FINEID - S2
VRK (PRC) CA-model and certificate contents

v4.0

Population Register Centre (VRK)
Certification Authority Services
P.O. Box 123
FIN-00531 Helsinki
Finland
http://www.fineid.fi

Authors

Name	Initials	Organisation	E-mail
Antti Partanen	AP	VRK	antti.partanen@vrk.fi
Jari Pirinen	JP	VRK	jari.pirinen@vrk.fi

Document history

Version	Date	Editor	Changes	Status
4.0			Chapter 0.2 Reference documentations' versioning removed. Netscape Certificate Extension documentation reference removed Chapter 3 Root CA model G2 update. Different removals of obsolete data; old root, netscape extension and old algorithms. Cross references checked and updated throughout the document. Chapter 5.1 updated to G2. Chapter 6 Certificate ASN.1 types from example columns. Chapter 6.1.9.2 Netscape extension removed. Chapter 6.2.2 and 6.3.3 signature algorithms updated. Chapter 6.3.63 Correct CA name updated. Chapter 6.3.6.3 Social welfare professional title added to table. Chapter 6.3.6.4.1 Postal Code and Street Address attributes added to server certificates. Chapter 6.3.7 SubjectPublicKeyInfo; EC curves added for citizen, service providers, social welfare and healthcare service providers and social welface and healthcare professional certificates. Chapter 9. Certificate information summary tables updated. Chapter 10. OCSP responder example added.	

Contents

0.1. Introduction

This document describes VRK (Väestörekisterikeskus, Population Register Centre PRC) CA-model and certificate contents.

0.2. About FINEID specifications in general

The FINEID specifications are publicly available documents describing how to implement a public key infrastructure (PKI) using certificates (and smart cards).

The corresponding documents are listed in the table below:

FINEID document	FINEID comments	Based on
FINEID S1	Framework for the Electronic ID application in the smart card.	ISO/IEC 7816-series
FINEID S2	CA-model and content of certificates published and administrated by Population Register Centre (VRK)	IETF RFC 5280 and ETSI EN 319 412-5 v2.2.1: Certificate Profiles; Part 5: QCStatements
FINEID S4-1	Implementation profile 1 of the FINEID S1 specification.	ISO/IEC 7816-15, PKCS#15 v1.1, FINEID S1 and FINEID S2
FINEID S4-2	Implementation profile 2 of the FINEID S1 specification.	FINEID S4-1
FINEID S5	Certificate Directory specification	IETF RFC 4510, LDAP

FINEID S4 series contains an implementation profile specifying how the FINEID S1 specification should be put into practice in FINEID context. FINEID S2 is mainly based on IETF RFC 5280 (Certificate and CRL Profile). FINEID S4-1 and S4-2 are based on International Standard ISO/IEC 7816-15 and RSA Data Security Inc. Public-Key Cryptography Standard #15 version 1.1.

Related FINEID specifications are listed below:

- FINEID S1 - Electronic Identity Application
- FINEID S4-1 - Implementation Profile 1 for Finnish Electronic ID Card
- FINEID S4-2 - Implementation Profile 2 for Organizational Usage
- FINEID S5 – Directory Specification

FINEID documentation is available at

- **http://www.fineid.fi**

IETF PKIX documentation and RFC’s are available at

- **https://www.ietf.org/standards/rfcs/**

ETSI Qualified Certificate profile standards are available at

- **https://portal.etsi.org**

Microsoft Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities

- **https://support.microsoft.com/fi-fi/help/281245/guidelines-for-enabling-smart-card-logon-with-third-party-certificatio**

RSA-based Cryptographic Schemes and Public-Key Cryptography Standards

- **http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm**
- **https://www.oasis-open.org/standards**

Secure Hash Standard (SHS) FIPS PUB 180-4 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) is available at

- **https://csrc.nist.gov/publications/fips/**

References:

- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). C. Adams Entrust, P. Cain BBN, D. Pinkas Integris, R. Zuccherato Entrust. August 2001.
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper, NIST et al., May 2008
- RFC 5480: Elliptic Curve Cryptography Subject Public Key Information, S. Turner, IECA et al., March 2009
- RFC 3739: Internet X.509 Public Key Infrastructure Qualified Certificates Profile, S. Santesson Microsoft, M. Nystrom RSA Security, T. Polk NIST, March 2004
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. S. Santesson 3xA Security, M. Myers TraceRoute Security, R. Ankney, A. Malpani CA Technologies, S. Galperin A9, C. Adams University of Ottawa. June 2013.
- ETSI EN 319 412-2 V2.1.1, Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons, ETSI, February 2016
- ETSI EN 319 412-3 1.1.1, Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons, ETSI, February 2016
- ETSI EN 319 412-4 V1.1.1, Certificate Profiles; Part 4: Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations, ETSI, February 2016
- ETSI EN 319 412-5 V2.2.1, Certificate Profiles; Part 5: QCStatements, ETSI, November 2017

- Microsoft Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities, Microsoft Knowledge Base article 281245, Microsoft Corporation, January 2017
- ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1998, Information technology - Open Systems Interconnection - The Directory: Authentication framework

1. FINEID S2

FINEID S2 specifies the contents of Root, intermediate CA and end entity certificates issued by Väestörekisterikeskus (VRK) - Population Register Centre (PRC). FINEID S2 describes also VRK's CA-hierarchy and contents of Authority and Certificate Revocation Lists. This specification describes also Qualified Certificate Profile extensions usage.

Nature of this document, like other FINEID specifications as well, is technical. Basic understanding of certificates and smart cards is needed for full benefit of FINEID documentation. It is not necessary for end users to fully understand technical details of smart cards they use.

In addition to FINEID specifications, software vendors, developers and service providers can also order test cards and test certificates from VRK.

The FINEID S2 certificate implementation is based heavily on the IETF RFC 5280. Some additional extensions are extracted from ETSI Qualified Certificate Profile specifications.

RSA algorithm and Public-Key Cryptography Standards (PKCS) are developed and published by RSA Laboratories. PKCS #11 is currently maintained by OASIS.

SHA-1 and SHA2 algorithm documentation (FIPS PUB 180-4) is published by NIST, http://csrc.nist.gov/publications/

Note: Not all certificates contain all attributes and extensions described in this specification. Optional attributes are marked as optional. Criticality of extension is also marked.

2. About VRK’s certificates

All certificates are issued and administrated by Population Register Centre (“Väestörekisterikeskus”), later VRK.

VRK issues two basic types of certificates: User certificates and service certificates. User certificates are typically stored in tokens. Smart cards contain Root and intermediate CA certificates and typically two end entity certificates: One for authentication and encryption, and another for non-repudiation digital signatures. All non-repudiation certificates issued by VRK are Qualified Certificates. Private keys associated with non-repudiation certificates are generated inside tokens (smart cards) and there are no copies of those keys.

VRK issues two types of service certificates. Server certificates and system signing certificates are issued based on PKCS#10 Certificate Request and private keys generated by service provider. Service certificate for email usage is a PKCS#12 format file that contains the certificate and corresponding private and public key. It is service providers duty to keep private keys secured using Hardware Security Module, encryption, passwords or by other means.

Certificate Revocation Lists contain information about those certificates which are not valid for some reason. Most common reason is that certificate is not needed anymore or token containing private keys is lost or stolen. Service providers and software products MUST always check validity of certificate against valid CRL or OCSP service before trusting a single certificate. Certificate expiration is not a reason to add certificate into CRL. Also, digital signatures and other transactions occurred BEFORE certificate revocation, are still valid despite of certificate been revoked. For this reason, CRLs contain exact time when revocation was made.

Authority Revocation Lists contain information about those intermediate CA certificates, which are not valid for some reason. Most common reason is that intermediate CA certificate is not needed anymore. This also provides mechanism for Root CA to revoke intermediate CA certificate if its private key is exposed. Service providers and software products SHALL always check validity of intermediate CA certificate against valid ARL or OCSP service before trusting an intermediate CA certificate. Certificate expiration is not a reason to add intermediate CA certificate into ARL. All certificates and CRLs issued by revoked intermediate CA are not valid after that CA’s revocation.

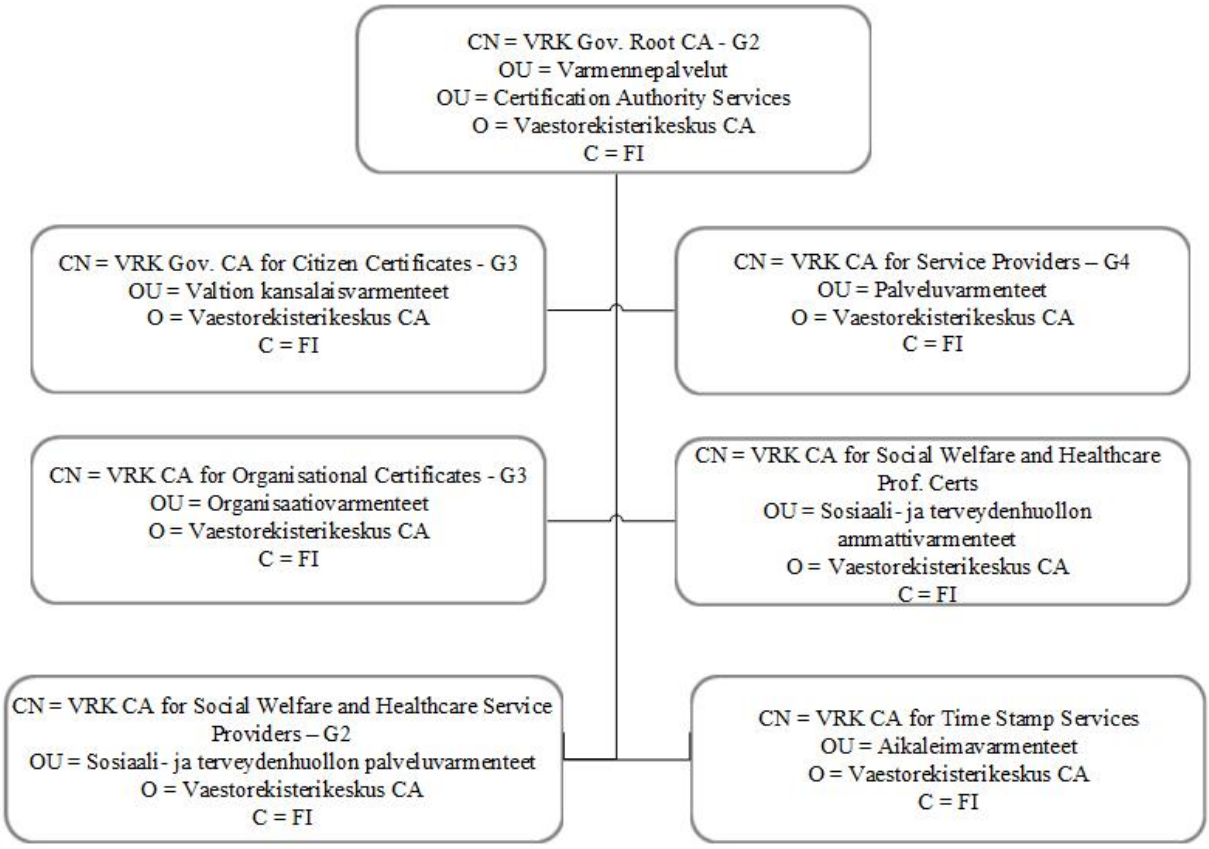
More detailed information is available in Certificate Policies (CP) and Certificate Practice Statements (CPS) available at http://www.fineid.fi/cps

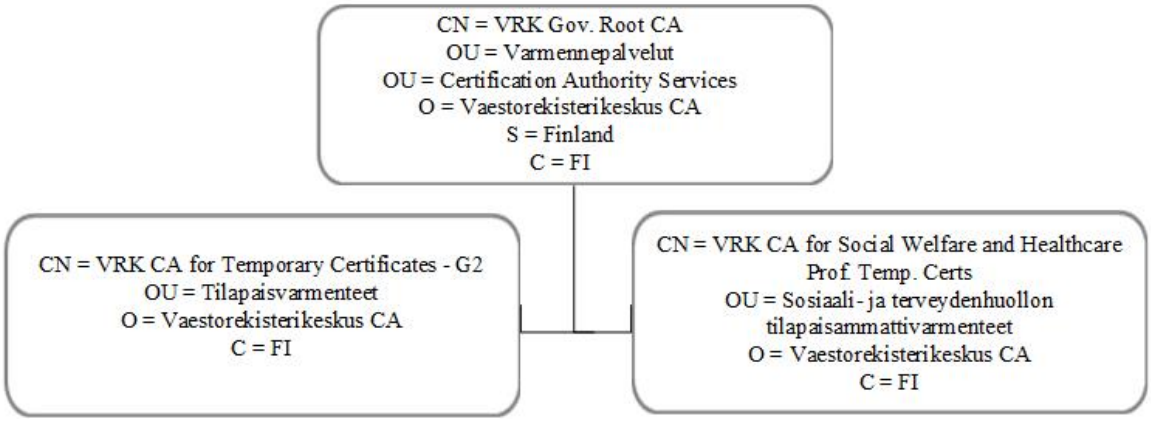
When handling certificates and/or digitally signed data, software products and network services SHALL perform Basic Path Validation as described in RFC 5280, section 6.1. Basic certificate fields. More specific needs can be fulfilled comparing CPS/policy ID numbers extracted from certificates and make trust decisions based on those.

In addition to http services at address proxy.fineid.fi, Root CA and intermediate CA certificates and ARLs and CRLs are also published into a public certificate directory, which is available with LDAP protocol at ldap.fineid.fi. Certificate directory contains also valid, public end user certificates. VRK’s public certificate directory is documented in FINEID S5 directory specification.

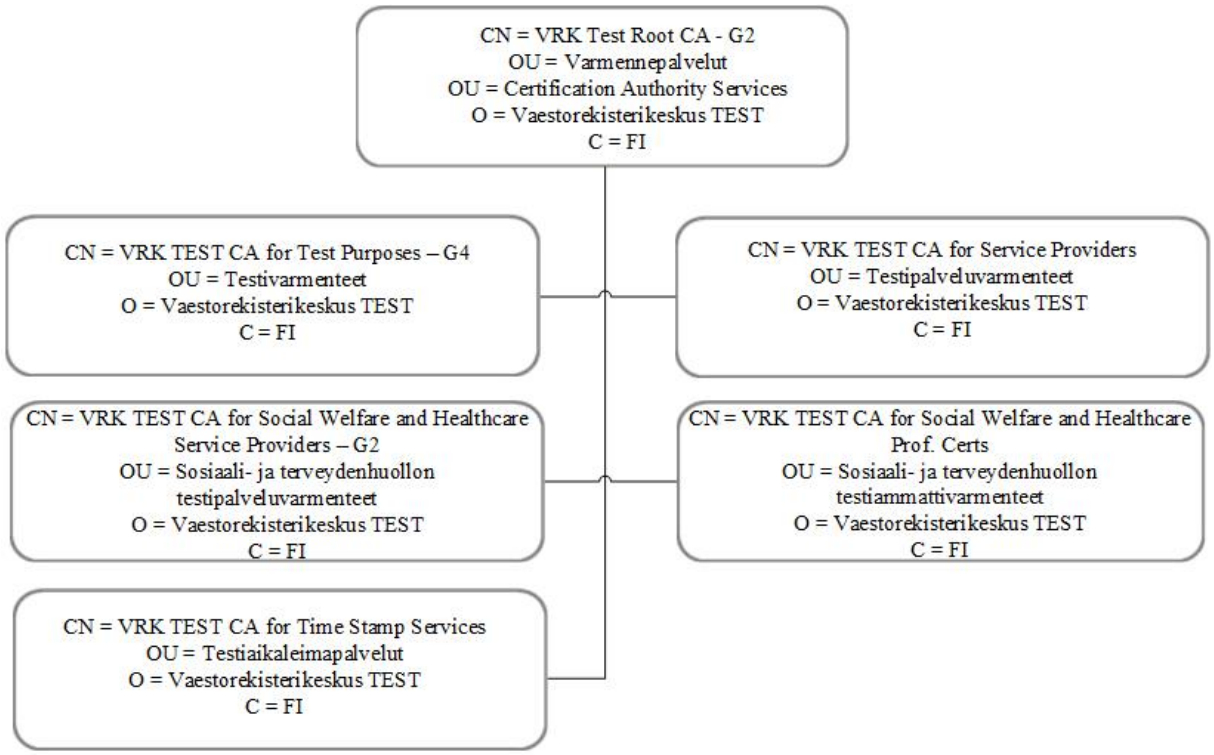
3. Root CA model

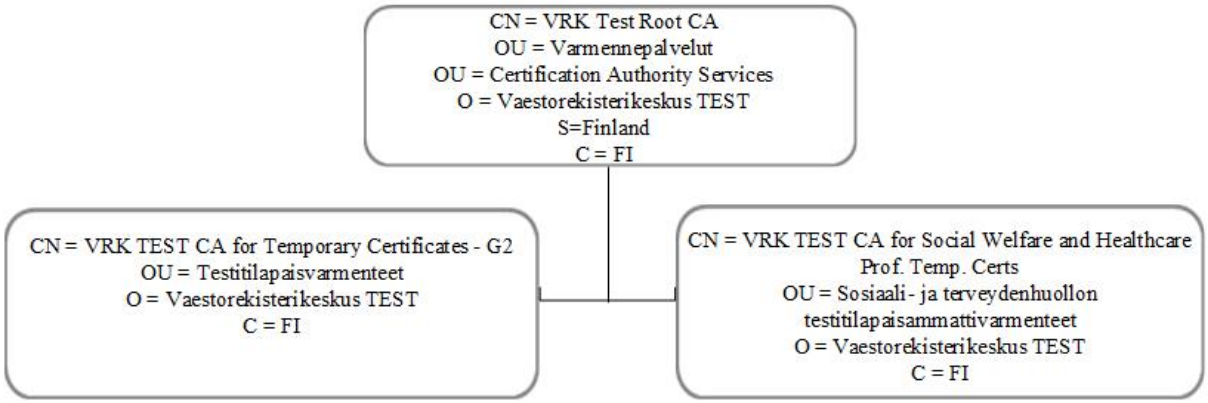
CA model is based on a common Root CA where Root Certificate is self-signed and other VRK's intermediate CAs are signed by VRK Root CA. VRK Gov. Root CA – G2 was created on the 14.12.2017. VRK CA for Temporary Certificates – G2 and VRK CA for Social Welfare and Healthcare Prof. Temp. Certs are signed by the VRK Gov. Root CA and these are documented in detail in FINEID S2 v3.2 specification.





Test Root CA – G2 model was created on the 11.10.2017. VRK TEST CA for Temporary Certificates – G2 and VRK TEST CA for Social Welfare and Healthcare Prof. Temp. Certs are signed by the VRK Gov. Root CA and these are documented in detail in FINEID S2 v3.2 specification.





It is easy to build complete PKI enabled solutions where end users and services can share a common trust point. Trust decision is made based on VRK's reputation as Certification Authority (CA). Of course, it is possible to build services where certificates issued by only a certain intermediate CA are accepted. Basic trust is however still present across all VRK intermediate CAs and end entity certificates.

4. Root certificate

Root CA Certificate	Public key length	Signed by
'VRK Gov. Root CA – G2'	4096 bit	Self-signed

The Root certificate shall look like an ordinary end user X.509v3 certificate with following exceptions:

- **subject** equals **issuer** in self-signed Root certificate
- key usages **keyCertSign** and **cRLSign** are used in the **keyUsage** extension in Root certificate
- the **basicConstraints** extension is mandatory and the value for the **cA** element shall be set to **TRUE**

Root certificate is introduced in a public directory. It is also available at various web sites. Cardholder's trusted Root certificate is also typically stored in smart cards issued. If in any doubt, it is possible to compare Root and intermediate certificates from different sources to make sure that the Root certificate is valid and issued by VRK. It is also trivial task to test VRK intermediate certificate signature against suspicious Root certificate.

VRK Root Certificate "fingerprints" (hashes) are also listed in **section 9. Certificate information summary.**

Complete description of Root certificate content is in section 6. Certificate contents.

5. Intermediate CA certificates

The intermediate CA certificates shall look like an ordinary end user X.509v3 certificate with following exceptions:

- key usages **keyCertSign** and **cRLSign** shall be used in the **keyUsage** extension in CA certificates
- **basicConstraints** extension shall be mandatory and the value for the **cA** element is set to **TRUE. MaxPathLen** attribute in CA certificates is 0 for security reasons.
- **certificatePolicies** extension is not mandatory but it is used.
- **http-uri pointing to VRK Gov. Root CA – G2 authorityRevocationList and Root's OCSP responder**

All CA certificates and possible cross-certificates are introduced in a public directory. They are also available at various web sites. In case of tokens, VRK's Root CA certificate and intermediate CA certificate are typically included in smart cards issued. If in any doubt, it is also possible to compare Root and intermediate CA certificates from different sources to make sure that the certificates are valid and issued by VRK. It is also trivial task to test end entity certificate signature against suspicious intermediate CA certificate.

For complete list of VRK Root and Intermediate CA Certificates, see **section 9. Certificate information summary.**

Complete description of CA certificate content is in section 6. Certificate contents.

5.1. CA certificates

VRK Root certificate and one intermediate CA shall be stored into the FINEID application on the token. These can be used as starting points of trust for the cardholder.

Intermediate CA Certificates	**Public RSA key length**	**Signed by**
'VRK Gov. CA for Citizen Certificates – G3'	4096 bit	'VRK Gov. Root CA – G2'
'VRK CA for Organisational Certificates – G3'	4096 bit	'VRK Gov. Root CA – G2'
'VRK CA for Service Providers – G4'	4096 bit	'VRK Gov. Root CA – G2'
'VRK CA for Temporary Certificates – G2'	4096 bit	'VRK Gov. Root CA'
'VRK CA for Time Stamp Services'	4096 bit	'VRK Gov. Root CA – G2'
Social Welfare and Healthcare CA Certificates		
'VRK CA for Social Welfare and Healthcare Prof. Certs'	4096 bit	'VRK Gov. Root CA – G2'
'VRK CA for Social Welfare and Healthcare Prof. Temp. Certs'	4096 bit	'VRK Gov. Root CA'
'VRK CA for Social Welfare and Healthcare Service Providers – G2'	4096 bit	'VRK Gov. Root CA – G2'

Note: Certificates issued by 'VRK CA for Service Providers – G4' and 'VRK CA for Social Welfare and Healthcare Service Providers – G2' CAs are not token based and therefore CA certificates are NOT stored into tokens.

6. Certificate contents

This section describes contents of all certificate types issued by VRK.

For complete description of certificate content, syntax and other PKI aspects, see IETF RFC 5280, X.509v3 and other reference documentation mentioned in reference list.

Section 10. Root, CA and End Entity Certificate examples and example of Certificate Revocation List contains examples of decoded certificates and CRL.

6.1. Basic certificate fields

The X.509 v3 certificate basic syntax is as follows.

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  EXPLICIT Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     extensions      [3]  EXPLICIT Extensions OPTIONAL
                          -- If present, version MUST be v3
     }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
     notBefore      Time,
     notAfter       Time }

Time ::= CHOICE {
     utcTime        UTCTime,
     generalTime    GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
```

```
      subjectPublicKey     BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
      extnID      OBJECT IDENTIFIER,
      critical    BOOLEAN DEFAULT FALSE,
      extnValue   OCTET STRING  }
```

The following items describe the X.509 v3 certificate for use in the FINEID context.

6.2. Certificate Fields

The Certificate is a SEQUENCE of three required fields. The fields are described in detail in the following subsections.

6.2.1. tbsCertificate

The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information. The tbsCertificate includes extensions.

6.2.2. signatureAlgorithm

The signatureAlgorithm field contains the identifier for the cryptographic algorithm used by the CA to sign this certificate.

The following algorithm SHALL be used:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertificate.

The temporary certificates issued by VRK CA for Temporary Certificates – G2 and VRK CA for Social Welfare and Healthcare Prof. Temp. Certs which are signed by VRK Gov. Root CA use the following cryptographic algorithm:

1.2.840.113549.1.1.11 - sha256WithRSAEncryption

6.2.3. signatureValue

The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as the input to the signature function. This signature value is encoded as a BIT STRING and included in the signature field.

By generating this signature, a CA certifies the validity of the information in the tbsCertificate field. In particular, the CA certifies the binding between the public key material and the subject of the certificate.

6.3. TBSCertificate

The sequence TBSCertificate contains information associated with the subject of the certificate and the CA who issued it. Every TBSCertificate contains the names of the subject and issuer, a public key associated with the subject, a validity period, a version number, and a serial number; some MAY contain optional unique identifier fields. The remainder of this section describes the syntax and semantics of these fields. A TBSCertificate includes extensions. Extensions for the FINEID implementation are described in **Section 6.3.8. Certificate extensions**.

6.3.1. version

RFC 5280 defines **Version** type as follows:

```
Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
```

Only version 3 certificates shall be used (the integer value is 2).

6.3.2. serialNumber

RFC 5280 defines **CertificateSerialNumber** type as follows:

```
CertificateSerialNumber  ::=  INTEGER
```

All certificates issued by one CA must have unique serial numbers (max. 20 octets).

6.3.3. signature

RFC 5280 defines **AlgorithmIdentifier** type as follows:

```
AlgorithmIdentifier ::= SEQUENCE {
    algorithm         OBJECT IDENTIFIER,
    parameters        ANY DEFINED BY algorithm OPTIONAL
}
```

The following algorithm SHALL be used:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

The temporary certificates issued by VRK CA for Temporary Certificates – G2 and VRK CA for Social Welfare and Healthcare Prof. Temp. Certs which are signed by VRK Gov. Root CA use the following cryptographic algorithm

1.2.840.113549.1.1.11 - sha256WithRSAEncryption

6.3.4. issuer

The issuer field identifies the entity that has signed and issued the certificate. The issuer field is defined as the X.501 type Name. Name type is defined by RFC 5280 as follows:

```
Name ::= CHOICE { -- only one possibility for now --
     rdnSequence  RDNSequence }

   RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

   RelativeDistinguishedName ::=
     SET SIZE (1..MAX) OF AttributeTypeAndValue

   AttributeTypeAndValue ::= SEQUENCE {
     type     AttributeType,
     value    AttributeValue }

   AttributeType ::= OBJECT IDENTIFIER

   AttributeValue ::= ANY -- DEFINED BY AttributeType

   DirectoryString ::= CHOICE {
         teletexString           TeletexString (SIZE (1..MAX)),
         printableString         PrintableString (SIZE (1..MAX)),
         universalString         UniversalString (SIZE (1..MAX)),
         utf8String              UTF8String (SIZE (1..MAX)),
         bmpString               BMPString (SIZE (1..MAX)) }
```

The DirectoryString shall be coded as UTF8String with ISO 8859-1 (ISO Latin-1) characters. In FINEID context, teletexString, universalString and bmpString types are not used.

The issuer identity is represented by at least the following attributes:

Attribute	OID	Description	ASN.1 type	Example
commonName	{ id-at 3 }	An informative unique (inside organisation) name of the CA	UTF8String	‘VRK Gov. CA for Citizen Certificates – G3’
organizationName	{ id-at 10 }	An informative unique name of the issuing organisation	UTF8String	‘Vaestorekisterikeskus CA’
organizationalUnitName	{ id-at 11 }	An informative name of the issuing organizationUnit. At FINEID context it is used as additional certificate type description in Finnish	UTF8String	‘Valtion kansalaisvarmenteet’
countryName	{ id-at 6 }	Abbreviation for country	PrintableString	‘FI’

Additional attributes may be used.

All VRK's CA certificates have same issuer:

```
o=Vaestorekisterikeskus CA
c=FI
```

Note: Population Register Centre's official Finnish name is "Väestörekisterikeskus" (VRK). For compatibility reasons word 'Väestörekisterikeskus' is written in certificates without diereses ('Vaestorekisterikeskus'). Letters 'CA' are also added to issuer organisation name (o='Vaestorekisterikeskus' vs. 'o=Vaestorekisterikeskus CA'). This method distinguishes VRK's role as normal organisation and VRK's role as Certification Authority for example in situations where VRK issues certificates for VRK's employees and information systems.

6.3.5. validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter).

RFC 5280 defines the **Validity** type as follows:

```
Validity ::= SEQUENCE {
     notBefore      Time,
     notAfter       Time  }

Time ::= CHOICE {
     utcTime        UTCTime,
     generalTime    GeneralizedTime }
```

CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.

The validity period for a certificate is the period of time from notBefore through notAfter, inclusive.

UTCTime values shall be expressed in Greenwich Mean Time (GMT) and they shall include seconds as follows:

YYMMDDhhmmssZ
YY two least significant digits of the year
MM month (01-12)
DD day (01-31)
hh hour (00-23)
mm minutes (00-59)
ss seconds (00-59)
Z indicates that the time is in GMT

Where YY is greater than or equal to 50, the year SHALL be interpreted as 19YY; and

Where YY is less than 50, the year SHALL be interpreted as 20YY.

Example: the time **18:57:20** on February 20, 2016, in Finland shall be represented as:
"160220**165720**Z**"**

Certificate's notBefore time expresses the moment when corresponding CRL service is available. Validity period starts from that point.

Validity period shall be set according to the certificate policy.

6.3.6. subject

The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension.

The subject field shall be coded with the same rules as the issuer field.

6.3.6.1. Citizen certificates

Certificates issued as citizen certificates may contain the following attributes:

Attribute	OID	Description	ASN.1 type	Example
commonName (mandatory)	{ id-at 3 }	Combination of subject's surname givenName and serialNumber	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Törmänen Päivi 12345678N'
surname (mandatory)	{ id-at 4 }	Family name of subject	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Virtanen' 'Törmänen'
givenName (mandatory)	{ id-at 42 }	One of the first names of subject	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Hilkka' 'Päivi'
serialNumber (mandatory)	{ id-at 5 }	Unique identifier of subject in Finland (FINUID)	PrintableString	'12345678N'
countryName (mandatory)	{ id-at 6 }	Abbreviation for country	PrintableString	'FI'

SubjectAltName extension MAY contain subject's email address (rfc822Name).

SerialNumber attribute contains a unique identifier (8 digits + checksum character) for a person that within Finland identifies the subject of certification from other persons having exactly the same name. The combination of serialNumber and other attributes of the subject name shall form a unique name for the subject within the CA. Common name is formed from surname, givenName and serialNumber.

6.3.6.2. User certificates for organisational usage

Certificates issued to persons for organisational usage may contain the following additional attributes:

Attribute	OID	Description	ASN.1 type	Example
title (optional)	{ id-at 12 }	Title of subject	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Projektisihteeri' 'Osastopäällikkö'
organizationalUnit Name (optional)	{ id-at 11 }	An informative unique name of subject's organisational unit	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Hallinto' 'Henkilöstö-osasto'
serialNumber (mandatory)	{ id-at 5 }	Unique identifier of subject within CA	PrintableString	'23456789L'
organizationName (mandatory)	{ id-at 10 }	An informative unique name of subject's organisation	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Yritys Oyj' 'Kehittämis-ministeriö'

SubjectAltName extension MAY contain subject's email address (rfc822Name) and user principal name (UPN), for more details see **section 6.3.8.5. subjectAltName.**

Additional attributes MAY be used.

SerialNumber attribute contains a unique identifier (8 digits + checksum character) that identifies the subject of certification from other persons having exactly the same name. In some contexts (e.g. employee certificates issued by a company) the serialNumber may not be by itself unique. However, the combination of serialNumber and other attributes of the subject name shall form a unique name for the subject within the CA. Common name is formed from surname, givenName and serialNumber.

6.3.6.3. User certificates for Social Welfare and Healthcare Professional usage

SerialNumber attribute contains a unique identifier (registration number, 11 digits) issued by the National Supervisory Authority for Welfare and Health.

Non-repudiation Digital Signature Certificates contain the following additional attributes:

Attribute	OID	Description	ASN.1 type	Example
title (mandatory)	{ id-at 12 }	Occupation title of subject in Finnish and in Swedish	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'001 lääkäri, läkare' '005 farmaseutti, farmaceut' '250 sosiaalityöntekijä, socialarbetare'
pseudonym (optional)	{ id-at 65 }	Doctor ID	PrintableString	'123455'

6.3.6.4. Service certificates

VRK issues three types of service certificates: server certificates, system signature certificates and PKCS#12 based certificates for email services:

6.3.6.4.1. Server certificates

Server certificates may contain the following attributes:

Attribute	OID	Description	ASN.1 type	Example
commonName (mandatory)	{ id-at 3 }	Server name (URL or IP address)	DirectoryString: PrintableString	'www.fineid.fi'
organizationalUnit Name (optional)	{ id-at 11 }	An informative unique name of subject's organisational unit	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Tietohallinto' 'Pääkonttori'
organizationName (mandatory)	{ id-at 10 }	An informative unique name of subject's organisation	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Yritys Oyj' 'Väestörekisterikeskus'
serialNumber (optional)	{ id-at 5 }	An identity code issued for example to companies, municipalities and natural persons engaged in business activities.	PrintableString	'0245437-2' 'FI02454372' '1.2.246.10.2454372'
localityName (mandatory)	{ id-at 7 }	An informative name of city, county or other geographic region where (headquarter of the) cerficate holder is located.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Jyväskylä'
stateOrProvinceName (mandatory)	{ id-at 8 }	An informative name of state. At FINEID context it is used as long form of subject's country name where (headquarter of the) cerficate holder is located.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Finland' 'Sweden'
postalCode (optional)	{ id-at 17}	Postal code.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'00530'
streetAddress (optional)	{ id-at 9}	Street address.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Lintulahdenkuja 4'
countryName (mandatory)	{ id-at 6 }	Abbreviation for country.	PrintableString	'FI'

SubjectAltName extension MAY contain subject's email address (rfc822Name) and SHALL contain subject's DNS name (dNSName).

Additional attributes MAY be used.

6.3.6.4.2. System signature certificates

System signature certificates may contain the following attributes:

Attribute	OID	Description	ASN.1 type	Example
commonName (mandatory)	{ id-at 3 }	Service name	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	‘Reseptikeskus’ ‘Sanoman välityspalvelu’
organizationalUnitName (optional)	{ id-at 11 }	An informative unique name of subject’s organisational unit	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	‘Tietohallinto’ ‘Pääkonttori’
organizationName (mandatory)	{ id-at 10 }	An informative unique name of subject’s organisation	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	‘Yritys Oyj’ ‘Väestörekisterikeskus’
serialNumber (mandatory)	{ id-at 5 }	An identity code issued for example to companies, municipalities and natural persons engaged in business activities.	PrintableString	‘0245437-2’ ‘FI02454372’ ‘1.2.246.10.2454372’
localityName (mandatory)	{ id-at 7 }	An informative name of city, county or other geographic region where (headquarter of the) cerficate holder is located.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	‘Jyväskylä’
stateOrProvinceName (mandatory)	{ id-at 8 }	An informative name of state. At FINEID context it is used as long form of subject’s country name where (headquarter of the) cerficate holder is located.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	‘Finland’ ‘Sweden’
countryName (mandatory)	{ id-at 6 }	Abbreviation for country.	PrintableString	‘FI’

SubjectAltName extension MAY contain subject’s email address (rfc822Name).

Additional attributes MAY be used.

KeyUsage for system signature certificates is digitalSignature and nonRepudiation (0xC0)

6.3.6.4.3. Service certificates for email usage

Service certificates for email usage may contain the following attributes:

Attribute	OID	Description	ASN.1 type	Example
commonName (mandatory)	{ id-at 3 }	Service name (name of the email account holder).	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Yritys Oyj' 'Maija Meikäläinen'
organizationName (mandatory)	{ id-at 10 }	An informative unique name of subject's organisation.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Yritys Oyj' 'Kehittämis-ministeriö'
organizationalUnit Name (optional)	{ id-at 11 }	An informative unique name of subject's organisational unit.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Tietohallinto'
serialNumber (mandatory)	{ id-at 5 }	An identity code issued for example to companies, municipalities and natural persons engaged in business activities. A code, consisting of a consecutive number and a control number, given to each party liable to register and by which the party can be identified; issued by NBPR (PRH).	PrintableString	'0245437-2'
localityName (mandatory)	{ id-at 7 }	An informative name of city, county or other geographic region where (headquarter of the) cerficate holder is located.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Jyväskylä'
stateOrProvinceName (mandatory)	{ id-at 8 }	An informative name of state. At FINEID context it is used as long form of subject's country name where (headquarter of the) cerficate holder is located.	DirectoryString: UTF8String. (including ISO Latin 8859-1 characters).	'Finland' 'Sweden'
countryName (mandatory)	{ id-at 6 }	Abbreviation for country	PrintableString	'FI'

SubjectAltName extension SHALL contain subject's email address (rfc822Name).

KeyUsage for email service certificates is digitalSignature, keyEncipherment, dataEncipherment (0xB0)

6.3.7. subjectPublicKeyInfo

This field is used to carry the public key and identify the algorithm with which the key is used (e.g. RSA or ECC).

RFC 5280 defines the **SubjectPublicKeyInfo** type as follows:

```
SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     subjectPublicKey     BIT STRING  }
```

The following algorithms shall be used:

1.2.840.113549.1.1.1 – rsaEncryption

1.2.840.10045.2.1 - ecPublicKey

In case of RSA, the value for the subjectPublicKey BIT STRING shall be the DER-encoding of the ASN.1 type **RSAPublicKey** defined in PKCS #1 v1.5:

```
RSAPublicKey ::= SEQUENCE {
   modulus            INTEGER,
   publicExponent     INTEGER
}
```

It should be noticed that if the most significant bit of the INTEGER value is set to 1, the value shall be interpreted as negative. If the modulus or public exponent should have the MSbit set to 1, an additional zero byte 00h shall be inserted as the most significant byte of the INTEGER value.

In case of ECC keys, the following curve shall be used:

Citizen certificates

1.2.840.10045.3.1.1.7 - secp256r1

1.3.132.0.34 - secp384r1

Organisational certificates,

Service Provider certificates,

Social Welfare and Healthcare Service Providers certificates and

Social Welfare and Healthcare Professional certificates

1.3.132.0.34 - secp384r1

6.3.8. Certificate extensions

This field is a SEQUENCE of one or more certificate extensions. The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing a certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry

information unique to those communities. Each extension in a certificate is designated as either critical or non-critical. A certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize; however, a non-critical extension MAY be ignored if it is not recognized. The following sections present recommended extensions used within FINEID certificates and standard locations for information.

RFC 5280 defines the **Extensions** type as follows:

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING  }
```

This FINEID S2 profile specifies some mandatory extensions in the table below. In addition, the criticality of each extension is also defined. The extensions that are not mandatory can be used with issuer's discretion (i.e. they are optional).

Extension name	FINEID S2		Used in VRK-FINEID environment
	Presence	Criticality	
Standard extensions			
authorityKeyIdentifier	**mandatory**	non-critical	**used**
subjectKeyIdentifier	**mandatory**	non-critical	**used**
keyUsage	**mandatory**	**critical**	**used**
certificatePolicies	**mandatory**	non-critical	**used**
subjectAltName	optional	non-critical	**used**
basicConstraints	**mandatory**	**critical**	**used**
cRLDistributionPoints	**mandatory**	non-critical	**used**
extKeyUsage	optional	non-critical	**used**
Private extensions			
authorityInformationAccess	**mandatory**	non-critical	**used**
qcStatements	**mandatory**	non-critical	**used** in non-repudiation qualified certificates; esign. **used** in server service certificates; web.

Additional extensions not listed above may be used, but they shall not be marked critical.

Mandatory and optional extensions of FINEID S2 are described in more detail below.

6.3.8.1. authorityKeyIdentifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.

RFC 5280 defines **authorityKeyIdentifier** extension as follows:

```
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 35 }

   AuthorityKeyIdentifier ::= SEQUENCE {
      keyIdentifier             [0] KeyIdentifier        OPTIONAL,
      authorityCertIssuer       [1] GeneralNames         OPTIONAL,
```

```
        authorityCertSerialNumber [2] CertificateSerialNumber
                                                    OPTIONAL  }
    KeyIdentifier ::= OCTET STRING
```

According to RFC 5280 this field is used to identify the public key to be used to verify the signature on this certificate or CRL. It enables distinct keys used by the same CA to be distinguished (e.g., as key updating occurs).

Only the **keyIdentifier** element shall be used.

This is a **non-critical** extension.

6.3.8.2. subjectKeyIdentifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key.

To facilitate certification path construction, this extension MUST appear in all conforming CA certificates, that is, all certificates including the basic constraints extension where the value of cA is TRUE. The value of the subject key identifier MUST be the value placed in the key identifier field of the Authority Key Identifier extension of certificates issued by the subject of this certificate.

For end entity certificates, the subject key identifier extension provides a means for identifying certificates containing the particular public key used in an application. Where an end entity has obtained multiple certificates, especially from multiple CAs, the subject key identifier provides a means to quickly identify the set of certificates containing a particular public key. To assist applications in identifying the appropriate end entity certificate, this extension SHOULD be included in all end entity certificates.

RFC 5280 defines **subjectKeyIdentifier** extension as follows:

```
KeyIdentifier ::= OCTET STRING

id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 14 }

SubjectKeyIdentifier ::= KeyIdentifier
```

According to RFC 5280 this field is used to identify the public key being certified. It enables distinct keys used by the same subject to be differentiated (e.g., as key updating occurs.).

This is a **non-critical** extension.

6.3.8.3. keyUsage

The key usage extension defines the purpose (e.g., encipherment, digital signature, certificate signing) of the key contained in the certificate. The usage restriction might be

employed when a key that could be used for more than one operation is to be restricted. For example, when an RSA key should be used only to verify signatures on objects other than public key certificates and CRLs, the digitalSignature or nonRepudiation bits would be asserted.

Likewise, when an RSA key should be used only for key management, the keyEncipherment bit would be asserted.

This extension MUST appear in certificates that contain public keys that are used to validate digital signatures on other public key certificates or CRLs.

RFC 5280 defines the **keyUsage** extension as follows:

```
id-ce-keyUsage OBJECT IDENTIFIER ::=  { id-ce 15 }

     KeyUsage ::= BIT STRING {
          digitalSignature        (0),
          nonRepudiation          (1),
          keyEncipherment         (2),
          dataEncipherment        (3),
          keyAgreement            (4),
          keyCertSign             (5),
          cRLSign                 (6),
          encipherOnly            (7),
          decipherOnly            (8) }
```

According to RFC 5280 this field indicates the purpose for which the certified public key is used.

The following key usages may be used for end entity certificates:

- **digitalSignature** When digital signatures are used but no non-repudiation services are required.
- **nonRepudiation** The public key shall be used to verify digital signatures used to provide a non-repudiation service. This bit shall not be combined with other bits.
- **keyEncipherment** The public key is used for key transport.
- **dataEncipherment** The public key is used for encrypting other user data than keys.
- **keyAgreement** The public key is used for key exchange.

This is a **critical** extension.

6.3.8.4. certificatePolicies

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.

Applications with specific policy requirements are expected to have a list of those policies, which they will accept, and to compare the policy OIDs in the certificate to that list.

RFC 5280 defines **certificatePolicies** extension as follows:

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::=  { id-ce 32 }

   anyPolicy OBJECT IDENTIFIER ::= { id-ce-certificate-policies 0 }

   CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF
                                              PolicyInformation

   PolicyInformation ::= SEQUENCE {
        policyIdentifier   CertPolicyId,
        policyQualifiers   SEQUENCE SIZE (1..MAX) OF
                                PolicyQualifierInfo OPTIONAL }

   CertPolicyId ::= OBJECT IDENTIFIER

   PolicyQualifierInfo ::= SEQUENCE {
        policyQualifierId  PolicyQualifierId,
        qualifier          ANY DEFINED BY policyQualifierId }

   -- policyQualifierIds for Internet policy qualifiers

   id-qt          OBJECT IDENTIFIER ::=  { id-pkix 2 }
   id-qt-cps      OBJECT IDENTIFIER ::=  { id-qt 1 }
   id-qt-unotice  OBJECT IDENTIFIER ::=  { id-qt 2 }

   PolicyQualifierId ::=
        OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )

   Qualifier ::= CHOICE {
        cPSuri           CPSuri,
        userNotice       UserNotice }

   CPSuri ::= IA5String

   UserNotice ::= SEQUENCE {
        noticeRef        NoticeReference OPTIONAL,
        explicitText     DisplayText OPTIONAL}

   NoticeReference ::= SEQUENCE {
        organization     DisplayText,
        noticeNumbers    SEQUENCE OF INTEGER }

   DisplayText ::= CHOICE {
        ia5String        IA5String      (SIZE (1..200)),
        visibleString    VisibleString  (SIZE (1..200)),
```

```
        bmpString       BMPString     (SIZE (1..200)),
        utf8String      UTF8String    (SIZE (1..200)) }
```

In an end entity certificate, these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.

This specification defines two policy qualifier types for use by certificate policy writers and certificate issuers. The qualifier types are the CPS Pointer and User Notice qualifiers.

The CPS Pointer qualifier contains a pointer to a Certification Practice Statement (CPS) published by the CA. The pointer is in the form of a URI.

User notice is intended for display to a relying party when a certificate is used. The application software SHOULD display all user notices in all certificates of the certification path used, except that if a notice is duplicated only one copy needs to be displayed.

FINEID:

The certificate policy of the CA defines whether this extension is single or multivalued.

This is a **non-critical** extension.

6.3.8.5. subjectAltName

The subject alternative names extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a DNS name, an IP address, and a uniform resource identifier (URI).

When the subjectAltName extension contains an Internet mail address, the address MUST be included as an rfc822Name. The format of an rfc822Name is an "addr-spec" as defined in RFC 822.

RFC 5280 defines **subjectAltName** extension as follows:

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }

   SubjectAltName ::= GeneralNames

   GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

   GeneralName ::= CHOICE {
        otherName                       [0]     OtherName,
        rfc822Name                      [1]     IA5String,
        dNSName                         [2]     IA5String,
        x400Address                     [3]     ORAddress,
        directoryName                   [4]     Name,
        ediPartyName                    [5]     EDIPartyName,
```

```
        uniformResourceIdentifier       [6]     IA5String,
        iPAddress                       [7]     OCTET STRING,
        registeredID                    [8]     OBJECT IDENTIFIER }

    OtherName ::= SEQUENCE {
        type-id    OBJECT IDENTIFIER,
        value      [0] EXPLICIT ANY DEFINED BY type-id }

    EDIPartyName ::= SEQUENCE {
        nameAssigner            [0]     DirectoryString OPTIONAL,
        partyName               [1]     DirectoryString }
```

To support proprietary Microsoft smart card logon functionality, authentication and encryption certificates for organisational and social welfare and healthcare professional usage contain also:

Subject Alternative Name = Other Name: Principal Name = (UPN)

The UPN OtherName OID is : "1.3.6.1.4.1.311.20.2.3"
The UPN OtherName value: Must be ASN1-encoded UTF8 string

Principal Name may be same as rfc822Name (certificate holder's valid email address) but it may also be another name form of the certificate holder that is used to identify users in Microsoft Active Directory.

For example:

UPN = user1@name.com
UPN = 1234567890@teonet.fi

Note: non-repudiation certificates do NOT contain Principal Name field.

This is a **non-critical** extension.

6.3.8.6. Basic Constraints

The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.

The cA boolean indicates whether the certified public key belongs to a CA.

The pathLenConstraint field is meaningful only if the cA boolean is asserted. In this case, it gives the maximum number of non-self-issued intermediate certificates that may follow this certificate in a valid certification path.

RFC 5280 defines **basicConstraints** extension as follows:

```
id-ce-basicConstraints OBJECT IDENTIFIER ::=  { id-ce 19 }
```

```
BasicConstraints ::= SEQUENCE {
     cA                      BOOLEAN DEFAULT FALSE,
     pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
```

This extension appears in all VRK's Root, intermediate CA and end entity certificates marked as **critical**.

6.3.8.7. extendedKeyUsage

This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates.

This extension is included into FINEID specification for software compatibility reasons only. Usage of this extension in software products is discouraged.

RFC 5280 defines **extendedKeyUsage** extension as follows:

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }

   ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

   KeyPurposeId ::= OBJECT IDENTIFIER
```

The following key usage purposes are defined:

```
id-kp-serverAuth             OBJECT IDENTIFIER ::= { id-kp 1 }
   -- TLS WWW server authentication

id-kp-clientAuth             OBJECT IDENTIFIER ::= { id-kp 2 }
   -- TLS WWW client authentication

id-kp-codeSigning            OBJECT IDENTIFIER ::= { id-kp 3 }
   -- Signing of downloadable executable code

id-kp-emailProtection        OBJECT IDENTIFIER ::= { id-kp 4 }
   -- E-mail protection

id-kp-timeStamping           OBJECT IDENTIFIER ::= { id-kp 8 }
   -- Binding the hash of an object to a time

id-kp-OCSPSigning            OBJECT IDENTIFIER ::= { id-kp 9 }
   -- Signing OCSP responses


Smart Card Logon OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.311.20.2.2 }
   -- Smart Card logon
```

This is a **non-critical** extension.

6.3.8.8. cRLDistributionPoints

The CRL distribution points extension identifies how CRL information is obtained. The cRLDistributionPoints extension is a SEQUENCE of DistributionPoint.

If the DistributionPointName contains multiple values, each name describes a different mechanism to obtain the same CRL. For example, the same CRL could be available for retrieval through both LDAP and HTTP.

Further discussion of CRL management is contained in section 7. Certificate and Authority Revocation Lists.

RFC 5280 defines **cRLDistributionPoints** extension as follows:

```
id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::=  { id-ce 31 }

   CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF
                                          DistributionPoint

   DistributionPoint ::= SEQUENCE {
        distributionPoint       [0]     DistributionPointName
                                                OPTIONAL,
        reasons                 [1]     ReasonFlags OPTIONAL,
        cRLIssuer               [2]     GeneralNames OPTIONAL }

   DistributionPointName ::= CHOICE {
        fullName                [0]     GeneralNames,
        nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }

   ReasonFlags ::= BIT STRING {
        unused                  (0),
        keyCompromise           (1),
        cACompromise            (2),
        affiliationChanged      (3),
        superseded              (4),
        cessationOfOperation    (5),
        certificateHold         (6),
        privilegeWithdrawn      (7),
        aACompromise            (8) }
```

This field identifies how CRL information is obtained. It is anticipated that the distributionPoint element of DistributionPoint SEQUENCE will contain a uniformResourceIdentifier (URI, element [6] of GeneralName CHOICE) pointing to the appropriate CRL for this certificate.

FINEID:

Examples of the URI containing an LDAP query pointing to the CRL:

- http://proxy.fineid.fi/crl/vrktpc.crl
- ldap://ldap.fineid.fi:389/cn%3dVRK%20CA%20for%20Test%20Purposes,ou%3dTestivarmenteet,o%3dVaestorekisterikeskus%20TEST,dmdName%3dFINEID,c%3dFI?certificateRevocationList
- All certificates contain HTTP CRL Distribution Point (CDP). The usage of LDAP CDP is deprecated.

This is a **non-critical** extension.

6.3.9. Private extensions

This section defines extension for use in the Internet Public Key Infrastructure. This extension may be used to direct applications to on-line information about the issuing CA or the subject. As the information may be available in multiple forms, each extension is a sequence of IA5String values, each of which represents a URI. The URI implicitly specifies the location and format of the information and the method for obtaining the information.

An object identifier is defined for the private extension. The object identifier associated with the private extension is defined under the arc id-pe within the arc id-pkix. Any future extensions defined for the Internet PKI are also expected to be defined under the arc id-pe.

```
id-pkix  OBJECT IDENTIFIER  ::=
               { iso(1) identified-organization(3) dod(6)
                 internet(1) security(5) mechanisms(5) pkix(7) }

      id-pe  OBJECT IDENTIFIER  ::=  { id-pkix 1 }
```

6.3.9.1. authorityInfoAccess

The authority information access extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears.

This profile defines two accessMethod OIDs: id-ad-caIssuers and id-ad-ocsp.

RFC 5280 defines **authorityInfoAccess** extension as follows:

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

   AuthorityInfoAccessSyntax  ::=
           SEQUENCE SIZE (1..MAX) OF AccessDescription

   AccessDescription  ::=  SEQUENCE {
           accessMethod          OBJECT IDENTIFIER,
           accessLocation        GeneralName  }
```

```
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }

id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }
```

The id-ad-caIssuers OID is used when the additional information lists CAs that have issued certificates superior to the CA that issued the certificate containing this extension. The referenced CA issuer's description is intended to help certificate users in the selection of a certification path that terminates at a point trusted by the certificate user. Except the Root CA certificate, all intermediate and end entity certificates contain caIssuers and OCSP attributes.

This is a **non-critical** extension.

6.3.9.2. qcStatements

Qualified Certificates Profile (ETSI EN 319 412-5) defines qcStatements extension as follows:

```
qcStatements  EXTENSION ::= {
          SYNTAX             QCStatements
          IDENTIFIED BY      id-pe-qcStatements }

      id-pe-qcStatements     OBJECT IDENTIFIER ::= { id-pe 3 }

      QCStatements ::= SEQUENCE OF QCStatement

      QCStatement ::= SEQUENCE {
          statementId   QC-STATEMENT.&Id({SupportedStatements}),
          statementInfo QC-STATEMENT.&Type
          ({SupportedStatements}{@statementId}) OPTIONAL }

       SupportedStatements QC-STATEMENT ::= {
              qcStatement-2 | esi4-qcStatement-1 | esi4-qcStatement-
              2 | esi4-qcStatement-3 | esi4-qcStatement-4 | esi4-
              qcStatement-5 | esi4-qcStatement-6, ...}
              (ETSI EN 319 412-5; Annex B (normative): ASN.1
              declarations)
```

According to Qualified Certificates Profile this section defines an extension for inclusion of predefined statements related to Qualified Certificates.

For example, a statement by the issuer that the certificate is issued as a Qualified Certificate is suitable for this extension. Other suitable statements for this extension are statements related to applicable legal jurisdiction within which the certificate is issued (e.g. a maximum reliance limit for the certificate indicating restrictions on CA's liability).

This extension is implemented in all Qualified Certificates. VRK uses the following ETSI defined statements:

```
id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }
id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
```

VRK encourages software developers to support the ETSI Qualified Certificate Statement extensions in software products.

More information about Certificate Profiles and Qualified Certificate Statement extensions can be found from ETSI EN 319 412 standards. Qualified Certificate Statements extension is defined in ETSI EN 319 412-5 standard:

- **ETSI EN 319 412-5 V2.2.1, Certificate Profiles; Part 5: QCStatements**

This is a **non-critical** extension.

7. Certificate and Authority Revocation Lists

For complete description of CRL content and syntax, see IETF RFC 5280.

Those parts of RFC 5280 that are implemented by VRK are listed here.

The X.509 v2 CRL syntax is as follows. For signature calculation, the data that is to be signed is ASN.1 DER encoded. ASN.1 DER encoding is a tag, length, value encoding system for each element.

```
   CertificateList  ::=  SEQUENCE  {
        tbsCertList          TBSCertList,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }

   TBSCertList  ::=  SEQUENCE  {
        version                 Version OPTIONAL,
                                     -- if present, MUST be v2
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate              Time,
        nextUpdate              Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE  {
             userCertificate         CertificateSerialNumber,
             revocationDate          Time,
             crlEntryExtensions      Extensions OPTIONAL
                                           -- if present, MUST be v2
                                   }  OPTIONAL,
        crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                           -- if present, MUST be v2
                                   }

   -- Version, Time, CertificateSerialNumber, and Extensions
   -- are all defined in section 7. Certificate and Authority
Revocation Lists

   -- AlgorithmIdentifier is defined in section 7. Certificate and
Authority Revocation Lists
```

7.1. CertificateList Fields

The CertificateList is a SEQUENCE of three required fields. The fields are described in detail in the following subsections.

7.1.1. tbsCertList

The first field in the sequence is the tbsCertList. This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the optional list of revoked certificates, and optional CRL extensions. When there are no revoked

certificates, the revoked certificates list is absent. When one or more certificates are revoked, each entry on the revoked certificate list is defined by a sequence of user certificate serial number, revocation date, and optional CRL entry extensions.

7.1.2. signatureAlgorithm

The signatureAlgorithm field contains the algorithm identifier for the algorithm used by the CRL issuer to sign the CertificateList.

This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertList.

The following algorithm SHALL be used:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

The temporary certificates issued by VRK CA for Temporary Certificates – G2 and VRK CA for Social Welfare and Healthcare Prof. Temp. Certs which are signed by VRK Gov. Root CA use the following cryptographic algorithm:

1.2.840.113549.1.1.11 - sha256WithRSAEncryption

7.1.3. signatureValue

The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is encoded as a BIT STRING and included in the CRL signatureValue field.

7.2. Certificate List "To Be Signed"

The certificate list to be signed, or TBSCertList, is a sequence of required and optional fields. The required fields identify the CRL issuer, the algorithm used to sign the CRL, the date and time the CRL was issued, and the date and time by which the CRL issuer will issue the next CRL.

Optional fields include lists of revoked certificates and CRL extensions. The revoked certificate list is optional to support the case where a CA has not revoked any unexpired certificates that it has issued. The profile requires conforming CRL issuers to use the CRL number and authority key identifier CRL extensions in all CRLs issued.

7.2.1. Version

This optional field describes the version of the encoded CRL. This field MUST be present and MUST specify version 2 (the integer value is 1).

7.2.2. Signature

This field contains the algorithm identifier for the algorithm used to sign the CRL.

This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence CertificateList.

The following algorithm SHALL be used:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

The temporary certificates issued by VRK CA for Temporary Certificates – G2 and VRK CA for Social Welfare and Healthcare Prof. Temp. Certs which are signed by VRK Gov. Root CA use the following cryptographic algorithm:

1.2.840.113549.1.1.11 - sha256WithRSAEncryption

7.2.3. Issuer Name

The issuer name identifies the entity that has signed and issued the CRL. The issuer identity is carried in the issuer name field.

7.2.4. This Update

This field indicates the issue date of this CRL. ThisUpdate may be encoded as UTCTime or GeneralizedTime.

CRL issuers conforming to this profile MUST encode thisUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode thisUpdate as GeneralizedTime for dates in the year 2050 or later.

7.2.5. Next Update

This field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date. CRL issuers SHOULD issue CRLs with a nextUpdate time equal to or later than all previous CRLs. nextUpdate may be encoded as UTCTime or GeneralizedTime.

CRL issuers conforming to this profile MUST encode nextUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode nextUpdate as GeneralizedTime for dates in the year 2050 or later.

7.2.6. Revoked Certificates

When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers. Certificates revoked by the CA are uniquely identified by the certificate serial number. The date on which the revocation occurred is specified. The time for revocationDate MUST be expressed. Additional information may be supplied in CRL entry extensions.

7.3. Extensions

This field is a sequence of one or more CRL extensions.

7.3.1. CRL Extensions

The extensions defined by ITU-T for X.509 v2 CRLs provide methods for associating additional attributes with CRLs. The X.509 v2 CRL format also allows communities to define private extensions to carry information unique to those communities. Each extension in a CRL may be designated as critical or non-critical. A CRL validation MUST fail if it encounters a critical extension which it does not know how to process. However, an unrecognized non-critical extension may be ignored. The following subsections present those extensions used within VRK CRLs.

7.3.1.1. Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. The identification can be based on either the key identifier (the subject key identifier in the CRL signer's certificate) or on the issuer name and serial number. This extension is especially useful where an issuer has more than one signing key, either due to multiple concurrent key pairs or due to changeover.

7.3.1.2. CRL Number

The CRL number is a non-critical CRL extension which conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer. This extension allows users to easily determine when a particular CRL supersedes another CRL. CRL numbers also support the identification of complementary complete CRLs and delta CRLs.

Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle CRLNumber values up to 20 octets.

```
id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }

CRLNumber ::= INTEGER (0..MAX)
```

7.3.1.3. Issuing Distribution Point

The issuing distribution point is a critical CRL extension that identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes. Although this extension is critical, conforming implementations are not required to support this extension.

If the distributionPoint field is absent, the CRL MUST contain entries for all revoked unexpired certificates issued by the CRL issuer, if any, within the scope of the CRL.

```
id-ce-issuingDistributionPoint OBJECT IDENTIFIER ::= { id-ce 28 }

issuingDistributionPoint ::= SEQUENCE {
     distributionPoint          [0] DistributionPointName OPTIONAL,
     onlyContainsUserCerts      [1] BOOLEAN DEFAULT FALSE,
     onlyContainsCACerts        [2] BOOLEAN DEFAULT FALSE,
     onlySomeReasons            [3] ReasonFlags OPTIONAL,
     indirectCRL                [4] BOOLEAN DEFAULT FALSE,
     onlyContainsAttributeCerts [5] BOOLEAN DEFAULT FALSE }
```

7.3.2. CRL Entry Extensions

The CRL entry extensions defined by ITU-T for X.509 v2 CRLs provide methods for associating additional attributes with CRL entries. Each extension in a CRL entry may be designated as critical or non-critical. A CRL validation MUST fail if it encounters a critical CRL entry extension which it does not know how to process. However, an unrecognized non-critical CRL entry extension may be ignored.

All CRL entry extensions used in this specification are non-critical. Support for these extensions is optional for conforming CRL issuers and applications. However, CRL issuers SHOULD include reason codes and invalidity dates whenever this information is available.

7.3.2.1. Reason Code

The reasonCode is a non-critical CRL entry extension that identifies the reason for the certificate revocation. CRL issuers are strongly encouraged to include meaningful reason codes in CRL entries.

```
id-ce-cRLReason OBJECT IDENTIFIER ::= { id-ce 21 }

-- reasonCode ::= { CRLReason }

CRLReason ::= ENUMERATED {
     unspecified             (0),
     keyCompromise           (1),
     cACompromise            (2),
     affiliationChanged      (3),
     superseded              (4),
     cessationOfOperation    (5),
     certificateHold         (6),
     removeFromCRL           (8),
     privilegeWithdrawn      (9),
     aACompromise           (10) }
```

7.3.2.2. Invalidity Date

The invalidity date is a non-critical CRL entry extension that provides the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the CRL entry, which is the date at which the CA processed the revocation. When a revocation is first posted by a CRL issuer in a CRL, the invalidity date may precede the date of issue of earlier CRLs, but the revocation date SHOULD NOT precede the date of issue of earlier CRLs.

The GeneralizedTime values included in this field MUST be expressed in Greenwich Mean Time (Zulu).

```
id-ce-invalidityDate OBJECT IDENTIFIER ::= { id-ce 24 }

invalidityDate ::=  GeneralizedTime
```

8. Summary Tables

8.1. Common subject and issuer attributes

Detailed information can be found in IETF RFCs 5280, 4512, 4519, 4523, 4524, and FINEID S5 specifications.

Contents of the attribute types are encoded in certificates as Printable Strings or UTF8 Strings using ISO Latin-1 (8859.1) character set.

For backward compatibility reasons software implementations SHALL support Latin-1 character set encoded as Teletext/T.61 and UTF8 string.

Software implementations SHALL recognize the following attributes.

```
id-at OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 4 }
id-ce OBJECT IDENTIFIER  ::= {joint-iso-ccitt(2) ds(5) 29}

id-at-commonName        AttributeType ::= { id-at 3 }
id-at-surname           AttributeType ::= { id-at 4 }
id-at-givenName         AttributeType ::= { id-at 42 }
id-at-serialNumber      AttributeType ::= { id-at 5 }
id-at-title             AttributeType ::= { id-at 12 }
id-at-pseudonym         AttributeType ::= { id-at 65 }
id-at-organizationalUnitName AttributeType ::= { id-at 11 }
id-at-organizationName  AttributeType ::= { id-at 10 }
id-at-stateOrProvinceName AttributeType ::= { id-at 8 }
id-at-localityName      AttributeType ::= { id-at 7 }
id-at-countryName       AttributeType ::= { id-at 6 }
id-at-dmdName           AttributeType ::= { id-at 54 }
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }
     -- for email addresses
```

Other attributes may be used.

9. Certificate information summary

Root and CA certificates:

Issuer Name	Certificate type	Signed by	Valid from	Valid until	Key length
VRK Gov. Root CA – G2	Root certificate	VRK Gov. Root CA – G2	14.12.2017	13.12.2038	4096
VRK Gov. CA for Citizen Certificates – G3	CA certificate	VRK Gov. Root CA – G2	3.5.2018	2.5.2038	4096
VRK CA for Organisational Certificates – G3	CA certificate	VRK Gov. Root CA – G2	3.5.2018	2.5.2038	4096
VRK CA for Service Providers – G4	CA certificate	VRK Gov. Root CA – G2	3.5.2018	2.5.2038	4096
VRK CA for Temporary Certificates – G2	CA certificate	VRK Gov. Root CA	3.5.2018	18.12.2023	4096
VRK CA for Social Welfare and Healthcare Service Providers – G2	CA certificate	VRK Gov. Root CA – G2	3.5.2018	2.5.2038	4096
VRK CA for Social Welfare and Healthcare Professionals Prof. Certs	CA certificate	VRK Gov. Root CA – G2	3.5.2018	2.5.2038	4096
VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	CA certificate	VRK Gov. Root CA	3.5.2018	18.12.2023	4096
VRK CA for Time Stamp Services	CA certificate	VRK Gov. Root CA – G2	3.5.2018	2.5.2038	4096

End entity certificates:

Issuer Name	Certificate type	Signed by	Validity period	Key length
VRK Gov. CA for Citizen Certificates – G3	Personal Citizen certificate	VRK Gov. CA for Citizen Qualified Certificates – G3	max. 5 years	2048/ EC256, EC384
VRK CA for Organisational Certificates – G3	Organisational certificate	VRK CA for Organisational Certificates – G3	max. 5 years	2048, 3072/ EC384
VRK CA for Service Providers – G4	Service certificate	VRK CA for Service Providers – G4	max 2 years	2048, 3072, 4096/ EC384
VRK CA for Temporary Certificates – G2	Personal certificate	VRK CA for Temporary Certificates – G2	max. 3 months	2048, 3072
VRK CA for Social Welfare and Healthcare Service Providers – G2	Service certificate	VRK CA for Social Welfare and Healthcare Service Providers – G2	max. 2 years	2048, 3072, 4096/ EC384
VRK CA for Social Welfare and Healthcare Prof. Certs	Personal certificate	VRK CA for Social Welfare and Healthcare Prof. Certs	max. 5 years	2048, 3072/ EC384
VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	Personal certificate	VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	max. 3 months	2048, 3072
VRK CA for Time Stamp Services	Time Stamp certificate	VRK CA for Time Stamp Services	max. 5 years	2048, 3072

Test Root and CA certificates:

Issuer Name	Certificate type	Signed by	Valid from	Valid until	Key length
VRK TEST Root CA – G2	TEST Root certificate	VRK TEST Root CA – G2	11.10.2017	11.10.2038	4096
VRK TEST CA for Test Purposes – G4	Test CA certificate	VRK TEST Root CA – G2	9.2.2018	10.10.2038	4096
VRK TEST CA for Service Providers	Test CA certificate	VRK TEST Root CA – G2	9.2.2018	10.10.2038	4096
VRK TEST CA for Social Welfare and Healthcare Prof. Certs	Test CA certificate	VRK TEST Root CA – G2	9.2.2018	10.10.2038	4096
VRK TEST CA for Social Welfare and Healthcare Service Prov. – G2	Test CA certificate	VRK TEST Root CA – G2	9.2.2018	10.10.2038	4096
VRK TEST CA for Time Stamp Services	Test CA certificate	VRK TEST Root CA – G2	5.4.2018	10.10.2038	4096

Test end entity certificates:

Issuer Name	Certificate type	Signed by	Validity period	Key length
VRK TEST CA for Test Purposes – G4	Test certificate	VRK Test CA for Test Purposes – G4	max. 5 years	2048, 3072/ EC256, EC384
VRK TEST CA for Service Providers	Test service certificate	VRK TEST CA for Service Providers	max. 2 years	2048, 3072, 4096/ EC384
VRK TEST CA for Social Welfare and Healthcare Prof. Certs	Test personal certificate	VRK TEST CA for Social Welfare and Healthcare Prof. Certs	max. 5 years	2048, 3072, 4096/ EC384
VRK TEST CA for Social Welfare and Healthcare Service Providers – G2	Test service certificate	VRK TEST CA for Social Welfare and Healthcare Service Providers – G2	max. 2 years	2048, 3072, 4096/ EC384
VRK TEST CA for Time Stamp Services	Test time stamp certificate	VRK TEST CA for Time Stamp Services	max. 5 years	2048, 3072

9.1. Root and CA Certificate Fingerprints (signature hashes)

Root and CA certificates:

	SHA-1 (160 bit)	SHA-256 (256 bit)
VRK Gov. Root CA – G2	F4:35:F8:5F:01:08:DA:68:4E:7B FD:51:7C:90:C6:27:BB:9A:6C:F5	34:FF:2A:44:09:DC:13:83:E9:F8 96:6E:8A:DF:E5:71:9E:BA:37:3F D0:AD:5E:2F:49:F9:0E:E0:7C:F5 D4:C1
VRK Gov. CA for Citizen Certificates – G3	CD:AE:65:03:D6:11:A4:86:F3:91 EF:4A:76:4A:5F:32:DB:E0:BF:DA	39:A8:35:B1:4B:6B:63:13:F7:78: 37:1C:79:CB:43:4D:D5:18:C8:FD: 32:5B:74:9D:9B:E6:69:DF:F2:03: 84:E8
VRK CA for Organisational Certificates – G3	32:6A:38:8B:4A:5C:3C:06:AC:F0 8F:49:5F:3B:29:50:0F:14:EC:9D	9C:0B:9E:BE:A9:55:90:D0:FA:FE: 4A:46:C6:2E:49:DD:0B:A6:CC:0A: 80:F8:90:19:A2:3D:03:7E:1A:4C: 1B:5B
VRK CA for Service Providers – G4	76:92:0B:96:96:D2:AF:C1:14:2F 11:6D:D1:1A:CD:7E:1D:B6:1E:97	1B:D3:87:0B:84:2F:F0:A6:37:28: 42:68:01:7E:18:E4:55:A7:FD:2D: 84:46:8F:3C:DF:7D:58:7C:7A:B3: 5C:9D
VRK CA for Temporary Certificates – G2	29:A0:19:98:B2:2F:7D:B6:E7:B0 B2:8B:6D:18:B0:CC:A1:01:55:AB	C0:1B:0D:65:E0:87:05:0D:2F:88: BB:14:35:1C:8A:57:30:44:C1:E1: 6E:0D:E5:CC:56:26:93:A2:CD:8A: DA:FD
VRK CA for Social Welfare and Healthcare Prof. Certs	2E:F8:3E:44:98:38:59:67:ED:D3 DD:57:99:69:F9:91:A0:58:52:CF	0E:83:9E:E6:8B:1E:EF:72:1D:31: E6:2E:58:9E:69:2C:03:18:0F:AA: DA:DE:48:A7:18:37:C2:50:90:B3: AC:C4
VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	DA:8B:B2:D3:E2:9B:61:81:B0:B1 97:77:46:89:63:7A:65:E3:AC:F9	61:F6:60:85:1B:6A:55:24:DE:F0: CB:9E:9E:A5:6F:68:8A:80:0D:F9: EA:18:29:CC:6D:02:98:20:72:B1: AF:A5
VRK CA for Social Welfare and Healthcare Service Providers – G2	87:25:10:FB:0D:14:39:6C:4F:36 C8:A1:4A:68:8E:3D:07:ED:78:A4	A6:B3:4F:7B:0E:87:44:63:62:BB: 1A:2B:F3:EE:95:DD:56:D8:BA:97: A9:FF:B0:3D:F4:10:31:37:7E:CD: D6:F8
VRK CA for Time Stamp Services	A0:E1:B3:D8:B8:8B:F6:76:F6:1A 74:C9:78:71:89:D0:1C:E5:79:01	95:FF:59:29:D6:01:B1:C5:23:9D: 04:5B:41:03:DB:F8:04:FE:8B:C5: D8:F3:BA:86:16:C3:2B:23:00:00: 64:0F

Test Root and CA certificates:

	SHA-1 (160 bit)	SHA-256 (256 bit)
VRK TEST Root CA – G2	C2:A1:5A:DE:44:91:BD:5D:E2:8D 56:47:0F:50:5E:F5:15:D8:D2:35	E1:82:3B:D1:00:2B:CA:77:52:A5 2F:5B:AD:A6:57:E4:68:98:57:D4 49:21:8F:87:EE:18:B6:D4:96:3E BB:B6
VRK TEST CA for Test Purposes – G4	78:C2:B0:8A:3D:4B:0A:0E:E8:50 29:C0:F1:6C:B8:B2:FC:D9:F6:DD	25:1F:45:B0:18:FF:59:08:15:45: CC:68:32:4D:42:A1:24:0A:D3:1C: 59:59:24:F5:53:13:4F:4B:A6:5C: 3A:DB
VRK TEST CA for Service Providers	5C:ED:A0:50:19:D1:AE:5E:AE:77 E3:A0:FE:1D:62:9F:99:32:26:E0	6E:DF:B5:0A:5C:DD:BA:FB:B5:DF: 15:88:EC:9E:36:35:95:0C:66:36: 83:1D:18:E1:53:8A:F3:4A:A2:69: 40:F3
VRK TEST CA for Social Welfare and Healthcare Prof. Certs	BF:5E:74:18:96:6A:7F:DA:27:AE 5D:A4:F1:4B:61:14:15:EA:0A:29	2A:41:10:82:E5:F2:C9:AB:04:34: 3E:46:B5:71:5E:7A:36:C5:94:87: 24:B5:7B:12:4B:3D:E7:32:8E:EF: 69:9E

VRK TEST CA for Social Welfare and Healthcare Service Prov. – G2	06:9E:C9:39:65:76:82:4D:C5:EC 8C:5A:64:60:66:3C:31:2D:7C:5B	7F:89:99:03:E1:D4:E8:62:2C:6B: 6B:8D:75:9A:FD:50:D8:D6:AD:B1: ED:1E:5A:7A:90:95:F8:41:C3:72: 44:F2
VRK TEST CA for Time Stamp Services	0A:62:F8:8E:6D:6B:94:69:BF:AB E0:B6:F4:EB:29:97:BC:96:7E:6B	33:20:5C:FD:45:03:92:DA:FF:1F: D2:F4:F2:9F:7B:55:5A:51:89:4E: A4:64:D6:CB:A4:57:80:52:25:FE: C3:95

Current software products use typically SHA-1 or SHA-256 fingerprints.

Older software products might still use MD5 fingerprints but use of MD5 is discouraged, thus MD5 fingerprints are excluded.

9.2. Root and CA Certificate AIA and CDP uris

Root and CA certificates:

CA	Authority Information Access-calssuers
VRK Gov. Root CA – G2	http://proxy.fineid.fi/ca/vrkroot2c.crt
VRK Gov. CA for Citizen Certificates – G3	http://proxy.fineid.fi/ca/vrkcqc3.crt
VRK CA for Organisational Certificates – G3	http://proxy.fineid.fi/ca/vrkqc3.crt
VRK CA for Service Providers – G4	http://proxy.fineid.fi/ca/vrksp4.crt
VRK CA for Temporary Certificates – G2	http://proxy.fineid.fi/ca/vrktc2.crt
VRK CA for Social Welfare and Healthcare Prof. Certs	http://proxy.fineid.fi/ca/vrkshp.crt
VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	http://proxy.fineid.fi/ca/vrkshpt.crt
VRK CA for Social Welfare and Healthcare Service Providers - G2	http://proxy.fineid.fi/ca/vrkshsp2.crt
VRK CA for Time Stamp Services	http://proxy.fineid.fi/ca/vrktss.crt

Test Root and CA certificates:

CA	Authority Information Access-calssuers
VRK TEST Root CA – G2	http://proxy.fineid.fi/ca/vrktest2c.crt
VRK TEST CA for Test Purposes – G4	http://proxy.fineid.fi/ca/vrktp4.crt
VRK TEST CA for Service Providers	http://proxy.fineid.fi/ca/vrktsp.crt
VRK TEST CA for Social Welfare and Healthcare Prof. Certs	http://proxy.fineid.fi/ca/vrktshcp.crt
VRK TEST CA for Social Welfare and Healthcare Service Prov. – G2	http://proxy.fineid.fi/ca/vrktshsp2.crt
VRK TEST CA for Time Stamp Services	http://proxy.fineid.fi/ca/vrkttss.crt

Root and CA certificates:

CA	ARL/CRL distribution points
VRK Gov. Root CA – G2	http://proxy.fineid.fi/arl/vrkroot2a.crl
VRK Gov. CA for Citizen Certificates – G3	http://proxy.fineid.fi/crl/vrkcqc3c.crl
VRK CA for Organisational Certificates – G3	http://proxy.fineid.fi/crl/vrkqc3c.crl
VRK CA for Service Providers – G4	http://proxy.fineid.fi/crl/vrksp4c.crl
VRK CA for Temporary Certificates – G2	http://proxy.fineid.fi/crl/vrktc2c.crl
VRK CA for Social Welfare and Healthcare Prof. Certs	http://proxy.fineid.fi/crl/vrkshpc.crl
VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	http://proxy.fineid.fi/crl/vrkshptc.crl
VRK CA for Social Welfare and Healthcare Service Providers - G2	http://proxy.fineid.fi/crl/vrkshsp2c.crl
VRK CA for Time Stamp Services	http://proxy.fineid.fi/crl/vrktssc.crl

Test Root and CA certificates:

CA	ARL/CRL distribution points
VRK TEST Root CA – G2	http://proxy.fineid.fi/arl/vrktest2a.crl
VRK TEST CA for Test Purposes – G4	http://proxy.fineid.fi/crl/vrktp4c.crl
VRK TEST CA for Service Providers	http://proxy.fineid.fi/crl/vrktspc.crl
VRK TEST CA for Social Welfare and Healthcare Prof. Certs	http://proxy.fineid.fi/crl/vrktshcpc.crl
VRK TEST CA for Social Welfare and Healthcare Service Prov. – G2	http://proxy.fineid.fi/crl/vrktshsp2c.crl
VRK TEST CA for Time Stamp Services	http://proxy.fineid.fi/crl/vrkttssc.crl

9.3. CA Certificate OCSP URLs

CA	Authority Information Access-calssuers
VRK Gov. Root CA – G2	http://ocsp.fineid.fi/vrkroot2c
VRK Gov. CA for Citizen Certificates – G3	http://ocsp.fineid.fi/vrkcqc3
VRK CA for Organisational Certificates – G3	http://ocsp.fineid.fi/vrkqc3
VRK CA for Service Providers – G4	http://ocsp.fineid.fi/vrksp4
VRK CA for Temporary Certificates – G2	http://ocsp.fineid.fi/vrktc2
VRK CA for Social Welfare and Healthcare Prof. Certs	http://ocsp.fineid.fi/vrkshp
VRK CA for Social Welfare and Healthcare Prof. Temp. Certs	http://ocsp.fineid.fi/vrkshpt
VRK CA for Social Welfare and Healthcare Service Providers - G2	http://ocsp.fineid.fi/vrkshsp2
VRK CA for Time Stamp Services	http://ocsp.fineid.fi/vrktss

Test CA certificates:

CA	Authority Information Access-calssuers
VRK TEST Root CA – G2	http://ocsptest.fineid.fi/vrktest2c
VRK TEST CA for Test Purposes – G4	http://ocsptest.fineid.fi/vrktp4
VRK TEST CA for Service Providers	http://ocsptest.fineid.fi/vrktsp
VRK TEST CA for Social Welfare and Healthcare Prof. Certs	http://ocsptest.fineid.fi/vrktshcp
VRK TEST CA for Social Welfare and Healthcare Service Prov. – G2	http://ocsptest.fineid.fi/vrktshsp2
VRK TEST CA for Time Stamp Services	http://ocsptest.fineid.fi/vrkttss

10. Root, CA and End Entity Certificate examples and example of Certificate Revocation List

Some examples of different types of certificates are provided here for a reference.

10.1. Root Certificate

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  220000; -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Certification Authority Services" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Varmennepalvelut" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST Root CA - G2" }
            }
         }
      },
      SEQUENCE {
```

```
      UTCTime { "171011100332Z" }, -- not before
      UTCTime { "381011100332Z" }  -- not after
   },
   SEQUENCE {
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
            PrintableString =  "FI";
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
            UTF8String { "Vaestorekisterikeskus TEST" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
            UTF8String { "Certification Authority Services" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
            UTF8String { "Varmennepalvelut" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String { "VRK TEST Root CA - G2" }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
         NULL =  "NULL";
      },
      BIT_STRING [ PRIMITIVE ] {
         #00,
         SEQUENCE {
            INTEGER {
               #00A5DD721A087DE9C983F4A5723AB3C3D9E46273CEB42858ED295182C5
               8E69EB5DCDC3F869C78EB29C7480D33640901C35AD1019D7CFCC0947EAF3
               E624610D4CF589F6A0365DC6B78FBAFF18EFF8792E8A5D80902467CE200E
               96DFD75749265E1E7A1C7C0985D1CB61BFCF7EEE13306E54BCFA4AB782F5
```

```
                  F95D7C4C2BAC06467F63B942F7C13400F5419D4765AE3F8DA9F1F8B4B77D
                  5DBDB533E4A0D1F64FD89521AE8C8CD69779AE78BD5FF3C7CB2BA7A2D887
                  F09E02E2F1EF7CC4D2A3D01842527DD0408632EE0A8CB78738FD4B0CD38A
                  D033A4A1251A201EC70F2EB929D1229AA8145EBABF0CB8FBBDFD4F94C83C
                  9C5D45DE2FABEAA9252322E4D1E8E827CD495CC0C6E2A7E41328E48AB185
                  690E5B37FE247439BC4282DB58DC8A0E4DA5BF524643F628E9630F94A8EA
                  F3C175ED7B5A39C33606CA4BCD0B07993EBDD4A3A9A5059602F67B121D01
                  0AB494DBDD0AA11468A774BD31BF5A8F6EE847A0D1CA31BE995C2E69E171
                  6D08FC963A6907B84CDE78FDE808A1B0045166B5EB27F849207FA39079AD
                  7F3E22FC5FABA64EBF90604851B9FBF64D4FCE312C105B0BA6ABDC30F593
                  9F3941736B8BBAF82BF5505EEFEF76F3EED505E93A50A9955F8B75681476
                  786E89F2CDF4212C653AB34172334FBF19FA03C326151B459FD4023ECFF8
                  F6E57E1F2677190783C308029088852394O6D49350233EFB0B7D934F2BD6
                  A22DF7A1
               },
               INTEGER =  65537; -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#853DA0E1FCB10927E4DABD1F868B400672420A81 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#853DA0E1FCB10927E4DABD1F868B400672420A81 } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #01, #06 } -- digitalSignature, nonRepudiation, keyCertSign,
cRLSign


               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #FF } -- CA Certificate=True
```

```
            }
         }
      }
   }
},
SEQUENCE {
   OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
   NULL =  "NULL";
},
BIT_STRING {
   #00,
   #13B430B45E81FF63AAE04D40E9A8FAF60CAA20AE55EF72AE99FD5AA3D8
   364D40B7350C9C8FC02243526909841DBD5AE6DAEABF457C01ADE1C287A7
   6AD9E6A5DA817DAC348803BBAB70CC0CAA071FC8DDB4E68526A33F36E855
   5AD9669863BAEEB49039617D853A0BC948F568D3CDC4DCADB64DC1E7A625
   8C997FCAE0A1ECDAC8ECDF31F32057712718712600417238 3E68F517C7E0
   9B34530AA1C1A41E77F93635CACEE8E2AEA498F1A4D8A9ED5D7FFB7300E5
   F96C8B9A52F5587879B42EA8A1BC718ADA5E9C02D89631DA75414AF08C42
   80340452BCD62514B82CA005D977880EC3401EF6C513094B5509407CDF74
   3DA163D556D86C8D23DA4CA1C00E4685D0B9E80327E8A55EF5DDB3D1CBC2
   28CF5303B8CA666A780808E9E4182C0B1C98DB75DE927635B1575316849E
   4557F981323F9E28572FBDA42434ECFB5FACC61F06673175F7E9A8D842EF
   B47736386735CC442485A83EA7125E9A523044F8BCAA126DB79C91695D1D
   9093C2411747B5076E56F89E4358751F1815F087F1C5AE1913E846D87715
   1C6F6A344E1DD70416614180F91C0E676233E99F200753CA02011E0CEEF7
   4D48650D446BEA3939227DFE5C048C182E5AFC4F4AE24A5E37669A4BD747
   8ED2F62AEDCC465C3F04D800BFEB277BAB7DBD0B336C63D472F0883D076C
   B9DD75FC4B0EDCAE6DF4ECCA0E13590B6E469A33FCC39A7133E89FA0FF2C
   188DF5
}
}
```

10.2. CA Certificate

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  220003; -- x509v3 certificate
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Certification Authority Services" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Varmennepalvelut" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST Root CA - G2" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180209100624Z" }, -- not before
         UTCTime { "381010100624Z" }  -- not after
      },
      SEQUENCE {
```

```
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
            PrintableString =  "FI";
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
            UTF8String { "Vaestorekisterikeskus TEST" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
            UTF8String { "Testivarmenteet" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String { "VRK TEST CA for Test Purposes - G4" }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
         NULL =  "NULL";
      },
      BIT_STRING [ PRIMITIVE ] {
         #00,
         SEQUENCE {
            INTEGER {
               #00C682B44AC08BE61A9E9DE3631A44B8A07006479FD3338A1DBCACF26D
               ECBC877B8AEEB1A55A32710D241A5E4C2D722346E08D32142703FA56627E
               F7FF8830CD0D195AF2F79F71E28E6A86BA1D6486C58720277DC828D41803
               0E734CB096C9CFEFCA291E98C208EAE36C8DDD9140439E642871214FA321
               E7D0247617E721DDE98955D767B28564FC4248CB3EADE9A9AA2375149346
               E07048E313A1C2E61E54F2A1930255B4282D508ED601B66596F3579AB3A2
               75375873CF64555EF7EC3989F5C3201807F09B6BD7C8EB403A32F16A87F9
               815AC5D69D7DFFAE9C3CDD94B435A7D95BF4DEBA01DABBE7224DEA653836
               BAC73B1403EC575729F764BFEA0AF66981559CCCDEBC64DDFAF47742D7EE
               DE6BB4B6DDACB5A24CB5A209FD521101E22AC5CC4AF670A3985C71CB0039
               87345620108D6412145E0254CCE1F2679DD80660373E0FEF6145BF93BEDB
               365DDAAE520BEB9B95B79ECABDE229B831A808C233DDBE2B172C7DFAD7DE
               853396586572EC8BB3C11B28C6DC280B06361854F87A1BED9D1E99302F39
               51C50E20B347A1238FCFBCEDD2A0DA37DBDE0E6402B62ADA92DFA7A66630
```

```
                03F932226E69526A6C57F711B61767B65A0608E72E3A83FEC25A45871B30
                756D99D2E611E1DE4A34E928D22F750F13F9BF8D7F05A2C69694C869D87D
                25BC54DFACB5F1F099A5717FA48E20AF42FD3BD28AAB7E409E0AAD57CEBC
                FB746A17
             },
             INTEGER =  65537; -- exponent
          }
       }
    },
    CONTEXT_SPECIFIC [ 3 ] {
       SEQUENCE {
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
             OCTET_STRING [ PRIMITIVE ] {
                SEQUENCE {
                   CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#853DA0E1FCB10927E4DABD1F868B400672420A81 }
                }
             }
          },
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
             OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 } }
          },
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
             BOOLEAN =  #FF; -- critical
             OCTET_STRING [ PRIMITIVE ] {
                BIT_STRING { #01, #06 } -- keyCertSign, cRLSign
             }
          },
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
             OCTET_STRING [ PRIMITIVE ] {
                SEQUENCE {
                   SEQUENCE {
                            OBJECT_IDENTIFIER { "1.2.246.517.99.10.201.1" }, -- VRK Test
    Purposes G4 CPS
                      SEQUENCE {
                         SEQUENCE {
                            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                            SEQUENCE {
                               VisibleString {
                                  "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                               }
                            }
                         },
```

```
                        SEQUENCE {
                           OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                           IA5String { "http://www.fineid.fi/cps99/" }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     BOOLEAN =  #FF; -- CA Certificate=True
                     INTEGER =  0; -- pathLenConstraint
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
                                 "http://proxy.fineid.fi/arl/vrktest2a.crl"
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority
      Information Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" },
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktest2c" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA issuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktest2c.crt" }
```

```
                    }
                 }
              }
           }
        }
     }
  },
  SEQUENCE {
     OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
     NULL =  "NULL";
  },
  BIT_STRING {
     #00,
     #1478BCE5316AB5647C99B04319AA4B2D1E1F175E2E6F2CA50024431E92
     5AA762DF4BCA752C1D859210DAB2FA872C38980998479D902BC078A1241A
     E252568E71F721C3264B5C9B04B4346A74CBB470C3A56CAB803A77C096FB
     BA26AAE6C26CE134DB08E766B432194FECBE50C33D92BA2641284338EA9C
     94AF64AB64C3F7766E1871607FB90261D24326FF231DD2526DDA7F462743
     FD24C29ECD279B714A02DA942BC87621212AB9647DBC755F490ABED0FE7B
     CCC59F9CC36851B1C4E6BBF7DB63B9ABD7A9DF02C6E1B3C37C802883674F
     8F25674EAEDCF4776A219335716055C433B409DFA847279FDC90CF4B6A5B
     FF6CEF1345A1B785E0D138E61137536FA8412FFA4D5F6E00DE588F302E9F
     717E135E3F2AB97058D5B35984BB154B447434F25082987A66C662B5F87E
     830513139B46F950E9B7D6216A2FDB7C4D1171840CCF9DC44FE6FA6BD175
     FB60B2AE681C957071901737CB3EF2AD2F33AB606FF980C2684194B1AD20
     5F515A67FBA462C24F89DB5BA61A5EDAB2DCB5E16F52D1021020DDC3B726
     A6ED6B6415A434F669DD57195C24B7A27F81CC93E623C91C716E7F3FAA6E
     BDFE416B5526151C50CD453CCDDE0BA47115FE8AB021115B05AD5426040E
     1BC7399E787F06E1C270706B0ACFF768C3127706E576D4CA4B1C6E9847A9
     AD21751B671CEC8DD1E8B6886D671989EA7DB2E6742D196EC4E96263C913
     7141BD
  }
}
```

10.3. Citizen Certificate - Authentication & Encryption (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  101500033;
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180704100546Z" }, -- not before
         UTCTime { "230705235959Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
```

```
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
            PrintableString { "123456789" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
            UTF8String { "Teppo" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
            UTF8String { "Testaaja" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String { "Testaaja Teppo 123456789" }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
         NULL =  "NULL";
      },
      BIT_STRING [ PRIMITIVE ] {
         #00,
         SEQUENCE {
            INTEGER {
               #00E4B4D170D28DA7CD14418B9E9BCD7A5DD9D0D03EB86E6E0427E053A3
               53656D75E71FA517D47C2ED82FA77B0F1B77E03ED6D8E0AA725C30D074DF
               D2FDE07F4E671F5F4333900563DE34AE83D2BA8432B0AE2BA02C8DBF90FB
               E653CD076D99236868A5C1E55CD08278D3C8FBCBF462F6FE7E0BC81390B9
               3BA54AC69C9327DF9E330F77656805755141DAD01E826C8A02970B545FF9
               C631D23F428037EAB15B32E10BC08CDBE95F0200701D68CD524B8093ECF1
               1939B01358628E4C65382668FAB2199BDD1FBC757D4A2E9D6D06901A822B
               821C0BF8C335851AF42AE806855BF3BCBB810876F0587AD1DA81038B8EC0
               C83234F027E506B846C583F563FC9EB937FB
            },
            INTEGER =  65537; -- exponent
         }
      }
   },
```

```
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#867DDEC60355132AD3F8A90FC1ED74E4DC687A8F } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #04, #B0 } -- digitalSignature, keyEncipherment,
dataEncipherment
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.2.246.517.99.10.202.1" }, -- Test Purposes G4
CPS
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               }
            },
```

```
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktp4c.crl" }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- caIssuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktp4.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktp4" }
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
```

```
      #64473876C033B29DA892FF0E89A1E8A99353FFCF1685CDE4430EA5B321
      191ECEB4AA43FAC6C00ECEAD0F7A96E789F4D7E1FB390227E56DA14F6E86
      ED59B9307FBB737DAE053F272453EADCAD30CFE7E5AB374F274D35F988EF
      82CA231B0157C21CA33F8FC539FAC5465AEBE5D32E1D7DFB724A841E4A0C
      0BCE923FBDD55E0FF36122255041809AE1B5AA51BBFC10199295F96871B0
      22CD0BE2C5C310EA88526B79CAD3CCDBCD952E816B862D6E81C5BED8BA4E
      D99E4155C65EA4B702B24AFE7ED0BC9068CBF3B2D6E999A61238B7EA1CC7
      487DB00D99654CE155BD67F136DC2F792EE0E1547F278E1093209791D452
      B9CF1E72B5BC8559018B189CC5EE8017216EED826A59AE27A972B37E23A4
      E7E7950CAC25E6FD5369B8961B5EA71B10DF7B3F1E1335029F9F1DD58C14
      35AA42257C4C9311D07B6207031C9B171DD93954A508ABCC2DC3F7851D12
      6AC6E3D3527DC40B885C1FB1EE5066E434EF7FC0CD55BE5CB683B0F8B358
      89522E826B3D33A4FB2FDD2F5151C4F988B1C91553814EFC709D4F02F1F0
      D294AE02ABBF59352D58D78685B3C2A2BC5AB8158D8673EA214CF0609313
      86E48D0DB3FF1FB2B2D02C8404040758EF35DC16C5216E85C355B1A0D16B
      10762C2A7224EC3801FA1611B36A16190A7DD5D23AEAC06D92B01ACF9A9A
      42CA00B7A257999843B7D801753DD80AD7864FF06CEFD3CC4C1784457BD5
      6A9854
   }
}
```

10.4. Citizen Certificate – Non-repudiation (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  101500035; -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180704111520Z" }, -- not before
         UTCTime { "230705235959Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
```

```
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
            PrintableString { "123456789" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
            UTF8String { "Teppo" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
            UTF8String { "Testaaja" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String { "Testaaja Teppo 123456789" }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
         NULL =  "NULL";
      },
      BIT_STRING [ PRIMITIVE ] {
         #00,
         SEQUENCE {
            INTEGER {
               #00D8F2B6CCE70562FD42FFA7FB014C74864BD9F2C17D3D259171C1FEC5
               271ED3CE5129121FA60036A89AA582D31E2A05E56C7377D23FB2F29DD6C9
               F6677FF1C559EB45D23BBF8956865DAD08B6AEAE2B1BC35E89CDA49ECFEF
               216A1E9EDFE7FDE45A19C283034D4589C5187454846F29005F230C8D2377
               028D5FF4BE3DC69DA9A35974356E42324BEAB6532B032D0F57CD871A885E
               1E22554843E266B8888A45287BA87D76B1A3AF44B63E81FAEC38FE69684E
               451C4BE534869041FA88BDE5C2C4E808527C51AE701EC839DD5BCB9FD327
               B07C2582EC1BF4E1F1D2EC8287C08A71127196F6C235235C06617393C32E
               5CCD840E20E2E68304D5735360ED45015775
            },
            INTEGER =  65537; -- exponent
         }
      }
   },
```

```
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#2D2BF06E9D9C3784D44E78BF25074014494F541D } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- nonRepudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.2.246.517.99.10.202.1" }, -- Test Purposes G4
CPS
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               }
            },
```

```
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktp4c.crl" }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- caIssuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktp4.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktp4" }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.3" }, -- qcStatements
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.1" } }, -- QcCompliance
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "0.4.0.1862.1.6" },
                        SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.6.1" } } -- esign
                     }
```

```
                }
             }
          }
       }
    }
  },
  SEQUENCE {
    OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
    NULL =  "NULL";
  },
  BIT_STRING {
    #00,
    #8D50CBB2F117B2865B3356EB4A2295FCEC14F3BE0BEC62E4E39B7D7057
    4BB577EC92AD0DAB0B9C8FADF80264C7C779663179B75CBA17A62700C2A2
    AC62E2D44A7BA46CE8F15CAA8D0CB2181ED92405924B3B993AED98818D10
    F53BF8FCAD92A3305D2D9409FA5331A8A4E79621F09E1539C12582ACBB64
    DEA86688DD59632BDA7F19302D16C20782842B6652CE61EF6F80D5694401
    64CC4A9EA4E4D3CEB99CA30936E5BDD94D9C84D514801A90D2D7C3155F67
    34AF86316DFFFAFCB43EF19DA23E48A36384612ABD99602C6607B5C579FC
    69C47405717566A9B3BC5EB8A9391662837192985D04B81B061F99B23E61
    59F41429BCF345B4117E771DB163ACE42D7C70C772D28D75679135699B36
    7181572FACA986803035FE71D8910CD99CA276D4DCE4C8819F19FDF8B9CC
    F756B1997CB51A9C08F3AECE58B961705AD8AE1C959CCC347349D0589970
    0ED9419AEEC9B0FE99FCCEC7B5916A1D2F93A20EA382D927337C815C693A
    1E3A04A650C66D0F95854B047C8336C31E7AB6ABBCD401819376EAB17755
    89BB6B4AA92A82EAF4D14CCC81C0C85DD3A4235C0D6EA0533D64A0A689D8
    1C3EC2813AEBE587446309D521AB60BADB4C895FEEEEBA9E9BB8244C5227
    2647D657CC53A4DEDCABA8E6171C1E04B190CAA0CC7AAD3A216B3DA902D6
    7D88640C5C0BA347A4EA1827F2EB0ACE7760A689509ADD80075245145720
    C2C831
  }
}
```

10.5. Citizen Certificate – Non-repudiation (ECC)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  101500034; -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180704101732Z" }, -- not before
         UTCTime { "230705235959Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
```

```
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
               PrintableString { "123456789" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
               UTF8String { "Teppo" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
               UTF8String { "Testaaja" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "Testaaja Teppo 123456789" }
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.2.840.10045.2.1" }, -- EC Public Key, Elliptic curve
cryptography
            OBJECT_IDENTIFIER { "1.2.840.10045.3.1.7" } -- 256bit curve szOID_ECC_CURVE_P256
         },
         BIT_STRING {
            #00,
            #04EE40D57FDB3ECD72C12DFD18DB04C923A37D58B558AFD8A4ADF95450
            2B62EA1E64873E1D6226953F24E7687B3294CDE4E4CD9AC54544ADC0FE49
            42690563FEC6
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
```

```
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#6FBD5C79F4F4027DA8BFB8DEF0470D5F8118C55F } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- nonRepudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.2.246.517.99.10.202.1" }, -- Test Purposes G4
CPS
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
```

```
                SEQUENCE {
                   SEQUENCE {
                      CONTEXT_SPECIFIC [ 0 ] {
                         CONTEXT_SPECIFIC [ 0 ] {
                            CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktp4c.crl" }
                         }
                      }
                   }
                }
             },
             SEQUENCE {
                OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
                OCTET_STRING [ PRIMITIVE ] {
                   SEQUENCE {
                      SEQUENCE {
                         OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                         CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktp4.crt" }
                      },
                      SEQUENCE {
                         OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                         CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktp4" }
                      }
                   }
                }
             },
             SEQUENCE {
                OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.3" }, -- qcStatements
                OCTET_STRING [ PRIMITIVE ] {
                   SEQUENCE {
                      SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.1" } }, -- QcCompliance
                      SEQUENCE {
                         OBJECT_IDENTIFIER { "0.4.0.1862.1.6" },
                         SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.6.1" } } -- esign
                      }
                   }
                }
             }
          }
       }
    },
    SEQUENCE {
       OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
       NULL =  "NULL";
    },
```

```
   BIT_STRING {
      #00,
      #224DC07B7DEE52221AFC6C956570EED0772AA7160917D3EB4DEC9910B6
      A87C4F99191C01801A72BFE40BCCB8A0543E4DC3741654D0AF3427DE232F
      7888D0D9DD3C658F4ECCFF8369E3DFC1199B74ACC7A4A4B4BEFC4271ED7A
      59A66F8D5ED74068917F0D31FD39F68F4E72CDF40641C64B51B110AFDA22
      0D26E4FA75CC339F7BBB0147FDE8531767B3F2317E2FFC342D440702E643
      8F97244A597C4754E729C550C00B7EF1BF35BCE9298076CE4118C9399DDD
      38454962EC518615C3EC08326EEF98541B18A45513DE136DC135FA0F7108
      D46592E2FC4716C580C15373C102EBEBAADAA5912F5AC85EBCA3095CE619
      AC0A39EBADCDD443CD7D49B66DD1DD27DA01F75DEFF6716A7A3234788E21
      6D24380FECB80D9CF3004B2FAEF8A41D4A1F430753D947946399F91404B4
      D7CF04C8574AF604DB718CE45B41B1EE0486BA7600494D02BF893AF2625E
      EAFB5E55CF25A6BC1603DEB10C8B60D81E0A075675C0026353819E4DD9F1
      575FF3733824880E8DAEEC8A9BFD367192B7B3EC317B1518707056557819
      92699BC8C48720C58DB147D5B77B682908E9CEC8813DD58398387AF93682
      DF7936CE3A168348D9FDB850BB12474899A0098390DB6FF2599136F668EF
      9F9C8C4196130B5E40C85E81D765FA8B26BC754345E1DE309C589675E2A4
      497D9C7E308514EB0702D77E2F6C236A463AE4E29E4AE9C653EB72C13E2E
      D8A753
   }
}
```

10.6. User Certificate for Organisational usage - Authentication & Encryption (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  101500031; -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180619110916Z" }, -- not before
         UTCTime { "230619205959Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
```

```
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
            UTF8String { "Oy Testi Ab" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
            UTF8String { "Test och prov" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.12";   -- id-at-title
            UTF8String { "Testchef" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
            PrintableString { "997558920" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
            UTF8String { "G4-testkortääö007" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
            UTF8String { "JAVA-PRÅVSTRÖM-ORG-G4" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String {
               "JAVA-PRÅVSTRÖM-ORG-G4 G4-testkortääö007 997558920"
            }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
```

```
            OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
            NULL =  "NULL";
         },
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {
                  #00A5822BC71178170E82EE064D474EE796B10C0A01554A5F489D9A0B37
                  17D69D4A1E8CBC134FFF0D2F686524B9FB05AF26082751EC1CA238B587CA
                  728C5BEEDDC73ED782D6448B6E0A1159BDBDC7E56B7F760767CF9E4BAEF5
                  60D773B115F25C89FF8913B294DAA8D5566F129B844224C840B234E8E4C9
                  C275B4848FC57E8C4060D2762F6464855427F830B8A6F365DC70F126CE0D
                  EB009DA5423FECDC4344C87D45F2D5E2D57CD5E31DE5F9EA0596D7D4802F
                  58CF493C5ECD6FFD7A7F09D888ADB1972E455DC29A2C26134FA230DADAA6
                  EBCB8AFFEE865D9A2057E8BB49C97356C3AED3A57702ACC3D3ACF4F29EF0
                  5A9599E95E642A8B3456B6CDF3E4B6ECE309
               },
               INTEGER =  65537; -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#FE7EC9E729D6E8C7D7E1E8F25C7488897D51E75E } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #04, #B0 } -- digitalSignature, keyEncipherment,
dataEncipherment
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
```

```
                    SEQUENCE {
                       OBJECT_IDENTIFIER { "1.2.246.517.99.10.203.1" }, -- VRK Test CPS
                       SEQUENCE {
                          SEQUENCE {
                             OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                             IA5String { "http://www.fineid.fi/cps99/" }
                          },
                          SEQUENCE {
                             OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                             SEQUENCE {
                                VisibleString {
                                   "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                }
                             }
                          }
                       }
                    }
                 }
              },
              SEQUENCE {
                 OBJECT_IDENTIFIER =  "2.5.29.17";   -- Subject Alternative Name
                 OCTET_STRING [ PRIMITIVE ] {
                    SEQUENCE {
                       CONTEXT_SPECIFIC [ 0 ] {
                          OBJECT_IDENTIFIER { "1.3.6.1.4.1.311.20.2.3" },   -- MS User Principal
Name (UPN)
                          CONTEXT_SPECIFIC [ 0 ] {
                             UTF8String { "G4testkort007.java-pravstrom@testi.fi" }
                          }
                       },
                       CONTEXT_SPECIFIC [ 1, "IMPLICIT" ] { "G4testkort007.java-
pravstrom@testi.fi" }
                    }
                 }
              },
              SEQUENCE {
                 OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
                 BOOLEAN =  #FF; -- critical
                 OCTET_STRING [ PRIMITIVE ] {
                    SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
                 }
              },
              SEQUENCE {
                 OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
                 OCTET_STRING [ PRIMITIVE ] {
                    SEQUENCE {
                       SEQUENCE {
```

```
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktp4c.crl" }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.37";   -- Extended Key Usage
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.2" },   -- Client authentication
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.4" },   -- eMail protection
                     OBJECT_IDENTIFIER { "1.3.6.1.4.1.311.20.2.2" } -- MS SmartCard Logon
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktp4.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktp4" }
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #676F08DF9B43D2D78B83856604F07627937BB54C0CB3C75A6DC227C8D7
      652C273FC2DBC996135F14E98FD84B7B87BD7229D87D9354204839118362
```

```
      1F88A3866C09591EB15ED11039CCE6A6DF8B9329675F70E33663836C067E
      FD43E55C66A7D1E97E80B4691C640A32F84DC56F2346EE6E0035A7F21DDD
      03296DAC2E74A03F80E229E2836B2FB4E93E8DF46C01CD5AF1EE19E7997A
      2F975C23077D66C35F161F2DAE365C4986675B41853F1BF890072C492A32
      9CF4F84900B3DB38B50BC7C24ECAB1C11DCB2C3A064EF4A4CE4C0A247BBD
      9331BA081B35B612EB3ADFB3CFD6BAF6B02DF9EA719FFDEE89C01051BA27
      D9B5121ADE81D7CC562C373FFF0AE5661F7D5DA056F8993F363715A4B9AF
      64DA43475F3613DA16B935754885FA93F15EDACA3464F6EE74C42122B205
      FE497E67AA320E0337BBD474F542E8FF617F59BC6BA0CA84D121165AC1E5
      86BA6D964A2F1F8BDBC1EA6DD6DB89B5891B1CC4A59BCD371E88884B54FF
      030DFB71A1F354ABEAA0D6E187E2B0D8ECFFE1F4E074D072DB8DA1873DBC
      CF4CA84C7BD0B0378A5F6DC2B352A06487B6A195C481111354378C581DA3
      FEBA84D525187E55869F32C0E11807A6200AB945E7D710F6B9A1CE400718
      105EB2A44890DB45B0825FC33DC985FD912424D0FB04B663261D4561B592
      E100D7598A40207B34BA45ED9FBB6F65EB27DEEB368C94CD61AAF0F11512
      626B55
   }
}
```

10.7. User Certificate for Organisational usage - Authentication & Encryption (ECC)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  101500167;
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180918090552Z" }, -- not before
         UTCTime { "230919235959Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
```

```
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Oy Testi Ab" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testausosasto" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
               PrintableString { "123456789" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
               UTF8String { "Teppo" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
               UTF8String { "Testaaja" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "Testaaja Teppo 123456789" }
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.2.840.10045.2.1" }, -- EC Public Key, Elliptic curve
cryptography
            OBJECT_IDENTIFIER { "1.3.132.0.34" } -- 384bit curve szOID_ECC_CURVE_P384
         },
         BIT_STRING {
            #00,
            #045B670AB10D8FCF4C8B300A8C8D31A5102D92EDDD96F9B7F475266C2B
            FC5146EBCA6836237F1C771624E23C0AF6507CCB6971B07255C8C33E43B3
```

```
            72DC0664309C10DC329532B8D5ADDEFE73D8ECA799A4353E63048BACD976
            CA077F22C3529FF4
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#78C8A4E8995FDBA8643BB7AD9B2A9675E09739FF } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #04, #B0 } -- digitalSignature, keyEncipherment,
dataEncipherment
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.2.246.517.99.10.203.1" }, -- VRK Test CPS
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
```

```
                  }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.29.17";   -- Subject Alternative Name
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  CONTEXT_SPECIFIC [ 1, "IMPLICIT" ] { "teppo.testaaja@testi.fi" }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
            BOOLEAN =  #FF; -- critical
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0 ] {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktp4c.crl" }
                        }
                     }
                  }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.29.37";   -- Extended Key Usage
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.2" },   -- Client authentication
                  OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.4" },   -- eMail protection
                  OBJECT_IDENTIFIER { "1.3.6.1.4.1.311.20.2.2" } -- MS SmartCard Logon
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
            OCTET_STRING [ PRIMITIVE ] {
```

```
                SEQUENCE {
                   SEQUENCE {
                      OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA issuers
                      CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktp4.crt" }
                   },
                   SEQUENCE {
                      OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                      CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktp4" }
                   }
                }
             }
          }
       }
    }
 },
 SEQUENCE {
    OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
    NULL =  "NULL";
 },
 BIT_STRING {
    #00,
    #5320F507426A97C8A101876CEB147CD7E2C6B278984698AB0AE41359A2
    6AC4D345B7D95D51671B69E418D7832510FDEBE9AD05D8D5E5D93650BBF7
    11E0D39F629AE9F708BC339ADC03904D3321ADA080358CA3BA494B124189
    C0BD0E6F667065083755204F6547B54B5102E70F4103D3350C7DD3EB4937
    27CD1B696106878981D46444E3633C2136D605AAAFF49A44A04191373414
    304938F9989F43C1D6CAF90C00FF1F3D84CA6E1EFC8DF234A434BEF4EEFF
    3A45F351EC516C0509BCADA0118422437F37ECCAD42A49038A4DC66805B3
    88E533FFBC08F93655C175523B283FFFD3A37179E49EFEEA67E09E66B681
    5DBEFC34619C8A8F868F0C5C08CAA76EC52E17A22A55DBB8F4608457CADD
    20E06DE7A03CDB87EAA911096C3B1893EACA9026EE60689813BFF57BEDCF
    747BE16526F4213222E93136C656D429AB6D5854765687484FDCBD58BD6B
    F250668F70C0FD962E0C1CC1978204A57458BD80E3F71ABA31AAD8F8B0A4
    AA2DC661340E48DF2675A34081AE4B48C12ACE5C9D8B8D59DE6DE3CC8EEA
    FD678B71AE9E23716865D7604DEF90A283B6BB2C23752B054725E44AC468
    01F5976965DF6412DBF08FF7D4FC11DB1B18B1B402309E1405CA64F981AD
    C7D994F85BD6EA0668B52A7EFDEF3CAFDF184103EF68BCD9DF5A10312E35
    AC16950385872A0122FB9F820F16D5324532C24DF418D75DE744A3834137
    33F855
 }
}
```

10.8. User Certificate for Organisational usage – Non-repudiation

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC[ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  101500032; -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180619110919Z" }, -- not before
         UTCTime { "230619205959Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
```

```
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
            UTF8String { "Oy Testi Ab" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
            UTF8String { "Test och prov" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.12";   -- id-at-title
            UTF8String { "Testchef" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
            PrintableString { "997558920" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
            UTF8String { "G4-testkortääö007" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
            UTF8String { "JAVA-PRÅVSTRÖM-ORG-G4" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String {
               "JAVA-PRÅVSTRÖM-ORG-G4 G4-testkortääö007 997558920"
            }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
```

```
            NULL =  "NULL";
         },
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {
                  #00B5510FD77EAC6621FF71B713F3A8FA2502838FFA3B7D738850FC1472
                  9ACDBBCA6DEE9E3CAD993616CE86A716378A20FE46CF211D9EB015A05F00
                  DC432A53CCD97B8695F5F8D641346D7A5AAEC116CE0B4B0F38479128CF30
                  E6FA9BB63CD4E96845320106F5C3EE4F153E25E0B8981E33FCB6BACD4065
                  6F5A102B432AA7C60A8541366A924757F638342BEC4D9832C80DF31DB73C
                  089A8F97A89D4F8288FEF2BE59D5B5CC867E8D80A7B20BE9A9A13C8A5C68
                  04582695C113F7C99DC447D906D3D88770509D255FAB6F231DF6C1A3C0F7
                  53929CB5CA75D8EDAEE95847B6124BFA0A2D65CF22D989653E70BCFDFB1F
                  B1F0A40F80BE8926AAB7F46BA9A29AEF2F07
               },
               INTEGER =  65537; -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#E01ECBF38A4F6CF39718C0D28F90B22AFD8B909A } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- non-repudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
```

```
                        OBJECT_IDENTIFIER { "1.2.246.517.99.10.203.1" }, -- VRK Test CPS
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.17";   -- Subject Alternative Name
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 1, "IMPLICIT" ] { "G4testkort007.java-
pravstrom@testi.fi" }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktp4c.crl" }
                           }
                        }
                     }
                  }
```

```
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA issuers
                     CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktp4.crt" }
                  },
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                     CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktp4" }
                  }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.3" }, -- qcStatements
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.1" } }, -- QcCompliance
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "0.4.0.1862.1.6" },
                     SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.6.1" } } -- esign
                  }
               }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #9EF2DC8B41051B8CD3CAC2BD2E538DA3F61132FF5D992B8C466C80ADCF
      1EF3B7D2E57168B148C9E42FFBBFE3FC9CED2F8857DD896DCB802E880F17
      30506F433BC078C54D8DA1DC83022A1B3F3CCA2A24291A1B523168DE7ACD
      DEF73BE71DF013C02943DE6315A36DB9DF5DE9EF8468950DD4B413732A59
      35D6649DA48AEFBB57B409EAEAAC4218514E4CD39B76BA1947EC8FBC54A9
      3BBAEA5A99A1943EE34AA42BFA87D7545DDC9C7D9C6DA3F4A2DFBC47E44D
      86E4B598572C156E8D833FA3DD22A589701B12B62E58FEB5651842E4B68E
      F373D81130868943D1074A175AD68392A56150194A0CCD9E25F45767E903
```

```
      2545465A15044AF7CA9E51B4CB2C825088161EAB80AAB6FA6322899A33DC
      E58F3F887DA0D9F74957B6CB23F1AA8B614728245E58F6A3878C7D4FDE35
      B3B81507E8EB72ADCAEFB9B9522D878600872875D6FDDD5D19B3B2B310D9
      E5DD767868B33282217A2EDB3EB90ADAA4C4114683B393E11C37C91F996E
      59CC470455A22AC6B3DB4C23245316C9DDE85740A43FE2FCC35BBB16F2CA
      9AFCF1B3C355A6694583E8080EE75B3E5B004BD6E595288B494E9EC2A9F5
      B12308E1CC958D8D38B7DA4D021F1EB7C795BA7F10BB153787CB79D5AE6E
      130E64E5BE41E0A0FCEAC3C7D1B70CD801C4731B4DF71065D7D6546FC43D
      178F43A84D7626EE399C17DD260901B9BD9BCFB6EE30E60412CDD1F911C6
      146187
   }
}
```

10.9. Service Certificate (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER { #0400000164650AFDBF2FCFD6979B8C22FD92 }, -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testipalveluvarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Service Providers" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180704104531Z" }, -- not before
         UTCTime { "201008235959Z" } -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
```

```
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.8";   -- id-at-stateOrProvinceName
      UTF8String { "Finland" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.7";   -- id-at-localityName
      UTF8String { "Helsinki" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.17";   -- id-at-postalCode
      UTF8String { "00531" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.9";   -- id-at-streetAddress
      UTF8String { "Lintulahdenkuja 4" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
      UTF8String { "Vaestorekisterikeskus TEST" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
      UTF8String { "Testivarmenteet" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
      PrintableString { "0245437-2" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
      UTF8String { "developer.fineid.fi" }
   }
}
```

```
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
            NULL =  "NULL";
         },
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {
                  #00B38BDF3AC545F6E50A3207C6097BFBF4DBB52BF253BA5E6C0FBD4DCC
                  274CD723AC0323F96C715502DD00813C9B2C7346270728A890C47F6A9580
                  D69D14E77646A78AD22468286AA5BB5A37DD106A69BB212F10BE8E040286
                  F36FE44E9FABCD762E88393E1D53C8B8648D9E1A2E014F0C05DE739E13DE
                  E722ED094E0611BABF6461069DD8B60AC7681D7AEC39AEB96CBED29D7C1A
                  0E1C6029CB40E2FC4B066FC4E1AE10BD82A1E259E58F63B6494E5CBCB84B
                  4365ECAC43ECA71AF764255F7E061B02FF3CF05F43D5104B8A805F673424
                  688EBA37556EDB38DAA83DF2DDC518A71FBB09724324DCC268F0CB895AE1
                  729C5AD559E8119DD9BD29D99A6C9D1DFCF9
               },
               INTEGER =  65537; -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#ABF1079E6C942DBC1E13A48B2C373C7A84488001 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#6238218482A5D8BFD171E635886060FBD721829D } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #04, #B0 } -- digitalSignature, keyEncipherment,
dataEncipherment
               }
            },
            SEQUENCE {
```

```
            OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.2042.1.7" } }, -- ETSI CPS
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.2.246.517.99.10.205.1" }, -- Test Service
Providers CPS
                     SEQUENCE {
                        SEQUENCE {
                           OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                           IA5String { "http://www.fineid.fi/cps99/" }
                        },
                        SEQUENCE {
                           OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                           SEQUENCE {
                              VisibleString {
                                 "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.17";   -- Subject Alternative Name
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 2, "IMPLICIT" ] { "developer.fineid.fi" },
                     CONTEXT_SPECIFIC [ 1, "IMPLICIT" ] { "vaestorekisterikeskus@vrk.fi" }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
```

```
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/crl/vrktspc.crl" }
                        }
                     }
                  }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.29.37";   -- Extended Key Usage
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.2" }, -- Client authentication
                  OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.1" }  -- Server authentication
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                     CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktsp.crt" }
                  },
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                     CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktsp" }
                  }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.3" }, -- qcStatements
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.1" } }, -- QcCompliance
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "0.4.0.1862.1.6" },
                     SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.6.3" } } -- web
                  }
               }
            }
         }
      }
```

```
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #61EE22BAE3ABF007771919375178D67567AB6C53E0DB191219BFAEB307
      6A6A86450E610174F812733942A9BE09710C5D0B23FE75F6FCE86A8CE88D
      00077EEE427ADB419E3C40D2115E159A1100223FA6A57480C1E9D38AF969
      E5094E415A03B30AE31EF10331B767AFA477BCFAB629ACA62A8C00EB00FB
      18548D7C754D57628392E4B1EC0CAA52DD806AAC49D238AEF0C97923B173
      D87D35B0C698E169CD24FAE172DB4128DB89621D0D9685C4FD8F58A347A2
      2AA319EFF9E1FF27CAD2F55077148FF87F7A707216645B6FAE4C7D85D0CD
      EB997D26CA0655B0CA366335B8D964864D91912050E54F37C134C00C5D62
      D291F1D7D89C02895E7CF4742E7B062A611021462FE99262A892E19D7586
      4C897CE1F8EA01B6DE5D3112F384757D47056685B26DC79BDD6CEE21E13F
      7EFBAF1269FEF39F1CD87B02356D1C961ED64DBD6F7489242564E57A624B
      71324FE5C54E99B5DC7D659DE22F982AFD7E870AEC1AE965835235C1D0BA
      3B3EDFECDAEE5DA7782D8000D0998F5D43A89CEF71DE34DB2E1DBDFC7DF0
      0BAF0B7CD18D99CD7718A70045ECA2F35706827AA564BEDC5D46C234ABA3
      E0A37A9DB6A4AD52AADF2BF0FD526E12AD48BE89976A77683B1AED6A61EB
      990B8E26EEFE672B3117B8055D500507C3BF47421B177C26F2314B4B5D48
      7A10BA794F798A6711BD11FD60E6583AAEF0C050A5C6DB0FC896915D6A4F
      86ECAB
   }
}
```

10.10. Certificate Revocation List

```
SEQUENCE {
   SEQUENCE {
      INTEGER =  1;
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testivarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Test Purposes - G4" }
            }
         }
      },
      UTCTime { "180702114158Z" }, -- this Update
      UTCTime { "180702134158Z" }, -- next Update
      SEQUENCE {
         SEQUENCE {
            INTEGER =  101500000; -- certificate serial number
            UTCTime { "1805091259442" }, -- UTC time of certificate revocation
            SEQUENCE {
               SEQUENCE {
                  OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
                  OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
               }
            }
```

```
},
SEQUENCE {
   INTEGER =  101500001;     -- certificate serial number
   UTCTime { "180509125944Z" }, -- UTC time of certificate revocation
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
         OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
      }
   }
},
SEQUENCE {
   INTEGER =  101500002; -- certificate serial number
   UTCTime { "180509130020Z" },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
         OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
      }
   }
},
SEQUENCE {
   INTEGER =  101500003; -- certificate serial number
   UTCTime { "180509130020Z" }, -- UTC time of certificate revocation
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
         OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
      }
   }
},
SEQUENCE {
   INTEGER =  101500004; -- certificate serial number
   UTCTime { "180509130020Z" }, -- UTC time of certificate revocation
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
         OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
      }
   }
},
SEQUENCE {
   INTEGER =  101500005; -- certificate serial number
   UTCTime { "180509130019Z" }, -- UTC time of certificate revocation
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
         OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
```

```
                }
             }
          },
          SEQUENCE {
             INTEGER =  101500006; -- certificate serial number
             UTCTime { "180509125840Z" }, -- UTC time of certificate revocation
             SEQUENCE {
                SEQUENCE {
                   OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
                   OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #00; }
                }
             }
          },
          SEQUENCE {
             INTEGER =  101500011; -- certificate serial number
             UTCTime { "180517130649Z" }, -- UTC time of certificate revocation
             SEQUENCE {
                SEQUENCE {
                   OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
                   OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #06; }
                },
                SEQUENCE {
                   OBJECT_IDENTIFIER =  "2.5.29.23";   -- Hold Instruction Code
                   OCTET_STRING [ PRIMITIVE ] { OBJECT_IDENTIFIER { "1.2.840.10040.2.3" }
}
                }
             }
          },
          SEQUENCE {
             INTEGER =  101500012; -- certificate serial number
             UTCTime { "180517130649Z" }, -- UTC time of certificate revocation
             SEQUENCE {
                SEQUENCE {
                   OBJECT_IDENTIFIER =  "2.5.29.21";   -- Reason code
                   OCTET_STRING [ PRIMITIVE ] { ENUMERATED =  #06; }
                },
                SEQUENCE {
                   OBJECT_IDENTIFIER =  "2.5.29.23";   -- Hold Instruction Code
                   OCTET_STRING [ PRIMITIVE ] { OBJECT_IDENTIFIER { "1.2.840.10040.2.3" }
}
                }
             }
          }
       },
       CONTEXT_SPECIFIC [ 0 ] {
          SEQUENCE {
             SEQUENCE {
                OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
```

```
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#3D9AA3B5F81511EF11CAEBC75C4D9380B2C73FC1 }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.20";   -- CRL Number
               OCTET_STRING [ PRIMITIVE ] { INTEGER =  2997; }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #9E3485F59017A40C44EC6F31BF3F1EAE919D3FDCA002B76FF6783A4F37
      94CFCC3A5CA9560859D4EAED5E7A0EDBADC4A432C05DF3B385AA98C2D043
      E9E7D2D26D0A4C69C98D4F1DD0867B519BA3DC064C8FA73D8B368D684ED9
      EE8C9BBA6848E0ADEA3EE628DFE31F1D3F3277786C736A1E7BAAAD4C6CC9
      E1E060EBE18A70E76F6E2822FEC34A5498297321EA205B8475B86FA8AB5E
      67CCA927E68A02D78CC6F2150F14F5A9149915C969A0743D6CE062B53BF1
      8749A095017327E2049A0DE8B8EF1BC65D6507B70E0E7D256275F475F791
      49C3DC46BDAF076B5DF89E7D1B6FA16F9383378A3139BC09271BA142FC12
      7B4E2D962C53ADC7010133DD7C8FAE673147467C8E0953722D447A5190B6
      A34B6ABB8C706F30A50350152CFA8C5B925ED45111BBE8E5C471A0436359
      5B4D54CC8790E0BC2737AE0F918AEF32275FD05313EC817D8AA57A7A2750
      001AF9B30A83A6F3BE1CBFB7960745D199B428E473317D56FD770471D4D4
      50D18BE97E0F18E8724B88DD7E94693BDE720D8ED16ADA98CD742D1B3FDB
      7A95F64F97E1A60073D2C7E61B834CAB7D8B74FFA18F23FB5C8910DEBA38
      1A92DCE843AF12BF3590CA5AC39082B435E9E7714B167027BD6F639F4373
      22052BCD5037C2BFB970B9FC86190823E1FBEA205E8025970A2DCE5A8A0F
      FFFFD841D87BA56780A830B671AC6C5B6E805298525365B9CE6414624608
      3A5D43
   }
}
```

10.11. OCSP Responder Certificate

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  300100010; -- Certificate serial number
      SEQUENCE {
   OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String {
                  "Sosiaali- ja terveydenhuollon testiammattivarmenteet"
               }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String {
                  "VRK TEST CA for Social Welfare and Healthcare Prof. Certs"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180612065526Z" }, -- not before
         UTCTime { "230614065526Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
```

```
            OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
            PrintableString =  "FI";
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
            UTF8String { "Vaestorekisterikeskus TEST" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
            UTF8String {
               "Sosiaali- ja terveydenhuollon testiammattivarmenteet"
            }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
            PrintableString { "0245437-2" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String { "OCSP Responder 3A" }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
         NULL =  "NULL";
      },
      BIT_STRING [ PRIMITIVE ] {
         #00,
         SEQUENCE {
            INTEGER {
               #00BCD0DFD08ED6364D06BD5981A44827486E35D4E454169A9586A6B57E
               A950E1B7A78578258021AEDA7AA5995DEAE53998A13A96AC01E9EA442EA0
               D1305D9D55A39AC9088D045853F484CF9999581F3C84FEE2963534127697
               FF99AB6E52014B9B40FFD46CE6242B3A63FAD071D6D6CB175825C2E8C44B
               7D511AAE44F63D39FC23700200A56AE6BE4753E4FEDE68DE2C2DE60C4F44
               8D55CD3228801031B2A8017373A092C92F3F61492679FD837A1EAE0E3432
               FEC5404098F200C1F35F9345444EF7EF58278BE98057D653742386B5C0C6
               E2E7EEC15F4236F0789325EF69CAE17EF3852BF75ACA63DA86474C83ABF2
```

```
                  00673C66C85A80F5F52381C8097E2F15BB4B
               },
               INTEGER =  65537; -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#2365BD40E0E6FC68AA1266DEEAE0B3EBB473CB5D }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#510CD96C45888F7C6488F702F77C027C7D557642 } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #05, #A0 } -- digitalSignature, keyEncipherment
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.2.246.517.99.10.206" },
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat
policy finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
```

```
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.17";   -- Subject Alternative Name
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 1, "IMPLICIT" ] { "vaestorekisterikeskus@vrk.fi"
   }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; --critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.37";   -- Extended Key Usage
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.9" } } -- OCSPSigning
               }
            },
            SEQUENCE {
          OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
   "http://proxy.fineid.fi/ca/vrktshcp.crt" }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1.5" }, -- OCSP No Check Extension
               OCTET_STRING { #0500 }
            }
         }
      }
   },
   SEQUENCE {
   OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
```

```
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #05782609A2E8B0EE334C8CE7B203374626E0ED01C3F9C3C0D2E3D22390
      9B42F1ABCCCA7CA7DC30CE45A4E91BF4BA385C8478AF409E22EB850A6B14
      EF4417658179615F4A708B2AA0518145474B713F95FFC812C865B11ACC2E
      E5311777AAA621074F3ABF0BBA58E87401D214B9B91F8A5012AEEB370F04
      D3D018C8CC54072A89C44244AD48431225AFE160D25045744EBA3FD4E358
      4B25AA90B571D2B88C1FE849E6F80409B3F6FEBD883BD3C9BB389FB7F431
      BEA678E2BE54F54C63236A06E30B0EE2D9E0691160583FF6474CBA24E622
      84DD2F4E32B385CE8A52EA54D18FA56DE7489D1E08EF2D1FB4F6B50638FA
      1B3035984A708A1984D9F169E415EF063AB6F5BCA03A98E4C05494ADD85A
      0E23F8A6E9EFD43CE23CDF1B92F455599C780B634438255C2256C50801AF
      F85B478E417D4BBC3D58153002655AEF402ED0A12D01C533FDCE525DD440
      8006EA183C11E49BB51ED11BA812F9CA2AAC7634669B8AF29BD163357369
      C77E7DA1DBA54036939CB0DDFB64B9AA2FADD2D583C0630E6FA3F3A38D5C
      3A81CE7FDD42DC0FF02B9571D2F80C04DA8BF9DC49462E5A8EB90DEAB51B
      7DC4EAD55494A820CFCAC9BDDDDBFEE41CD3A5A7F5E4C7E0C28B31D36A6A
      90C15BFEF0394FA1E8A78E01D0E0E9546D451289F2B7504FAC6D39AF85DF
      AE590735230C7CD02D0D484610EF31D39BDDFAAA558E5C85D0CFFD1BBC13
      392F3F
   }
}
```

10.12. Time Stamping Certificate

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER { #0600000165C8BE28EEFB4F323EC3411D9D8D }, -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String { "Testiaikaleimavarmenteet" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "VRK TEST CA for Time Stamp Services" }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180911123143Z" }, -- not before
         UTCTime { "230910130143Z" }  -- not after
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
```

```
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.8";   -- id-at-stateOrProvinceName
      UTF8String { "Finland" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.7";   -- id-at-localityName
      UTF8String { "Helsinki" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.17";   -- id-at-postalCode
      UTF8String { "00531" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.9";   -- id-at-streetAddress
      UTF8String { "Lintulahdenkuja 4" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
      UTF8String { "Vaestorekisterikeskus TEST" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
      UTF8String { "Testiaikaleimavarmenteet" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
      PrintableString { "0245437-2" }
   }
},
SET {
   SEQUENCE {
      OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
      UTF8String { "tsatest.fineid.fi" }
   }
}
```

```
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
            NULL =  "NULL";
         },
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {
                  #009D9748EEB868ADE8C58236AFF5F623BF956300E769FECA06004ACDE2
                  D0DF5447A4F97CF5A98C0B8B99C5E320E29530021115076588E02A323EAB
                  C813D5F889594CAF6D797F3188847F63CDBE617F70213283DE1983433362
                  44C5797D5C0D3E3E244ECDBBACBB71533E032C7FD9ACD90FC2AB10582C6E
                  906F812D32311E10D4C4C25D658852CEC8D8DFB45A44A7C30111795D1E2E
                  1968AECC4B9CA62638B374AA00779DB34F4CEC2BCB09C621856262EAF0B6
                  01F3E482F0779DF66BEECE5A5D05DB747961EAC852BDCB3720958A01F49A
                  4147B0CD2FA16E1A8D4B4A0ABFF53B0AA26F499ABB01FD487B8CD5962B9C
                  6F3AD5192D8674BBB08D9CB012ECC5B3B5F4F671B389A7BC055F1FB7FCB2
                  31FEF114F0C256C35659D51BA482EB2C05F74CF6EED3C0FC189CAF93EF58
                  22C1E543A2003F98B77457716C22C209B456EC2B23E1D41296477D975676
                  1F495A8006A7E49C7268E07DDD5BBB55C83D08FF207684E41086821BF0A7
                  648C16EFFAE5A230912DABB57A27A06718D5E19CFE2CC02EBC9D
               },
               INTEGER =  65537;
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#57C6149BFA8A24C7D8CEDEA6B49A1CD697666AEA }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#381EDC63A6D61A7790096735097E0A2F35E59DD6 } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
```

```
            BIT_STRING { #05, #A0 } -- digitalSignature, keyEncipherment
         }
      },
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
         OCTET_STRING [ PRIMITIVE ] {
            SEQUENCE {
               SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.2023.1.1" } }, -- ETSI CPS
               SEQUENCE {
                  OBJECT_IDENTIFIER { "1.2.246.517.99.10.209.1" }, -- Test Time Stamp
Services CPS
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                        IA5String { "http://www.fineid.fi/cps99/" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                        SEQUENCE {
                           VisibleString {
                              "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                           }
                        }
                     }
                  }
               }
            }
         }
      },
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.17";   -- Subject Alternative Name
         OCTET_STRING [ PRIMITIVE ] {
            SEQUENCE {
               CONTEXT_SPECIFIC [ 1, "IMPLICIT" ] { "vaestorekisterikeskus@vrk.fi" }
            }
         }
      },
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
         BOOLEAN =  #FF; -- critical
         OCTET_STRING [ PRIMITIVE ] {
            SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
         }
      },
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.29.37";   -- Extended Key Usage
         BOOLEAN =  #FF; -- critical
```

```
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.8" } } -- timeStamping
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrkttss.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktts" }
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #4F497481CD3F14746CD5DBE6C828F8F14F0FDD41A9F269D5725BD9594A
      85258CBB94D548A67BE9899FF0E8A9EDC4DDEE9C4583E39E71383B7FF399
      C080C727CF9712A43B818FE1E8E8F5436DFE2A3A6EE7EA0CA0F0D81AD158
      54C774D28FA4E90413FADA93D00C82FF0DEA3F4B00AD36731EC94B86864A
      5F1BC67D19C9CF1CA752A6C1D86CAB4008E47FF4DB6F3C2440BAA8911EDB
      41C55F35E32645F3D22D280924E33CE3D1B7AA44E78DE92FBCE84041F4AF
      FEC323C26E3EAD9A7D8A676C446DCF6DFCE80A97EC2EBE578BBC4051047A
      C548185F8240FD4901A8425CA4586A84775D4C7B2403F9E7A29C344E066A
      93F14A89D0979C8F0FC8F56B9E3BDA3D7394FF0424400677D289DD27442A
      03E87F64057F581819129802B84D7F739F6F67FE4E405AF3CB21458560B0
      3A7F837B336A28F937E0E58F6160E5C7C3A62CBCEC91254D5C29FBF65C73
      BDDE42FC680E4BA304AD82F7A807BB9E1223F8F7C31E0248AA255F741151
      5CF852A56F1F106829BA2C9A7C891C3F1919F70D25A3691753ACD146A15C
      04DF7508C3C7654008A6A7B476CBEE3443BBDAA698C86FF6F11C4F969645
      3A9020D16238682266B9C7C933AD0D758FB2A049C1596396DDD8D18B0064
      321EE229534BD63CA0B7AED4D968F0CF7D7A2691DADBB057A71F66B2BBD5
      90F8345AAB2315FCDCD007A1B9EB7447AF213599246ECCF8E7C9A19C00EB
      9DEE4F
```

```
    }
}
```

10.13. Social Welfare and Healthcare Professional Certificate – Authentication & Encryption (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  300100058;
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String {
                  "Sosiaali- ja terveydenhuollon testiammattivarmenteet"
               }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String {
                  "VRK TEST CA for Social Welfare and Healthcare Prof. Certs"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180912130525Z" }, -- not before
         UTCTime { "230913235959Z" }  -- not after
      },
      SEQUENCE {
         SET {
```

```
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
         PrintableString =  "FI";
      }
   },
   SET {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
         PrintableString { "12345678901" }
      }
   },
   SET {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
         UTF8String { "Lauri" }
      }
   },
   SET {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
         UTF8String { "Lääkäri" }
      }
   },
   SET {
      SEQUENCE {
         OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
         UTF8String { "Lääkäri Lauri 12345678901" }
      }
   }
},
SEQUENCE {
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
      NULL =  "NULL";
   },
   BIT_STRING [ PRIMITIVE ] {
      #00,
      SEQUENCE {
         INTEGER {
            #00AD6055AB694794ACA84F15175F6A3DB0859B3FFF68352CFD418F823C
            1E41A79D382B84F8E39DF7B34A829C16C2C7E9C0F7300F5061BD7B592589
            41BEBE08AB65C6733726C065246A9F775F58A9B3A5D157243ABC725F0564
            AB0C023604C4109FF7AC48F5B530A54C6F4BFB26E7BE862B9221A6AA4BF8
            0165D8411188021B4B693F8C58924FA6263D361A10A2FB151E506627F6F0
            C72F59FCFDAD5B429D3A0EA2F0A3CE62EAEC6839FDA64658138D6FC3C824
            17D9466E2F7789330F94CDD6BF83AE0B4E3533E312659948E9F3D2725EA4
            FD2EE24DC134362C6C7C8B940D6B3432FF057FA5E3F9FB90FC628F8C5829
            F64F01D3F39DB0F126FC676A74D7048A0E2C7B9368A38A5A745676206EC1
```

```
                F15950E4D8F54CA217757466BDE5FB261505868AB729CE3860754143C5F7
                1219B7F848DA39D8D1E0E0BB3E5CB4396F05AEE84E850C3BAACD0AABAC95
                86273F156260ED8F48CBADFCBE670873CB7C759A4ED6104B672624659BA2
                1CEABC329F591A50CD033D046CBEB7A165D24CA2B6292885AA87
             },
             INTEGER =  65537;
          }
       }
    },
    CONTEXT_SPECIFIC [ 3 ] {
       SEQUENCE {
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
             OCTET_STRING [ PRIMITIVE ] {
                SEQUENCE {
                   CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#2365BD40E0E6FC68AA1266DEEAE0B3EBB473CB5D }
                }
             }
          },
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
             OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#8DE0B74CC90F06DA7B7DF6BB61EA7D3CDE60A232 } }
          },
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
             BOOLEAN =  #FF; -- critical
             OCTET_STRING [ PRIMITIVE ] {
                BIT_STRING { #04, #B0 } -- digitalSignature, keyEncipherment,
dataEncipherment
             }
          },
          SEQUENCE {
             OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
             OCTET_STRING [ PRIMITIVE ] {
                SEQUENCE {
                   SEQUENCE {
                      OBJECT_IDENTIFIER { "1.2.246.517.99.206.1" }, -- TEST CA for Social
Welfare and Healthcare Prof. Certs CPS
                      SEQUENCE {
                         SEQUENCE {
                            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                            IA5String { "http://www.fineid.fi/cps99/" }
                         },
                         SEQUENCE {
                            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                            SEQUENCE {
                               VisibleString {
```

```
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
                                 "http://proxy.fineid.fi/crl/vrktshcpc.crl"
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.37";   -- Extended Key Usage
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.2" },   -- Client authentication
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.3.4" },   -- eMail protection
                     OBJECT_IDENTIFIER { "1.3.6.1.4.1.311.20.2.2" } -- MS SmartCard Logon
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
```

```
                    SEQUENCE {
                       OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                       CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktshcp.crt" }
                    },
                    SEQUENCE {
                       OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                       CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktshcp" }
                    }
                 }
              }
           }
        }
     },
     SEQUENCE {
        OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
        NULL =  "NULL";
     },
     BIT_STRING {
        #00,
        #504618EC92337F5AF38B64701897828FC9EE15B1AEF2DDCFA4A161DBB7
        274F2AAD4563B5D4354B064B4F6C709F833851FBFAB3270AFE9C580621F3
        8ACCB4A4E4D591189ADA1240E9A9558F2271399FCF62F6644EB6E03E524E
        59BF1D3F12B6A6D3456DFEEA36DD16320FA63BFFE0EC13D21296C83CE8BF
        E37277D7768C502C142F287CC2C6EA8EA679F1C48B15466D61C26ABE04BC
        2B097AC348B31D403D7F4160F301398A99D2B05FEF232A3C2DFDE2E2777E
        0512418D2DC4C6FEED3B4EE2BEA97BE1A1CA64F7F4851E39599B7625BC6D
        0521E62A63CD604ED4C55BF95E08265813AD8A0DDC63450A281BE3806C8D
        71510A1DB96E9CC7B5509F1A22D782F2CA83918A8A1553113EBDF21F3254
        8761BC964E5B3C0145A544D24FEEAAF1E61FC4776CBADCF999F31505F367
        E1708CEB5C4EFE559A568C7EF158B00B68478EC4FB2A5F5334C6362A7F41
        495F0EC03EDD46B4A1F3390CEB7D91E580489B50C7F9B2B09E94EE3D594F
        22FC3E423F6036BD9D190601E1A127F99FE57EF45347B946B5737B95CEFF
        314946C2AB81AFF6363D5366605212B26CB5F32726C70E445BF0F2D39C0C
        9796404D1FADD9BD17D87FE6983B53EAEC14F0E9EC40B49C9651748D87D8
        C8D4F4F6D1135D7E9788D956660A29EA24A3AB50381187907C34B18ACFA3
        115FDE116117A2DB27ED23AB28681FF68088D29EA3D0ACCA525E8AF3D5E2
        49CB83
     }
}
```

10.14. Social Welfare and Healthcare Professional Certificate – Non-repudiation (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  300100057; -- Certificate serial number
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String {
                  "Sosiaali- ja terveydenhuollon testiammattivarmenteet"
               }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String {
                  "VRK TEST CA for Social Welfare and Healthcare Prof. Certs"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180912125829Z" }, -- not before
         UTCTime { "230913235959Z" }  -- not after
      },
      SEQUENCE {
```

```
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
            PrintableString =  "FI";
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.12";   -- id-at-title
            UTF8String { "001 lääkäri, läkare" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.65";   -- id-at-pseudonym
            UTF8String { "123455" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
            PrintableString { "12345678901" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
            UTF8String { "Lauri" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
            UTF8String { "Lääkäri" }
         }
      },
      SET {
         SEQUENCE {
            OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
            UTF8String { "Lääkäri Lauri 12345678901" }
         }
      }
   },
   SEQUENCE {
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.1" },   -- RSA encryption
         NULL =  "NULL";
      },
```

```
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {
                  #00F0CAFB83BF5AA841DD68DF06A8B234DE73042F1699B5DBA66F364F49
                  C2677A1531B0AC410C951EC6F9AC9FD23D200C634D39F44848755DEF9163
                  160593C8B46D0A32542B481F01DC2212002124BEB1E7F3CAA1D15A9B0534
                  984501278385CEADF916BA7E1C9B00765E10F50E534418E89434BA4D9215
                  95129AA793D8510ACD1C2A13000B32931693BDE2B3AE08CE8A5EF5EC8816
                  64E3C882DF029B4AA395F6D89CF1AE30AA83CB7188A34C2231B059EA6CC0
                  DF5157D05452BF2728B463E351BCF7A9AE6DD6455BC2CF22EA49E7AB03AF
                  B8D4D8ABE0C17ABF310F783A44BBA4EEAFE8289FC27EF427B36BC14F1554
                  611C8505F99A41D1D68BC73A73FEB767E29E4DC28355B7116CC86E43E050
                  461073B30760DB40B58AAE0B876B118B01EC9798FE434546D88E46BFDC8F
                  C4F696C22B6D67CEF9C3A76462F5B90BD0E0480F7F3133D941FC0B1EF3F3
                  62245E320687A82102838EB7614195EDFDEBF239F03B3E1FC998B9A23946
                  E57C58A56065323EFD40A02E268C9CEB4692D597C7357FCC8419
               },
               INTEGER =  65537;
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#2365BD40E0E6FC68AA1266DEEAE0B3EBB473CB5D }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#6032AC8A3FE86F55912C11BB82E25C7B98A049CA } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- nonRepudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
```

```
                SEQUENCE {
                   SEQUENCE {
                      OBJECT_IDENTIFIER { "1.2.246.517.99.206.1" }, -- TEST CA for Social
Welfare and Healthcare Prof. Certs CPS
                      SEQUENCE {
                         SEQUENCE {
                            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                            IA5String { "http://www.fineid.fi/cps99/" }
                         },
                         SEQUENCE {
                            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                            SEQUENCE {
                               VisibleString {
                                  "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
                               }
                            }
                         }
                      }
                   }
                }
             },
             SEQUENCE {
                OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
                BOOLEAN =  #FF; -- critical
                OCTET_STRING [ PRIMITIVE ] {
                   SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
                }
             },
             SEQUENCE {
                OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
                OCTET_STRING [ PRIMITIVE ] {
                   SEQUENCE {
                      SEQUENCE {
                         CONTEXT_SPECIFIC [ 0 ] {
                            CONTEXT_SPECIFIC [ 0 ] {
                               CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
                                  "http://proxy.fineid.fi/crl/vrktshcpc.crl"
                               }
                            }
                         }
                      }
                   }
                }
             },
             SEQUENCE {
                OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
```

```
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                     CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktshcp.crt" }
                  },
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                     CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktshcp" }
                  }
               }
            }
         },
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.3" }, -- qcStatements
            OCTET_STRING [ PRIMITIVE ] {
               SEQUENCE {
                  SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.1" } }, -- QcCompliance
                  SEQUENCE {
                     OBJECT_IDENTIFIER { "0.4.0.1862.1.6" },
                     SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.6.1" } } -- esign
                  }
               }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #92995984F18EAD143C77E27D82F185BC6BC20ED50CC779212EF75CF4B0
      41958663A137F16D1079C727F3B279DB9F34E0B47BBD92A111652A8A5CD8
      47CFC724100F3E8343524703EA08E6743285E1BB6BD96D288D5B916892DF
      5E0E5D777288D1160A7167D53828EE1C18952E02EA95E7A65ECC65F7C892
      0ABCC8E34CFA46C00C0BE7F94B7F312FA5740C3851C0F222776F2E066101
      AA1C0516E4F83309E1943AF24DB08022FE010A79C03CE2ACB764D2CDB30B
      CEE25B99DE65A2CE1C5D60F218FAC64B291FADFA4CBF24A1FA6B9F5BE577
      31BF7388ECA1C9EC5C341CC75C77A103F04EAA93DFB37A74B8F8BFDA6EB1
      D060502C41CAE2F89FE63FC822BA5250CCD3AFFA1D289CEA79C19D8D18C4
      30100F0A3A650859F8A5C9FA4D3C17B45A33E614322926D6DAEE3ADB1676
      E74EA5969DF479EBC94055104758B8C615F4389D74B9C243DD9BEA87351D
      3190C1F137C1467A0EB4D470911D09FD1578FD1B925E127F2DA6E029EB07
```

```
      F3E47928325CDA5A381B9FC25E80EAC1E7498AE035C1FF019764AD72D031
      82FF3872D3FCA5B5C573E18292E00C573EB54EAE20102198466E2F2BDD48
      F25D02843CF9111BD775BD87D3F7BFEE12589918622AFFF84A256BBC4A93
      DD6ADAC0F463FCBC0CCAFBA7BFC74CDA7591CD1EAD586B5EDC4FD31A91F2
      8A7A657EBB2827A6EC13A4017CF8F577900509DD34D4D44E70BAB33FF081
      16E070
   }
}
```

10.15. Social Welfare and Healthcare Professional Certificate – Non-repudiation (ECC)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER =  2; }, -- x509v3 certificate
      INTEGER =  300100056;
      SEQUENCE {
         OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
         NULL =  "NULL";
      },
      SEQUENCE {
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.10";   -- id-at-organizationName
               UTF8String { "Vaestorekisterikeskus TEST" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.11";   -- id-at-organizationalUnitName
               UTF8String {
                  "Sosiaali- ja terveydenhuollon testiammattivarmenteet"
               }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String {
                  "VRK TEST CA for Social Welfare and Healthcare Prof. Certs"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime { "180911122741Z" }, -- not before
         UTCTime { "230912235959Z" }  -- not after
      },
      SEQUENCE {
         SET {
```

```
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.6";   -- id-at-countryName
               PrintableString =  "FI";
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.12";   -- id-at-title
               UTF8String { "001 lääkäri, läkare" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.65";   -- id-at-pseudonym
               UTF8String { "123455" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.5";   -- id-at-serialNumber
               PrintableString { "12345678901" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.42";   -- id-at-givenName
               UTF8String { "Lauri" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.4";   -- id-at-surName
               UTF8String { "Lääkäri" }
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.4.3";   -- id-at-commonName
               UTF8String { "Lääkäri Lauri 12345678901" }
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER { "1.2.840.10045.2.1" }, -- EC Public Key, Elliptic curve
cryptography
            OBJECT_IDENTIFIER { "1.3.132.0.34" } -- 384bit curve szOID_ECC_CURVE_P384
         },
```

```
         BIT_STRING {
            #00,
            #04C2027A9977B07719111C35D25419E6786B64865D4DC559002972F560
            3D69DEB973E878DE9D40D1CB9AFE1E89B7A13B9B9EBD76D9456D2BBDFC56
            3A58AFD74F1C3BDFCCBBB0F68F815B0BA26BC1035B850DD26AF3529CE917
            42D4E645DF1C96A0
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.35";   -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0, "IMPLICIT" ] {
#2365BD40E0E6FC68AA1266DEEAE0B3EBB473CB5D }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.14";   -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING {
#F9B467A917216B057257D2C60DB56901E10505CA } }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.15";   -- Key Usage
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- nonRepudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.32";   -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.2.246.517.99.206.1" }, -- TEST CA for Social
Welfare and Healthcare Prof. Certs CPS
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.1" }, -- CPS
                              IA5String { "http://www.fineid.fi/cps99/" }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.2.2" }, -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikat policy
finns - Certificate policy is available http://www.fineid.fi/cps99"
```

```
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.19";   -- Basic Constraints
               BOOLEAN =  #FF; -- critical
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN =  #00; } -- CA Certificate=False
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER =  "2.5.29.31";   -- CRL Distribution Points
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        CONTEXT_SPECIFIC [ 0 ] {
                           CONTEXT_SPECIFIC [ 0 ] {
                              CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
                                 "http://proxy.fineid.fi/crl/vrktshcpc.crl"
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.1" }, -- AIA point (Authority Information
Access)
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.2" }, -- CA Issuers
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://proxy.fineid.fi/ca/vrktshcp.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.48.1" }, -- OCSP
                        CONTEXT_SPECIFIC [ 6, "IMPLICIT" ] {
"http://ocsptest.fineid.fi/vrktshcp" }
                     }
                  }
               }
            },
```

```
            SEQUENCE {
               OBJECT_IDENTIFIER { "1.3.6.1.5.5.7.1.3" }, -- qcStatements
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.1" } }, -- QcCompliance
                     SEQUENCE {
                        OBJECT_IDENTIFIER { "0.4.0.1862.1.6" },
                        SEQUENCE { OBJECT_IDENTIFIER { "0.4.0.1862.1.6.1" } } -- esign
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE {
      OBJECT_IDENTIFIER { "1.2.840.113549.1.1.13" }, -- SHA-512 with RSA Encryption
      NULL =  "NULL";
   },
   BIT_STRING {
      #00,
      #5FE87BA8F764F371D75003B74B8CF34A064E3D0A0649DF7F475E278EBF
      FCDB67A37ACF5328432ADEB0CF970E6ECF55217F3B0E8D193214627C1D08
      3B8ED4B7FC35583D42867EC67A11402A24985BB6F521C84BFDC02EADF52D
      1BE3D0AF1C435C923989EACAFA0105D8A7A74A1D961E72EFA48AE2E939FD
      69D50BEC478658296CF323FF7B522B96E6B72D7F92B4832036F17809D48F
      9F4664DEDE3CC3662B6588C2B64F460E0855BB008992C75DA7D98C93669D
      A8FE3F26FDD115F886AE05B1AC9D888018CD7EE2A9A2775233C57A21D185
      E111AD6B8BEFC1FF0CEAF7D706154480A33BBFD8C007B9452439A3300F1A
      75095F4D650A5A2849C518B93C06C6542D65FD403DCC514FB3799A66D323
      BFFEE0BA3409065FCD8D1C87CD8422554274C38D9746628543594A8FA9B7
      D8C46A4C77395F859EBFC3AC8B62EEA90E6134A5493CF193B8DF81980DFC
      885E1A6360927AD6AEC57441E00082FD3C3B903CD60FFF711049BB5ECAC8
      F2945A034856349957A6A9B378FBC5947DCF8FA0BEB66D056713C34C5220
      746EF8509C8CAD9211C67D8836C706732C403F2A6536F5756B76AAF9937A
      A65C752A9D7AB36D66068075283CA06531CFBBEEF67DBC4A3F5C39A45DEE
      55B77B6E4C484B4F5DEA48208493FE2590C0BED381F77EB0E757B3AEF4A4
      E0F97BFDEB6C41A7877AF266A753810FB3FB246BE5755262CE94CC6295FC
      4122B8
   }
}
```