Ο ΠΕΡΙ ΑΡΧΕΙΟΥ ΠΛΗΘΥΣΜΟΥ ΝΟΜΟΣ

ΔΙΑΤΑΓΜΑ ΔΥΝΑΜΕΙ ΤΟΥ ΑΡΘΡΟΥ 65 (Ζ) (Δ)

SPECIFICATION DOCUMENT SD 01

Cyprus National eID Scheme – Electronic Identification Certificate

0 Foreword

Public key certificates based on the international standard ISO/IEC 95948 (X.509) are important components of security systems. This specification document is based on the Cyprus Electronic Identification certificate specification, drafted within the National EID Scheme of the Cyprus Government.

This specification revision has taken into account the new version of the X.509 standard and has been written to be as compliant as possible with the latest available draft version of the "Internet X.509 Public Key Infrastructure Certificate and CLR Profile" (IETF PKIX).

1 Scope

This specification describes the contents of the certificate for Electronic Identification, using HSM server (QTSP) to store the private keys. The certification is based on ISO/IEC 9594-8 (X.509). This specification is thus an implementation **profile for X.509 certificates**.

2 References

The following standards contain provisions which, through reference in this text, constitute provisions of this specification. All standards are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

ISO/IEC 3166	Country Codes
ISO 8859-1:1987	Information Processing – 8 bit single-byte coded graphic character sets- Part 1: Latin alphabet No. 1.
ISO/IEC 9594-8: 1997 X.509	Information Technology – Open systems interconnection – The Directory – Part 8: Authentication framework.
IETF RFC 8017	PKCS#1: RSA Encryption
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements

3 Definitions and Abbreviations

3.1 Definitions

3.1.1 **authentication:** The process of corroborating a claimed identity.

3.1.2 **certificate:** The public keys of a user, together with some other information, rendered unforgeable by decipherment with the private key of the certification authority which issued it [ISO 9594-8].

3.1.3 **electronic signature:** Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of that data to prove the source and integrity of the data unit. It protects against forgery, even by the recipient [ISO 7498-2].

3.1.4 **electronic ID (eID):** Private keys, certificates and other information, to be used for secure identification of users of information systems and other basic security services such as authentication and non-repudiation with digital signatures and distribution of encryption keys for confidentiality.

3.1.5 **identification:** The process of confirming the identity of a person or an object.

3.1.6 **message digest:** Data of a defined length resulting from a hash function applied on a message of arbitrary length.

3.2 Abbreviations

ASN Abstract Syntax Notation

BCD Binary Coded Decimal

QTSP Qualified Trust Service Provider

eIDP Electronic Identity Service provider

DER Distinquished Encoding Rules

EID Electronic Identification

RSA Rivest, Shamir, Adleman

URL Uniform Resource Locator

4 Certificate contents

4.1 Basic certificate fields

4.1.1 Version

The version field shall be set to 2, indicating the version is v3.

4.1.2 Serial number

The serial number of certificates shall be unique for all certificates generated by the same issuer (i.e. the issuer name or abbreviation and serial number jointly identifiy a unique certificate). The binary value of the certificate serial number may not exceed 8 bytes (64 bits) in length.

4.1.3 Signature

This field contains the algorithm identifier for the algorithm used by the eIDP to sign the certificate.

The algorithm identifier of the signature shall be set to the following, as defined in the RFC 8017:

Algorithm	Object Identifier
sha-256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

4.1.4 Issuer

In the issuer field of the EID certificate, the issuer's identity shall be represented by at least the following three mandatory attributes in accordance with X.520:

Parameter	Attribute	OID (X.520)
Country	countryName	{ id-at 6 }
Organization	organizationName	{ id-at 10 }
Name	commonName	{id-at 3 }
Issuer Identifier	organizationIdentifier	{id-at 97}

The **Country** parameter shall always be set to the two character country code "CY" for Cyprus according to ISO 3166

The **Organization** parameter shall contain the full Company Name of the Issuer as it is registered with the Cyprus Registrar of Companies.

The **Name** parameter shall contain the common name of the issuer (certification authority) and the policy being used. Example: “Organization X PRDXXX”.

It is strongly recommended that all issuer parameters are encoded as PrintableString. If this is not possible, the string shall be represented as BMPString (also known as Unicode).

The **Issuer Identifier** parameter shall contain the **company registered organization number** of the eIDP, which is unique within the country. For example “HE 330022”.

To simplify later directory search, the RDN Sequence shall contain multiple Relative Distinguished Names, which each contain only one Attribute Value Assertion:

RelativeDistinquishedName **::= SET SIZE (1) OF AttributeTypeAndValue**

4.1.5 Validity

The Validity period must be defined according to the European Standard ETSI EN 319 412-5, Section A.3 and comply to the IETF RFC 5280 [i.9] or the latest standard.

Certificate issuers conforming to this profile shall always encode certificate validation dates through the year 2049 as UTCTime; certificates validity dates in 2050 or later shall be encoded as GeneralizedTime.

The universal time type, UTCTime, is a standard ASN.1 type intended for international applications where local tome alone is not adequate. UTCTime specifies the year through the two low order digits and time is specified to the precision of one minute or one second. UTCTime includes either Z(for Zulu, or Greenwich Mean Time) or a time differential.

In certificates conforming to this profile, UTCTime values shall be expressed as Greenwich Mean Time (Zulu) and shall include seconds (i.e. times are given as YYMMDDHHMMSSZ), even where the number of seconds is zero. Conforming systems shall interpret the year field as follows:

> 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.

The generalized time type, GeneralizedTime, is a standard ASN.1 type for variable precision representation of time. Optionally, the GeneralizedTime field can include a representation of the time differential between local and Greenwich Mean Time.

In the certificates conforming to this profile, GeneralizedTime values shall be expressed as Greenwich Mean Time (Zulu) and shall include seconds (i.e., times are given as YYYYMMDDHHMMSSZ), even where the number of seconds is zero. Generalized
Time values shall not include fractional seconds.

4.1.6 Subject

The subject shall always be a **physical person**, citizen of the republic of Cyprus, and the subject's identity shall be represented only by the following mandatory attributes in accordance with X.520, included in the given order.

The Citizen's Distinguished Name shall be derived from the National Identity Management System (Civil Registry System) during the registration process.

It is made up of the following attributes:

Parameter	Attribute	OID (X.520)
Country	countryName	{ id-at 6 }
Last Name	surname	{ id-at 4 }
First Name	givenName	{id-at 42 }
Full Name	commonName	{id-at 3 }
Personal Identifier	serialNumber	{id-at 5 }

The **Country** parameter shall be always set to the two character country code "CY" for Cyprus according to ISO 3166 .

The **First Name** and **Last Name** parameters shall be entered with upper-case letters, and represented as follows:

a) If the character set is sufficient, the string shall be represented as PrintableString (A-Z).
b) If this is not possible, the string shall be represented as BMPString (also known as Unicode).

The **Full Name** parameter shall be entered with upper-case letters, and represented as a string derived from the concatenation of the previously defined First Name and Last Name separated by a space character.

The **Personal Identifier** parameter shall contain the National Personal Identification Number of the citizen that is unique for the Country. The Personal Identifier shall be encoded in the serialNumber attribute in the subject field and shall contain information using the following structure in the presented order:

- 3 character natural identity type reference;
- 2 character ISO 3166 [2] country code;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
  and
- identifier (10-digit format of Identity Card Number).

The three initial characters shall always have the following defined value:
"IDC" for identification based on national identity card number.
The country code shall always be set to "CY".

EXAMPLE: "IDCCY-000012345678".

The certificate issuer shall in his Certificate Practice Statement or in a referred Certificate Policy describe the content of the Personal Identifier.

To simplify later directory search, the RDN Sequence shall contain multiple Relative Distinguished Names, which each contain only one Attribute Value Assertion:

RelativeDistinquishedName **::= SET SIZE (1) OF AttributeTypeAndValue**

4.1.7 Subject public key

The algorithm identifier of the subject's public key shall be set to the following:

Algorithm	Object Identifier
rsaEncryption	{ iso(1) member-body(2) US(840) rsadsi (113549) pkcs(1) 1 1 }

4.1.8 Issuer unique identifier

The issuer unique identifier field shall be omitted from the EID certificates.

4.1.9 Subject unique identifier

The subject unique identifier field shall be omitted from the EID certificates.

4.2 Standard certificate extension fields

The X.509 v3 standard extension are defined ISO/IEC 959408:1997 (X.509). Below, it is specified which of these extensions that are mandatory or not to be used.
For most extensions, this document does not specify whether an extension shall be marked as critical or not, but leaves that to the certificate policy. The only exception is the Key Usage extension, which shall be marked as critical.

4.2.1 Authority key identifier extension

The **mandatory** authority key extension provides a means of identifying the particular private eIDP key used to sign a certificate. The extension shall only use the keyIdentifier element.

4.2.2 subject key identifier extension

The **mandatory** subject key extension provides a means of identifying the particular public key used in an application. It shall contain a key identifier value that shall be unique for each user key.

The value of the subjectKeyIdentifier is recommended to be constructed as a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding tag, length and indicator of number of unused bits).

4.2.3 Key usage extension

The **mandatory** key usage defines the purpose of the key contained in the certificate. This extension shall be marked as **critical. The key usage settings must be defined according to the European Standard ETSI EN 319 412-2, Section 4.3.2**

FOR DIGITAL AUTHENTICATION ONLY

The following KeyUsage type bits must be included in the EID certificate:

The **digitalSignature** bit must be set according to section 4.3.2 of the European Standard ETSI EN 319 412-2 **key usage setting C**.

The **digitalSignature** bit is set when the subject public key is used with a digital signature mechanism to support security services other than non-repudiation.

Digital signature mechanisms are often used for entity authentication and data origin authentication with integrity.

4.2.4 Certificate policies extension

The **mandatory** certificate policies extension shall contain at least on policy identifier OID. Presence of a policy identifier is a statement by the issuing eIDP that, during the validity period of the certificate, all requirements in that policy is fulfilled with respect to certificate issuance and related maintenance services.

The suitability of a certified key pair for a specific application is primarily a decision based on the certificate policy and secondarily on the content of the certificate. This specification does only specify the content structure of certificates and is either independent or subordinate to a certificate policy specification. Requirements on suitable certificate policies is therefore outside the scope of this specification but the certificate content, i.e. by reference to this specification.

4.2.5 Subject directory attributes extension

The **subject directory attributes extension** shall be represented by the following attributes in accordance with X520, included in the given order.

Parameter	Attribute	OID
Date of birth	dateOfBirth	{ id-pda 1}
Gender	gender	{ id-pda 3 }

The **Date of birth** parameter shall contain the value of the date of birth of the subject. The date of birth is defined in the Generalized Time format and should specify GMT 12.00.00 (noon) down to the granularity of seconds, in order to prevent accidental change of date due to time zone adjustments. For example, a birth date of September 27, 1959 is encoded as "19590927120000Z".

Compliant certificate parsing applications **SHOULD** ignore any time data and just present the contained date without any time zone adjustments.

The **Gender** parameter shall contain the value of the gender of the subject. For females the value "F" (or "f"), and for males the value "M" (or "m"), have to be used.

4.2.6 Extended key usage extension

The extended key usage extension field **shall not** be present in the EID certificates.