required for the provision of the requested service. This does not exclude the possibility of the Service Provider also requesting data that allow it to perform its activity more effectively. The provision of these data is not obligatory, and the processing thereof shall be based on the consent of the data subject.

9.4.3. Information not deemed private

The Service Provider does not consider the data referred to in Chapter 9.4.2 to be personal.

TRANSLATION

9.4.4. Protection of personal data

The Service Provider shall store the personal information pertaining to Certificate issuance but not included in the certificate in a secure manner and shall protect it, in compliance with the applicable requirements (see Chapter 9.4.1). Suitable measures shall be implemented to protect the data from unauthorized access and modifications, especially when forwarding those between the Client and the Service Provider's various units. They shall furthermore be protected against data loss, damage, and unauthorized processing. See also: Chapters 5.3.1, 5.5.1, 5.7.1, 5.7.4, and 9.3.3

9.4.5. Usage of private information

The Service Provider may only disclose the personal data included in the certificate if the preliminary written consent of the Client has been given.

With regard to the requirments set out in the Privacy Act of Hungary, the Services Provider may only use the personal data in a manner and to the extent that is required for the actions related to the certificate (e.g. issuance, status change, renewal, modification, re-key).

9.4.6. Data management

The ground for processing by Service Provider is primarily meeting the statutory obligation. In the case of data falling out of the scope of meeting any statutory obligation, the ground for processing is the lawful interest of the Service Provider and the data subject, as well as the prior, informed and specific consent of the data subject.

Service Provider shall store and process the personal data in the light of the provisions enlisted in Chapter 9.4.1 and in accordance with the applicable procedural rules set out in Chapter 5, and the personal data may be disclosed by Service Provider to statutorily specified third parties only in the cases enlisted in Chapter 9.3.3 and in the cases set out in the applicable legislation.

9.4.7. Other information disclosure circumstances

In the interest of uncovering and preventing crimes with the use of the services that it provides, as well as for reasons of national security, the Service Provider shall forward data free of charge to investigating authorities and national security services if the conditions for data requests set forth in separate legislation are met; the above extends to data certifying the personal identity of the involved parties and other data. The fact of the data provision is recorded by the Service Provider; however, it does not inform the Relying parties of the data provision (see 9.3.3).

9.5 Intellectual property rights

All of the

TRANSLATION

- names,
- products,
- software and hardware components

used during the course of the service activity are owned by the Service Provider, or the Service Provider uses those lawfully.

Furthermore, the

- regulations,
- contractual conditions,
- other documents and information prepared by it,
- certificates,
- certificate status service data,
- and individual identifiers disclosed/issued/created by the Service Provider are also owned by the Service Provider.

The Subscriber is the owner of the public and private keys issued by the Service Provider.

The End-User is the user with full rights of the end-user certificate, the public key included therein, and the permanent identifier.

The Service Provider may publish, reproduce, revoke, and manage by other means the end-user certificates (including the public keys and other data in them) that it has issued (see Chapter 4).

During its operations, the Service Provider takes care not to infringe upon the intellectual property rights of third parties.

9.6 Representations and warranties

The Service Provider is liable for damage caused intentionally or through negligence to any natural or legal person due to a failure to comply with undertaken obligations.

In the case of non-eIDAS services, the Service Provider's intentional / negligent actions are assumed until the Service Provider proves otherwise.

The Service Provider is not responsible for damages that exceed beyond the restrictions applicable to the use of services (see this Statement, the Service Policy, the GTC, and the service agreement for the restrictions).

The Service Provider is liable for the service activities performed in the framework of its regulations and for the operations of its Registration and Certification Authority even if any functions are performed by SP Partners.

TRANSLATION

9.6.1. The Certification Authority's responsibilities

See Chapter 9.6.1 of the Service Policy.

9.6.2. The RA's responsibilities

See Chapter 9.6.2 of the Service Policy.

9.6.3. Client representations and warranties

See Chapter 9.6.3 of the Service Policy.

The Applicant is responsible for:

- providing and verifying the data required for processing applications (see Chapter 4)
- the veracity, accuracy, and validity of the data provided during registration and application;
- cooperating with the check outlined in Chapter 3 pertaining to identity and the data provided during application, and for taking all steps that can be expected of it to ensure that the process can be completed as quickly as possible;
- checking the data in the certificate after its issuance and for notifying the Service Provider if it uncovers any deviations;
- reporting without delay any changes to data and requesting the suspension or revocation of the Service Provider and for the suspension of the use of the keys;
- becoming familiar with the contents of the Service Policy, this Service Policy, the GTC, and the service agreement before making use of the services.

The End-User is responsible for:

- using its Client device, key, and certificate in accordance with the regulations;
- the secure handling of its Client device, key, and activation data,
- notifying the Service Provider without delay and providing comprehensive information in any disputes regarding the certificate or its use before using legal means to settle the dispute;
- using the services in the manner required by law and this Statement;
- using certificates for the purposes and with the restrictions indicated therein;
- the use of private keys belonging to test certificates without actual commitment and for testing purposes;
- if the End-User's private key, Client device, or activation data ends up in unauthorised hands or suspicion of such arises, the End-User is obligated to inform the Service Provider without delay and to initiate the suspension or revocation of the certificate(s), and the use of the certificate must be terminated.

TRANSLATION

The Subscriber is responsible for:

- familiarizing itself with the Service Provider's regulations before making use of the service;
- the veracity, accuracy, and validity of the data provided during application;
- cooperating with the check outlined in Chapter 3 pertaining to the data provided during application, and for taking all steps that can be expected of it to ensure that the process can be completed as quickly as possible;
- initiating the modification, re-key, or revocation of the certificate as per Chapters 9.6.3 and 4.9.1 of the Service Policy and Chapters 4.7 and 4.8 of this Statement;
- adhering to the End-User's obligations to the degree it effects those;
- notifying the Service Provider without delay and providing comprehensive information in any disputes regarding the certificate or its use;
- ensuring that unauthorised persons cannot access the data and devices required for making use of the services;
- assuming liability for adhering to the End-User's obligations to the degree it effects those;
- meeting its fee payment obligations.

9.6.4. Relying party representations and warranties

See Chapter 9.6.4 of the Service Policy.

In the interest of the circumspect procedure required for maintaining the security level guaranteed by the Service Provider, it is recommended that Relying Parties:

- adhere to the requirements and rules set out in the Service Provider's Service Policy and this Statement;
- use reliable IT environments and applications;
- check certificate statuses with the current CRL or OCSP response (see Chapter 4.9.6);
- take into consideration all restrictions (indicated in the policies and the certificate) applicable to certificate usage.

Relying Parties are authorised to decide at their own discretion and/or on the basis of their own policies on whether to accept certificates and on the method for doing so.

9.6.5. Representations and warranties of other participants

No requirements.

TRANSLATION

9.7 Disclaimers of warranties

The Service Provider will reject claims for warranty, guarantee, or compensation against the Service Provider for its services if

- the event on which it is based can be traced back to the Client's omission, failure to meet an obligation or responsibility, or an external, unforeseeable event;
- the regulations applied by Relying Parties do not meet the requirements of the present Statement;
- the Service Provider is unable to fulfil its obligations regarding communication due to a fault of the internet or a part thereof;
- the damages are a result of the fault or weakness in the cryptographic algorithms approved by the Supervisory Body.

9.8 Limitations of liability

The Service Provider limits its liability as set forth in Chapter 9.16.5 and below.

The Service Provider is not liable for damages resulting from a circumstance subject to the exclusion of the Service Provider's warranty as defined in Chapter 9.7, or if the Client or Relying Party did not proceed with proper diligence, proceeded contrary to the Service Provider's Conditions, or proceeded unlawfully.

The Service Provider is only liable against third persons for contractual and non-contractual damages related to its services to the extent that they were caused by its own fault, from a breach of its obligations, or for a reason attributable to it, and if the damages can be proven.

The Service Provider does not assume liability for using test certificates for other purposes than testing.

See also the contents of Chapter 9.2 and 9.6 for liability and its limitations.

9.9 Indemnities

The Service Provider has liability insurance to cover its indemnification obligations (see Chapter 9.2).

The Client is obligated to indemnify the Service Provider for any proven losses or damages that are incurred by the Service Provider as a result of the Client failing to meet obligations or adhere to recommendations either intentionally or through negligence.

The general provisions of the Civil Code are applicable to compensation and indemnification proceedings; the Service Provider provides details on the procedure in its GTC.

TRANSLATION

As regards proving liability, see Chapter 9.6 and the contents of 9.7 and 9.8 for warranty, guarantee, and compensation and indemnification claims.

9.10 Term and termination

9.10.1. Term

The term of this Statement starts on the day this version becomes effective as indicated on the cover (effective date).

The personal scope of this Statement extends to the Service Provider's trusted employees, the Service Provider's partners, to Clients, and to all Relying Parties.

The scope of this Statement includes the provision and usage of services as defined in Chapter 1.1 of this Practice Statement.

9.10.2. Termination

The Statement remains valid until the service is terminated, the Statement is revoked, or until a new version enters into effect. As regards the validity of the certificates issued during the term of this Statement, Chapter 9 of the Statement shall be applied even after the validity of the Statement itself, regardless of the manner for the termination of its validity.

9.10.3. Effect of termination

If the present Statement is revoked, the Service Provider shall publish on its website the detailed rules for revocation and the rights and obligations that remain in effect thereafter. The Service Provider undertakes to guarantee that the regulations pertaining to the protection of confidential information as defined by relevant legislation shall remain in effect even if the Practice Statement is revoked.

9.11 Individual notices and communications with participants

In the interest of communicating with its Clients, the Service Provider operates a customer service office and telephone service, which is available at the contacts provided in Chapter 1.1.2 (also see Chapter 1.3.2).

During the administration of service usage and other tasks related to end-user certificates, Customer Service primarily communicates with Clients via emails. Customer service can also be contacted both by phone and in person.

TRANSLATION

The Service Provider provides a unique identifier to all Customer Service emails sent to Clients, based on which the given data or topic can be easily identified if contacted by the Client. If a Client responds to such an email, the subject of the email should be kept the same in order to facilitate the process.

If the Client sends an email other than a response to a Customer Service email, it should take all steps necessary to ensure that the email can be identified as easily as possible, e.g. by providing an electronic signature/seal to the email and/or sending it from the email address in the certificate in question.

In the course of contact by email, it is also necessary for the service or certificate in question to be unequivocally identifiable.

If the Client contacts the Service Provider by email or fax, the Registration Administrator is responsible for deciding what steps can be taken on the basis of the fax or email. If the Service Provider requires more information, it provides information in its response. If doubt arises regarding the identifiability of the Client, the Service Provider will attempt to contact the Client by phone to conciliate personal information.

In addition to communication by email, the following channels of communication are also open to Clients.

Phone
A customer service representative is only available at the customer service number during the indicated times; otherwise, a message can be left (except for certificate revocation, see Chapter 4.9.4).

Personally in the customer service office
The Service Provider only provides personal service at its customer service office (see Chapter 1.1.2) with appointments.

9.12 Modifications

If any changes occur in normative regulations, security requirements, the market environment, or other circumstances, the Service Provider will amend its Practice Statement.

Compliance of regulations with each other, relevant legislation, and applicable standards is examined at least annually. The regulations are to be reviewed and amended whenever justified by changes in relevant legislation and/or the environment of technical standards. Based on the experience it has gained during its operations, the Service Provider continuously reviews its Practice Statement.

TRANSLATION

The amended statement may enter into effect on the day of the publication thereof, at the earliest, but in extraordinary cases, such amendments may even enter into effect immediately.

See also Chapter 1.5 and 2.1.

9.12.1. Amendments

The Service Provider collects requests for changes (see 1.5), performs the amendments, fulfils internal and external information provision obligations, and has the changes enter into effect.

The Service Provider will examine requests for amendments as regards their compliance with the content requirements defined in the Service Policy, the law, and standards. If no objections are raised regarding either, it accepts the request for amendment and commences its processing.

By collecting the modifications, the Policy Adopting Unit shall create internal, non-public drafts of the statements, which shall be subject to an internal review before the publication. Service Provider shall, if possible, batch the changes into a new version of the statement, in order to reduce the number of issues of the statements.

The person who approved the Statement (see 1.5) approves the amendments, prior to which the above requirements regarding content and form are again checked. Clients and Relying Parties are then notified (see 9.12.2). The Service Provider has final liability and responsibility for approving the Policy.

The versions of the amended statements – including the public drafts – shall always be published with new version numbers.

9.12.2. Notification mechanism and period

There is no obligation to notify the Trust Service Supervisory Body in case of non-eIDAS certification.

9.12.3. Circumstances under which OID must be changed

New public versions of the Practice Statement – also the drafts – are published with new version numbers, i.e. two documents with different contents shall not have an identical OID.

The identifier of the document shall is comprised of the following elements – the elements are separated by dots:

- Service Provider OID (1.3.6.1.4.1.3555),
- marking of public documents (1),
- marking of Practice Statements (1),

TRANSLATION

- the unique serial number of this document among the public Practice Statements (17),
- an indication that the document is not an annex (0),
- version (which is the effective date in short date format),
-
- i.e. in the case of the present Statement: 1.3.6.1.4.1.3555.1.1.17.0.YYMMDD

Please note that the new Practice Statement will only be applicable to certificates issued after its effective date. Any certificate issued prior to the release of the Statement will not be subject to the new guidelines.

9.13 Dispute resolution

The Service Provider (including service provider partners) receives questions, objections, and complaints pertaining to its activities by email, phone, or in person at the Service Provider's customer service offices (see Chapter 1.1.2).

If any disputes or complaints occur, Clients are obligated and Relying Parties and other third parties are recommended to notify the Service Provider immediately before taking legal steps and to inform the Service Provider of all aspects of the case. The Parties will always attempt to settle disputes by amicable means through negotiations.

9.13.1. Dispute resolution provisions

The Service Provider will examine complaints within 30 calendar days of their having been reported and will inform the complainant by email of the results of the inspection, unless agreed on otherwise by the parties. If the examination of the complaint is expected to take more than 30 calendar days due to the nature of the complaint, the Service Provider will inform the Client that submitted the complaint.

In case of complaints filed in person or by phone, the Service Provider will draw up records on the receipt of the complaint.

After examining the complaint, the Service Provider will fix (if applicable) the error within the time technically justified and will inform the reporting party about this activity in writing.

If the reporting Client does not accept the response, it can initiate negotiations with the Service Provider. If the Service Provider rejects an application for negotiations or if the negotiations do not lead to results within 20 workdays of their commencement, the dispute can be settled according to Chapter 9.13.2.

TRANSLATION

9.13.2. Amicable dispute resolution through negotiations

If the negotiations between the Client and the Service Provider do not lead to results, the Client is recommended to turn to the Budapesti Békéltető Testület [Budapest Conciliatory Body] before initiating court proceedings.

The contact information of the competent bodies as of the entry into effect of this Statement:

Budapesti Békéltető Testület [Budapest Conciliatory Body]:

- Address: 1016 Budapest, Krisztina krt. 99. III. em. 310.
- Mailing address: 1253 Budapest, Pf.: 10.
- Email address: bekelteto.testulet@bkik.hu
- Website: www.bekeltet.hu

Budapest Főváros Kormányhivatala Fogyasztóvédelmi Osztály [Budapest Government Office, Consumer Protection Department]:

- Address: 1056 Budapest, Váci utca 62-64.
- Phone: +36-1 328 5862
- Mailing address: 1364 Bp., Pf.: 234
- Email: budapest@bfkh.gov.hu

9.13.3. Litigious dispute resolution

If the dispute cannot be settled with any of the negotiation methods outlined in Chapter 9.13, the Parties will take the case to court. In this case, the Parties subject themselves to the sole competence of the Court of Budapest Districts II and III.

9.14 Governing law

The Service Provider shall perform its activity in accordance with relevant Hungarian and European Union legislation. Hungarian law is governing regarding the Service Provider's agreements and policies and for their fulfilment, and they are to be interpreted in accordance with Hungarian law (see chapter 9.15).

9.15 Compliance with applicable law and standards

The Service Provider provides its services in accordance with the relevant European Union and Hungarian regulations.

According to present Statement, SP is not obligated services to compliance to the laws and regulations for EU trust services (eIDAS), however these services typically compliance the requirements of these regulations to maintain uniform conditions.

TRANSLATION

Relevant applicable laws, other normative requirements and recommendations, in force at the day of entering into effect of Present Statement:

- **Civil Code**: Act V of 2013 on the Civil Code
- **Government Decree 45/2014** of 26 February on the detailed rules on agreements between consumers and companies
- **Consumer Protection** Act: Act CLV of 1997 on Consumer Protection
- **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- **Information Act**: Act CXII of 2011 on Informational Self-Determination and Freedom of Information
- Public Root Provider Certificate Practice Statement;
- **X.509**: International Telecommunication Union X.509 "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"
- **ISO 3166** English Country Names and Code Elements,
- **FIPS PUB 140-2** (May 2001): "Security Requirements for Cryptographic Modules"

- **RFC 5280** (previously RFC 3280) and RFC 6818 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- **RFC 3647** (previously RFC 2527) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - As regards regulation structure
- **RFC 6960** Online Certificate Status Protocol (OCSP)
- **RFC 6844** DNS Certification Authority Authorization (CAA) Resource Record
- **RFC 2616** Hypertext Transfer Protocol -- HTTP/1.1
- **RFC 6962** Certificate Transparency

- **ETSI EN 319 401** V2.2.1 (2018-04); General Policy Requirements for Trust Service Providers
- **ETSI EN 319 411-1** V1.2.2 (2018-04) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- **ETSI EN 319 412-1** V1.1.1 (2016-02) Certificate Profiles; Part 1: Overview and common data structures
- **ETSI EN 319 412-2** V2.1.1 (2016-02) Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

TRANSLATION

- **ETSI EN 319 412-3** V1.1.1 (2016-02) Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- **ETSI EN 319 412-4** V1.1.1 (2016-02) Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations
- **ETSI TS 119 461** V1.1.1 (2021-07) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- **ETSI TS 119 511** V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- **ETSI EN 301 549** V2.1.2 (2018-08) Accessibility requirements for ICT products and services
- LCP: Lightweight Certificate Policy, OID: 0.4.0.2042.1.3;
- NCP: Normalized Certificate Policy, OID: 0.4.0.2042.1.1;
- NCP+: Extended Normalized Certificate Policy (requires the use of a cryptographic device), OID: 0.4.2042.1.2;
- **CA/Browser Forum Baseline Requirements** Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates

9.16 Miscellaneous provisions

9.16.1. Entire agreement

The Service Provider provides no merger clause.

9.16.2. Transferral

Any service providers included in the provision of services may only assign their rights and delegate their obligations to third parties if granted the Service Provider's preliminary written consent.

9.16.3. Partial invalidity

If any provisions of the present Statement become invalid for any reason, the remaining provisions shall remain in effect unchanged.

9.16.4. Enforcement

In the interest of receiving compensation for the damages, losses, and costs caused by partners or clients, the Service Provider may claim compensation and the reimbursement of attorneys'

TRANSLATION

fees. If the Service Provider does not exercise its right of validating compensation, this does not mean that it renounces its right to validate compensation for damages in any future cases or if any other provisions of the Practice Statement are violated.

9.16.5. Force Majeure

The Service Provider is not liable for the faulty or late performance of any requirements set out in the Statement if the fault or delay was caused by an unforeseen circumstance outside its scope of inspection.

9.17 Miscellaneous provisions

The Service Provider's Registration and Certification Authorities perform their activities regarding the service subject to the present Statement and regulated by Chapters 3 and 4 independently and in their own competence.

The executive employee(s) of the Registration and Certification Authorities are independent of any business, financial, and other influences that can have a negative influence on trust in the services.

TRANSLATION