NETLOCK Informatics and Network Security Services Limited Liability Company

PRICE LIST

Certificate, timestamping,electronic signature services, and fees for optional and other services and related devices

Published: 12. 03. 2026.

Effective date: 13. 03. 2026

Contents

Price table

Our prices are net prices and do not include VAT. Gross prices are shown in brackets.

CERTIFICATES

The fee for certificates stored on the client device does not include the cost of the smart card and optional card reader for key generation. The optional card types are listed under QSCD and SCD Client Devices.

	VALIDITY OF CERTIFICATE	
	1 year	**2 years**
Qualified sigtanture/seal certificate	***45 000 HUF*** *(57 150 HUF)*	***80 000 HUF*** *(101 600 HUF)*
Non-qualified sigtanture/seal certificate (personal profil)	***19 000 HUF*** *(24 130 HUF)*	***34 000 HUF*** *(43 180 HUF)*
Non-qualified sigtanture/seal certificate (business profil)	***22 000 HUF*** *(27 940 HUF)*	***39 000 HUF*** *(49 530 HUF)*
Encryption/authentication certificates (personal profil)	***20 000 HUF*** *(25 400 HUF)*	***36 000 HUF*** *(45 720 HUF)*
Encryption/authentication certificates (business profil)	***30 000 HUF*** *(38 100 HUF)*	***54 000 HUF*** *(68 580 HUF)*
Advanced SW authentication certificate (EESZT certificate) (organizational profile)		***30 000 HUF*** *(38 100 HUF)*

CERTIFICATE PACKAGES

NETLOCK SIGN Business (NLSB) cloud certificate packages

Packages include: signature/seal certificate with cloud-based key storage (remote key management service with a liability value of HUF 5 million for qualified certificates and HUF 3 million for non-qualified certificates), bundled signature transaction including time stamping as follows.

	VALIDITY OF CERTIFICATE	
	1 year	**2 years**
NLSB Qualified Base package 1000pcs transactions/year	***50 000 HUF*** *(63 500 HUF)*	***90 000 HUF*** *(114 300 HUF)*
Other transactions	***180 HUF*** *(229 HUF)*	***180 HUF*** *(229 HUF)*
NLSB Qualified Plus package 3000pcs transactions/year	***75 000 HUF*** *(95 250 HUF)*	***135 000 HUF*** *(171 450 HUF)*
Other transactions	***160 HUF*** *(203 HUF)*	***160 HUF*** *(203 HUF)*
NLSB Qualified 5k package 5000pcs transactions/year	***120 000 HUF*** *(152 400 HUF)*	***215 000 HUF*** *(273 050 HUF)*
Other transactions	***140 HUF*** *(178 HUF)*	***140 HUF*** *(178 HUF)*
NLSB Qualified 10k package 10 000pcs transactions/year	***200 000 HUF*** *(254 000 HUF)*	***350 000 HUF*** *(444 500 HUF)*
Other transactions	***100 HUF*** *(127 HUF)*	***100 HUF*** *(127 HUF)*
NLSB Non Qualified Base package 1000pcs transactions/year	***40 000 HUF*** *(50 800 HUF)*	***70 000 HUF*** *(88 900 HUF)*
Other transactions	***180 HUF*** *(229 HUF)*	***180 HUF*** *(229 HUF)*
NLSB Non Qualified Plus package 3000pcs transactions/year	***70 000 HUF*** *(88 900 HUF)*	***125 000 HUF*** *(158 750 HUF)*
Other transactions	***160 HUF*** *(203 HUF)*	***160 HUF*** *(203 HUF)*

NETLOCK eBUSINESS and eSEAL cloud certificate packages

Packages include: qualified business signature/seal certificate with 2 years validity with cloud-based key storage, (remote key management service with a liability value of HUF 5 million), remote video registration identification, Android & iOS mobile app.

	Netlock eBUSINESS signature package	Netlock eSEAL package	Netlock individual package
One-year fee	***33 000Ft*** *(41 910 Ft)*		
Two-year fee	***60 000 Ft*** *(76 200 Ft)*		
Three-year fee	***83 000 Ft*** *(105 410 Ft)*		

CARD-BASED CERTIFICATE PACKAGES

Packages include: qualified or non-qualified signature/seal certificate with card-based (QSCD, SCD client device) key storage, bundled transaction as below, card and card reader, bundled signature transaction including time stamping as below. The Basic and Advocate packages are available with a bank card size, the Plus package is available with a bank card or SIM card size and a reader for use with it.

	VALIDITY OF CERTIFICATE	
	1 year	**2 years**
Qualified Base package 1000pcs transactions/year	***59 000 HUF*** *(74 930 HUF)*	***105 000 HUF*** *(133 350 HUF)*
Qualified Plus package 2000pcs transactions/year	***99 000 HUF*** *(125 730 HUF)*	***175 000 HUF*** *(222 250 HUF)*
Non qualified package 500pcs transactions/year	***39 000 HUF*** *(49 530 HUF)*	***70 000 HUF*** *(88 900 HUF)*
Additional certificate package encryption and authentication certificate together	***25 000 HUF*** *(31 750 HUF)*	***40 000 HUF*** *(50 800 HUF)*
Lawyer certificate package 1000pcs transactions/year	***59 000 HUF*** *(74 930 HUF)*	***105 000 HUF*** *(133 350 HUF)*
Additional certificate package for lawyer package	***5 000 HUF*** *(6 350 HUF)*	***10 000 HUF*** *(12 700 HUF)*

authentication certificate	

TIMESTAMPING

	Annual fee	Unit price HUF/pc	Overuse HUF/pc
Timestamp package TS1000 1000pcs	***18 000 HUF*** *(22 860 HUF)*	***18 HUF*** *(23 HUF)*	***27 HUF*** *(34 HUF)*
Timestamp package TS5000 5000pcs	***75 000 HUF*** *(95 250 HUF)*	***15 HUF*** *(19 HUF)*	***20 HUF*** *(25 HUF)*

For larger quantities, please ask for our price offer!

WEBSITE AUTHENTICATION (SSL) CERTIFICATES

Partner certificates

SSL/TLS certificates – Valid for 199 days

	EV SSL	Wildcard OV SSL	OV SSL	DV SSL
1 domain	89 000 HUF (113 030 HUF)	44 500 HUF (56 515 HUF)	30 100 HUF (38 227 HUF)	6 900 HUF (8 763 HUF)
2-5 domains	267 000 HUF (339 090 HUF)	137 000 HUF (173 990 HUF)	89 000 HUF (113 030 HUF)	
6-10 domains	356 000 HUF (452 120 HUF)	226 000 HUF (287 020 HUF)	110 000 HUF (139 700 Ft)	

For larger quantities, please ask for our price offer!

Code signing certificate – with cloud-based key storage

	459 days
Code signing certificate	**94 300 HUF** (119 761 HUF)

Qualified code signing certificate	**150 800 HUF** (191 516 HUF)

S/MIME certificate

	1 year	2 years
S/MIME certificate – personal profile	9 000 HUF (11 430 HUF)	14 500 HUF (18 415 HUF)
S/MIME certificate – organizational profile	12 000 HUF (15 240 HUF)	19 500 HUF (24 765 HUF)

Netlock certificates

Single domain certificates

	Qualified (QCP-w)	A Class	B Class	C Class
Annual fee	***130 000 HUF*** *(165 100 HUF)*	***51 000 HUF*** *(64 770 HUF)*	***44 000 HUF*** *(55 880 HUF)*	***28 000 HUF*** *(35 560 HUF)*

Multidomain and Wildcard certificates

	Number of domains	Qualified (QCP-w)	OV A Class	OV B Class	OV C
Annual fee	2-5	***390 000 HUF*** *(495 300 HUF)*	***154 000 HUF*** *(195 580 HUF)*	***133 000 HUF*** *(168 910 HUF)*	***85 000 HUF*** *(107 950 HUF)*
	6-10	***519 000 HUF*** *(659 130 HUF)*	***205 000 HUF*** *(260 350 HUF)*	***177 000 HUF*** *(224 790 HUF)*	***114 000 HUF*** *(144 780 HUF)*
	11-20	***649 000 HUF*** *(824 230 HUF)*	***257 000 HUF*** *(326 390 HUF)*	***221 000 HUF*** *(280 670 HUF)*	***142 000 HUF*** *(180 340 HUF)*
	21-30	***909 000 HUF*** *(1 154 430 HUF)*	***359 000 HUF*** *(455 930 HUF)*	***309 000 HUF*** *(392 430 HUF)*	***199 000 HUF*** *(252 730 HUF)*
	31-43	***1 299 000 HUF*** *(1 649 730 HUF)*	***513 000 HUF*** *(651 510 HUF)*	***442 000 HUF*** *(561 340 HUF)*	***285 000 HUF*** *(361 950 HUF)*
	44-70	***1 948 000 HUF*** *(2 473 960 HUF)*	***770 000 HUF*** *(977 900 HUF)*	***663 000 HUF*** *(842 010 HUF)*	***427 000 HUF*** *(542 290 HUF)*

71-99	***2 597 000 HUF*** *(3 298 190 HUF)*	***1 027 000 HUF*** *(1 304 290 HUF)*	***884 000 HUF*** *(1 122 680 HUF)*	***569 000 HUF*** *(722 630 HUF)*

OPTIONAL SERVICES

MobilRA (identification at the Client's premises)

Base fee Fee to be charged at the time of use of the service. (/application)	***50 000 HUF*** *(63 500 HUF)*
Identification fee Unit fee per person identified. (/person)	***5 000 HUF*** *(6 350 HUF)*
Hourly rate Unit charge per hour of identification and/or waiting time. (/ hour started)	***15 000 HUF*** *(19 050 HUF)*
Km baes fee In case of rural identification from the administrative boundary of Budapest, the fee is payable on a pro rata basis of the distance travelled as a round trip. (/km).	***250 HUF*** *(318 HUF)*

Expedited issuance

	1 working day	3 working days
Gyorsított tanúsítványkiadási szolgáltatás	***50 000 HUF*** *(63 500 HUF)*	***40 000 HUF*** *(50 800 HUF)*

QSCD and SCD client devices

	Bank card size	SIM card size
Smart card	***21 000 HUF*** *(26 670 HUF)*	***21 000 HUF*** *(26 670 HUF)*
Card reader	***23 000 HUF*** *(29 210 HUF)*	***26 500 HUF*** *(33 655 HUF)*

Liability options

	1 year	2 years
up to 20 000 000 Ft	***14 000 HUF*** *(17 780 HUF)*	***25 000 HUF*** *(31 750 HUF)*
up to 50 000 000 Ft	***45 000 HUF*** *(57 150 HUF)*	***75 000 HUF*** *(95 250 HUF)*
up to 100 000 000 Ft	***70 000 HUF*** *(88 900 HUF)*	***125 000 HUF*** *(158 750 HUF)*

Other services

Delivery agent service (/ocassion)	***5 500 HUF*** *(6 985 HUF)*
Project management (/day*)	***280 000 HUF*** *(355 600 HUF)*
Business analyst (/day*)	***280 000 HUF*** *(355 600 HUF)*
Establishment support: Operator (/day*)	***200 000 HUF*** *(254 000 HUF)*
Technical procedure fee (/ocassion)	***12 990 HUF*** *(16 497 HUF)*
Card inspection (/pc)	***free of charge***
Unlock a blocked device by issuing a SO PIN (/pc)	***free of charge***
Key generation (/pc)	***free of charge***
Renewal (/pc)	***same as the current fee for the certificate to be renewed***
Modification (/pc)	***same as the current fee for the certificate concerned***
Change of certificate status (/pc)	***free of charge***
Software key replacement within 1 month (/pc)	***free of charge***

Request for a new key due to loss or compromise within 1 month (/pc)	***50% of the current fee of the certificate concerned***
Request for a new key due to loss or compromise over 1 month (/pc)	***same as the current fee for the certificate concerned***
Certificate usage fee (/pc)	***free of charge***
Certificate status information access fee (/ocassion)	***free of charge***
Reader replacement (/pc)	***same as reader fee***
Card replacement (/pc)	***same as card fee***
Replacement of a faulty reader (/pc)	***free of charge***
Replacement of a faulty card (/pc)	***free of charge***
Individual procedure fee (/ocassion)	***individual fee***
PKI consulting (/day*)	***200 000 HUF*** *254 000 HUF*
PKI assistant (/day*)	***150 000 HUF*** *190 500 HUF*
Developer support: Junior developer (/day*)	***180 000 HUF*** *228 600 HUF*
Developer support: Intermediate developer (/day*)	***240 000 HUF*** *304 800 HUF*
Developer support: Senior developer (/day*)	***360 000 HUF*** *(457 200 HUF)*
Developer support: Tester (/day*)	***180 000 HUF*** *(228 600 HUF)*
14-working-day expedited issuance – postpaid (/certificate)	***10 000 HUF*** *(12 700 HUF)*

**A day as a unit represents 8 working hours.*

Information

OVERVIEW

This document (hereinafter: Price List) of NETLOCK Informatics and Network Security Services Limited Liability Company (NETLOCK Ltd., website: https://netlock.hu) contains public prices for its trust and other services, as well as basic information about the services, their use, payment of fees and billing.

Policies and regulations

The Price List is to be interpreted together with the General Terms and Conditions (GTC) in effect at the time of publication, taking into account the relevant Service Policies and Service Practice Statements as well.

Scope of the price list

This current Prise List shall be effective from the day following its publication for new contracts and shall remain in force until revoked or until the effective date of a new version

Billing and payment information

The prices in the price list are net prices and do not include VAT. Gross prices are shown in brackets below the net prices in the Price List. For detailed billing and payment information see the final section of the of this document. If you have any questions, please send an e-mail to szamlazas@netlock.hu. Download GTC, rules and regulations from netlock.hu/aktualis-szabalyzatok

INFORMATION ABOUT CERTIFICATE SERVICE FEES

Fees

The fee for the service includes the production, issuance and storage of the certificate, as well as its continuous availability through the Client Menu, furthermore, the provision of status services until the end of the validity period. However, the fee does not include key storage devices, which may be necessary for using certain certificates. The two-year fee can only be used in the case of a two-year certificate and a lump sum payment.

Identification of identity

The identity of the Client requesting a qualified certificate containing the data of a natural person must be verified by NETLOCK in the context of a personal meeting or in an equivalent manner. For optional identification procedures and fees, see Optional Services.

General Terms and Conditions

You can find information about the detailed rules for providing and using the service in our Service Practice Statements and on our product support page.

Key generation

In the case of certificates where Clients generate the key pair themselves, they can do this by logging into their own Client Menu when applying for the certificate. With regards to those certificates where NETLOCK generates the key, the Client accrues no additional cost. If you do not renew your certificate in time upon its expiration and consequently, your certificate expires, NETLOCK will not generate a new private key for your existing device. In this case you always need to apply for a new card, which you must collect in person, and you will also be responsible for the associated costs. The cost of the new card and certificate equals the cost of ordering the new service package.

Devices

Generating the private key of device certificates issued by NETLOCK is only possible for devices supported by NETLOCK. In the case of device-based key storage, if you do not yet have a key storage device supported by NETLOCK, please consider the cost of the device as well!

INFORMATION ABOUT QUALIFIED SIGNATURE AND SEAL CERTIFICATES

In the framework of certification services as trust services, we issue both qualified and non-qualified signature and seal certificates in compliance with the regulations of eIDAS and DAP Act.

Available types

The following types are available in the NETLOCK Qualified Client Menu	Key storage method	Key is generated by	Generated signature
Qualified personal/business signature or seal – QSCD	*QSCD*	*NETLOCK*	*Qualified signature/seal based on qualified certificate*
Qualified personal/business signature or seal – SCD – CAMS	*SCD*	*NETLOCK*	*Advanced signature/seal based on a qualified certificate*
Qualified personal/business signature or seal – SCD	*SCD*	*Client*	
Qualified personal/business signature or seal – SW	*SW*	*Client*	

Issuance of the certificate

In order to issue the signature certificates, identification via the personal presence of the requesting Client is required. The ways to perform personal identification are listed in Optional Services.

In the case of a certificate that also contains organizational data, a Client must also submit documents proving their right to apply, or present these at the time of personal identification. See more details on our product support page.

Data content of certificates

Signature certificates can be requested with a personal or business profile, and seal certificates can only be requested with an organizational profile. The profile of the certificate determines what subject data is included in it.

- PERSONAL: The certificate contains only personal data.
- BUSINESS: Personal and organizational data are also indicated in the certificate. SEAL: The certificate contains only organizational data.
- SEAL: The certificate contains only organizational data.

Service provider liability

Qualified signature and seal certificates are subject to a HUF 5 million service provider liability, which is stated in the certificate and the Service Agreement as well. Certificates with a higher liability value can be requested for optional fee(s). (see below)

Key storage

- QSCD: Qualified Signature Creation Device;
- SCD: Signature Creation Device;
- SW: software key storage.

In the case of device-based (QSCD, SCD) key storage, if you do not have a suitable device, please consider the cost of the device as well!

Legal effect

The qualified signature and qualified seal, as well as the advanced signature and seal based on a qualified certificate, pursuant to by Act CXXX of 2016 on the Code of Civil Procedure, Section 325 (1) point f (as of January 1, 2018), is suitable for creating a private document and a public document with full conclusive evidence. The qualified signature is accepted as a handwritten signature in the EU.

Liability Option Fees

NETLOCK has liability insurance to cover the possible compensation of Clients and Relying Parties and other extraordinary costs. Each certificate has a specified liability value, which is the maximum amount of liability per damage event proven to be caused as a result of the fault of the Service Provider. In the case of qualified certificate services, the following liability values can be requested for an optional fee to be paid in addition to the basic certificate fee. Detailed information on service provider liability is contained in our Service Practice Statements.

INFORMATION ABOUT NON-QUALIFIED SIGNATURE AND SEAL CERTIFICATES

Documents authenticated with a non-qualified certificate are private documents with no full conclusive evidence. These have different legal effects in Hungary and in each EU member state.

Available types

The following types are available in the NETLOCK Advanced Client Menu	Key storage method	Key is generated by	Generated signature
EXPRESS personal/business signature or seal – SCD – CAMS	*SCD*	*NETLOCK*	*Advanced signature/seal*
EXPRESS personal/business signature or seal – SCD	*SCD*	*Client*	
EXPRESS personal/business signature or seal – SW	*SW*	*Client*	

Certificate issuance

In the case of the above certificates, the identity of the requesting Client is established based on a copy of the identity document sent by the Client, and its verification in a public register. In the case of a certificate that also contains organizational data, the Client must also submit documents proving their right to apply or present the organization at the time of personal identification. See more details on our product support page.

Data content of certificates

Signature certificates can be requested with a personal or organizational profile, and seal certificates can only be requested with an organizational profile. The profile of the certificate determines what subject data are included in it.

- PERSONAL: The certificate contains only personal data.
- BUSINESS: Personal and organizational data are also indicated in the certificate.
- SEAL: The certificate contains only organizational data.

Service provider liability

The above certificates are subject to HUF 3 million service provider liability. Detailed information on service provider liability is contained in our Service Practice Statements.

Key storage

- SCD: Signature Creation Device;
- SW: software key storage.

In the case of device-based (SCD) key storage, if you do not have a suitable device yet, please consider the cost of the device as well!

Legal effect

Based on Act CXXX of 2016 on the Code of Civil Procedure, Section 326 (as of January 1, 2018), the signature and seal with increased security are suitable for the creation of a simple private document with the note that the legislator assigned a higher level of legal effect to it described in Section 325 (5) of the Code of Civil Procedure.

INFORMATION ABOUT WEBSITE AUTHENTICATION (SSL) CERTIFICATES

In the framework of the certificate service provided as a trust service, in accordance with the regulations of eIDAS and the DAP Act, we issue both qualified and non-qualified website authentication certificates.

Please note that certificates with a single wildcard domain are still billed according to the table for multidomain and wildcard certificates.

Wildcard elements cannot be added to our single domain certificates and qualified certificates.

Data content of certificates

In the case of website(s) operated by an organization, in addition to the domain(s), the organization's data is included in the certificate (OV SSL, QUALIFIED SSL).

Issuance of the certificate

In the case of certificates containing organizational data (OV), the identity of the requesting Client is established on the basis of a copy of the personal identification document sent by the Client.

In the case of QUALIFIED OV SSL certificates, a personal appearance or equivalent identification is required to establish the identity of the requesting Client.

If organizational data is indicated in the certificate (QUALIFIED and OV SSL), the Client must also provide documents proving their right to apply on behalf of the organization. See more details on our product support page.

Service provider liability

- CLASS C: HUF 3,000,000;
- CLASS B: HUF 4,000,000;
- CLASS A: HUF 5,000,000;
- QUALIFIED: HUF 5,000,000.

Detailed information on service provider liability is contained in our Service Practice Statements.

INFORMATION ABOUT ENCRYPTION AND AUTHENTICATION CERTIFICATES

The encryption and authentication certificate service is not under the scope of the eIDAS and the DAP Act, therefore no legal effect is attached to them, but at the same time, such certificates are also issued according to rules similar to those contained in these laws.

The EESZT authentication certificate fee is billed annually

From November 1, 2017, all health care providers (general practitioners' surgeries, specialized care institutions) and pharmacies providing publicly funded healthcare must use the EESZT services.

It is a legal requirement for organizations, doctors and institutions providing health services to obtain "advanced" authentication certificates.

Encryption certificate

The private key of encryption certificates – with the associated public key – is suitable for decrypting encrypted files. For two-way encrypted message exchange, both parties need to have an encryption certificate. Encryption certificates can only be requested with software key storage, and the fee also includes the so-called key deposit service, which provides the possibility of restoring the key in case of loss of the private key in order to decrypt encrypted messages.

Authentication certificate

The private key of authentication certificates is suitable for certificate-based user identification in IT systems. Authentication certificates can be requested with software and hardware key storage. In the case of device-based (SCD) key storage, if you do not have a suitable device yet, please consider the cost of the device as well!

Issuance of the certificates

In the case of the above certificates, the identity of the requesting Client is established based on a copy of the identity document sent by the Client, and its verification in a public register. In the case of a certificate that also contains organizational data, the Client must also submit documents proving their right to apply. In the case of seal and organizational profile certificates (i.e. where the owner recorded in the certificate is not a natural person – CN), there is no request for a copy of an identity document and no verification in the central register. See more details on our product support page.

Data content of certificates

Encryption and authentication certificates can be requested with a personal, business or organizational profile. The profile of the certificate determines what so-called subject data are included in it.

- PERSONAL: The certificate contains only personal data.
- BUSINESS: Personal and organizational data are also indicated in the certificate.
- ORGANIZATIONAL: The certificate contains only organizational data.

INFORMATION ABOUT THE TIMESTAMP SERVICE

NETLOCK's timestamping service is a qualified service according to eIDAS, which aims at connecting authentic time data to electronic documents or other electronic files. The timestamping service with normal parameters can be used by pre-paying the selected fee package or as part of our service packages. In case of individual requests (e.g., larger quantities, leased line access, service guarantee, etc.), request an offer at ajanlat@netlock.hu.

OPTIONAL SERVICE FEES

Optional services are additional services that can be utilized in addition to the certificate services or in connection with their request.

Fee for personal identification procedures

The personal identification of the requesting Client by personal presence is carried out at the Customer Service of NETLOCK and/or within the framework of the Mobile Registration Service (MobilRA) at the Client's premises. The fee for the services must be paid together with the fee for the requested certificate(s).

Identification at NETLOCK Customer Service

Identification will be carried out free of charge during customer service hours by one of our staff members after booking an appointment. Please bring your identity card with you.

MobilRA – identification at the Client's premises

The MobilRA fee consists of the base fee, the identification fee, the hourly rate and the kilometer-based fare for locations outside of the administrative boundaries of Budapest.

Other personal identification options

Personal identification by personal presence can be replaced by the qualified signature of the requesting Client based on a qualified certificate, or by a public notary's signature authentication. See more details on our product support page.

OTHER OPTIONAL SERVICES

In relation to certificate services, the following other optional services are available. The incidental fees must be paid together with the fee for the requested certificate(s).

14-working-day expedited issuance – postpaid

In the case of requesting our postpaid service, it is not a prerequisite for the issuance of the certificate that the service fee be credited to NETLOCK's account. In this case, we will issue your certificate within 14 working days after successful data verification, personal identification, and contract conclusion following the application.

1 or 3-working-day expedited issuance – postpaid

In the case of the 1 or 3-working-day expedited certificate issuance service, it is not a prerequisite for the issuance of the certificate that the service fee be credited to NETLOCK's account. In this case, after the successful data verification, identification, and conclusion of the contract. We will process it with priority administration and issue the requested certificate within 3 working days. The duration for supplying the missing information is not included in the deadline for processing the certificate application. If you wish to request a 1 or 3-working-day expedited release for an already submitted certificate application, please send the full name (CN) and email address (E) entered in the certificate to gyorsitott@netlock.hu; in the subject of the email, please write "1 or3-day expedited issuance". In this case, the 1 or 3 working days start from the subsequent request for the accelerated release.

Delivery agent service

If the personal identification is not carried out at our Customer Service or within the framework of the MobilRA service, you can collect your device from our delivery agent on weekdays between 9 a.m. and 5 p.m.

Card inspection

The card inspection takes place exclusively in person at the NETLOCK Customer Service and always in the presence of the owner of the certificate at a pre-arranged time. The place of inspection is the reception of NETLOCK. During the card inspection, the owner must enter his/her PIN code on a specially dedicated device.

Unlock a blocked device by issuing a SO PIN

Cards blocked for any reason cannot be unlocked by NETLOCK. If the card is blocked, NETLOCK will provide the security unlocking PIN code (SO PIN) to the card owner after the client's personal identification. After the transfer, knowing the SO PIN, the Client can unlock the card and set a new PIN code in the card management program. At the same time as the transfer, NETLOCK deletes the SO PIN code from its own system and records, so it will not be able to provide it again. After the transfer,

it is the Client's responsibility to preserve and securely store the SO PIN code. If the card is permanently blocked, it is not possible to unlock the card. In that case, the new card, certificate and other associated costs will be charged to the Client.

Key generation

Generation of the key pair for the certificate in the requested Client device.

CERTIFICATE MANAGEMENT FEES

Certificate management services can be used in connection with issued certificates. The fees for certificate management services include the fee for the processing and fulfilment of the given service request, and if the issuance of a new certificate is also associated with it, the fee for the issuance of the certificate and the performance of all subsequent service provider tasks. You can find more information about certificate management services on our product support page.

Renewal

Renewal procedure for a certificate expiring within 30 days and issuance of the renewed certificate.

Renewal service package

Renewal of all certificates requested in the package within 30 days before their expiration.

Modification

Issuance of a new certificate and revocation of the original certificate due to a change in certificate data.

Change of certificate status

Permanent revocation of the certificate, temporary suspension of a maximum of 30 days or activation of the suspended certificate, i.e. termination of the suspension.

Software key replacement within 1 month

Issuance of a new certificate and revocation of the original certificate due to the loss or compromise of a private key belonging to a software certificate within 30 days of the original issuance.

Request for a new key due to loss or compromise within 1 month

Issuance of a new certificate and revocation of the original certificate due to the loss or compromise of a private key belonging to a device-based certificate within 30 days of the original issuance. If, in addition to the replacement of the key – due to its loss –, the chip card must also be replaced, in addition to this service fee, the Client must also pay the fee for the new chip card. In this case, the fee for the new certificate is 50% of the fee according to the current price list.

Request for a new key due to loss or compromise over 1 month

Issuance of a new certificate and revocation of the original certificate due to the loss or compromise of a private key belonging to a certificate. If, in addition to the replacement of the key – due to its loss –, the chip card must also be replaced, in addition to this service fee, the Client must also pay the fee for the new chip card.

CERTIFICATE STORE USAGE AND STATUS INFORMATION FEES

Based on the certificate applicant's consent, NETLOCK publishes the subject data of all end-user certificates in its public certificate repository. Netlock also provides status information services (CRL, OCSP) regarding the status of issued certificates.

NETLOCK does not charge a fee for manually querying the certificate store on the website and for normal access to certificate status information. To use the certificate store and status information in other ways (e.g., mass computer query), request an offer at ajanlat@netlock.hu.

Certificate usage fee

Search in the data of the issued certificates in the certificate library available on the NETLOCK website.

Certificate status information access fee

Standard retrieval of information on the status of issued certificates (CRL, OCSP) with normal frequency (does not enable DoS protection).

You can find information about certificate status change services on our product support page.

Detailed information on the publication of information on certificates and the normal use of records can be found in Sections 2 and 4.10 of the relevant Service Practice Statements. You can download our regulations at netlock.hu/aktualis-szabalyzatok.

CLIENT DEVICES

Client devices are cryptographic tools for storing and protecting the private keys of end users and the readers necessary for their use, respectively. If you wish to store the private key belonging to the requested certificate on a device rather than on your computer (in software – SW) and you do not yet have the appropriate device, you can choose from the following devices during the application. Devices can be applied for even without a certificate application; in this case, please send us an e-mail with the exact name of the device and the required number of pieces to igenylesek@netlock.hu or request an offer at ajanlat@netlock.hu.

Smart cards and readers

Smart cards available in NetLock's range are all Qualified Signature Creation Devices (QSCDs). It means that their key storage solution is able to create qualified signatures or seals when using the private key of a qualified certificate. If you require a certificate with SCD key storage, accordingly, the corresponding key will be generated outside of the QSCD container. Thus, the device will not be suitable for creating qualified signatures or seals. Yet, this enables batch and automatic authentication, which is not possible when using the QSCD container.További eszközökről (pl. pinpados kártyaolvasó,) és szerverekhez alkalmazható kulcstároló modulokról (HSM-ekről) érdeklődjön ügyfélszolgálatunkon az info@netlock.hu címen vagy kérjen ajánlatot az ajanlat@netlock.hu címen.

Please contact our Client Service at info@netlock.hu or request an offer at ajanlat@netlock.hu about other devices (e.g., card reader with pin pad, card body that can be combined with an access control system, etc.) and key storage modules (HSMs) that can be used for servers.

INFORMATION ABOUT SERVICE PACKAGES

With the NETLOCK service packages, you can get access to products and services enabling document authentication (signature, seal and timestamping), receiving encrypted files and certificate-based user identification (authentication).

Areas of use of the packages

Find out about the areas of use of the packages on our website under menu point Solutions / Custom Solutions.

Package fees

The package fees include the production, issuance and storage of the certificates in the package, as well as their continuous availability through the Client Menu, furthermore, the provision of status services until the end of the validity period.

The package fee also includes the timestamping service, within the framework of which a specified amount of timestamps can be used within the validity period of the certificates issued in the package. Any remaining amount cannot be carried over to the next subscription period.

The private key for the certificates is created on a signature creation device, and we provide you with client devices – without having to pay a separate fee –, which you can collect after the first request for the package. In the case of a two-year fee, the certificates are valid for two years, and the subscription fee must be paid in

one lumpsum payment. The renewal of the package can be initiated by requesting the renewal of the certificates before the subscription period, i.e. before the expiration of the certificates, in which case we provide the timestamp and certificate service for the new subscription period as well.

The package renewal fee equals the original package fee.

Certificate management fees for packages

In the case of service packages, the basis of the percentage certificate management fees are the package fees, for which we perform the requested service for all certificates issued in the package.

Key generation in the case of an expiring certificate

If you do not renew your certificate in time at the end of its validity and consequently your certificate expires, NETLOCK will not generate a new private key for your existing device. In this case you always need to apply for a new card, which you must collect in person, and you will also be responsible for the associated costs. The cost of the new card and certificate equals the cost of ordering the new service package.

NETLOCK SIGN BUSINESS SERVICE

NETLOCK SIGN is a new generation electronic signature service based on cloud-based key storage, which enables the electronic signature/sealing and timestamping of documents via a browser without a chip card or card reader. The NETLOCK SIGN BUSINESS service is publicly available to anyone in the packages below. The package fees are for a specified number of signature transactions, which also include qualified timestamps.

More information and service request: netlock.hu/netlock-sign-business

ENTERPRISE SOLUTIONS

The price of our products and solutions recommended for large companies largely depends on the specific objectives to be achieved, the corporate IT environment, existing workflows and many other factors. If you are interested in such a solution, request an offer at ajanlat@netlock.hu.

You can find more information about our corporate solutions under the Solutions menu item on our website.

NETLOCK SIGN Enterprise

NETLOCK SIGN is a new generation electronic signature service based on cloud-based key storage, which enables the electronic signature/sealing and timestamping of documents via a browser without a chip card or card reader.

NETLOCK SIGN ENTERPRISE provides a secure solution for large and medium-sized companies, which want to use the new generation electronic signature service embedded in their IT system. This solution replaces both the complex smart card-based key storage and the related card readers and software products; thus, it can fully support mobility and the use of mobile devices.

More information: netlock.hu/netlock-sign-enterprise

NETLOCK SIGNASSIST

NETLOCK SIGNASSIST is a server-side authentication and process control application that integrates with modular structure, and can be adapted to universal and corporate IT systems. Furthermore, it is able to perform complex and large number of

cryptographic operations. Thus, by means of our NETLOCK SIGNASSIST solution, a high reliability, high security level centralized signature environment can be created that supports both software and hardware key management.

Main functions and features of NETLOCK SIGNASSIST

- batch electronic signatures, seals, timestamps applied to any file format;
- verification of authenticated documents;
- placing signature images and meta data on PDF documents;
- simultaneous cooperation with several systems that require authentication and accept authenticated files;
- management of multiple software or hardware signing keys;
- handling multiple types of signature formats (ETSI BASELINE XAdES, PAdES, CAdES, ASIC);
- communication through different integration interfaces, even with several different systems simultaneously;
- multiple connectivity alternatives to other systems (e.g., REST API, FILE SYSTEM [NFS / PIPELINE], SOAP);
- authentication process control operations, signature profiles and their priority order, managing pre- and post-operations;
- redundancy, high availability, scalability;
- service quality (SQ-) measurements;
- logging processes, log archiving.

NLToken 2.0 web signing module

Modern HTML5 browser applications do not support the running of signed JAVA applications from the browser, so the development of web applications that support client-side key storage requires a different solution. This problem is addressed by NETLOCK's NLToken 2.0 product, which is a browser-side Plugin/Add-on application capable of managing traditional chip card key storage devices using a native communication channel from supported browsers and electronic authentication with a key available in the local Windows certificate store. Depending on the type of certificate used, it ensures the creation of advanced or qualified electronic signatures, seals and timestamps in accordance with the 910/2014/EC eIDAS Regulation, the optional verification of the completed signature and, in the case of PDF documents, the embedding of the completed signatures into the original document.

NLToken 2.0 is sold as an optional add-on module to SIGNASSIST. SIGNASSIST and the client-side NLToken 2.0 application work with each other in a server-client architecture. NLToken 2.0 supports browser-side communication with key storage devices and the execution of PKCS #1 signatures, all other authentication operations (formation of fingerprints, insertion into electronic documents, timestamps, management of long-term revocation information) are carried out using the basic module of SIGNASSIST.

The operating systems supported by the NLToken 2.0 web signing module are:

- Microsoft Windows 11 (64-bit)
- Microsoft Windows 10 (64-bit)
- Microsoft Windows 8.1 (64-bit)
- Microsoft Windows 7 SP1 (64-bit)

Windows NT, XP, Vista and Windows 8 operating systems are no longer supported, so NLToken 2.0 is no longer supported on these operating systems.

The NLToken 2.0 web signing module supports the following browsers:

- Microsoft EDGE (Chrome based)
- Google Chrome
- Mozilla Firefox 75.1+

The solution also supports Windows Terminal Server-based operation. Always enable NLToken 2.0 as an extension after installing it in your browser.

NETLOCK EBUSINESS ÉS ESEAL CLOUD CERTIFICATE PACKAGES

~~Calculating t~~Transactions ~~definition~~

During a signature transaction (hereinafter referred to as "Transaction"), the document uploaded to the System is signed and time-stamped.

Invoicing transactions

The initiation of the signature process is included in the business partner's unlimited package and will not incur additional charges. The signing (completion) of the document is determined by the recipient party's current billing package.

~~6~~ 12 months loyalty & e-invoice

By requesting this service, the requestor agrees that we will issue an e-invoice and that his/her order will have a ~~6~~12-month loyalty period.

INCIDENTAL FEES FOR LARGE ENTERPRISE SOLUTIONS

Project management

Comprehensive project management adapted to the particularities of the given investment – from planning to implementation.

PKI consulting

In the framework of PKI (Public Key Infrastructure) consulting, we provide professional assistance for the construction and system integration of public key infrastructure.

PKI assistant

We support the utilization and use of the electronic signature device and service system with PKI consulting and training.

Developer support: Junior, intermediate or senior developer

This activity ensures that the supported application always remains up-to-date and compatible in the rapidly changing world of IT, and thus continuously maintaining its value.

Developer support: Tester

The tester prepares the testing plan based on the submitted documentation. Creates test cases that cover the functionality to be tested to the expected extent.

Business analyst

Analysis of business processes, tracking of changes, participation in projects, analysis and documentation of the impacts of business decisions.

Establishment support: Operator

Design and operation with business challenges in mind. Our expert staff and qualifications guarantee reliable, continuous operation.

Comfort certificate, renewal package

Optional services are additional services that can be utilized in addition to the certificate services or in connection with their request. In relation to certificate services, the following other optional services are available. The incidental fees must be paid together with the fee for the requested certificate(s). The service is available with a 14-working-day processing time if the signing certificate is still valid, which can be significantly accelerated by using the expedited issuance service.

- Coordination and correction of subject data
- Coordination and correction of organizational data
- Coordination and correction of certificate application data
- Initiation of renewal
- Preparation and sending of a Service Agreement

ADMINISTRATIVE AND OTHER INCIDENTAL FEES

Technical procedure fee

We may charge a technical procedure fee for all occasional client requests that we can fulfil by using NETLOCK's operating staff individually (e.g., examination of system logs).

Card replacement

In case of damage or loss of the smart chip card, NETLOCK may invoice the card replacement fee within the validity period of the certificate or at the latest when the certificate is renewed. The key belonging to the old certificate cannot be transferred to the new card, so in the event of a card replacement, it is also necessary to account for the costs of the key change.

Replacement of a faulty card

In the event of a failure of the smart chip card – if the failure clearly occurred independently of the user – NETLOCK will replace the card and the key/certificate on it free of charge. Other costs that may arise in connection with the replacement (transportation, mobile registration/identification) are borne by the Client, the amount of which will be provided in advance.

Reader replacement

In case of damage or loss of the card reader, NETLOCK may invoice the reader replacement fee within the validity period of the certificate or at the latest when the certificate is renewed.

Replacement of a faulty reader

In the event of a failure of the card reader – if the failure clearly occurred independently of the user – NETLOCK will replace the reader free of charge.

Individual procedure fee

In all cases where NETLOCK deviates from its usual procedure at the Client's request, it may charge an individual procedure fee. Examples of such cases include, but are not limited to, the creation of an individual Service Agreement (within 5 working days), the displaying of unique content in the certificate, the request for a service provider liability value other than the optional ones, etc. Inquire about your individual needs at info@netlock.hu.

BILLING AND PAYMENT INFORMATION

Payment

The services can only be utilized (or, where applicable, the transfer of devices) after the full amount indicated on the invoice has been received (i.e. credited to NETLOCK's bank account) – unless the applicant has requested a post-payment service (see Optional services).

The service provider undertakes to issue certificates related to fee payments received on its account by 09:00 on working days on the same day in case of complete documentation.

Transfer

In case of payment of the fee on the invoice by bank transfer, the bank account number of NETLOCK Ltd. is the following:

Accounting Bank: Oberbank AG Magyarországi Fióktelep

Bank Account Number: 18400010-10000506-10406964

Swift (BIC) Code:-OBKLHUHB

IBAN (HUF:HU09 1840 0010 1000 0506 1040 6964

IBAN (EUR): HU80 1840 0010 1000 0506 1040 7044

In the communication of the transfer order, please make sure to include the serial number of the invoice!

Online payment by bank card

NETLOCK provides bank card payment options for the payment of certain services on the online application interfaces.

Billing

By default, NETLOCK issues its invoices in the form of an electronic invoice. The issuing of electronic invoices is carried out in accordance with the provisions of Section 175 of Act CXXII of 2007 on general sales tax, i.e. they are authenticated with a non-qualified electronic signature and a qualified timestamp. When requesting products and services, with a few exceptions the Client has the option to request a paper-based invoice instead of an electronic one.

Checking and cancelling an issued invoice

Please be sure to check the data on the invoice before settling the invoice, and if you notice any discrepancy, report it immediately, but no later than 15 calendar days from the invoice date to szamlazas@netlock.hu.

In the case of financially settled invoices, it is possible to cancel the invoice and/or issue a new invoice within a maximum of 15 calendar days from the settlement of the invoice free of charge. After that, the full cost of the cancellation and the issuance of a new invoice (including the full fee and cost of the self-audit to the tax authorities) may be borne by the recipient of the invoice.