FINEID - S2
DVV CA model and certificate contents

v5.0

Digital and Population Data Services Agency (DVV)
Certification Authority Services
P.O. Box 123
FIN-00531 Helsinki
Finland
https://dvv.fi/varmenteet

Authors

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

Document history

Version	Date	Editor	Changes	Status
5.0	2.12.2021	JP	Updated specifications and examples according to G3 root hierarchy.	Accepted
4.01	9.9.2020	JP	Fixed some of the test CA hashes that were calculated accidentally from PEM encoded certificates instead of DER. Production CA certificates were not affected. Changed VRK to DVV for administrative purposes. This does not affect CA hierarchy.	Accepted
4.0	19.9.2018	JP	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.	Accepted

Contents

0.1. Introduction 1
0.2. About FINEID specifications in general 1
1. FINEID S2 4
2. About DVV's certificates 5
3. Root CA model 6
4. Root certificates 10
5. Intermediate CA certificates 10
5.1. CA certificates 11
6. Certificate contents 12
6.1. Basic certificate fields 12
6.2. Certificate Fields 13
6.2.1. tbsCertificate 13
6.2.2. signatureAlgorithm 13
6.2.3. signatureValue 13
6.3. TBSCertificate 14
6.3.1. version 14
6.3.2. serialNumber 14
6.3.3. signature 14
6.3.4. issuer 15
6.3.5. validity 16
6.3.6. subject 17
6.3.6.1. Citizen certificates 18
6.3.6.2. User certificates for organisational usage 19
6.3.6.3. User certificates for Social Welfare and Healthcare Professional usage 19
6.3.6.4. Service certificates 21
6.3.6.4.1. Server certificates 21
6.3.6.4.2. System signature certificates 22
6.3.6.4.3. Service certificates for email usage 23
6.3.7. subjectPublicKeyInfo 24
6.3.8. Certificate extensions 24
6.3.8.1. authorityKeyIdentifier 25
6.3.8.2. subjectKeyIdentifier 26
6.3.8.3. keyUsage 27
6.3.8.4. certificatePolicies 28
6.3.8.5. subjectAltName 29

6.3.8.6. Basic Constraints 30
6.3.8.7. extendedKeyUsage 31
6.3.8.5. cRLDistributionPoints 32
6.3.9. Private extensions 33
6.3.9.1. authorityInfoAccess 33
6.3.9.2. qcStatements 34
7. Certificate and Authority Revocation Lists 36
7.1. CertificateList Fields 36
7.1.1. tbsCertList 36
7.1.2. signatureAlgorithm 37
7.1.3. signatureValue 37
7.2. Certificate List "To Be Signed" 37
7.2.1. Version 37
7.2.2. Signature 37
7.2.3. Issuer Name 38
7.2.4. This Update 38
7.2.5. Next Update 38
7.2.6. Revoked Certificates 38
7.3. Extensions 38
7.3.1. CRL Extensions 38
7.3.1.1. Authority Key Identifier 39
7.3.1.2. CRL Number 39
7.3.1.3. Issuing Distribution Point 39
7.3.2. CRL Entry Extensions 40
7.3.2.1. Reason Code 40
7.3.2.2. Invalidity Date 40
Certificate information summary 42
8.1. Common subject and issuer attributes 42
Root and CA certificates: 43
End entity certificates: 44
Test Root and CA certificates: 46
Test end entity certificates: 47
8.2. Root and CA Certificate Fingerprints (hash digests) 48
Root and CA certificates: 48
Test Root and CA certificates: 49
8.3. Root and CA Certificate AIA and CDP uris 50
Root and CA certificates: 50

Test Root and CA certificates: 50
Root and CA certificates: 52
Test Root and CA certificates: 52
8.4. CA Certificate OCSP URLs 53
Root and CA certificates: 53
Test CA certificates: 53
9. Root, CA and End Entity Certificate examples and example of Certificate Revocation List 54
9.1. Root Certificate (RSA) 54
9.2. Root Certificate (ECC) 57
9.3. CA Certificate (RSA) 59
9.4. CA Certificate (ECC) 62
9.5. Citizen Certificate - Authentication & Encryption (RSA) (old example) 65
9.6. Citizen Certificate – Non-repudiation (RSA) (old example) 68
9.7. Citizen Certificate – Non-repudiation (ECC) (old example) 71
9.8. User Certificate for Organisational usage - Authentication & Encryption (RSA) 74
9.9. User Certificate for Organisational usage - Authentication & Encryption (ECC) 77
9.10. User Certificate for Organisational usage – Non-repudiation 80
9.11. Service Certificate (RSA) (old example) 83
9.12. Certificate Revocation List 87
9.13. OCSP Responder Certificate 88
9.14. Time Stamping Certificate (old example) 91
9.15. Social Welfare and Healthcare Professional Certificate – Authentication & Encryption (RSA) 95
9.16. Social Welfare and Healthcare Professional Certificate – Non-repudiation (RSA) 98

0.1. Introduction

This document describes the CA model and certificate contents issued by Digital and Population Data Services Agency (DVV).

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 Digital and Population Data Services Agency (DVV)	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

https://dvv.fi/en/fineid-specifications

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://docs.microsoft.com/en-US/troubleshoot/windows-server/windows-security/enabling-smart-card-logon-third-party-certification-authorities

RSA-based Cryptographic Schemes and Public-Key Cryptography Standards

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/

CA/Browser Forum Baseline Requirements (BR) document available at

https://cabforum.org/baseline-requirements-documents/

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 Digi- ja väestötietovirasto (DVV) – Digital and Population Data Services Agency. FINEID S2 also describes DVV's CA hierarchy and contents of Authority and Certificate Revocation Lists. This specification also describes Qualified Certificate Profile extensions usage.

The 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 the smart cards they use.

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

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 DVV's certificates

All certificates are issued and administrated by Digital and Population Data Services Agency (Digi- ja väestötietovirasto, DVV), formerly known as Population Register Centre (Väestörekisterikeskus, VRK).

DVV 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. Private keys associated with non-repudiation certificates are generated inside tokens (smart cards) and there are no copies of those keys.

DVV 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 provider's 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, CRL or OCSP service before trusting an intermediate CA certificate. Certificate expiration is not a reason to add intermediate CA certificate into ARL or CRL. Any certificates and CRLs issued by a revoked intermediate CA are invalid after that CA's revocation.

More detailed information is available in Certificate Policies (CP) and Certificate Practice Statements (CPS) available at https://dvv.fi/en/root-certificate-g3.

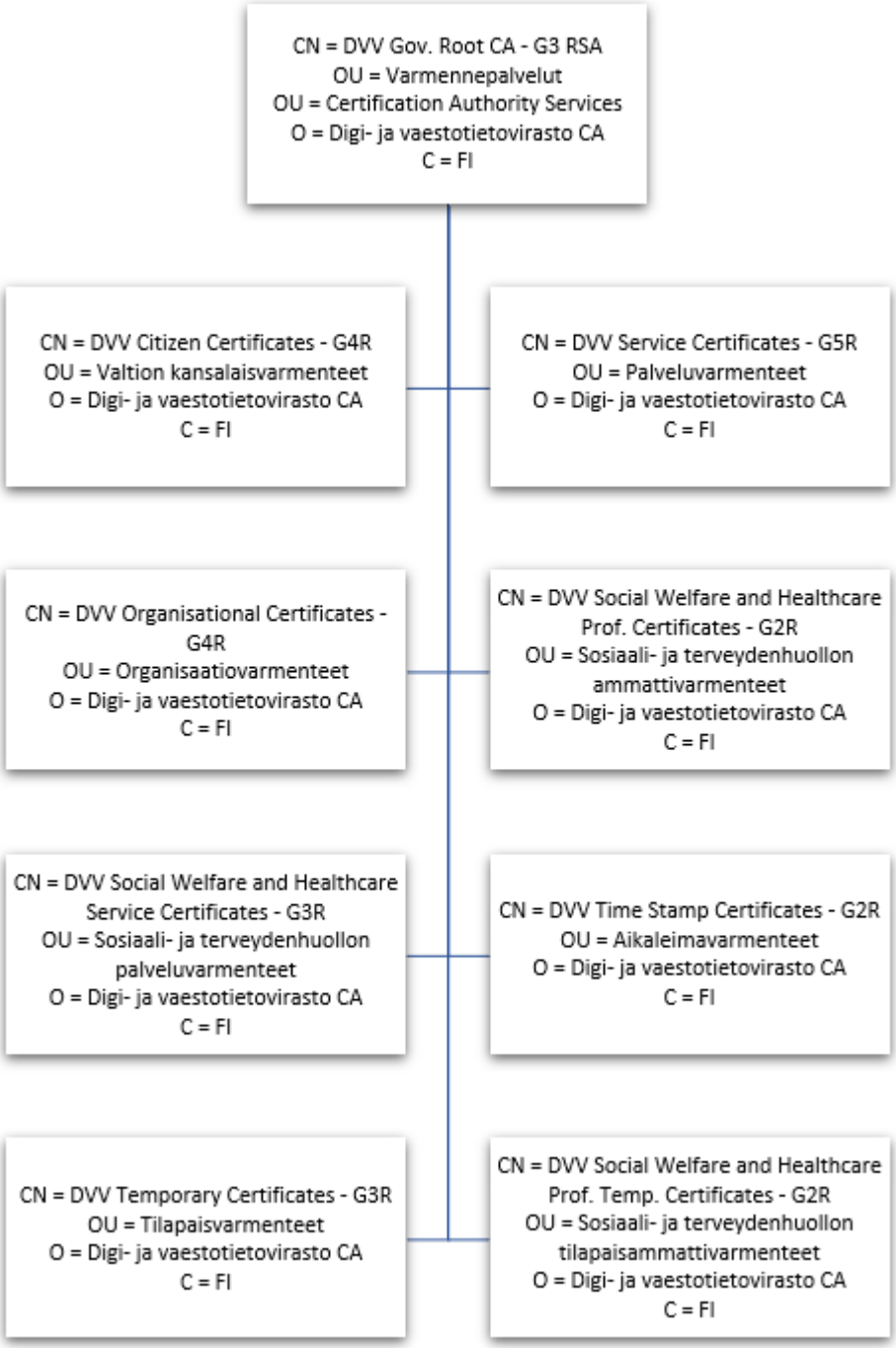
When handling certificates and/or digitally signed data, software products and network services SHALL perform Basic Path Validation as described in RFC 5280, section 6.1. Basic certificate fields. More specific needs can be fulfilled by comparing CPS/policy ID numbers extracted from certificates and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

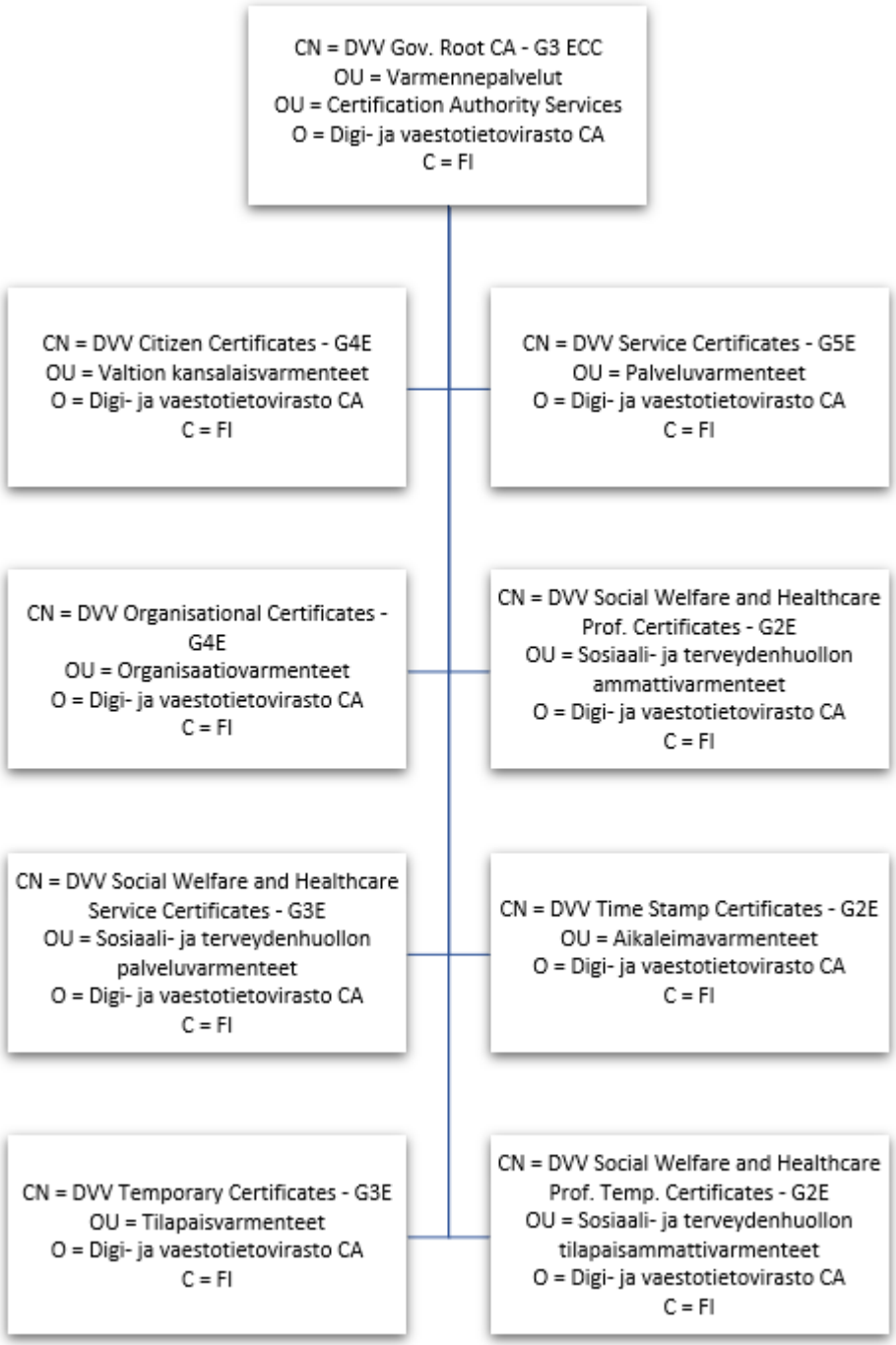
In addition to http services at address proxy.fineid.fi, Root CA and intermediate CA certificates and ARLs and CRLs are also published into a public certificate directory, which is available using LDAP protocol at ldap.fineid.fi. Certificate directory contains also valid, public end user certificates.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

3. Root CA model

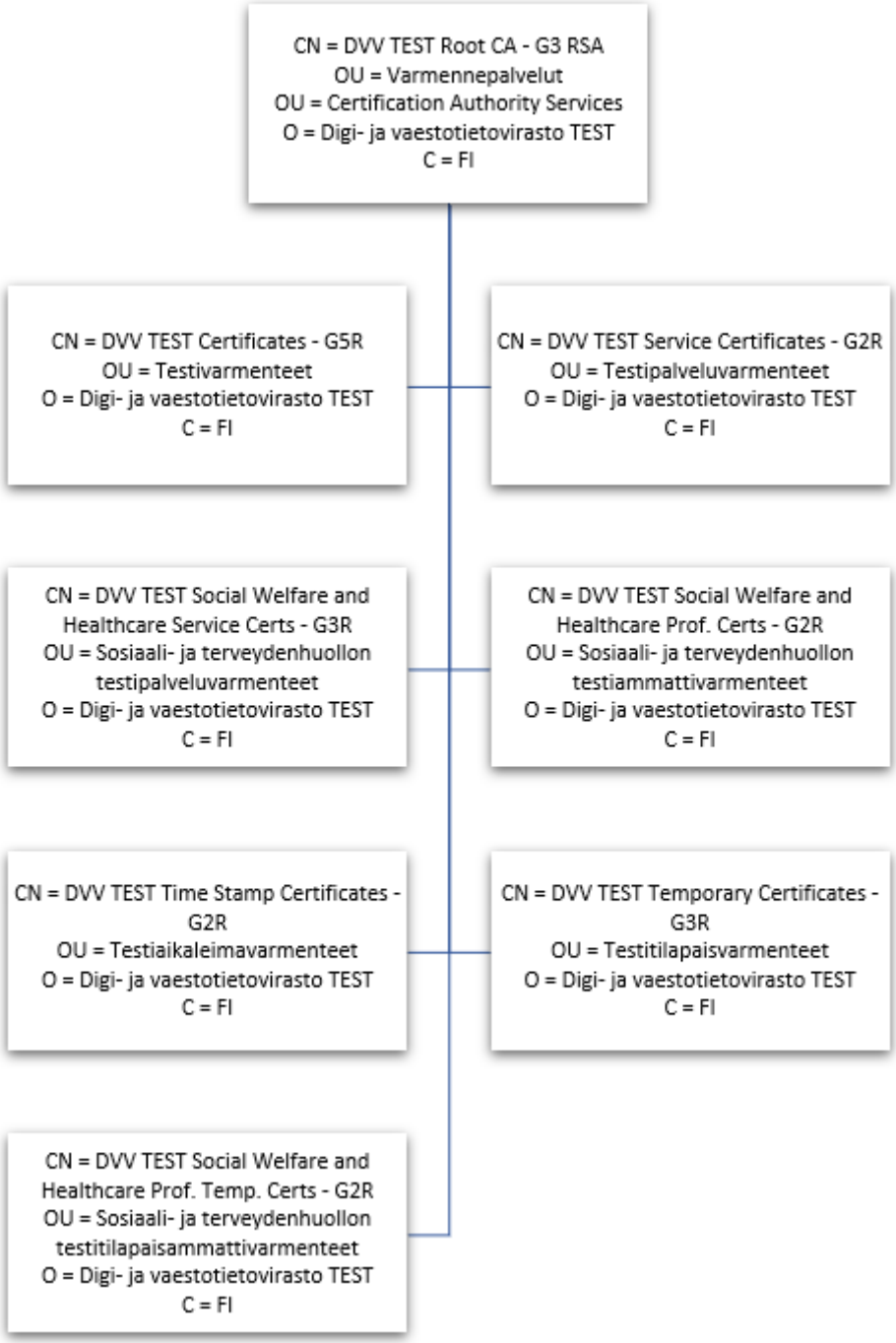
The CA model is based on a common Root CA where Root Certificate is self-signed and other DVV's intermediate CAs are signed by DVV Root CA. The G3 Root Certificates DVV Gov. Root CA - G3 RSA and DVV Gov. Root CA - G3 ECC were created on 06.05.2021.

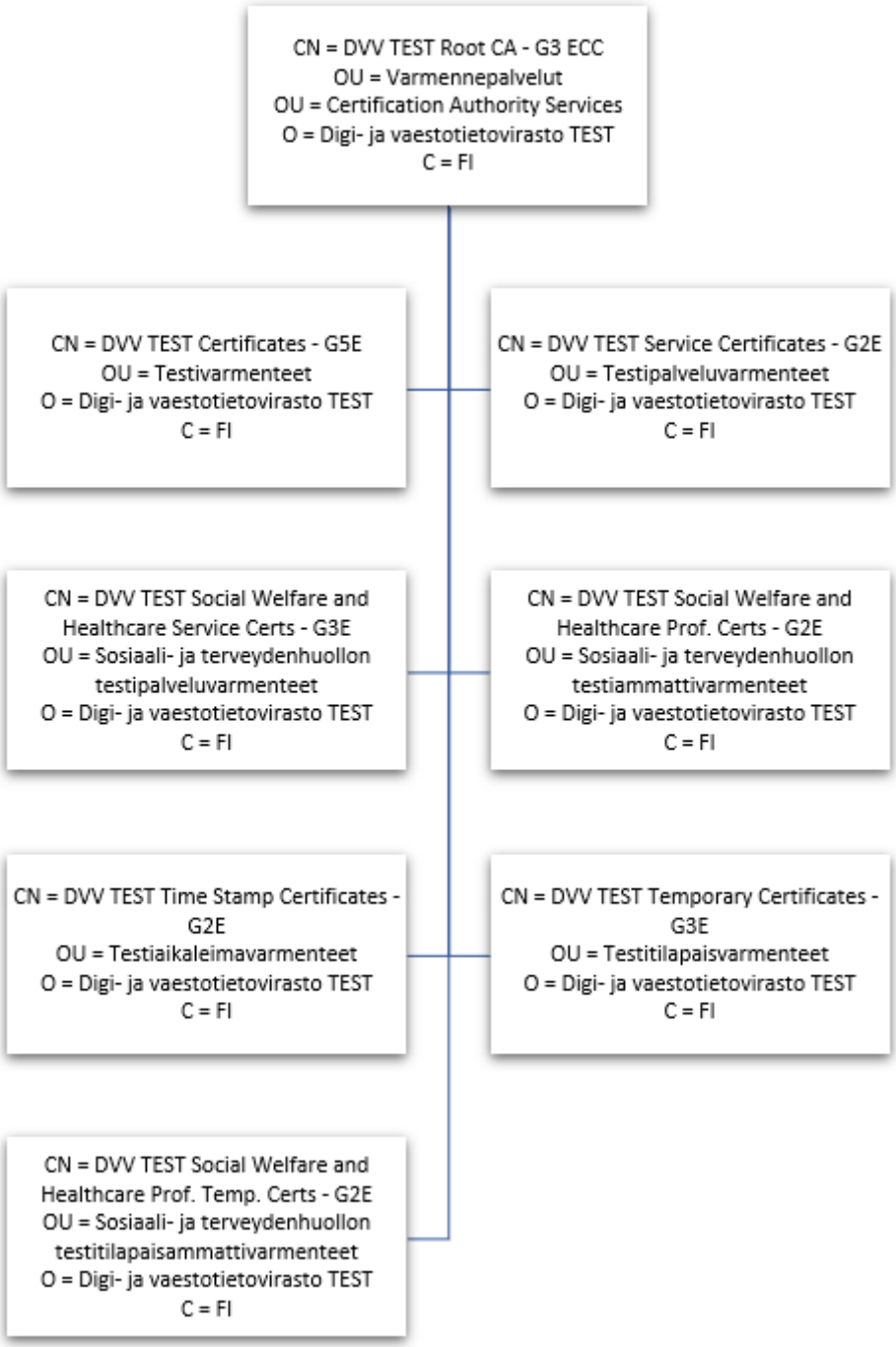
Intermediate CAs for ECC temporary certificates DVV Temporary Certificates - G3E and DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E will be issued at a later date due to technical reasons.




CN = DVV Gov. Root CA - G3 ECC
OU = Varmennepalvelut
OU = Certification Authority Services
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Citizen Certificates - G4E
OU = Valtion kansalaisvarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Service Certificates - G5E
OU = Palveluvarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Organisational Certificates - G4E
OU = Organisaatiovarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Social Welfare and Healthcare Prof. Certificates - G2E
OU = Sosiaali- ja terveydenhuollon ammattivarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Social Welfare and Healthcare Service Certificates - G3E
OU = Sosiaali- ja terveydenhuollon palveluvarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Time Stamp Certificates - G2E
OU = Aikaleimavarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Temporary Certificates - G3E
OU = Tilapaisvarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI
CN = DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E
OU = Sosiaali- ja terveydenhuollon tilapaisammattivarmenteet
O = Digi- ja vaestotietovirasto CA
C = FI

The G3 Test Roots were created on 26.04.2021. Intermediate CAs for ECC test temporary certificates DVV TEST Temporary Certificates - G3E and DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2E will be issued at a later date due to technical reasons.





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 DVV'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 DVV intermediate CAs and end entity certificates.

4. Root certificates

Root CA Certificate	Public key length	Signed by
'DVV Gov. Root CA – G3 RSA'	4096 bit RSA	Self-signed
'DVV Gov. Root CA – G3 ECC'	384 bit ECDSA	Self-signed

The Root certificate shall look like an ordinary end user X.509v3 certificate with the 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 DVV. It is also a trivial task to test DVV intermediate certificate signature against suspicious Root certificate.

DVV Root Certificate "fingerprints" (hashes) are also listed in **section** Virhe. Viitteen lähdettä ei löytynyt.**.**

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 the 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 Root Certificate certificateRevocationList 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, DVV'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 DVV. It

is also a trivial task to test end entity certificate signature against a suspicious intermediate CA certificate.

For complete list of DVV Root and Intermediate CA Certificates, see **section** Virhe. Viitteen lähdettä ei löytynyt.**.**

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

5.1. CA certificates

DVV Root certificate and issuing 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 key length**	**Signed by**
'DVV Citizen Certificates – G4R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Organisational Certificates – G4R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Service Certificates – G5R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Temporary Certificates – G3R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Time Stamp Certificates – G2R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Citizen Certificates – G4E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
'DVV Organisational Certificates – G4E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
'DVV Service Certificates – G5E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
'DVV Temporary Certificates – G3E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
'DVV Time Stamp Certificates – G2E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
Social Welfare and Healthcare CA Certificates		
'DVV Social Welfare and Healthcare Prof. Certificates - G2R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Social Welfare and Healthcare Service Certificates – G3R'	4096 bit	'DVV Gov. Root CA – G3 RSA'
'DVV Social Welfare and Healthcare Prof. Certificates - G2E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
'DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'
'DVV Social Welfare and Healthcare Service Certificates – G3E'	384 bit EC	'DVV Gov. Root CA – G3 ECC'

Note: Certificates issued by 'DVV Service Certificates – G5R', 'DVV Service Certificates – G5E', 'DVV Social Welfare and Healthcare Service Certificates – G3R', 'DVV Social Welfare and Healthcare Service Certificates – G3E', 'DVV Time Stamp Certificates – G2R' and 'DVV Time Stamp Certificates – G2E' 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 DVV.

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 9. 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 for RSA certificates:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

The following algorithm SHALL be used for ECC certificates:

1.2.840.10045.4.3.3 – ecdsa-with-SHA384

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

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 and adhere to CA/Browser Forum requirements on serial number entropy.

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 for RSA certificates:

```
1.2.840.113549.1.1.13 – sha512WithRSAEncryption
```

The following algorithm SHALL be used for ECC certificates:

```
1.2.840.10045.4.3.3 – ecdsa-with-SHA384
```

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	‘DVV Citizen Certificates – G4R’
organizationName	{ id-at 10 }	An informative unique name of the issuing organisation	UTF8String	‘Digi- ja vaestotietovirasto 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 DVV's CA certificates have same issuer:

```
o=Digi- ja vaestotietovirasto CA
c=FI
```

Note: DVV's official Finnish name is "Digi- ja väestötietovirasto". For compatibility reasons, the name 'Digi- ja väestötietovirasto' is written in certificates without diereses ('Digi- ja vaestotietovirasto'). Letters 'CA' are also added to issuer organisation name (o='Digi- ja vaestotietovirasto' vs. 'o=Digi- ja vaestotietovirasto CA'). This method distinguishes DVV's role as a normal organisation and DVV's role as Certification Authority for example in situations where DVV issues certificates for DVV's own 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

DVV 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.dvv.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 2'
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’
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’ ‘Digi- ja väestötietovirasto’
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

1.2.840.10045.3.1.7 - secp256r1

1.3.132.0.34 - secp384r1

Organisational certificates,

Service certificates,

Social Welfare and Healthcare Service 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 DVV-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 and qscd. **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.

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.

6.3.8.5. 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 a HTTP query pointing to the CRL:

- http://proxy.fineid.fi/crl/dvvsp5rc.crl
- 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. DVV 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 }
id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
```

DVV 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 DVV 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 for RSA certificates:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

The following algorithm SHALL be used for ECC certificates:

1.2.840.10045.4.3.3 – ecdsa-with-SHA384

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 for RSA certificates:

1.2.840.113549.1.1.13 – sha512WithRSAEncryption

The following algorithm SHALL be used for ECC certificates:

1.2.840.10045.4.3.3 – ecdsa-with-SHA384

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 DVV 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
```

Certificate information summary

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.

Root and CA certificates:

Issuer Name	Certificate type	Signed by	Valid from	Valid until	Key length
DVV Gov. Root CA – G3 RSA	Root certificate	DVV Gov. Root CA – G3 RSA	6.5.2021	5.5.2042	4096
DVV Citizen Certificates – G4R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Organisational Certificates – G4R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Service Certificates – G5R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Temporary Certificates – G3R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Social Welfare and Healthcare Service Providers – G3R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Social Welfare and Healthcare Prof. Certificates - G2R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Time Stamp Certificates - G2R	CA certificate	DVV Gov. Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV Gov. Root CA – G3 ECC	Root certificate	DVV Gov. Root CA – G3 ECC	6.5.2021	5.5.2042	EC384
DVV Citizen Certificates – G4E	CA certificate	DVV Gov. Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV Organisational Certificates – G4E	CA certificate	DVV Gov. Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV Service Certificates – G5E	CA certificate	DVV Gov. Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV Temporary Certificates – G3E	CA certificate	DVV Gov. Root CA – G3 ECC			EC384
DVV Social Welfare and Healthcare Service Certificates – G3E	CA certificate	DVV Gov. Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV Social Welfare and Healthcare Prof. Certificates - G2E	CA certificate	DVV Gov. Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E	CA certificate	DVV Gov. Root CA – G3 ECC			EC384
DVV Time Stamp Certificates - G2E	CA certificate	DVV Gov. Root CA – G3 ECC	25.5.2021	20.5.2041	EC384

End entity certificates:

Issuer Name	Certificate type	Signed by	Validity period	Key length
DVV Citizen Certificates – G4R	Personal Citizen certificate	DVV Citizen Certificates – G4R	max. 5 years	3072/ EC256
DVV Organisational Certificates – G4R	Organisational certificate	DVV Organisational Certificates – G4R	max. 5 years	3072
DVV Service Certificates – G5R	Service certificate	DVV Service Certificates – G5R	max. 2 years	2048, 3072, 4096
DVV Temporary Certificates – G3R	Personal certificate	DVV Temporary Certificates – G3R	max. 3 months	3072
DVV Social Welfare and Healthcare Service Certificates – G3R	Service certificate	DVV Social Welfare and Healthcare Service Certificates – G3R	max. 2 years	2048, 3072, 4096
DVV Social Welfare and Healthcare Prof. Certificates - G2R	Personal certificate	DVV Social Welfare and Healthcare Prof. Certificates - G2R	max. 5 years	3072
DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R	Personal certificate	DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2R	max. 3 months	3072
DVV Time Stamp Certificates - G2R	Time Stamp certificate	DVV Time Stamp Certificates - G2R	max. 5 years	2048, 3072
DVV Citizen Certificates – G4E	Personal Citizen certificate	DVV Citizen Certificates – G4E	max. 5 years	EC384
DVV Organisational Certificates – G4E	Organisational certificate	DVV Organisational Certificates – G4E	max. 5 years	EC384
DVV Service Certificates – G5E	Service certificate	DVV Service Certificates – G5E	max. 2 years	EC256, EC384
DVV Temporary Certificates – G3E	Personal certificate	DVV Temporary Certificates – G3E	max. 3 months	EC384
DVV Social Welfare and Healthcare Service Certificates – G3E	Service certificate	DVV Social Welfare and Healthcare Service Certificates – G3E	max. 2 years	EC256, EC384
DVV Social Welfare and Healthcare Prof. Certificates - G2E	Personal certificate	DVV Social Welfare and Healthcare Prof. Certificates - G2E	max. 5 years	EC384

DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E	Personal certificate	DVV Social Welfare and Healthcare Prof. Temp. Certificates - G2E	max. 3 months	EC384
DVV Time Stamp Certificates - G2E	Time Stamp certificate	DVV Time Stamp Certificates - G2E	max. 5 years	EC256, EC384

Test Root and CA certificates:

Issuer Name	Certificate type	Signed by	Valid from	Valid until	Key length
DVV TEST Root CA – G3 RSA	TEST Root certificate	DVV TEST Root CA – G3 RSA	26.4.2021	25.4.2042	4096
DVV TEST Certificates – G5R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Service Certificates - G2R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Social Welfare and Healthcare Prof. Certs - G2R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Social Welfare and Healthcare Service Certs – G3R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Time Stamp Certificates - G2R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Temporary Certificates - G3R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2R	Test CA certificate	DVV TEST Root CA – G3 RSA	25.5.2021	20.5.2041	4096
DVV TEST Root CA – G3 ECC	TEST Root certificate	DVV TEST Root CA – G3 ECC	26.4.2021	25.4.2042	EC384
DVV TEST Certificates – G5E	Test CA certificate	DVV TEST Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV TEST Service Certificates - G2E	Test CA certificate	DVV TEST Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV TEST Social Welfare and Healthcare Prof. Certs - G2E	Test CA certificate	DVV TEST Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV TEST Social Welfare and Healthcare Service Certs – G3E	Test CA certificate	DVV TEST Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV TEST Time Stamp Certificates - G2E	Test CA certificate	DVV TEST Root CA – G3 ECC	25.5.2021	20.5.2041	EC384
DVV TEST Temporary Certificates - G3E	Test CA certificate	DVV TEST Root CA – G3 ECC			EC384
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2E	Test CA certificate	DVV TEST Root CA – G3 ECC			EC384

Test end entity certificates:

Issuer Name	Certificate type	Signed by	Validity period	Key length
DVV TEST Certificates – G5R	Test certificate	DVV TEST Certificates - G5R	max. 5 years	3072/ EC256
DVV TEST Service Certificates - G2R	Test service certificate	DVV TEST Service Certificates - G2R	max. 2 years	2048, 3072, 4096
DVV TEST Social Welfare and Healthcare Prof. Certs - G2R	Test personal certificate	DVV TEST Social Welfare and Healthcare Prof. Certs - G2R	max. 5 years	3072
DVV TEST Social Welfare and Healthcare Service Certs – G3R	Test service certificate	DVV TEST Social Welfare and Healthcare Service Certs – G3R	max. 2 years	2048, 3072, 4096
DVV TEST Time Stamp Certificates - G2R	Test time stamp certificate	DVV TEST Time Stamp Certificates - G2R	max. 5 years	2048, 3072
DVV TEST Temporary Certificates - G3R	Test temporary certificate	DVV TEST Temporary Certificates - G3R	max. 3 months	3072
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2R	Test temporary certificate	DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2R	max. 3 months	3072
DVV TEST Certificates – G5E	Test certificate	DVV TEST Certificates - G5E	max. 5 years	EC384
DVV TEST Service Certificates - G2E	Test service certificate	DVV TEST Service Certificates - G2E	max. 2 years	EC256, EC384
DVV TEST Social Welfare and Healthcare Prof. Certs - G2E	Test personal certificate	DVV TEST Social Welfare and Healthcare Prof. Certs - G2E	max. 5 years	EC384
DVV TEST Social Welfare and Healthcare Service Certs – G3E	Test service certificate	DVV TEST Social Welfare and Healthcare Service Certs – G3E	max. 2 years	EC256, EC384
DVV TEST Time Stamp Certificates - G2E	Test time stamp certificate	DVV TEST Time Stamp Certificates - G2E	max. 5 years	EC256, EC384
DVV TEST Temporary Certificates - G3E	Test temporary certificate	DVV TEST Temporary Certificates - G3E	max. 3 months	EC384
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2E	Test temporary certificate	DVV TEST Social Welfare and Healthcare Prof. Temp. Certs - G2E	max. 3 months	EC384

8.2. Root and CA Certificate Fingerprints (hash digests)

Root and CA certificates:

	SHA-1 (160 bit)	SHA-256 (256 bit)
DVV Gov. Root CA – G3 RSA	EAF83D8427897576CDD1B30957773E5F74B9B7CC	D3ED3FC40AD26B52E001E1E18F4B9449529DEB75A81D5EB680D7B62DB23BA96D
DVV Citizen Certificates – G4R	D412037B6A1E106FD0CCCCA0A15B6667A9E8729B	2176C05E69EE24946A140D13F9EFA222B3F1E768E1E2A67B313969CC03B82064
DVV Organisational Certificates – G4R	0E1A48FCCBFD0B37474FBB8588D9727D5D7CC1CB	DFC3E965176F883A9CF0F68CEAEEAB663EDFD8E79DE3294373C28A856984006F
DVV Service Certificates – G5R	928C568120BA24DFF5BF322C300F3ED58BE0BFF8	46319C69041DB9A0D93DAE802E3002CC615365931FE0976D392E8863E3F3BE31
DVV Temporary Certificates – G3R	EC851F00D657FF550091562ED03DC26111129D35	428089726472CA75A47F8E011AEB6483036973C72CF05478953B2FC2E012B731
DVV Social Welfare and Healthcare Prof. Certificates – G2R	561E1CDD7E6FD225E03D3C99E9A528D69A73C05A	6073359DE6BDFBF83874CBD53D4BDE3D8165A8E7A9F772F02A7C6A48A8E7B77B
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2R	F2D93D816EA98831B7EE4269A871941616B90681	6E73C6A3422AE3BB37AF6D3933092A1F6959C09EB17F0A7E14F539665F50C949
DVV Social Welfare and Healthcare Service Certificates – G3R	CD546F6E432D431DA8C96A7D861F1C3C82405DE0	9D433C237C3AEE7A676C9A2ED4ECCB9E40ED17914655571624F0A89969B634BF
DVV Time Stamp Certificates – G2R	0BDBDFEB7E50FE7E29637650F1813F25170D0926	0D31AAB5D24E108F6F942BE974E1DDFEDD02D7B551E0D6F415D70D31A13E394C
DVV Gov. Root CA – G3 ECC	B2142AA969EB0DDB5CE9024684CD850B69E418E5	5546A52504FBA74F61FFD4890067529ADE3B9C9D07E502592831CCDA9B369FD3
DVV Citizen Certificates – G4E	42CC3F1DA5071357FFBAE213CE338E132904C581	AAD1BEAC4696102A88BF9D518D64F8B014F78F9B152579C9599983131979 24D7
DVV Organisational Certificates – G4E	38CD23716894F1F86257FA2E5C69C5443A712AA2	8FDBDCCB5820F1C79EF8BCE190E2B3CD2CC3D0B6BD8311B1F75FBD48BBC230D4
DVV Service Certificates – G5E	CDB057EA6290E7492E6F36DEDB6B5645B32D8095	93C176167ECA02A1B262B16517AC5FB5FC25D3568D97ECDDD04E3A6126B6C7BA
DVV Temporary Certificates – G3E		
DVV Social Welfare and Healthcare Prof. Certificates – G2E	9E00CB9BFEF5BB44C0F06E814364224D907BF61A	A155B9FB8A372683A3825054F9A5265C55430A68616BAD8A1726E70F09F95A26
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2E		
DVV Social Welfare and Healthcare Service Certificates – G3E	83BEEDDA2D7DED31163E90A5C6FAA3DA52BDF5CA	A5C53CF6843A395E6EC244E9B27D58413295428DED97586FD4F67AA4AB8D49A0
DVV Time Stamp Certificates – G2E	0642099FFF1BCD9CE3C5E1E398A662C316D4AFB2	A4D257032F26F27298679D156E9DF96C6F7ED8C36C096338DFEB24214AC665EE

Test Root and CA certificates:

	SHA-1 (160 bit)	SHA-256 (256 bit)
DVV TEST Root CA – G3 RSA	2F7D6FD3736FA5B0C1997104C1B3948CCCEC3DCB	EEFF5B757F242ED2AF2F4E7E2A6F056CF343986A3D71EF13557084731893E4AA
DVV TEST Certificates – G5R	9A1A86E597145D3D306EA788555CEE00734466E1	25EBB2A40BCD9D740B0FBFAFFC2EF903D85FFDCD46C4AB113667501B1617E2A4
DVV TEST Service Certificates – G2R	18F5ABD86E3E57C07B70BFCA35DBB66EDE490F98	1C6EDDC23BC439DDDC8CCA0F31EAD5748022CE4DD6247EB60434AE480047BB0A
DVV TEST Social Welfare and Healthcare Prof. Certs – G2R	081C863F01D8A4BF6C80E98898AD65550D1B3103	A621F4327B854842364C743CDA22A7B1A5B5522AF5675A08097B963ED0E3C9FE
DVV TEST Social Welfare and Healthcare Service Certs – G3R	CBB9FAB8F2098A895FEDBC0D34660FBC6EAE28A2	1C6EDDC23BC439DDDC8CCA0F31EAD5748022CE4DD6247EB60434AE480047BB0A
DVV TEST Time Stamp Certificates – G2R	1C855C5BF891D2BC9DADF3B1B5F0539710329EEA	3FDF1C52C1642E1F129373E62053F307F425DA12C4E173B59064BBE6497FE408
DVV TEST Temporary Certificates – G3R	142E30BE314F9063141BFAB55A8A58A5992E6263	CF8C69823B430FB3C9682D176B0758D323AED5DCD786FDAE2AB0D58FFF74D978
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2R	4B29CA6F7718A87C1C02BBB4530F6CCD4C84008C	DCBC3E2642028E761A12B1A33C1E8F2B744F3118D2110117DF93649EAAF04F37
DVV TEST Root CA – G3 ECC	82C8BDA4B25FE7AFB7A8E00857BDDC713366394A	BD674BACA77CFD0684C509B291C2D2EB24F67C389B586037CEC7529672A91FCA
DVV TEST Certificates – G5E	83FD76B6144CC24DAEB275611A26896F3B0B52DB	3EABE1D1EF7BD30DB09734B7DE258F4C4B8B3D9BCBA433B5E96CAD84F914A58D
DVV TEST Service Certificates – G2E	4517D963052EC4723D349C1149479E63DC9CD5A3	8B973FFE7F4B6ABE16232EF6D49DAED1D632BA74AC41CCC4FBF70938AE4A21EB
DVV TEST Social Welfare and Healthcare Prof. Certs – G2E	CB865756B72AF02C91E7AFA7E364752862FEF9AA	669C026FBA7C5772F5DC9753738AE1AD1098D2B2196E7558A5C1228DE55EC99B
DVV TEST Social Welfare and Healthcare Service Certs – G3E	5727DA812336F3A6BEC880C7A5FF195AACC15FDC	CB4E7205C177D57FCCA936384CA8DDA02A4E028D371E2F94178A5B207F95D41C
DVV TEST Time Stamp Certificates – G2E	C4D8E8B2F434BB26273C22BFB131732ECEA04565	00182EEBD3AA7B5CF49903B5C35C457812A63329F53F848AD1BCD1ED6E013C72
DVV TEST Temporary Certificates – G3E		
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2E		

Current software products typically use 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.

8.3. Root and CA Certificate AIA and CDP uris

Root and CA certificates:

CA	Authority Information Access-calssuers
DVV Gov. Root CA – G3 RSA	http://proxy.fineid.fi/ca/dvvroot3rc.crt
DVV Citizen Certificates – G4R	http://proxy.fineid.fi/ca/dvvcqc4rc.crt
DVV Organisational Certificates – G4R	http://proxy.fineid.fi/ca/dvvqc4rc.crt
DVV Service Certificates – G5R	http://proxy.fineid.fi/ca/dvvsp5rc.crt
DVV Temporary Certificates – G3R	http://proxy.fineid.fi/ca/dvvtc3rc.crt
DVV Social Welfare and Healthcare Prof. Certificates – G2R	http://proxy.fineid.fi/ca/dvvshp2rc.crt
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2R	http://proxy.fineid.fi/ca/dvvshpt2rc.crt
DVV Social Welfare and Healthcare Service Certificates – G3R	http://proxy.fineid.fi/ca/dvvshsp3rc.crt
DVV Time Stamp Certificates – G2R	http://proxy.fineid.fi/ca/dvvtss2rc.crt
DVV Gov. Root CA – G3 ECC	http://proxy.fineid.fi/ca/dvvroot3ec.crt
DVV Citizen Certificates – G4E	http://proxy.fineid.fi/ca/dvvcqc4ec.crt
DVV Organisational Certificates – G4E	http://proxy.fineid.fi/ca/dvvqc4ec.crt
DVV Service Certificates – G5E	http://proxy.fineid.fi/ca/dvvsp5ec.crt
DVV Temporary Certificates – G3E	
DVV Social Welfare and Healthcare Prof. Certificates – G2E	http://proxy.fineid.fi/ca/dvvshp2ec.crt
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2E	
DVV Social Welfare and Healthcare Service Certificates – G3E	http://proxy.fineid.fi/ca/dvvshsp3ec.crt
DVV Time Stamp Certificates – G2E	http://proxy.fineid.fi/ca/dvvtss2ec.crt

Test Root and CA certificates:

CA	Authority Information Access-calssuers
DVV TEST Root CA – G3 RSA	http://proxy.fineid.fi/ca/dvvtest3rc.crt
DVV TEST Certificates – G5R	http://proxy.fineid.fi/ca/dvvtp5rc.crt
DVV TEST Service Certificates – G2R	http://proxy.fineid.fi/ca/dvvtsp2rc.crt
DVV TEST Social Welfare and Healthcare Prof. Certificates – G2R	http://proxy.fineid.fi/ca/dvvtshp2rc.crt
DVV TEST CA for Social Welfare and Healthcare Service Certs – G3R	http://proxy.fineid.fi/ca/dvvtshsp3rc.crt
DVV TEST Time Stamp Certificates – G2R	http://proxy.fineid.fi/ca/dvvttss2rc.crt
DVV TEST Temporary Certificates – G3R	http://proxy.fineid.fi/ca/dvvttc3rc.crt
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2R	http://proxy.fineid.fi/ca/dvvtshpt2rc.crt
DVV TEST Root CA – G3 ECC	http://proxy.fineid.fi/ca/dvvtest3ec.crt
DVV TEST Certificates – G5E	http://proxy.fineid.fi/ca/dvvtp5ec.crt
DVV TEST Service Certificates – G2E	http://proxy.fineid.fi/ca/dvvtsp2ec.crt

DVV TEST Social Welfare and Healthcare Prof. Certificates – G2E	http://proxy.fineid.fi/ca/dvvtshp2ec.crt
DVV TEST CA for Social Welfare and Healthcare Service Certs – G3E	http://proxy.fineid.fi/ca/dvvtshsp3ec.crt
DVV TEST Time Stamp Certificates – G2E	http://proxy.fineid.fi/ca/dvvttss2ec.crt
DVV TEST Temporary Certificates – G3E	
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2E	

Root and CA certificates:

CA	CRL distribution points
DVV Gov. Root CA – G3 RSA	http://proxy.fineid.fi/crl/dvvroot3rc.crl
DVV Citizen Certificates – G4R	http://proxy.fineid.fi/crl/dvvcqc4rc.crl
DVV Organisational Certificates – G4R	http://proxy.fineid.fi/crl/dvvqc4rc.crl
DVV Service Certificates – G5R	http://proxy.fineid.fi/crl/dvvsp5rc.crl
DVV Temporary Certificates – G3R	http://proxy.fineid.fi/crl/dvvtc3rc.crl
DVV Social Welfare and Healthcare Prof. Certificates – G2R	http://proxy.fineid.fi/crl/dvvshp2rc.crl
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2R	http://proxy.fineid.fi/crl/dvvshpt2rc.crl
DVV Social Welfare and Healthcare Service Certificates – G3R	http://proxy.fineid.fi/crl/dvvshsp3rc.crl
DVV Time Stamp Certificates – G2R	http://proxy.fineid.fi/crl/dvvtss2rc.crl
DVV Gov. Root CA – G3 ECC	http://proxy.fineid.fi/crl/dvvroot3ec.crl
DVV Citizen Certificates – G4E	http://proxy.fineid.fi/crl/dvvcqc4ec.crl
DVV Organisational Certificates – G4E	http://proxy.fineid.fi/crl/dvvqc4ec.crl
DVV Service Certificates – G5E	http://proxy.fineid.fi/crl/dvvsp5ec.crl
DVV Temporary Certificates – G3E	
DVV Social Welfare and Healthcare Prof. Certificates – G2E	http://proxy.fineid.fi/crl/dvvshp2ec.crl
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2E	
DVV Social Welfare and Healthcare Service Certificates – G3E	http://proxy.fineid.fi/crl/dvvshsp3ec.crl
DVV Time Stamp Certificates – G2E	http://proxy.fineid.fi/crl/dvvtss2ec.crl

Test Root and CA certificates:

CA	CRL distribution points
DVV TEST Root CA – G3 RSA	http://proxy.fineid.fi/crl/dvvtest3rc.crl
DVV TEST Certificates – G5R	http://proxy.fineid.fi/crl/dvvtp5rc.crl
DVV TEST Service Certificates – G2R	http://proxy.fineid.fi/crl/dvvtsp2rc.crl
DVV TEST Temporary Certificates – G3R	http://proxy.fineid.fi/crl/dvvttc3rc.crl
DVV TEST Social Welfare and Healthcare Prof. Certs – G2R	http://proxy.fineid.fi/crl/dvvtshp2rc.crl
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2R	http://proxy.fineid.fi/crl/dvvtshpt2rc.crl
DVV TEST Social Welfare and Healthcare Service Certs – G3R	http://proxy.fineid.fi/crl/dvvtshsp3rc.crl
DVV TEST Time Stamp Certificates – G2R	http://proxy.fineid.fi/crl/dvvttss2rc.crl
DVV TEST Root CA – G3 ECC	http://proxy.fineid.fi/crl/dvvtest3ec.crl
DVV TEST Certificates – G5E	http://proxy.fineid.fi/crl/dvvtp5ec.crl
DVV TEST Service Certificates – G2E	http://proxy.fineid.fi/crl/dvvtsp2ec.crl
DVV TEST Temporary Certificates – G3E	
DVV TEST Social Welfare and Healthcare Prof. Certs – G2E	http://proxy.fineid.fi/crl/dvvtshp2ec.crl
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2E	
DVV TEST Social Welfare and Healthcare Service Certs – G3E	http://proxy.fineid.fi/crl/dvvtshsp3ec.crl
DVV TEST Time Stamp Certificates – G2E	http://proxy.fineid.fi/crl/dvvttss2ec.crl

8.4. CA Certificate OCSP URLs

Root and CA certificates:

CA	Authority Information Access-calssuers
DVV Gov. Root CA – G3 RSA	http://ocsp.fineid.fi/dvvroot3rc
DVV Citizen Certificates – G4R	http://ocsp.fineid.fi/dvvcqc4rc
DVV Organisational Certificates – G4R	http://ocsp.fineid.fi/dvvqc4rc
DVV Service Certificates – G5R	http://ocsp.fineid.fi/dvvsp5rc
DVV Temporary Certificates – G3R	http://ocsp.fineid.fi/dvvtc3rc
DVV Social Welfare and Healthcare Prof. Certificates – G2R	http://ocsp.fineid.fi/dvvshp2rc
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2R	http://ocsp.fineid.fi/dvvshpt2rc
DVV Social Welfare and Healthcare Service Certificates – G3R	http://ocsp.fineid.fi/dvvshsp3rc
DVV Time Stamp Certificates – G2R	http://ocsp.fineid.fi/dvvtss2rc
DVV Gov. Root CA – G3 ECC	http://ocsp.fineid.fi/dvvroot3ec
DVV Citizen Certificates – G4E	http://ocsp.fineid.fi/dvvcqc4ec
DVV Organisational Certificates – G4E	http://ocsp.fineid.fi/dvvqc4ec
DVV Service Certificates – G5E	http://ocsp.fineid.fi/dvvsp5ec
DVV Temporary Certificates – G3E	
DVV Social Welfare and Healthcare Prof. Certificates – G2E	http://ocsp.fineid.fi/dvvshp2ec
DVV Social Welfare and Healthcare Prof. Temp. Certificates – G2E	
DVV Social Welfare and Healthcare Service Certificates – G3E	http://ocsp.fineid.fi/dvvshsp3ec
DVV Time Stamp Certificates – G2E	http://ocsp.fineid.fi/dvvtss2ec

Test CA certificates:

CA	Authority Information Access-calssuers
DVV TEST Root CA – G3 RSA	http://ocsptest.fineid.fi/dvvtest3rc
DVV TEST Certificates – G5R	http://ocsptest.fineid.fi/dvvtp5rc
DVV TEST Service Certificates – G2R	http://ocsptest.fineid.fi/dvvtsp2rc
DVV TEST Temporary Certificates – G3R	http://ocsptest.fineid.fi/dvvttc3rc
DVV TEST Social Welfare and Healthcare Prof. Certs – G2R	http://ocsptest.fineid.fi/dvvtshp2rc
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2R	http://ocsptest.fineid.fi/dvvtshpt2rc
DVV TEST Social Welfare and Healthcare Service Certs – G3R	http://ocsptest.fineid.fi/dvvtshsp3rc
DVV TEST Time Stamp Certificates – G2R	http://ocsptest.fineid.fi/dvvttss2rc
DVV TEST Root CA – G3 ECC	http://ocsptest.fineid.fi/dvvtest3ec
DVV TEST Certificates – G5E	http://ocsptest.fineid.fi/dvvtp5ec
DVV TEST Service Certificates – G2E	http://ocsptest.fineid.fi/dvvtsp2ec
DVV TEST Temporary Certificates – G3E	
DVV TEST Social Welfare and Healthcare Prof. Certs – G2E	http://ocsptest.fineid.fi/dvvtshp2ec
DVV TEST Social Welfare and Healthcare Prof. Temp. Certs – G2E	

DVV TEST Social Welfare and Healthcare Service Certs – G3E	http://ocsptest.fineid.fi/dvvtshsp3ec
DVV TEST Time Stamp Certificates – G2E	http://ocsptest.fineid.fi/dvvttss2ec

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

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

9.1. Root Certificate (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017940CBF49AFEC66649C9F07905DB, -- Certificate serial number
      SEQUENCE {
        OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
      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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         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 = "DVV Gov. Root CA - G3 RSA"
            }
         }
      },
      SEQUENCE {
         UTCTime = "210506083042Z", -- not before
         UTCTime = "420505083042Z" -- 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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         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 = "DVV Gov. Root CA - G3 RSA"
            }
         }
      },
      SEQUENCE {
         SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {

#00C19F0280812D898461664B1B3BA304E1519A1D20088A1660A4F33C4CEA1B903C61292CFF1E4A29
DF442FA76795E7C47792860B5AAD3E25678EBCF8C2F02B9FB195905D115CA7935E49318B5212ADFE
B01EE7E13163C42574E2AC39E50956363A62F8086A6971414AE08FBB78F678EBDD1269F49E483B87
C704EAFF3B885F7F44DC2C4534DA6AEC3684047B1F4C011AA9621F9C7703D49BD988BC46D1EBCD51
1F2AED3D4D060711BFC1733632E9C11A82DE4346AD8296EEE0A8A93E6EB9F22B0B64F3D1934D7B8E
F0C5167BCD1304859FB3D5EF6DD713B92F7E1BDD179B6B84D49CF2667B7592D79142031EE9A9F9B6
1003E6DD262F46EFA24533539D97BE557BAE22858462E638210915A3250757628DD73DF30CDC642A
26836A072FC3095F4BF3F04ED8EA365F66359DE22DF83BA0ECD30B258258CFBF020318E370BA64BA
AA2B860F3AF7BAE8559FE6E8FB7294AEB92299EDA158CA7707BA55EB79A8BA73964380ACD398E173
5E567794AE411759156C804BCF5AB041DE0BACC6162DC7E339D8C5AC39CE3F9ADFB7D64F7EBE8A9F
C229164F05CA00C928898C91191A05CD755B0A3727E02252582D583AB462F3093FBCCCE0633D7AE9
F1EDA0BCFCE9F9E127AF454BD244347AA016487233A95D274F15DA4D8E1D9E56B1645790A8F9DC48
ED660540F4541BD681E27AD17336078C3BF3DADA835B5F0C7876A3FD9D1525DE87
               },
               INTEGER = 65537  -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#5B01E0CF5ED0C480B5508A8138878392BF150C8C }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#5B01E0CF5ED0C480B5508A8138878392BF150C8C }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #01, #06 } -- digitalSignature, nonRepudiation, keyCertSign,
cRLSign
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN = #FF } -- CA Certificate=True
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
Encryption
   BIT_STRING {
      #00,
      #95D1A67C1DD432D3CBBD40C1C4CB73E3FFCBF76B3787006551D24B67068745813FCFE5BACB3D72C6
      7456B5314E3AA11430647AF1A8BA06B2F42DA4B764DA5D3FF24F9C79C92B327AD9E86FC9A1C74EEE
      284CFF65FC1DCB2D011298C344C334C317AA3A5F44D0C11FD2C364920C3E81F4CF888EE8F7E09933
```

```
      015BAEC9CDB004FA794D14B5162925D6DCEC08AED27467AAD9BE7B948C9C07E0E716E0FCF44FC619
      CC2F261215987B3A6860F7D11AC03C31D48D4975AEC23E2E8EAEE85C57A5984AC79A5FFC143454BE
      16E567E6426FE7FD7B774598194A6B7E61718C18E4EBADAA22979E585898174DE7761F40D18E240D
      BFD4172F9560C53DD72A1D63AF89EBF47CE6B57950E801550555EA2C458C5ECDC6A3F2796B85930D
      F9534B5B5A6707CC45DD8CB83D524AA1D8937008B51E22F755C0668D01C48BA21BCE86150BB2218A
      003A8FC6253C8EDC456DE5604AABDAEB2F76731C7A114D76B95797503BA8080982BCFAAD9B9E6851
      0A5E425372D9D9B53F4192793D2817A5A20690D9A59EEAB5E635F8BC08A0E8DD149EC2F35CE60094
      BEBE465DDAD0C14A2880609CFE4AE5ED8B60A991A55606F163288F6DB77A158C7C8ED03CE52CE495
      EEB0DA59A84D58AF80B3E4344B344FF56F586C3CE67D7CC17AB8457A5D17E54A931B546408F0C1AC
      9D55946F224200466591C82519E917ADF85C90BAA8843B94EA73BCDC102357E3
   }
}
```

9.2. Root Certificate (ECC)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017940A7B5DA7D901CA94BF25AAEAE, -- Certificate serial number
      SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
      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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         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 = "DVV Gov. Root CA - G3 ECC"
            }
         }
      },
      SEQUENCE {
         UTCTime = "210506075130Z", -- not before
         UTCTime = "420505075130Z"  -- 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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         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 = "DVV Gov. Root CA - G3 ECC"
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
```

```
            OBJECT_IDENTIFIER = "1.2.840.10045.2.1", -- EC Public Key
            OBJECT_IDENTIFIER = "1.3.132.0.34" -- EC Curve secp384r1
         },
         BIT_STRING {
            #00,
            #04B32DCA3F8AAE92240A92CA05E6E26B0D7DCF2F89ABA75A55F706A6605EA32EAF486DDD0EC4332A
            CAAB54997A888ACFB32F1328D6DDEBB3A8D659CAE7C51A0EDC8D8AACB06B6D5186EF944AFAE8BE4B
            ED5671F01DEA4BB5F5635912B8AF89B130
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0 ] = #B97680C383F8CF22DA85EBCE144E55AC5E5A0A90
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  OCTET_STRING = #B97680C383F8CF22DA85EBCE144E55AC5E5A0A90
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #01, #06 } -- digitalSignature, nonRepudiation, keyCertSign,
cRLSign
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { BOOLEAN = #FF } -- CA Certificate=True
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
   BIT_STRING [ PRIMITIVE ] {
      #00,
      SEQUENCE {
         INTEGER {
            #00BC25EEE1565F7566E84021D47245A55F3B77FACEC720560E7968A5B1BEF0E2F525810C8FA268C2
            5DC96A453F7639AD24
         },
         INTEGER {
            #448368E6613213B185F26DD53CB5FE87B01336CC57F71E3BD96A53E41AEA40FB2DBB5DAD0BEE0100
            4347487975F8BE73
         }
      }
   }
}
```

9.3. CA Certificate (RSA)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #0179A35977CC9256B26B7E9318A576, -- Certificate serial number
      SEQUENCE {
        OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
      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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         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 = "DVV Gov. Root CA - G3 RSA"
            }
         }
      },
      SEQUENCE {
         UTCTime = "210525111442Z", -- not before
         UTCTime = "4105201144422"  -- 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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.11", -- id-at-organizationalUnitName
               UTF8String = "Valtion kansalaisvarmenteet"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "DVV Citizen Certificates - G4R"
            }
         }
      },
      SEQUENCE {
         SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {
```

```
#00AC2030BBA0502F19EA82FD9B49CB1F0A780CD52DBF90B4D82BEB14F2B299BD65ADCFE35B102754
A0303B91A55C762DE324A8EDF0FCBB1E96DD7B8B42A0F2E05006A3F820BF57626675EE859F0082C9
86F4ADC5F3FEBD836440FE8F23A72A37CE3DD73F532E6DE0F905812AF5B138A6A3760226529F5846
814D336DC70CA9D377DA62D50FBE08DBC08A8941DE778DA9C4E7FEB773607764BAB492F55070F995
27B2610CA728CD6C86E3B9E2EBE34A9AE2B4BD8A8A35A0F1CF9D8F87355E46219132884EE0200CD0
C2E222FF97BFDBA945CD3F0D7F0256E66F1E48CDFFCEE97B624D3B93B210D54C73878530BDE495A7
F14CBB0BBA8A8AC4456827CBC5E4380F46E2F175602935A07754D78F86241F92A8243EA10AF129F1
D2C0081738D44625141C4765571C73B25CE6EB1422DFE47A35920B488318A712375AB8A74B6B70F7
F9D982715A9A870A4390CD0D996DC152BD2F71F6D293CDB7CE98BD8208DF159867140F7338D94D94
7EFB535B2DB8C2F8E7FBD1CF54331E45E8B9CA4EC068CE816A2BB5616BE27244DD06B1C31D27B693
A1CF4B56952CE062EDB68E58E5AA083296B4CFE8815E7AB31CD2488C040D5764AD14233B61C72B55
319B58833276C4FADB7192D6B2753B84A0573AF2044F2EBE7666CEB8859D0D59DD05DC67606FE180
6AD3CAACBE83C46EB345A2D5FB9FF03EB12248A2C9170CDD1BAC2DC2BB655BFA5B
               },
               INTEGER = 65537 -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#5B01E0CF5ED0C480B5508A8138878392BF150C8C }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#08D14EB9F21359FFBBF51C2ED823DCD6C1FE3FC4 }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               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 = "1.2.246.517.1.10.301.1",
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.2.2", -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikatpolicy finns
- Certificate Policy is available http://www.fineid.fi/cps51/"
                                 }
                              }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.2.1", -- CPS
                              IA5String = "http://www.fineid.fi/cps51/"
                           }
                        }
                     }
                  }
               }
            },
            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 ] {
                                "http://proxy.fineid.fi/crl/dvvroot3rc.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", -- OCSP
                       CONTEXT_SPECIFIC [ 6 ] = "http://ocsp.fineid.fi/dvvroot3rc"
                    },
                    SEQUENCE {
                       OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.2", -- CA issuers
                       CONTEXT_SPECIFIC [ 6 ] { "http://proxy.fineid.fi/ca/dvvroot3rc.crt" }
                    }
                 }
              }
           }
        }
     }
  },
  SEQUENCE {
       OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
  BIT_STRING {
     #00,
     #90E299F6BCBA748EE3EC0929ABDF2A6EC50BFCACFABAC32D277331F480C09890F055D7D706E847C1
     C8BB8968E73708EE9E70E6B3C1DED87962011C36C7C488A982879D1551C9EB7A325552393E948AEE
     A429B6A617C4034903D608623631DBB9E6F0785BA3C3E945C038FC2443C8D1EF34D0E85C176FD94E
     AFBD3F63E1186992FDFADAC45C13312872AA2C98C644FE115CA5F507B9DB5ADF605C2D6036A9E657
     DC230EC8CD449575C42F74203ED756923696EAE52FD67D8943EACF41706CE46DD72174F34E03FEF3
     B9CC3F486931C9795A54B28CAC4B2F7CBDB337804AD37DBD924EFBD59CBC000005B5AF1F4A84BAE5
     78E3B1BAA38CAF7C24C18C91CE7D229ED44616A4212F2A4AAE05039910814F8696BDFA8AC9935CD1
     C312BB038E5317075BBEBD3215FE46268137162FFA4B29A771D8296A196C8AD8036A5F1A25B36508
     B362C5BA5AF3C3D1B7F97016C6405943F683303AAF1A023BE55EC8C76D5223F1F33215858C0196B7
     C65EA274A5E54A7076783901790F727E4FD64E93FFD76BADE7A87776FB4513606D7B0ED94CC8356B
     05E80FEC3C7EF5C483268AE8CCEDF85E038F8C2537E3D526A49363C89799867601CE5C2CECA71D0F
     625F6D4ED5BD24CF0769465B93593C878A8CB9C17E892E323B4963CBA02F9A14BF559F9ACB2152FC
     E2B39029B0AFDBF1280EE793552AD4A26D2FB2CC0427043DCA5F575A12C40873
  }
}
```

9.4. CA Certificate (ECC)

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #0179A3670FB3CCC2E867398A0103AE, -- Certificate serial number
      SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
      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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         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 = "DVV Gov. Root CA - G3 ECC"
            }
         }
      },
      SEQUENCE {
         UTCTime = "210525113038Z", -- not before
         UTCTime = "410520120038Z"  -- 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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.11", -- id-at-organizationalUnitName
               UTF8String = "Organisaatiovarmenteet"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "DVV Organisational Certificates - G4E"
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER = "1.2.840.10045.2.1", -- EC Public Key
            OBJECT_IDENTIFIER = "1.3.132.0.34" -- EC Curve secp384r1
         },
         BIT_STRING {
            #00,
            #044D62EC9E17645DBA74E36D17333C20675B292E6F88364F77E9C8B64A5C76D57D3BE17C9B2B691B
            2A4CAC3DE00015EF1547F6B3649B4956749191165103 45B40FD07BCF23FBBCEF41F6BF11BC140D51
```

```
            65AD9DC31A401E51299C23649F41A38A33
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0 ] = #B97680C383F8CF22DA85EBCE144E55AC5E5A0A90
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  OCTET_STRING = #67F1355FF184535F6155649A3B207D62B4627698
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               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 = "1.2.246.517.1.10.351.2",
                        SEQUENCE {
                           SEQUENCE {
                              OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.2.2", -- User notice
                              SEQUENCE {
                                 VisibleString {
                                    "Varmennepolitiikka on saatavilla - Certifikatpolicy finns
- Certificate Policy is available http://www.fineid.fi/cps62/"
                                 }
                              }
                           },
                           SEQUENCE {
                              OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.2.1", -- CPS
                              IA5String = "http://www.fineid.fi/cps62/"
                           }
                        }
                     }
                  }
               }
            },
            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 ] {
                                 "http://proxy.fineid.fi/crl/dvvroot3ec.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", -- OCSP
                        CONTEXT_SPECIFIC [ 6 ] = "http://ocsp.fineid.fi/dvvroot3ec"
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.2", -- CA issuers
                        CONTEXT_SPECIFIC [ 6 ] { "http://proxy.fineid.fi/ca/dvvroot3ec.crt" }
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
   BIT_STRING [ PRIMITIVE ] {
      #00,
      SEQUENCE {
         INTEGER {
            #727B1A8AE0DF8119A412DE5F20A7C802D6C6E9CC895A93A612D1B97EB7C665498CBB0DA6BC5A48CA
            0B08996C28DE3E8F
         },
         INTEGER {
            #0D08F53CB1A0D9031C2AB954F7574CAAFF8E5832A694F0C473606E4FFB01128C2BFD99AD1448DB49
            99EE0ADD5619D732
         }
      }
   }
}
```

9.5. Citizen Certificate - Authentication & Encryption (RSA) (old example)

```
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 { "2307052359592" }  -- 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
      }
}
```

9.6. Citizen Certificate – Non-repudiation (RSA) (old example)

```
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
   }
}
```

9.7. Citizen Certificate – Non-repudiation (ECC) (old example)

```
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 { "2307052359592" }  -- 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
   }
}
```

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

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017CC65F069AC44FEBF5854B941193, -- Certificate serial number
      SEQUENCE {
        OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
      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 = "Digi- ja vaestotietovirasto 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 = "DVV TEST Certificates - G5R"
            }
         }
      },
      SEQUENCE {
         UTCTime = "2110281007547", -- not before
         UTCTime = "2609072059597"  -- 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 = "Testiorganisaatio Oy"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.5", -- id-at-serialNumber
               PrintableString = "999052289"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.42", -- id-at-givenName
               UTF8String = "Helena"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.4", -- id-at-surName
               UTF8String = "Huhta"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "Huhta Helena 999052289"
            }
         }
      },
```

```
      SEQUENCE {
         SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {

#00D5ED33DE28145415C98CF0F88B880574DA0288A7E7D8B2BE364410D0BE9000F1C8D6B052FD0752

46BB846821B3198F3264A0F7ADCE2809112415305F92649A21291E7413A69E4C4CAE565871263DE2

E5C05BFF68DEADEBD7BE5C9B81D662881DE1BF2311A8F461674A4E0975E9BCA439F007AD079E3E84

4CF6E2E74BFE002E1665C24BF98551479DC9E9FD1B6ED8DC17D2E6CBB3CCBF732C8CD9636371F377

68C9ED30D5738F2716189442CEDCFBFABBF0E8F54B5361C5AC8C07FDFE71E44472249446230EBA60

BAFC9D41D04ABE3769851D37B287CD67255B4CC78DA8B778204C9F1D4DDE887ECC3EF9ECD517748D

7D906675F2A21778DFCCDD7E93CE621BCA600AF847BB875E7B74EDC299B8C3EA57EDA9E76AB971D6

D84F7DEC65E1EBA27D8C555F16F4C51B3406EB62D47904B471ADF340D6F6C24002CA19440F773D03

8102E15DA0B9BA79FBFFF45FDE71475D930697302074AEC1FBD709C4F371CCEE8C930AEE8CB0C191
                  4C39CB30ACB498E462EB42C5B579E63963992E0893F3C7D331
               },
               INTEGER = 65537 -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#0FAFB7DB485F6076E900F786075FB6C559804F9A }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#5AFAAEA7CB983A69091A35AABA85F6DF9024E3E3 }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               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 = "1.2.246.517.99.10.303.1", -- DVV 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 - Certifikatpolicy 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 UPN
                        CONTEXT_SPECIFIC [ 0 ] { UTF8String = "helena.huhta2@teonet.org" }
                     },
                     CONTEXT_SPECIFIC [ 1 ] = "helena.huhta2@teonet.org"
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               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 ] =
"http://proxy.fineid.fi/crl/dvvtp5rc.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 ] = "http://proxy.fineid.fi/ca/dvvtp5rc.crt"
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.1", -- OCSP
                        CONTEXT_SPECIFIC [ 6 ] = "http://ocsptest.fineid.fi/dvvtp5rc"
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
Encryption
   BIT_STRING {
      #00,
      #7B0D8FB0C33B038BA4EA185AE278921B8A91F9D5BCF013C417F6AD2FB1AD608219E26F75F7141D48
      FE59EA63417CBB8F778193ED2A09BC9CD8AA3D729B8CB7FF083CAA468DF59FABF127E3FDAF4164A9
      83425106A1197C35EA1252C35963C2189DCB3EF6155035BA28604440466FBE981D4387931AE758A1
      9D41FD72FBC67729D623A2E5645FFE080AAF7C249C577E2100768647008EFFDDA4A320E0CE594767
      9DB53CD3A655AC471F0AEE1C29607B64EFDF5C496F2C68B83335BBB0A85080BD94559CC7184DC33B
      D9E119B9E1EED6E9198483083A9666E1FB33CB384DB497290858B570F0E21F26E29DAF0D2AE00A1B
      0EC82DBF7D3F124E15DE9AF70408B1CE4152DFDC3B5C25E4406A94A2C86504C9A4C38A69D4D271A6
      0DDD006AF279DC3935CF823068E56C8952D3B8DC40CCE97AFD09414F53CD77039EE5A2E31A153ACC
      69F81D54F64949402F95528358A9D1862F11F972F81ADB2027F43CDBE364E1BC172C8E18ED7D8EA2
      835EC1D92D896AE83113D64EF302A2C4703735EED72818935DE3B05B095C0C141737DADFA472C9C2
      AEEFE25BC7E0F888F03ECECB2EE479F69DEC5026E00C03E71EA96256710913FC2B38B1EB3CDB1DD0
      FE3B1ACFAED3682CB4A81D05D5A7DC6A0BFAAC8D95C1970B143371DDC41E18A59365AEE51C9FA90F
      3826ADE4CFC5B301B1CA6C76606BDAD86F17510B56282DB5E66BC9D29CE59E09
   }
}
```

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

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017D36CD0C67623683D219D23799E3, -- serial number
      SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
      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 = "Digi- ja vaestotietovirasto 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 = "DVV TEST Certificates - G5E"
            }
         }
      },
      SEQUENCE {
         UTCTime = "2111190605452", -- not before
         UTCTime = "2611122159592"  -- 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 = "Testiorganisaatio Oy"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.5", -- id-at-serialNumber
               PrintableString = "99905236J"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.42", -- id-at-givenName
               UTF8String = "Roman"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.4", -- id-at-surName
               UTF8String = "Kekäläinen"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "Kekäläinen Roman 99905236J"
            }
         }
      },
      SEQUENCE {
```

```
         SEQUENCE {
            OBJECT_IDENTIFIER = "1.2.840.10045.2.1", -- EC Public Key
            OBJECT_IDENTIFIER = "1.3.132.0.34" -- EC Curve secp384r1
         },
         BIT_STRING {
            #00,
            #0478E254337405A5475AB260F1D08509368D10A8A9B03C76C945A46855CF8E265F9E26A8113D4D69
            EE6225FDB3D7A4E708A24F83CC6A29C774FBE19F8AC1D8A7FF72F7A4D6461419E14348671E9E1FD5
            42DB5019C3CC13B205AE3B8A2AE9B652B5
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#129EB7E228C7F3946A8BBD4DC6F4C23697524208 }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#6366CB6E6ADB97494E39EA9EF61A123EEA412A45 }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #03, #88 } -- digitalSignature, keyAgreement
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.32", -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.2.246.517.99.10.353.1",  -- DVV 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 - Certifikatpolicy 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 = "roman.kekalainen@teonet.org" }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               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 ] =
"http://proxy.fineid.fi/crl/dvvtp5ec.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 ] = "http://proxy.fineid.fi/ca/dvvtp5ec.crt"
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.1", -- OCSP
                        CONTEXT_SPECIFIC [ 6 ] = "http://ocsptest.fineid.fi/dvvtp5ec"
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
   BIT_STRING [ PRIMITIVE ] {
      #00,
      SEQUENCE {
         INTEGER {
            #520ACA3D04BBE50AAEDAFEA78414D3FD4B0DBF8939A0A98A884D87C4A58CAE87A54014C2AC24D4F6
            ACAA3396C40D283C
         },
         INTEGER {
            #4BC8827F68385CA18745C82CFDF8A2B0E9433489BE6F48A0066E2283CB0A75D7A20AB941748E627F
            0021F402D8742748
         }
      }
   }
```

9.10. User Certificate for Organisational usage – Non-repudiation

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017CC65F14DAE3B3A3B68E1EBE00EB, -- Certificate serial number
      SEQUENCE {
        OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
      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 = "Digi- ja vaestotietovirasto 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 = "DVV TEST Certificates - G5R"
            }
         }
      },
      SEQUENCE {
         UTCTime = "2110281007582", -- not before
         UTCTime = "2609072059592"  -- 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 = "Testiorganisaatio Oy"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.5", -- id-at-serialNumber
               PrintableString = "999052289"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.42", -- id-at-givenName
               UTF8String = "Helena"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.4", -- id-at-surName
               UTF8String = "Huhta"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "Huhta Helena 999052289"
            }
         }
      },
      SEQUENCE {
```

```
         SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {

#00E1ED1776A21BA60C9A09B43E5110C0DA8BBCEF4FD17E822045E5C1C3471BA3DDCAD957DF364EC8

13D45CE524FB106943CF7B21D5BEDE3174CF56266768AA610CC58DF2FE90BFF7D0394A907076B35E

965DB533F3ECB29AD70EC310947AA7628271FB10A5239C695A0FC75B7DF438C2626BA6A3469D4552

A6EB51D14BC343B0933AA96424D69A6878FA6ADCD600634024902DCC7C0BB7FC28D050D2875784A6

236DAF771431EB39984B8C4AEF313237D3D095670210CC9330A1366E5251CD7F7D306A65AE3F6F38

B1E77EEE5A0FBBDAF6C9AA0E1E051365A6BC240F23F5192B40A8C2FE57AA992C0FBEF5570BFB9A89

7E2FDF8AF7283EEB0F0C2C8871C746D547508E234CF7AF572ED005A608F60B015ACBFBA90CF75257

64263095D29DBFE3B8E8D4A0E0B02EDD323125D21BBBCB1B1381687FED42604E309BB0650BC6D66A

210CACD019621BB0C1425E95EF7C7CF6ED94BF7A179AE1945DEE499B8DA4C91D499788C1D9080B52
                  184094FE9C3DB638D2A36DD0CDA3028D0D84B966FCF33220C1
               },
               INTEGER = 65537 -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#0FAFB7DB485F6076E900F786075FB6C559804F9A }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  OCTET_STRING = #22BE1A0B9E84375B0A451B10F0C7A27C3EBADC26
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               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 = "1.2.246.517.99.10.303.1", -- DVV 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 - Certifikatpolicy 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 ] = "helena.huhta2@teonet.org" }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               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 ] =
"http://proxy.fineid.fi/crl/dvvtp5rc.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 ] = "http://proxy.fineid.fi/ca/dvvtp5rc.crt"
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.1", -- OCSP
                        CONTEXT_SPECIFIC [ 6 ] = "http://ocsptest.fineid.fi/dvvtp5rc"
                     }
                  }
               }
            },
            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 = "0.4.0.1862.1.4" } -- QSCD
                  }
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
Encryption
   BIT_STRING {
      #00,
      #2F58CA932FEFFAF2B17A208DC1E5ED3AB4D86BCBB56D1EBB0477BE5A88E7C56172C9FDFC4B62249F
      A6A5344272B0292D4E15AA77DC2F51690B1DFE664E4F0EE139F0289B9E40D7B29047E0D4711BC051
      847C0859FFBA225BFBF725745249A13AFEF2B6D7F7804D1A04A5BC6A233669D675FE4385E98AA9CC
      E160B452BF4E38E608DF9051F58FA93735C696580A171AD23D4ECAE3226FBAD3210791726BF693DB
      45FE982AFFB582E2064D2B709FF8007B882387986DF47B11AD2B39B42837DF22EF4CE00124013E5C
      20B22A6215595A67FA2BA69DE500C6AAB6BDB0127759F888185F95532512CCAC4E2E350BBBC1A234
      B3DF46A96CDC1B992EA9462AB134A5AB7137C439E54FAA5B01A53F48BC8495E8993D9AD177105144
      CA5A3EFEC9FE4C20AE82E2F6508CD62F3509E6AF14F24556B02430C311B5C917119B18F051E407ED
      52C8BAD9E3856F003EFD9A454CE11A49EB3D9AF1BEA5F2F6B22BE1B7BEBB3A16D454F34741DD611C
      B66004F7B35F77AED5DDB93D8EAEA783904C6BE1F6C5FB7022AF5DBD34810923ADD2E4F71DC1A7F8
      172A10F50F9DF6EBE7C9A5C4859A08FC1AF3A9E77BA5F6ECE39F5463B27F3192229A3E9AF4F892DB
      15C535F169A61FC90CC61C16BA6341BF284B1A7C5936781DA0E99B1012C2D6FB6BE12BEECB1CBA8D
      2E647FD394E8C95CADD053058D3198E81DDFB9BF11EBEDC5827C3AE538F4AB56
   }
}
```

9.11. Service Certificate (RSA) (old example)

```
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 { "2010082359592" } -- 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
   }
}
```

9.12. Certificate Revocation List

```
SEQUENCE {
   SEQUENCE {
      INTEGER = 1,
      SEQUENCE {
         OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
  Encryption
      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 = "Digi- ja vaestotietovirasto CA"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.11", -- id-at-organizationalUnitName
               UTF8String = "Valtion kansalaisvarmenteet"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "DVV Citizen Certificates - G4R"
            }
         }
      },
      UTCTime = "2111121104006Z", -- this Update
      UTCTime = "2111121184006Z", -- next Update
      CONTEXT_SPECIFIC [ 0 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#08D14EB9F21359FFBBF51C2ED823DCD6C1FE3FC4 }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.20", -- CRL Number
               OCTET_STRING [ PRIMITIVE ] { INTEGER = 3587 }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
Encryption
   BIT_STRING {
      #00,
      #800085AF0004BFD195F6F08BFEB2ACF3112600B9D6674E0D95DAA31ABD7FADE4827704F730BCB159
      00FBEDDE5F9BC01DA02A1E59AD8D21611402E5C56FFE50A022A21C78D10A4F1DCAE7004A9CDE80EE
      9E25CC1D20E8CCBFE7DEC73D7206484A2C62C260CBD05B506E195B14C21651B9123258C79694A4F9
      FC8221966025AF8DBAC0160814D80FB1D32C32426250004F60F37ED8DA39B8E28507B4F0FA507079
      D9DDA6E1448099D10BDFA721AD01A83C880BB2534BED3FBF277E690D0633391585FF58183CC141E2
      F1F506158C745D94EE2439B23904C13516CC9F92DE1CEE32DA9536A8E36650268D9EB40B651CD157
      F7F144B4E7DC9C8A6B44B9BD47625DF5C8D1ED5133CDC5997A799C6CF39DCE0657B366D8EEC97499
      718BB3371D5404B5FC053323B103CDB646F6B070A77A4AFABB7A87ED8C68E715A384930F0C734FCC
      024382A2E366A55AAA591482082C551207CCDC297ED46778AB2FEFE4B32D1DD1349FDF98C22DEF5D
      6E82DFC746369C2C0739E94CBB72F6788CE279F5B5D54F3F7FADCB957AB77B19453BEEDB530F6C3B
      FFE31A7A2CBE59D0FD6B71DD43694EA6A3D7275D292933F78A280E0F75D9BC94DFFCC34546AD6A2C
      75BB80A8ED7E44FF26EFC060CEF86A3555F8681EC4A7FC51CE8446484D16B39E0B16FCD0207DED31
      A02E741D774C69B7D3DA273AE87A079A8147EA249B8D5A67649697B1176085A7
   }
}
```

9.13. OCSP Responder Certificate

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #0179A3139B1FE22E4FEC34E2390FC6, -- Certificate serial number
      SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with
RSA Encryption
      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 = "Digi- ja vaestotietovirasto 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 = "DVV TEST Root CA - G3 RSA"
            }
         }
      },
      SEQUENCE {
         UTCTime = "210525095547Z", -- not before
         UTCTime = "260524102547Z"  -- 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 = "Digi- ja vaestotietovirasto 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 = "2.5.4.5", -- id-at-serialNumber
               PrintableString = "0245437-2"
            }
         },
         SET {
            SEQUENCE {
```

```
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String {
                  "DVV TEST Root CA - G3 RSA OCSP Responder 1A"
               }
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
                OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {

#009FDA5BFFAF5B9596562C4157D4E25AF1FF32587EE066DC368CDC660C58B98FBA1C653FE5B2BABE

B29AA1403ACE9E3B7E046E6742428312799E70894294493B4CEA390817466925F861CF4C9601AA32

3A644AFCCB60E634060BB1FBE571B5BF5CD5FC1C732420118D5C4E314D30E93A4C3B23FAC8BB6010

BFAE72D633EC841898D808EB860EF5689B1445DE57AB0252B84B5C933B5A0E780A312C9E8315A88D

ECA86EC05EC1B367309898AB0C4D6BF7E6D2BC60A00949523D9F73D476345B3F686D0E841BE9288E

79ED0C08060F6849F32CD78E6CD4D67CCB48751C518484FFC6A3C0C60C4639F56B01E47FE722335A
                  5C7F992AA9744CEE474C326E3AECA7075F
               },
               INTEGER = 65537 -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#E88F971CDC5745912DC82DC8A734BF8254BB49B4 }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#5B215BB105A45FAD8A24E0DAB8C76B6CC8AEB3BB }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #05, #A0 } -- digitalSignature, keyEncipherment
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.17", -- Subject Alternative Name
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 1 ] = "kirjaamo@dvv.fi" }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               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 ] {
      "http://proxy.fineid.fi/ca/dvvtest3rc.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", NULL }, -- SHA-512 with RSA
             Encryption
         BIT_STRING {
            #00,
            #48FFFDFB0BDF42622951220CBDB79CA9F3367A20C5C63977F189089838D8531D55BABCDF824054B6
            2005B541502DF7BB091D09AEB6D053C744BBF94FBF7CF6E772E54CC6DBC1F2B8FFD660E7B07A285C
            A08B4B6230D299BBC27BA1DE5DCBB5DAB6FF0B28435D49B2EFE83DA84B6123A6931FB8B442D89552
            2FD61ECB33BAE4BB57F57C2A1C4CE661BAD82EF387912E86F6978F9083F3D28C88E06F7F96C64252
            90D6DDFCF199E045F4D082923C6DC5DC9B9098AAF3E8140F46A633B3D98E78DA0D40C45EB921A8D0
            AE3DD6481B1127D827F31BF153E408884B7ACF520865F6D7435CFE25DA223CF16548D3A933DD364A
            F2DAEEB969D8D15D80C2F4740FD2E44B8C3A909B059B291E8BDAE5AB361106E11EE528CBCC19FDF3
            3E02FFBDE8B3713DE60AC25A843524EB2A6BE0489FF855E111A9F3F47DDA0CFE69FB3E17C91354BE
            8D7A37502478A6D0617265BAB3931D4E32B6F2B6E5AE7BC0B75BEC5D4B4A32E7243848264962271D
            834FA0BF85B74375180658367EA8CD11B198CF29EC71F080701671F4DDDB0B37560D980ABD388687
            A850A1DF71707B9B5DD03DB51F8135DA4D5D200C4B93A4AEFDA43A71245FAB9B0E676F0D25C86EE0
            C1AF00EC67F2EE64155F3982ACEE14CBF79B841E2B11E2FACDFEF444C6C8E8CDDE7CAD96774DDFC3
            6075A4EAE7F6DDEED679493B62D58B82FCDFCE320639FA3AF88AAF5B96F7E78D
         }
}
```

9.14. Time Stamping Certificate (old example)

```
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 { "2309101301143Z" }  -- 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
   }
}
```

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

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017CC65DEFB39AF0D1ADAB2501B4BD,  -- serial number
      SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
Encryption
      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 = "Digi- ja vaestotietovirasto 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 {
                  "DVV TEST Social Welfare and Healthcare Prof. Certs - G2R"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime = "2110280936572", -- not before
         UTCTime = "2610292359592"  -- 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 = "00098706724"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.42", -- id-at-givenName
               UTF8String = "Inna"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.4", -- id-at-surName
               UTF8String = "Naukkarinen"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "Naukkarinen Inna 00098706724"
            }
         }
      },
      SEQUENCE {
         SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
```

```
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {

#00DAEBD12669350EFAEF0341A84E5B1ECAE65F3984DE591EDB398E80F8073814BF895A3B9E1267DA

B6F7E7FEECB7311A68443C2A3E140D9B22CB8D003FD840ABD0B53A8672CF18948384A596C2B721F6

E3F9FC9FC9911F13191B09B9CBF232955D074C39AB3A709F1DA9F4D4C05AE70FC76CB1350EBFC569

511E1FE2F3580A7D67E0A8210245F1491DE7E71B8D1B6D1A893224B189A8AB786AFF3AA6A9096784

F5B95B92133A5A7DCE2E6FD1BEFA94ADE09135B5C41FB4E7126C73F838F9D3182FB413CF357E64EE

FA0FE6F926C4739B6A5418AC1AD0B9C9FAB71B3D25FC6A89FD08323D89CB72C481C016F08D7F4CC5

A2B127546008038AC112A24727ED1CEFC552C195A104F3FF6F8AE39D3A4154EB4572EAF1357A9EB8

C0C5E15A649E27E969EA97464422A22306B626994FEE5F87E031FFECD9F7DA48098A44B4893B55BA

E7927BE5E218F84A2EE776C326CFA7A0C655C2CDE87A360A9D5EDBC908686DD65C125BBC2D4902F3
                  953C273A9209F3F4F12B046D86BA68B9A154F64F661FBC66BB
               },
               INTEGER = 65537  -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0 ] = #6F6B4A3B4ADAD42BA13852CC90CE0951863E1F73
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#3DD7722DF8B09CFCD40C86D853C87FD056D9212F }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               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 = "1.2.246.517.99.10.306.1", -- DVV 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 - Certifikatpolicy 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
szOID_NT_PRINCIPAL_NAME
                        CONTEXT_SPECIFIC [ 0 ] { UTF8String = "00098706724@teonet.fi" }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               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 ] {
                                 "http://proxy.fineid.fi/crl/dvvtshp2rc.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 ] { "http://proxy.fineid.fi/ca/dvvtshp2rc.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.1", -- OCSP
                        CONTEXT_SPECIFIC [ 6 ] = "http://ocsptest.fineid.fi/dvvtshp2rc"
                     }
                  }
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA
Encryption
   BIT_STRING {
      #00,
      #3E32DA88331129F40B50974022A270B17AA0E100E8B28F79F401A2AE0762A7AC97AADB88D2193289
      221528D55060B0B09D24B153C955083AE3987AAAD591E162E75475BD1066845C3DB7697D52E763DF
      5D4DF8494731982A7D2ECFEA811C864E64CC29FF6D4B90FC3BD712446616D27EB49233C4DAC3DC2F
      940E41ED24634576E10B912143CC438F272E03A2B0E84497AB3753A093BEE9937BF5E56B6BC91227
      B659FC51ECB587EC13B66341D302DB244B727E908AF3D7B43427BAF690C0B4D3B46498905D5A0C0C
      C49430C308C83A310C9D51392A90E16275A57C30DE561DA3664D94CC30E3F06CA3C9AD4ACF656FD7
      954B204A0AF19DF69D763FA3EADFB0A858A786495CB618A0B7F145F87513F3B548938B1A85A7A0AA
      0C0FE14EC0867C61D469290C0111B5316159709F6DF715350691F3AE078881E471053DD46193DC08
      13BA7A318CAF6E55BCFC667E8ECB31ABA8273ECD776B09D2926A368DE414D7871867999D0B226052
      E6C1CD09C6AA9000A2A29207459A55D900566CA720D985FB06EAED22D389BF1DBF9FAC3A00F489C6
      A7605F7FA353D78ED89C33320D5754A6409EC3703745D14703F4900D7CB5B68FCE8118C8CC7903E3
      65E754A13EF58091A32EC951F1761AD856B1BD54A289821B589476274B10208DA07344BF899E687F
      C70AE012BA776C5E35B25F73706F5CC020E0419C25943AC657F1E31331F8EA8F
   }
```

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

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017CC65E004F672B7A1DADD5758A67, -- Certificate serial number
      SEQUENCE {
        OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
      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 = "Digi- ja vaestotietovirasto 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 {
                  "DVV TEST Social Welfare and Healthcare Prof. Certs - G2R"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime = "211028093701Z", -- not before
         UTCTime = "261029235959Z"  -- 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 = "033134"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.5", -- id-at-serialNumber
               PrintableString = "00098706724"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.42", -- id-at-givenName
               UTF8String = "Inna"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.4", -- id-at-surName
```

```
               UTF8String = "Naukkarinen"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "Naukkarinen Inna 00098706724"
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
               OBJECT_IDENTIFIER = "1.2.840.113549.1.1.1", NULL }, -- RSA encryption
         BIT_STRING [ PRIMITIVE ] {
            #00,
            SEQUENCE {
               INTEGER {

#00C5621D5063D694DDE5B1EB60B3888E1FDE5EF7FE4FF0A9B461F3845896171A6C4BFBD335113D93

088BDA56E0357F9F9A6A5D781DB4ABE2BD57C9EF2EB826CB37B3AD0D4590A5772487F21EE527E6DC

E5EFB5975A4DEB937768BB6F5C01673C526C0C8CED6BE9A7D27646EEB1728F74FEEE05FF3C990C7E

68FA3E340BEEC544F3310F8C6952B6464FF07BC16F6F9E4C8EB05E1E98081D06AD86294EE4E9B23B

3A7CD41EEBA2FADBAF3C10F9856AEE97B498BEEDE52B1A65EA64DF5E4DAFC9A6FB4B901746D7460B

09DAF4D3BB816830778F3B12F99395AA223D8969C9C42CB438588DE7005B764C42CA9D5619883841

0BFACB7A8980A9109A3D5EA1785DE49F2BD3297A9747B9E8AFD8650CAE7213FCEFD203ED667AC82B

92C3C3721FDBFDE99BA5E9319DB17770369D82961427019919EB4A84ACF005CFF0C0B4FF35041C2F

42700F38A5F78E1C8922411B598E2C7AC5C3A89B693166BC73E986C3B777D2C460D6370B2EE0BA0C
                  6C49EE975975B4F564B1766C9DA904608A555253A177E2A50B
               },
               INTEGER = 65537  -- exponent
            }
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     CONTEXT_SPECIFIC [ 0 ] = #6F6B4A3B4ADAD42BA13852CC90CE0951863E1F73
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#D8B179909EE2B530830C5198469144445A69595E7 }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- nonRepudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.32", -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.2.246.517.99.10.306.1", -- DVV 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 - Certifikatpolicy finns
- Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               },
               SEQUENCE {
                  OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
                  BOOLEAN = #FF,
                  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 ] {
                                    "http://proxy.fineid.fi/crl/dvvtshp2rc.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 ] { "http://proxy.fineid.fi/ca/dvvtshp2rc.crt" }
                        },
                        SEQUENCE {
                           OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.1", -- OCSP
                           CONTEXT_SPECIFIC [ 6 ] = "http://ocsptest.fineid.fi/dvvtshp2rc"
                        }
                     }
                  }
               },
               SEQUENCE {
                  OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.1.3", -- qcStatements
                  OCTET_STRING [ PRIMITIVE ] {
                     SEQUENCE {
                        SEQUENCE { OBJECT_IDENTIFIER = "0.4.0.1862.1.4" } -- QSCD
                     }
                  }
               }
            }
         }
      },
      SEQUENCE {
           OBJECT_IDENTIFIER = "1.2.840.113549.1.1.13", NULL }, -- SHA-512 with RSA Encryption
      BIT_STRING {
         #00,
         #2EDE63E347D7B33077D227568022EBAAF1C7CEDE60A255D4037F0A3C1E02223403A9730613A26ECA
         72A970F6CFFB425F06E2D6C0EFB7AF5DDF9B5D4A61F284FB6A58C8E0B095E2FE3FE946690966A048
         407C18EEC3DD774680983A192DC0A4A3F70259D6C0F121577FEB951335952C0DE7DA499ED2EE0BDE
         34DC82C1B3B3B042A5F84620E9017E0755549EF3A9F561A6076D8450C30123953B0C5F5E44099622
         BFA5C7DA73ECC91165B89E84B08429471553540844FA07DFF3396AAAEDAAE4E21C95FBAEF1E7602F
         E377829DF44B3014C5EC6F686ED92C0840CA335BEC6A3C1BA1480521BB6D142FC9332ACAC00103EF
         D975C4ADD256DC860F1852339E182D5F53671C8DB2DE293B5EED9558987A8288E52FAC571CD7BB94
         FDF2C6B32B6440CC724F11556C4E58FBD3FC295544DA7D148FDB76C43052BCCE4B3978578EA173F1
         3E731C3F4D71EC79A2599E79547AE424C21D819F619F4E31651A035C8795FEF201C326B6993D7578
         319C97189DBA0D56AB342391E41EBB27B83FD509B61311F01C0ED9ECC8B8255ED2112A45CB4868EF
         EE7538E263DDCB10728F8D1C79E01EFA98C61432A10B85488381A2BE53D6A51388E7B0685B3795C9
         F03E1FE36CD88EC0220DB7FAD2296A5632AC4EFC74EE0C79BFE33A25228EF408C35FF92F14E5FA4B
         7048B6CEF3A2CE10983A310731552763B6773ED90A8D17B87941613202EC82D9
      }
   }
```

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

```
SEQUENCE {
   SEQUENCE {
      CONTEXT_SPECIFIC [ 0 ] { INTEGER = 2 }, -- x509v3 certificate
      INTEGER = #017CEF83110277CD10BA701FEA47F2,
      SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
      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 = "Digi- ja vaestotietovirasto 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 {
                  "DVV TEST Social Welfare and Healthcare Prof. Certs - G2E"
               }
            }
         }
      },
      SEQUENCE {
         UTCTime = "211105092156Z", -- not before
         UTCTime = "261106235959Z"  -- 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 = "030593"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.5", -- id-at-serialNumber
               PrintableString = "00198704199"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.42", -- id-at-givenName
               UTF8String = "Katri"
            }
         },
```

```
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.4", -- id-at-surName
               UTF8String = "Koivukangas"
            }
         },
         SET {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.4.3", -- id-at-commonName
               UTF8String = "Koivukangas Katri 00198704199"
            }
         }
      },
      SEQUENCE {
         SEQUENCE {
            OBJECT_IDENTIFIER = "1.2.840.10045.2.1", -- EC Public Key
            OBJECT_IDENTIFIER = "1.3.132.0.34" -- EC Curve secp384r1
         },
         BIT_STRING {
            #00,
            #040744B71C93A02FEBA89162CA36AAEA728DB25CE3D6B3436E0A4582EF46973ED6136D3C121BC519
            59B464479E15277D1D2931945309599A09F1F2FF0DC5173EDBDF5A3468CD8D41E9561BAB83910977
            BB88DA6342A23867C6EC96B37F0A558B44
         }
      },
      CONTEXT_SPECIFIC [ 3 ] {
         SEQUENCE {
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.35", -- Authority Key Identifier
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE { CONTEXT_SPECIFIC [ 0 ] =
#0CCAF8022BF7DCBBCCD58950614CC5E63539BD1A }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.14", -- Subject Key Identifier
               OCTET_STRING [ PRIMITIVE ] { OCTET_STRING =
#75B67F9F12047B5388CF9D18F4B31C8443079973 }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.15", -- Key Usage
               BOOLEAN = #FF,
               OCTET_STRING [ PRIMITIVE ] {
                  BIT_STRING { #06, #40 } -- nonRepudiation
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.32", -- Certificate Policies
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.2.246.517.99.10.356.1", -- DVV 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 - Certifikatpolicy finns
- Certificate policy is available http://www.fineid.fi/cps99"
                                 }
                              }
                           }
                        }
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "2.5.29.19", -- Basic Constraints
               BOOLEAN = #FF,
               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 ] {
                                 "http://proxy.fineid.fi/crl/dvvtshp2ec.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 ] { "http://proxy.fineid.fi/ca/dvvtshp2ec.crt" }
                     },
                     SEQUENCE {
                        OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.48.1", -- OCSP
                        CONTEXT_SPECIFIC [ 6 ] = "http://ocsptest.fineid.fi/dvvtshp2ec"
                     }
                  }
               }
            },
            SEQUENCE {
               OBJECT_IDENTIFIER = "1.3.6.1.5.5.7.1.3", -- qcStatements
               OCTET_STRING [ PRIMITIVE ] {
                  SEQUENCE {
                     SEQUENCE { OBJECT_IDENTIFIER = "0.4.0.1862.1.4" } -- QSCD
                  }
               }
            }
         }
      }
   },
   SEQUENCE { OBJECT_IDENTIFIER = "1.2.840.10045.4.3.3" }, -- ecdsa-with-SHA384
   BIT_STRING [ PRIMITIVE ] {
      #00,
      SEQUENCE {
         INTEGER {
            #00A661494903831D14F6AA5592B690F4C7926669D2BB8C802C9516F0713A8EA1E6E911F9836887E2
            FA6BAB6DD56DD5C4C0
         },
         INTEGER {
            #46A61C2126A7A8977C0BB10ACD11A3D6F69C0C94938D95805308E10D48B5A773B11D8F2F7AEAD300
            BA5634D81DDB791B
         }
      }
   }
}
```