NETLOCK KFT
CA hierarchy

NETLOCK Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Azonosító szám (OID):	***1.3.6.1.4.1.3555.1.61.20170411***
Jóváhagyás időpontja:	***2017.04.11***
Hatály kezdőnapja:	***2017.04.11***
Oldalak száma:	***15 oldal,*** *azaz* ***tizenöt oldal***
Készítette:	***Varga Viktor chief architect***
Jóváhagyta:	***Dr. Fehér Zsófia Jogtanácsos***

Tartalom

1 Introduction 3
2 SHA1 CA hierarchy 4
2.1 General description 4
2.2 Issued certificate types 4
2.3 CA certificates and CRLs 4
2.4 Structure 5
3 SHA256 CA hierarchy 6
3.1 General description 6
3.2 Issued certificate types 6
3.2.1 Roots 6
3.2.2 Qualified CAs 6
3.2.3 Non qualified Signer CAs 7
3.2.4 Non qualified Non-signer CAs 7
3.2.5 Non qualified SMIME Encryption CAs 7
3.2.6 Online SSL CA (OLSSLGCA) 8
3.2.7 Codesign CA 8
3.3 CA certificates and CRLs 8
3.4 Structure 10
4 Cross certifications 12
5 CA certificates not covered by any root programs 13
5.1 SHA1 Governmental CA hierarchy 13
5.1.1 General description 13
5.1.2 Issued certificate types 13
5.1.3 Structure 14
5.2 SHA256 Governmental CA hierarchy 14
5.2.1 General description 14
5.2.2 Issued certificate types 14
5.2.3 CA certificates and CRLs 14
5.2.4 Structure 15

1 Introduction

This document describes the Netlock CA hierarchy.

The general requirements specified in ETSI EN 319 401 [8], clause 6.1: The Certification Practice Statement (CPS) shall include the complete CA hierarchy, including root and subordinate CA's. The CPS also shall include the signature algorithms and parameters employed.

2 SHA1 CA hierarchy

2.1 General description

The Netlock at the end of 2012 stopped the issuance of SHA1 based certifiates, and started using its SHA256 based CA infrastructure.

From the old SHA1 structure only OCSP responder certificates are issued for revocation checking, no enduser certificates are issued.

These roots are subjects to remove them from Root programs.

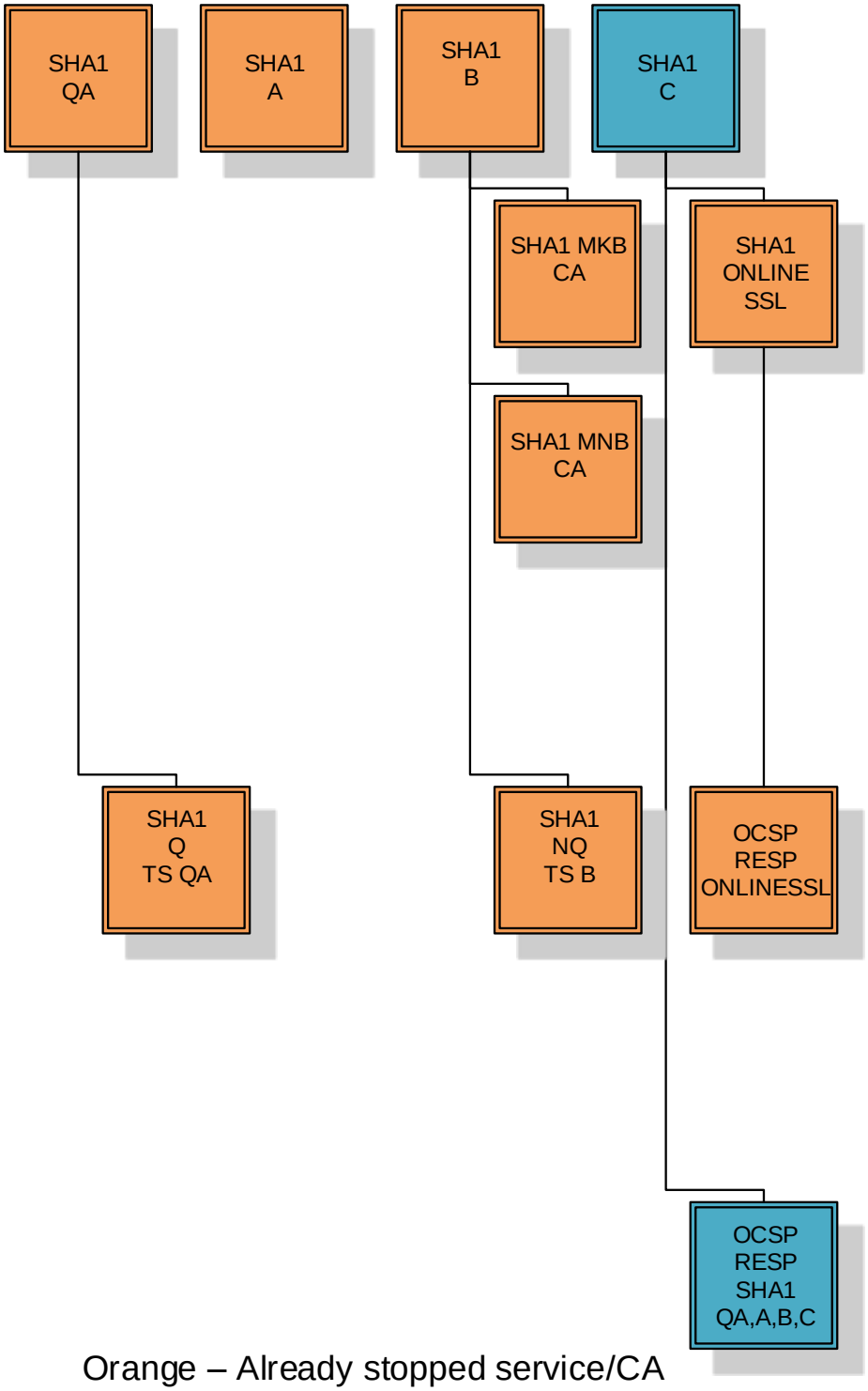
2.2 Issued certificate types

It issues only OCSP certificates for revocation checks.
Each of them now having long time valid CRLs.

2.3 CA certificates and CRLs

Short name in structure	**Full name**	**CA availability**	**CRL availability**
SHA1 QA	Netlock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado	www.netlock.hu/index.cgi?ca=mshea	www.netlock.hu/index.cgi?crl=mshea
SHA1 A	Netlock Kozjegyzoi (Class A) Tanusitvanykiado	www.netlock.hu/index.cgi?ca=kozjegyzoi	www.netlock.hu/index.cgi?crl=kozjegyzoi
SHA1 B	Netlock Uzleti (Class B) Tanusitvanykiado	www.netlock.hu/index.cgi?ca=uzleti	www.netlock.hu/index.cgi?crl=uzleti
SHA1 C	Netlock Expressz (Class C) Tanusitvanykiado	www.netlock.hu/index.cgi?ca=expressz	www.netlock.hu/index.cgi?crl=expressz
SHA1 MKB	Netlock controlled CA for MKB Bank, Hungary	already archived	already archived
SHA1 MNB	Netlock controlled CA for MNB Bank, Hungary	already archived	already archived
SHA1 OnlineSSL	Netlock OnlineSSL Hitelesito Alegyseg	already archived	already archived

2.4 Structure



Orange – Already stopped service/CA
Blue – There is no more certificate issuance, waits to stop
Yellow – CA not controlled by Netlock
TS – time stamping certificate
OCSP – OCSP certificate

3 SHA256 CA hierarchy

3.1 General description

The Netlocks SHA256 hierarchy started at the end of 2012 when the SHA1 roots are stopped.

Following the new standards it was chained under the root Netlock Arany (Gold)

The changes were:

- signer and non-singer purposes were separated by CA, for the signer CA-s only signer certificates were allowed to issue,
- the same identification levels were introduced, so the transition was seamless for the users
  (signer cert issued by a signer iCA, encryption cert issued by a non-signer iCA
- Netlocks got cross certification from Microsoft on its roots for Kernel Mode Code Signing

3.2 Issued certificate types

3.2.1 Roots

They are issuing only iCA and OCSP certificates.

These are:

- **NetLock Arany (Class Gold) Főtanúsítvány**
  It's the actual root of the structure
- **NetLock Platina (Class Platinum) Főtanúsítvány**
  It's the planed root of the EV and EV Codesigning line, but it was hard to find audit partner for this previously in Hungary.

3.2.2 Qualified CAs

They are issuing signer certificates, applicable normalized policy is: NCP+
NETLOCK Qualified Trust EV CA normalized policy is: EVCP

These are:

- **NetLock Minősített Eat. (Class Q Legal) Tanúsítványkiadó**
  Its only issues qualified signer certificates for natural persons on SSCD, or on device
  Its also issues the Time Stamping certificates too for Netlocks time stamping service.
- **NetLock Minősített Eat. (Class Q Legal S) Tanúsítványkiadó**
  Its only issues qualified signer certificates for legal persons on SSCD, or on device.
- **NETLOCK Qualified Trust CA**
  Issues EIDAS compliant qualified certificates
- **NETLOCK Qualified Trust SCD CA**

Issues EIDAS compliant qualified certificates on SCD

- **NETLOCK Qualified Trust QSCD CA**
  Issues EIDAS compliant qualified certificates on QSCD
- **NETLOCK Qualified Trust EV CA**
  Issues EIDAS compliant qualified web-site authentication certificates for legal persons.

3.2.3 Non qualified Signer CAs

They are issuing signer end entity certificates only, applicable normalized policies are: NCP, NCP+

These are:

- NetLock Közjegyzői Eat. (Class A Legal) Tanúsítványkiadó (under rolling out)
- NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó (under rolling out)
- NetLock Expressz Eat. (Class C Legal) Tanúsítványkiadó (under rolling out)
- MNB Eat. Tanúsítványkiadó
- KELER Eat. Tanúsítványkiadó
- MKB Tanúsítványkiadó
- NETLOCK Trust Advanced CA
- NETLOCK Trust Advanced Plus CA (issues only NCP+ certificates)

3.2.4 Non qualified Non-signer CAs

They are issuing authentication, encryption, and IV, OV and EV SSL certificates, applicable normalized policies are: NCP, NCP+, IVCP, OVCP, EVCP

These are:

- NetLock Közjegyzői (Class A) Tanúsítványkiadó
- NetLock Üzleti (Class B) Tanúsítványkiadó
- NetLock Expressz (Class C) Tanúsítványkiadó
- NETLOCK Trust CA
- NETLOCK Trust EV CA (issues only EV SSL certificates)

3.2.5 Non qualified SMIME Encryption CAs

They are issuing encryption certificates, applicable normalized policies are: NCP, NCP+

These are:

- MNB Tanúsítványkiadó
- KELER Tanúsítványkiadó

3.2.6 Online SSL CA (OLSSLGCA)

It issues DV SSL certificates only, applicable normalized policies are: DVCP

3.2.7 Codesign CA

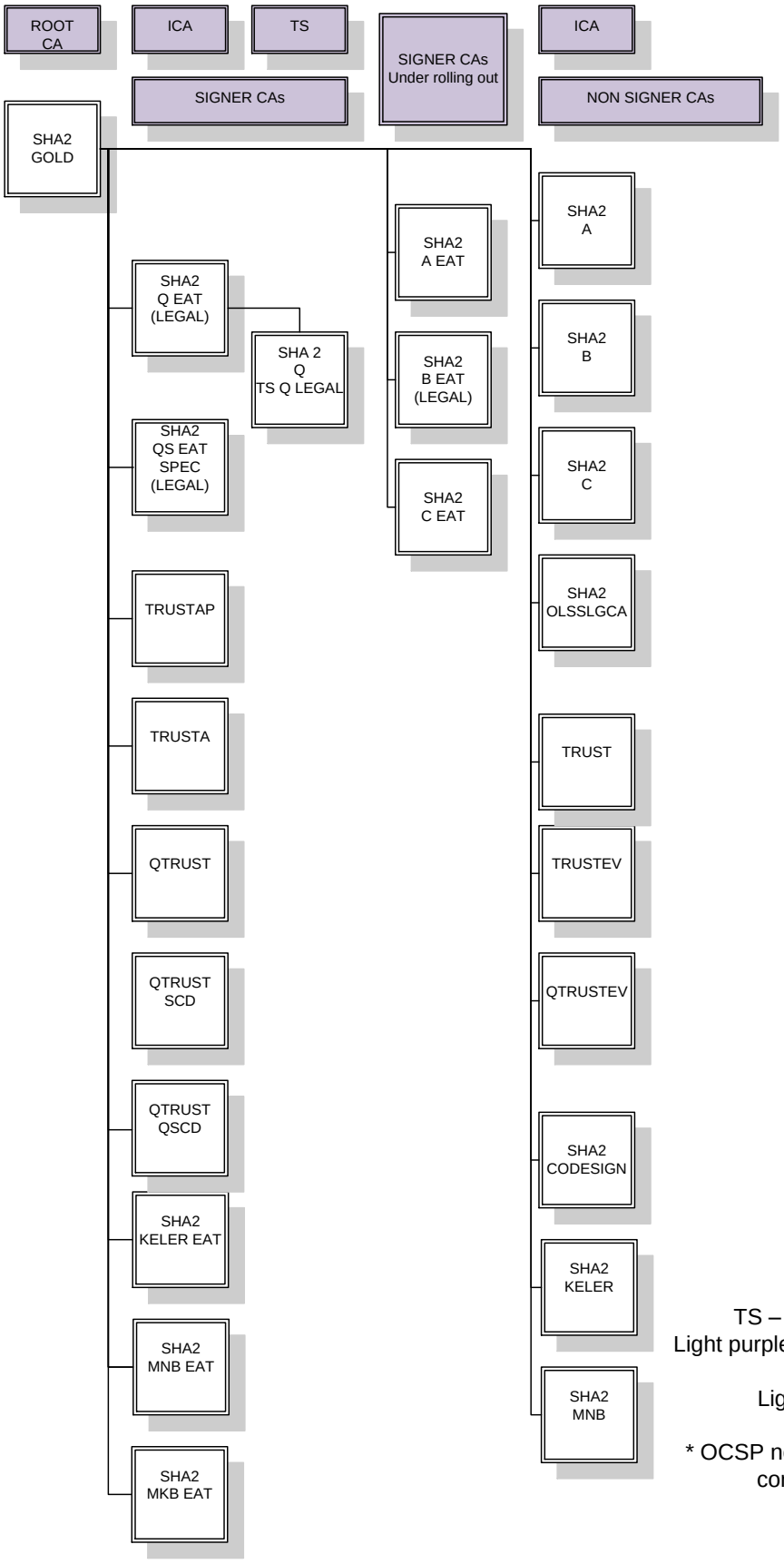
It issues simple CodeSign certificates. Applicable normalized policy: NCP, NCP+

3.3 CA certificates and CRLs

Short name in structure	Full name	CA availability	CRL availability
SHA2 GOLD	NetLock Arany (Class Gold) Főtanúsítvány	www.netlock.hu/index.cgi?ca=gold	www.netlock.hu/index.cgi?crl=gold
SHA2 PLATINUM	NetLock Platina (Class Platinum) Főtanúsítvány	www.netlock.hu/index.cgi?ca=platinum	www.netlock.hu/index.cgi?crl=platinum
SHA2 Q EAT	NetLock Minősített Eat. (Class Q Legal) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=cqlca	www.netlock.hu/index.cgi?crl=cqlca
SHA2 QS EAT	NetLock Minősített Eat. (Class Q Legal S) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=cqlsca	www.netlock.hu/index.cgi?crl=cqlsca
QTRUST	NETLOCK Qualified Trust CA	www.netlock.hu/index.cgi?ca=qtrust	www.netlock.hu/index.cgi?crl=qtrust
QTRUST SCD	NETLOCK Qualified Trust SCD CA	www.netlock.hu/index.cgi?ca=qtrustscd	www.netlock.hu/index.cgi?crl=qtrustscd
QTRUST QSCD	NETLOCK Qualified Trust QSCD CA	www.netlock.hu/index.cgi?ca=qtrustqscd	www.netlock.hu/index.cgi?cel=qtrustqscd
QTRUST EV	NETLOCK Qualified Trust EV CA	www.netlock.hu/index.cgi?ca=qtrustev	www.netlock.hu/index.cgi?crl=qtrustev
TRUSTEV	NETLOCK Trust EV CA	www.netlock.hu/index.cgi?ca=trustev	www.netlock.hu/index.cgi?crl=trustev
TRUSTAP	NETLOCK Trust Advanced Plus	www.netlock.hu/index.cgi?ca=trustap	www.netlock.hu/index.cgi?crl=trustap
TRUSTA	NETLOCK Trust Advanced Plus	www.netlock.hu/index.cgi?ca=trusta	www.netlock.hu/index.cgi?crl=trusta

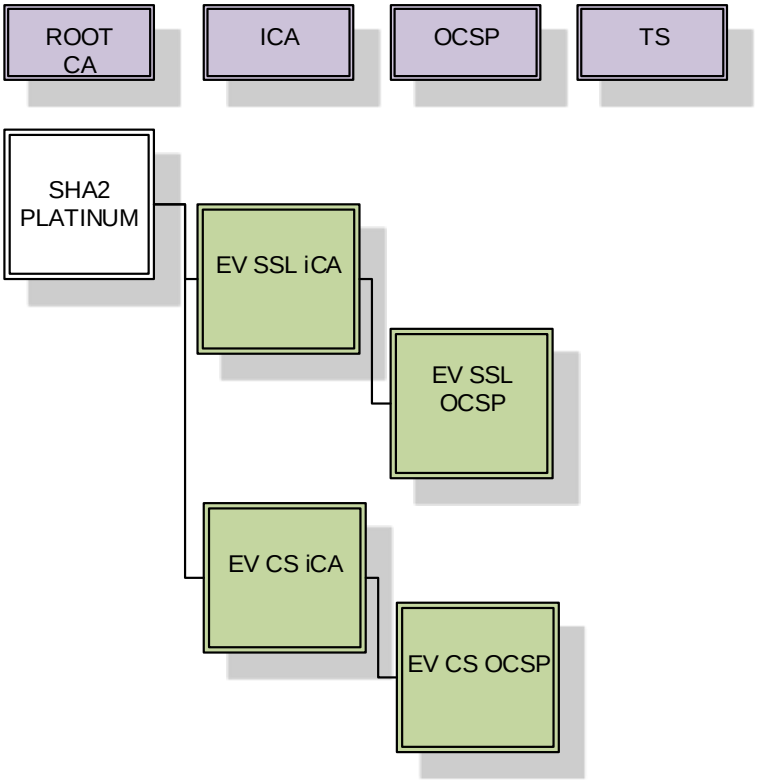
TRUST	NETLOCK Trust Advanced Plus	www.netlock.hu/index.cgi?ca=trust	www.netlock.hu/index.cgi?crl=trust
SHA2 A EAT	NetLock Közjegyzői Eat. (Class A Legal) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=calca	www.netlock.hu/index.cgi?crl=calca
SHA2 B EAT	NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=cblca	www.netlock.hu/index.cgi?crl=cblca
SHA2 C EAT	NetLock Expressz Eat. (Class C Legal) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=cclca	www.netlock.hu/index.cgi?crl=cclca
SHA2 A	NetLock Közjegyzői (Class A) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=caca	www.netlock.hu/index.cgi?crl=caca
SHA2 B	NetLock Üzleti (Class B) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=cbca	www.netlock.hu/index.cgi?crl=cbca
SHA2 C	NetLock Expressz (Class C) Tanúsítványkiadó	www.netlock.hu/index.cgi?ca=ccca	www.netlock.hu/index.cgi?crl=ccca
SHA2 MKB EAT	MKB Tanúsítványkiadó	http://crl.mkb.hu/CA4.crt	http://crl.mkb.hu/CA4.crl
SHA2 MNB EAT	MNB Eat. Tanúsítványkiadó	http://cdp.mnb.hu/LHSZ1.crt	http://cdp.mnb.hu/LHSZ1.crl
SHA2 KELER EAT	KELER Eat. Tanúsítványkiadó	http://www.keler.hu/crl/lhsz2.crt	http://www.keler.hu/crl/lhsz2.crl
SHA2 MNB	MNB Tanúsítványkiadó	http://cdp.mnb.hu/LHSZ1.crt	http://cdp.mnb.hu/LHSZ1.crl
SHA2 KELER	KELER Tanúsítványkiadó	http://www.keler.hu/crl/lhsz2.crt	http://www.keler.hu/crl/lhsz2.crl

3.4 Structure



TS – time stamping certificate
Light purple – Grouping by certificate type and purpose
Light green – in progress

* OCSP not displayed, each CA has it's corresponding responder



TS – time stamping certificate
OCSP – OCSP certificate
Light purple – Grouping by certificate type and purpose
Light green – in progress

4 Cross certifications

The Netlock has only cross certifications from Microsoft. They are intended to use for Kernel Mode Code Signing certificate root, but now the Kernel Mode Signing is strongly tied to EV Rules, after the Webtrust for EV or similar audit is possible to move forward.

MCCA SHA2 GOLD	NetLock Arany (Class Gold) Főtanúsítvány	www.netlock.hu/index.cgi?ca=mccagold
MCCA SHA2 PLATINUM	NetLock Platina (Class Platinum) Főtanúsítvány	www.netlock.hu/index.cgi?ca=mccaplatinum

5 CA certificates not covered by any root programs

5.1 SHA1 Governmental CA hierarchy

5.1.1 General description

The Netlock has Intermediate certificates which are certified by the former overnmental CA KGYHSZ in Hungary.

The Netlock at the end of 2012 stopped the issuance of SHA1 based certifiates, and started using its SHA256 based CA infrastructure.

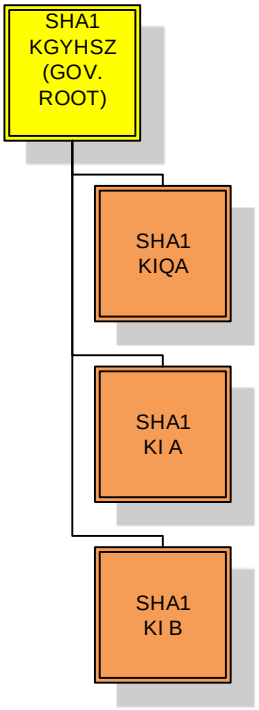
From the old SHA1 Governmental structure there is no certificate issuance.

These roots are not subjects any Root programs, they are in separated tree.

5.1.2 Issued certificate types

It’s not issuing any certificates.
Each of them now having long time valid CRLs.

5.1.3 Structure



Orange – Already stopped service/CA
Blue – There is no more certificate issuance, waits to stop
Yellow – CA not controlled by Netlock
TS – time stamping certificate
OCSP – OCSP certificate

5.2 SHA256 Governmental CA hierarchy

5.2.1 General description

The Netlock has Intermediate certificates which are certified by the SHA256 root of the governmental CA KGYHSZ.

These roots are issuing singer certificates for public administration purposes

These roots are not subjects any Root programs, they are in separated tree.

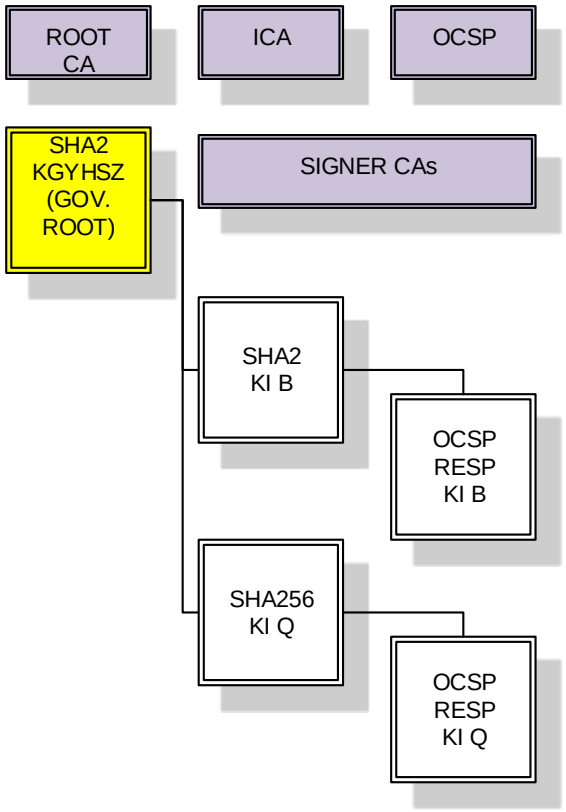
5.2.2 Issued certificate types

From these iCAs singer and authentication certificates can be bought for public administration purposes.

5.2.3 CA certificates and CRLs

Short name in structure	Full name	CA availability	CRL availability
SHA2 KGYHSZ	KGYHSZ (Public Administration Root CA - Hungary) Govermental root in Hungary, not Netlock owned.	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.cer	http://www.kgyhsz.gov.hu/KGYHSZ_CA_20091210.crl
SHA2 KI Q	NetLock Minősített Közigazgatási (Class Q) Tanúsítványkiadó	https://www.netlock.hu/index.cgi?ca=mkozig256	https://www.netlock.hu/index.cgi?crl=mkozig256
SHA2 KI B	NetLock Közigazgatási Üzleti (Class B) Tanúsítványkiadó	https://www.netlock.hu/index.cgi?ca=bkozig256	https://www.netlock.hu/index.cgi?crl=bkozig256

5.2.4 Structure



Yellow – CA not controlled by Netlock
TS – time stamping certificate
OCSP – OCSP certificate
Light purple – Grouping by certificate type and purpose