Ε.Ε. Παρ. III(I)
Αρ. 5683, 18.3.2022
Αριθμός 125

Κ.Δ.Π. 125/2022

ΟΙ ΠΕΡΙ ΑΡΧΕΙΟΥ ΠΛΗΘΥΣΜΟΥ ΝΟΜΟΙ ΤΟΥ 2002 ΕΩΣ 2021

Διάταγμα δυνάμει του άρθρου 65Ζ(δ)

141(I) του 2002
65(I) του 2003
76(I) του 2003
62(I) του 2004
13(I) του 2006
123(I) του 2007
92(I) του 2009
81(I) του 2010
44(I) του 2011
36(I) του 2013
174(I) του 2013
15(I) του 2015
16(I) του 2015
44(I) του 2015
166(I) του 2015
168(I) του 2017
9(I) του 2019
65(I) του 2019
86(I) του 2020
113(I) του 2020
145(I) του 2020
59(I) του 2021.

Ο Υπουργός Εσωτερικών, ασκώντας τις εξουσίες που του παρέχονται από την παράγραφο (δ) του άρθρου 65Ζ των περί Αρχείου Πληθυσμού Νόμων του 2002 έως 2021, εκδίδει το ακόλουθο Διάταγμα.

Συνοπτικός τίτλος.

1. Το παρόν Διάταγμα θα αναφέρεται ως το περί των Χαρακτηριστικών και των τεχνικών προδιαγραφών των ηλεκτρονικών πιστοποιητικών που περιλαμβάνει η ηλεκτρονική ταυτότητα Διάταγμα του 2022.

Ερμηνεία.

2.-(1) Στο παρόν Διάταγμα, εκτός αν από το κείμενο προκύπτει διαφορετική έννοια-

«Νόμος» σημαίνει τον περί Αρχείου Πληθυσμού Νόμο.

(2) Οποιοιδήποτε όροι, που περιέχονται στο παρόν Διάταγμα και δεν ορίζονται ειδικά σε αυτό, έχουν την έννοια που τους αποδίδεται από το Νόμο και τους δυνάμει αυτού εκδιδόμενους Κανονισμούς ή Διατάγματα.

Χαρακτηριστικά και τεχνικές προδιαγραφές διασύνδεσης Παράρτημα Α.

3. Τα χαρακτηριστικά και οι τεχνικές προδιαγραφές των ηλεκτρονικών πιστοποιητικών που περιλαμβάνει η ηλεκτρονική ταυτότητα καθορίζονται στο Παράρτημα Α (Οδηγός Αναφοράς).

ΠΑΡΑΡΤΗΜΑ «Α»
(άρθρο 3)

ΕΓΓΡΑΦΟ ΠΡΟΔΙΑΓΡΑΦΩΝ SD 01

Εθνικό Σχήμα ηΤαυτότητας της Κύπρου – Πιστοποιητικό Ηλεκτρονικής Ταυτοποίησης

0 Πρόλογος

Τα πιστοποιητικά δημοσίου κλειδιού που βασίζονται στο διεθνές πρότυπο ITU-T X.509 αποτελούν σημαντικά συστατικά στοιχεία της ασφάλειας των συστημάτων. Το παρόν έγγραφο προδιαγραφών είναι βασισμένο στην προδιαγραφή Ηλεκτρονικής Ταυτοποίησης της Κύπρου που συντάχθηκε εντός του Εθνικού Σχήματος ηΤαυτοποίησης της Κυπριακής Κυβέρνησης.

Η αναθεώρηση της προδιαγραφής αυτής, έγινε λαμβάνοντας υπόψη την νέα έκδοση του προτύπου ITU-T X.509 και συντάχθηκε με γνώμονα την όσο τον δυνατόν συμμόρφωση με την τελευταία διαθέσιμη προσχέδια έκδοση του προτύπου "Internet X.509 Public Key Infrastructure Certificate and CLR Profile" (IETF PKIX).

1 Πεδίο Εφαρμογής

Η προδιαγραφή περιγράφει τα περιεχόμενα του πιστοποιητικού για την Ηλεκτρονική Ταυτοποίηση, χρησιμοποιώντας Remote Qualified Signature Creation Device (QSCD) operated by a QTSP για την αποθήκευση των ιδιωτικών κλειδιών. Η πιστοποίηση βασίζεται στο πρότυπο on ISO/IEC 9594-8 (X.509). Συνεπώς, η παρούσα προδιαγραφή αποτελεί **προφίλ υλοποίησης για πιστοποιητικά X.509.**

2 Βιβλιογραφικές Αναφορές

Τα ακόλουθα πρότυπα περιέχουν διατάξεις οι οποίες, μέσω αναφοράς σε αυτό το κείμενο, αποτελούν διατάξεις και αυτής της προδιαγραφής. Όλα τα πρότυπα υπόκεινται σε αναθεώρηση και τα συμβαλλόμενα μέρη με βάση συμφωνίας την προδιαγραφή αυτή, ενθαρρύνονται να διερευνήσουν τη δυνατότητα εφαρμογής των πιο πρόσφατων εκδόσεων των προτύπων που αναφέρονται παρακάτω.

ISO 3166-1	Codes for the representation of names of countries and their subdivisions--Part 1: Country code
ISO 8859-1:1987	Information Processing – 8 bit single-byte coded graphic character sets- Part 1: Latin alphabet No. 1.
ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
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
ITU -X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types

3 Ορισμοί και συντομογραφίες

3.1 Ορισμοί

3.1.1 αυθεντικοποίηση: Η διαδικασία επιβεβαίωσης μιας αξιωμένης ταυτότητας.

3.1.2 πιστοποιητικό: Το δημόσιο κλειδί και η ταυτότητα μιας οντότητας μαζί με ορισμένες άλλες πληροφορίες που καθίστανται αδύνατο να πλαστογραφηθούν, υπογράφοντας τις πληροφορίες του πιστοποιητικού με το ιδιωτικό κλειδί της αρχής πιστοποίησης που εξέδωσε το πιστοποιητικό [ISO 9594-8].

3.1.3 ηλεκτρονική υπογραφή: Δεδομένα που επισυνάπτονται σε μια μονάδα δεδομένων ή ένας κρυπτογραφικός μετασχηματισμός μιας μονάδας δεδομένων, που επιτρέπει στον παραλήπτη αυτών των δεδομένων να αποδείξει την πηγή και την ακεραιότητα της μονάδας δεδομένων. Προστατεύει από την πλαστογραφία, ακόμη και από τον παραλήπτη. [ISO 7498-2].

3.1.4 ηλεκτρονική ταυτότητα (ηΤαυτότητα): Ιδιωτικά κλειδιά, πιστοποιητικά και άλλες πληροφορίες, προς χρήση για τους σκοπούς της ασφαλούς ταυτοποίησης των χρηστών των πληροφοριακών συστημάτων και άλλων βασικών υπηρεσιών ασφαλείας, όπως έλεγχος ταυτότητας και μη αποποίησης με χρήση ψηφιακών υπογραφών και διανομή κλειδιών κρυπτογράφησης για εμπιστευτικότητα.

3.1.5 ταυτοποίηση: Η διαδικασία επιβεβαίωσης της ταυτότητας ενός ατόμου ή ενός αντικειμένου.

3.1.6 σύνοψη μηνύματος (message digest): Δεδομένα καθορισμένου μήκους που προκύπτουν από μια συνάρτηση κατακερματισμού που εφαρμόζεται σε ένα μήνυμα αυθαίρετου μήκους.

3.2 Συντομογραφίες

ASN Abstract Syntax Notation

BCD Binary Coded Decimal

QTSP Qualified Trust Service Provider

eIDP electronic identification provider

DER Distinguished Encoding Rules

EID Electronic Identification

RSA Rivest, Shamir, Adleman

URL Uniform Resource Locator

4 Περιεχόμενα πιστοποιητικών

4.1 Βασικά πεδία πιστοποιητικού

4.1.1 Version

Το πεδίο της έκδοση θα πρέπει να έχει την τιμή 2, που σημαίνει ότι η έκδοση είναι v3.

4.1.2 Serial number

Ο σειριακός αριθμός των πιστοποιητικών πρέπει να είναι μοναδικός για όλα τα πιστοποιητικά που δημιουργούνται από τον ίδιο εκδότη (δηλαδή το όνομα του εκδότη ή η συντομογραφία και ο σειριακός αριθμός προσδιορίζουν από κοινού ένα μοναδικό πιστοποιητικό). Η δυαδική τιμή του σειριακού αριθμού πιστοποιητικού δεν μπορεί να υπερβαίνει τα 8 byte (64 bit) σε μήκος.

4.1.3 Signature

Αυτό το πεδίο περιέχει το αναγνωριστικό αλγορίθμου για τον αλγόριθμο που χρησιμοποιείται από τον eIDP για την υπογραφή του πιστοποιητικού.

Το αναγνωριστικό αλγορίθμου της υπογραφής ορίζεται ως ακολούθως, σύμφωνα με το 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

Αυτό το πεδίο προσδιορίζει τον εκδότη του πιστοποιητικού EID και η ταυτότητά του αντιπροσωπεύεται από τουλάχιστον τα ακόλουθα τρία υποχρεωτικά χαρακτηριστικά, σύμφωνα με το πρότυπο 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}

Η παράμετρος **Country** θα πρέπει πάντα να έχει την τιμή των δύο χαρακτήρων του κωδικού χώρας της Κύπρου “CY”, σύμφωνα με το πρότυπο ISO 3166.

Η παράμετρος **Organization** θα πρέπει να περιέχει το πλήρες Όνομα Εταιρείας του εκδότη, όπως αυτό έχει καταχωρηθεί στον Έφορο Εταιρειών.

Η παράμετρος **Name** θα πρέπει να περιέχει το κοινό όνομα του εκδότη (αρχή πιστοποίησης) και την πολιτική που χρησιμοποιείται. Για παράδειγμα: “Όνομα Εταιρίας eID CA XX”.

Συνιστάται όλες οι παράμετροι του εκδότη να κωδικοποιούνται ως PrintableString. Εάν αυτό δεν είναι δυνατό, η συμβολοσειρά θα αναπαρασταθεί ως BMPString (επίσης γνωστή ως Unicode).

Η παράμετρος **Αναγνωριστικού Εκδότη** περιέχει τον **αριθμό εγγραφής ΦΠΑ** του eIDP, ο οποίος είναι μοναδικός στη χώρα. Το Αναγνωριστικό Εκδότη κωδικοποιείται στο χαρακτηριστικό OrganizationIdentifier του πεδίου Subject και περιέχει πληροφορίες χρησιμοποιώντας την ακόλουθη δομή με την παρουσιαζόμενη σειρά:

- 3 χαρακτήρες της αναφοράς τύπου ταυτότητας νομικού προσώπου
- 2 χαρακτήρες του κωδικού χώρας ISO 3166 [2]
- παύλα "-" (0x2D (ASCII), U+002D (UTF-8))
- αναγνωριστικό (μορφοποίηση Αριθμού Εγγραφής ΦΠΑ Καταχώρησης Εταιρείας/Οργανισμού).

Οι τρεις αρχικοί χαρακτήρες θα έχουν πάντα την ακόλουθη, καθορισμένη τιμή:
"VAT" για ταυτοποίηση βάσει του Αριθμού Εγγραφής ΦΠΑ στο Τμήμα Φορολογίας.

Ο κωδικός χώρας θα πρέπει πάντα να ορίζεται ως "CY".

ΠΑΡΑΔΕΙΓΜΑ: "VATCY-VAT number".

Για την απλοποίηση αναζητήσεων στον κατάλογο, η Ακολουθία RDN θα περιέχει πολλαπλά Relative Distinguished Names, καθένα από τα οποία θα περιέχει μόνο μία Τιμή Χαρακτηριστικού::

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

4.1.5 Validity

Η τιμή του πεδίου Validity θα πρέπει να ορίζεται σύμφωνα με το Ευρωπαϊκό Πρότυπο ETSI EN 319 412-5, Τμήμα A.3 και να συμμορφώνεται με το πρότυπο IETF RFC 5280 [i.9] ή το πιο πρόσφατο πρότυπο.

Οι εκδότες πιστοποιητικών που συμμορφώνονται με αυτό το προφίλ θα πρέπει πάντα να κωδικοποιούν τις περιόδους validity των πιστοποιητικών έως το έτος 2049 ως UTCTime. Οι ημερομηνίες ισχύος των πιστοποιητικών με έτος 2050 ή μεταγενέστερες θα πρέπει να κωδικοποιούνται ως GeneralizedTime.

Ο τύπος καθολικής ώρας, UTCTime, είναι ένας καθορισμένος τύπος ASN.1 που προορίζεται για διεθνείς εφαρμογές όπου ο τοπικός τόμος από μόνος του δεν είναι επαρκής. Το UTCTime καθορίζει το έτος με τα δύο ψηφία χαμηλής σημασίας και ο χρόνος καθορίζεται με ακρίβεια ενός λεπτού ή ενός δευτερολέπτου. Το UTCTime περιλαμβάνει είτε τον χαρακτήρα Z (για Zulu ή Greenwich Mean Time) είτε μια χρονική διαφορά.

Σε πιστοποιητικά που συμμορφώνονται με αυτό το προφίλ, οι τιμές UTCTime θα πρέπει να εκφράζονται ως Μέση Ώρα Γκρίνουιτς (Ζουλού) και θα πρέπει να περιλαμβάνουν δευτερόλεπτα (δηλ. οι χρόνοι δηλώνονται ως YYMMDDHHMMSSZ), ακόμη και όταν ο αριθμός των δευτερολέπτων είναι μηδέν. Τα συστήματα που συμμορφώνονται με αυτό το προφίλ θα πρέπει να ερμηνεύουν το πεδίο έτους ως εξής:

Όπου ο αριθμός YY είναι μεγαλύτερος ή ίσος του 50, το έτος θα πρέπει να ερμηνεύεται ως 19YY.
Όπου ο αριθμός YY είναι μικρότερος του 50, το έτος θα πρέπει να ερμηνεύεται ως 20YY.

Ο Γενικευμένος Τύπος Χρόνου, GeneralizedTime, είναι ένας τυπικός τύπος ASN.1 για μεταβλητή αναπαράσταση ακριβείας του χρόνου. Προαιρετικά, το πεδίο GeneralizedTime μπορεί να περιλαμβάνει μια αναπαράσταση της χρονικής διαφοράς μεταξύ τοπικής και μέσης ώρας Greenwich.

Στα πιστοποιητικά που συμμορφώνονται με αυτό το προφίλ, οι τιμές GeneralizedTime θα πρέπει να εκφράζονται ως Μέση Ώρα Γκρίνουιτς (Zulu) και θα πρέπει να περιλαμβάνουν δευτερόλεπτα (δηλαδή, οι χρόνοι δίνονται ως YYYYMMDDHHMMSSZ), ακόμη και όταν ο αριθμός των δευτερολέπτων είναι μηδέν.

Οι τιμές του πεδίου Γενικευμένος Τύπου Χρόνου δεν περιλαμβάνουν κλασματικά δευτερόλεπτα.

4.1.6 Subject

Το πεδίο subject θα πρέπει πάντα να αντιστοιχεί σε **φυσικό πρόσωπο**, πολίτη της Κυπριακής Δημοκρατίας και η ταυτότητα του ατόμου θα πρέπει να αντιπροσωπεύεται μόνο από τα ακόλουθα υποχρεωτικά χαρακτηριστικά σύμφωνα με το πρότυπο ITU X.520, σύμφωνα με την σειρά που ορίζεται στο πρότυπο.

Το Διακεκριμένο Όνομα του Πολίτη (Citizen’s Distinguished Name) θα πρέπει να προέρχεται από το Εθνικό Μητρώο Εγγραφής Πολιτών (Σύστημα Αρχείου Πληθυσμού) κατά τη διαδικασία εγγραφής.

Αποτελείται από τα ακόλουθα χαρακτηριστικά:

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 }

Η παράμετρος **Country** θα πρέπει πάντα να έχει την τιμή των 2 χαρακτήρων του κωδικού χώρας της Κύπρου, “CY”, σύμφωνα με το πρότυπο ISO 3166 -1 .

Οι παράμετροι **First Name** και **Last Name** θα πρέπει να παίρνουν τιμές με κεφαλαίους χαρακτήρες και θα πρέπει να αναπαρίστανται ως εξής:
a) Αν το σύνολο χαρακτήρων είναι επαρκές, η συμβολοσειρά θα πρέπει να αναπαρίσταται με μορφή PrintableString (A-Z).
b) Αν δεν είναι δυνατόν, η συμβολοσειρά θα πρέπει να αναπαρίσταται με την μορφή BMPString (γνωστή ως Unicode).

Η παράμετρος **Full Name** θα πρέπει να παίρνει τιμή με κεφαλαίους χαρακτήρες και θα πρέπει να αναπαρίσταται ως συμβολοσειρά που προκύπτει από την συνένωση των προηγουμένως καταχωρημένων παραμέτρων First Name και Last Name, διαχωρισμένες με ένα κενό χαρακτήρα.

Η παράμετρος **Personal Identifier** θα πρέπει να περιέχει τον Προσωπικό Αριθμό Εγγραφής του πολίτη, ο οποίος είναι μοναδικός για την Χώρα. Η τιμή της παραμέτρου Personal Identifier θα πρέπει να κωδικοποιείται στο χαρακτηριστικό serialNumber του πεδίου Subject και θα πρέπει να περιέχει πληροφορία χρησιμοποιώντας την ακόλουθη δομή, στην σειρά που παρουσιάζεται:

- 3 χαρακτήρες της αναφοράς τύπου ταυτότητας φυσικού προσώπου
- 2 χαρακτήρες του κωδικού χώρας ISO 3166 [2]
- παύλα "-" (0x2D (ASCII), U+002D (UTF-8))
- αναγνωριστικό (10-ψήφιο format of Αριθμού Ταυτότητας).

Οι τρεις αρχικοί χαρακτήρες θα έχουν πάντα την ακόλουθη καθορισμένη τιμή:
"IDC" για ταυτοποίηση με βάση τον αριθμό της πολιτικής ταυτότητας.
Το πεδίο country code θα πρέπει πάντα να παίρνει την τιμή "CY".

ΠΑΡΑΔΕΙΓΜΑ: "IDCCY-000012345678".

Ο εκδότης πιστοποιητικού θα αναφέρει στη Δήλωση Πρακτικής του Πιστοποιητικού ή σε μια αναφερόμενη Πολιτική πιστοποιητικού το περιεχόμενο του Προσωπικού Αναγνωριστικού.

Για την απλοποίηση αναζητήσεων στον κατάλογο, η Ακολουθία RDN θα περιέχει πολλαπλά Relative Distinguished Names, καθένα από τα οποία θα περιέχει μόνο μία Τιμή Χαρακτηριστικού:

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

4.1.7 Subject public key

Το πεδίο subject public key περιλαμβάνει ένα αναγνωριστικό αλγορίθμου και θα πρέπει να ορίζεται ως ακολούθως:

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

4.2 Τυπικά πεδία επέκτασης πιστοποιητικού

Η επέκταση του προτύπου X.509 v3 ορίζεται κατά το πρότυπο ISO / IEC 959408: 1997 (X.509). Παρακάτω, προσδιορίζεται ποια από αυτές τις επεκτάσεις είναι υποχρεωτική ή όχι. Για τις περισσότερες επεκτάσεις, αυτό το έγγραφο δεν διευκρινίζει εάν μια επέκταση θα πρέπει να επισημανθεί ως κρίσιμη ή όχι, αλλά το αφήνει στην πολιτική πιστοποιητικών. Η μόνη εξαίρεση είναι η επέκταση "Key Usage", η οποία θα πρέπει να επισημανθεί ως κρίσιμη.

4.2.1 Επέκταση Authority Key Identifier

Η **υποχρεωτική** επέκταση authority key identifier παρέχει ένα μέσο αναγνώρισης του συγκεκριμένου ιδιωτικού κλειδιού eIDP που χρησιμοποιείται για την υπογραφή ενός πιστοποιητικού. Η επέκταση χρησιμοποιεί μόνο το στοιχείο keyIdentifier.

4.2.2 Επέκταση Subject Key Identifier

Η **υποχρεωτική** επέκταση subject key παρέχει ένα μέσο αναγνώρισης του συγκεκριμένου δημόσιου κλειδιού που χρησιμοποιείται σε μια εφαρμογή. Περιέχει μια τιμή αναγνώρισης κλειδιού που θα είναι μοναδική για κάθε κλειδί χρήστη.

Η τιμή του subjectKeyIdentifier προτείνεται να σχηματίζεται ως ένα πεδίο τεσσάρων bit με την τιμή 0100, ακολουθούμενη από τα 60 bit χαμηλής σημασίας της σειράς κατακερματισμού κατά SHA-1 της τιμής BIT STRING του πεδίου subjectPublicKey (εξαιρώντας το tag, length και indicator of number of unused bits).

4.2.3 Επέκταση Key Usage

Η **υποχρεωτική** επέκταση key usage ορίζει τον σκοπό του κλειδιού που περιέχεται στο πιστοποιητικό. Αυτή η επέκταση θα πρέπει να επισημανθεί ως **κρίσιμη** (**critical**). **The key usage settings must be defined σύμφωνα με το Ευρωπαϊκό Πρότυπο ETSI EN 319 412-2, Τμήμα 4.3.2.**

ΜΟΝΟ ΓΙΑ ΨΗΦΙΑΚΗ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Τα παρακάτω bit τύπου Χρήσης Κλειδιού (KeyUsage type bits) θα πρέπει να περιλαμβάνονται στο πιστοποιητικό EID:

Το **digitalSignature** bit θα πρέπει να ορίζεται σύμφωνα με την παράγραφο 4.3.2 του Ευρωπαϊκού Προτύπου ETSI EN 319 412-2 **key usage setting C**.

Το **digitalSignature** bit παίρνει τιμή μόνο όταν το δημόσιο κλειδί του υποκειμένου (subject public key) χρησιμοποιείται μαζί με ένα μηχανισμό ψηφιακής υπογραφής για να υποστηριχθούν υπηρεσίες ασφαλείας, διαφορετικές από την μη-αποποίηση.

Οι μηχανισμοί ψηφιακής υπογραφής χρησιμοποιούνται συχνά για τον έλεγχο ταυτότητας οντοτήτων και τον έλεγχο ταυτότητας προέλευσης δεδομένων με ακεραιότητα.

4.2.4 Επέκταση Certificate Policies

Η **υποχρεωτική** επέκταση certificate policies θα πρέπει να περιλαμβάνει τουλάχιστον ένα αναγνωριστικό πολιτικής OID. Η παρουσία ενός αναγνωριστικού πολιτικής είναι μια δήλωση του εκδότη eIDP ότι, κατά τη διάρκεια ισχύος του πιστοποιητικού, πληρούνται όλες οι απαιτήσεις της πολιτικής όσον αφορά την έκδοση πιστοποιητικών και τις σχετικές υπηρεσίες συντήρησής του.

Η καταλληλότητα ενός πιστοποιημένου ζεύγους κλειδιών για μια συγκεκριμένη εφαρμογή είναι κατά κύριο λόγο μια απόφαση που βασίζεται στην πολιτική πιστοποιητικών και δευτερευόντως στο περιεχόμενο του πιστοποιητικού. Αυτή η προδιαγραφή προσδιορίζει μόνο τη δομή περιεχομένου των πιστοποιητικών και είναι είτε ανεξάρτητη είτε εξαρτάται από μια προδιαγραφή πολιτικής πιστοποιητικών. Επομένως, οι απαιτήσεις για κατάλληλες πολιτικές πιστοποιητικών δεν εμπίπτουν στο πεδίο εφαρμογής αυτής της προδιαγραφής, αλλά το περιεχόμενο του πιστοποιητικού, δηλαδή με αναφορά σε αυτήν την προδιαγραφή.

4.2.5 Επέκταση Subject Directory Attributes

Η επέκταση **subject directory attributes δεν θα πρέπει να υπάρχει.**

4.2.6 Επέκταση Extended Key Usage

Η επέκταση extended key usage **δεν θα πρέπει** να υπάρχει στα πιστοποιητικά EID.

Τυπώθηκε στο Τυπογραφείο της Κυπριακής Δημοκρατίας, 1445 Λευκωσία, Κύπρος
Τηλ.: 22405824, Φαξ: 22303175 - www.mof.gov.cy/gpo
Αντίτυπα της Επίσημης Εφημερίδας πωλούνται προς €2,00 το καθένα