

Republika e Shqipërisë

Autoriteti Kombëtar për
Certifikimin Elektronik



Udhëzues mbi shërbimin e certifikimit elektronik

Udhëzimi Nr. 003
Buletini Shtator 2011
Versioni 1.4

Përmbajtje

Kapitulli 1 - Hyrje	6
1.1 Qëllimi i dokumentit	6
1.2 Struktura e dokumentit	6
1.3 Sistemi i certifikimit elektronik në Shqipëri.....	7
Kapitulli 2 – Standardet e Referimit	8
2.1 Standardet ISO/IEC	8
2.2 IETF	9
2.2.1 Working Group Public-Key Infrastructure (X.509)	9
2.2.2 Working Group S/MIME Mail Security.....	10
2.3 EESSI	10
2.3.1 CEN W-sign WS.....	11
2.3.2 ETSI ESI.....	11
2.4 ISO/IEC 17799; 27001	12
Kapitulli 3 – Shkurtime dhe përkufizime	13
3.1 Përkufizime	13
3.2 Shkurtime	15
Kapitulli 4 - Referime	16
Kapitulli 5 – Modaliteti i Kontrollit	17
5.1 Ofruesi i shërbimit të certifikimit.....	17
5.2 Organizmi testimit dhe konfirmimit	17
5.3 Modaliteti i inspektimit	19

Kapitulli 6 – Specifikime Teknike.....	20
1. Karakteristika të përgjithshme për krijimin dhe verifikimin e nënshkrimit.....	20
2. Gjenerimi i çelësave.....	20
3. Modaliteti i gjenerimit të çelësave.....	20
4. Ruajtja e çelësave.....	21
5. Gjenerimi i çelësave jashtë pajisjeve të krijimit të nënshkrimit	21
6. Pajisjet e sigurt dhe procedurat për gjenerimin e nënshkrimit.....	22
7. Verifikimi i nënshkrimit elektronik.	22
8. Gjenerimi i çelësave të certifikimit.	22
9. Gjenerimi i certifikatave të kualifikuara.	22
10. Informacionet e përfshira në certifikatat e kualifikuara.	22
11. Revokimi i certifikatës se kualifikuar.....	23
12. Pezullimi i certifikatës se kualifikuar.	23
13. Zëvendësimi i çelësave të certifikimit.	24
14. Revokimi i certifikatave që përmbajnë çelësa certifikimi.	24
15. Kërkesat e sigurisë për sistemet operative.	24
16. Sistemi i gjenerimit të certifikatave të kualifikuara.....	24
17. Plani mbi sigurinë.....	25
18. Aksesit i certifikatave nga publiku.....	25
19. Sistemi i cilësisë të ofruesit të shërbimit.	25
20. Organizimi i personelit të ofruesit të shërbimit.	26
21. Kodi i emergjencës.....	26
22. Manuali operativ.....	26
23. Detyrimet e ofruesit të shërbimit të certifikimit.	27
24. Lista e ofruesve të shërbimit të certifikimit.	28
25. Kufizimet e përdorimit.....	28

Kapitulli 7 – Rregulla për vlefshmërinë kohore dhe për mbrojtjen e dokumenteve elektronike	29
26. Vlefshmëria kohore	29
27. Informacione të përfshira në vulën kohore	29
28. Precizioni i sistemeve të vlefshmërisë kohore.	29
29. Çelësat e vulave kohore.....	30
30. Mirëmbajtja e certifikatave dhe çelësave të vulave kohore	30
31. Siguria e sistemeve të vulave kohore.	30
32. Regjistrimi i vulave të krijuara.....	31
33. Kërkesa për vlefshmëri kohore.....	31
34. Zgjatja e vlefshmërisë së dokumentit elektronik.	31
Kapitulli 8 – Mbi algoritmet.....	32
35. Algoritmet e krijimit dhe verifikimit të nënshkrimit.	32
Kapitulli 9 - Profili i certifikatave të kualifikuara	33
36. Norma të përgjithshme	33
37. Profili i certifikatave të kualifikuara.	33
Kapitulli 10 - Profili i certifikatave të certifikimit dhe certifikatave të vulosjes kohore	37
38. Profili i certifikatave të certifikimit dhe atyre të vulosjes kohore.....	37
39. Përdorimi i shtesave në certifikatat e certifikimit.	37
Kapitulli 11 - Përdorimi i shtesave në certifikatat e vulosjes kohore.....	38
40. Profili i certifikatave të vulosjes kohore.....	38
Kapitulli 12 - Rregulla për shërbimet e vlerësimit kohor	39

Kapitulli 13 - Informacione mbi shfuqizimin dhe revokimin e certifikatave	40
Kapitulli 14 - Formatet dhe aplikimet e nënshkrimit	41

Hyrje

Në mbështetje të nenit 10 të Ligjit Nr. 9880, datë 25.02.2008, “Për nënshkrimin elektronik”, Autoriteti Kombëtar për Certifikimin Elektronik (AKCE) është institucioni që mbikëqyr zbatimin e këtij ligji dhe akteve të tjera nënligjore të nxjerra në zbatim të tij. Në ushtrim të funksioneve të veta, si autoriteti i vetëm kompetent, AKCE ka të drejtë të nxjerrë udhëzime të hollësishme për procedurat teknike dhe ligjore, për rregullimin e të gjithë aktiviteteve në fushën e certifikimit elektronik, duke mundësuar përdorimin e ndërsjelle të nënshkrimit elektronik me shtetet anëtare të BE dhe vende të tjera të zonës ekonomike evropiane, që kanë vënë në zbatim të njëjtat masa teknike dhe organizative ose masa të barasvlershme me Direktivën 1993/93/CE.

1.1 Qëllimi i dokumentit

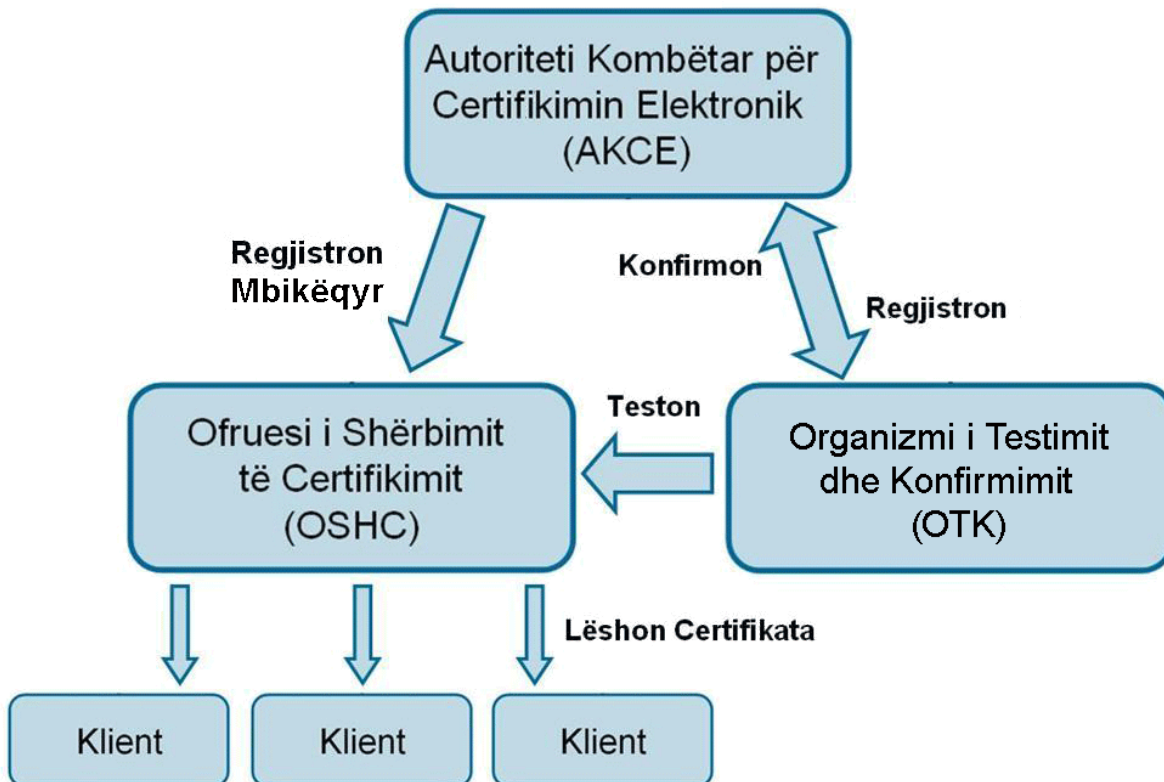
Meqenëse ligji “Për nënshkrimin elektronik” nuk përcakton në mënyrë të detajuar të gjitha specifikimet teknike që duhet të zbatohen në aktivitetin e një subjekti që ofron shërbime në fushën e nënshkrimit elektronik, me të drejtën që i jep Ligji, Autoriteti harton udhëzime të detajuara, ndjek zbatimin e tyre, reflekton ndaj çdo ndryshimi teknologjik apo standardesh, duke luajtur rolin e rregullatorit dhe garantuesit të koherencës së gjithë procesit të nënshkrimit elektronik, nëpërmjet pasqyrit të tyre në ligjshmëri dhe urdhra e udhëzime.

1.2 Struktura e dokumentit

Ky dokument bazohet në specifikimet teknike ETSI TS 101 456, ETSI TS 102 023, ETSI TS 101 862, ETSI TS 101 861 dhe Technical Report ETSI TR 102 437. Këto dokumente janë formuluar nga European Telecommunications Standards Institute. Sipas ETSI 101 456 është e nevojshme të citohen referimet e standardeve ISO/IEC, që zakonisht adoptohen në fushën e sigurisë të sistemeve informatike. Në veçanti, duhet theksuar se ky dokument për sa i përket niveleve të sigurisë, bën referim në standardet ISO/IEC 17799, ISO/IEC 27001 dhe ISO/IEC 15408.

1.3 Sistemi i Certifikimit Elektronik në Shqipëri

Ky sistem është i organizuar sipas skemës së mëposhtme:



Standardet e Referimit

Aspektet teknike bazë për nënshkrimin elektronik dhe certifikatat e kualifikuara janë të rekomanduara nga dy organizata ndërkombëtare standardizimi: Internet Engineering Task Force (IETF), e cila lëshon të ashtuquajturat RFC, dhe International Organization for Standardization / International Electrotechnical Commission (ISO/IEC). Ndërsa në Evropë në vitin 2000 u krijua EESSI, që operon duke u mbështetur në dy organizatat e standardizimit evropian ETSI (European Telecommunications Standardisation Institute) dhe CEN (Comité Européen de Normalisation).

2.1 Standardet ISO/IEC

Standardet ISO/IEC, që zakonisht janë të përdorura në nënshkrimin elektronik, janë ato që i përkasin serisë X. 500. Këto janë nxjerrë në fillim si rekomandime nga ITU-T (Internet Telecommunication Union), që është agjencia e telekomunikacioneve në Kombet e Bashkuara, dhe më vonë janë pranuar si standarde të plota nga ISO/IEC. Kjo e fundit i publikon në sferën e familjes së standardeve ISO/IEC 9594 me titull të përgjithshëm: “Information technology – Open Systems Interconnection – The Directory”.

Komponentët e kësaj familje janë aktualisht, siç vijon më poshtë:

Part 1: Overview of concepts, models and services

Part 2: Models

Part 3: Abstract service definition

Part 4: Procedures for distributed operation

Part 5: Protocol specifications

Part 6: Selected attribute types

Part 7: Selected object classes

Part 8: Public-key and attribute certificate frameworks

Part 9: Replication

Part 10: Use of systems management for administration of the Directory

Standarde të tjera, të cilat i bashkëngjiten serisë 9594, janë ato të cilat kanë të bëjnë me sigurinë e aparaturave si p.sh. atyre të nënshkrimeve (ISO/IEC 15408), me algoritmet kriptografie (ISO/IEC 10118). Përveç këtyre të mësipërme, ekzistojnë dhe standardet që kanë të bëjnë me teknikat e sigurisë: “Information security management systems”, të përmbledhura në familjen 27000, në të cilat bashkohet edhe ISO/IEC 17799.

2.2 IETF

Internet Engineering Task Force, vetëquhet: “një komunitet ndërkombëtar i hapur projektuesish, operatorësh dhe kërkuesish në fushën e rrjeteve kompjuterike”.

Grupe të ndryshme pune (Working Groups) janë të organizuara në tetë fusha interesi. Në njëren nga ato, atë të Security Area operojnë dy grupet që i interesojnë më shumë nënshkrimin elektronik: pkix - Public-Key Infrastructure (X.509) dhe smime- S/ MIME Mail Security. Lista publike e RFC-ve të nxjerra nga këto dy Working Groups është shumë e gjatë dhe për këtë arsye kufizohemi të përmendim ato kryesoret, që kanë të bëjnë më shumë me fushën e nënshkrimin elektronik.

Lista e plotë e RFC-ve të publikuara mund të gjendet në faqen e mëposhtme:

<http://rfc.net/rfc-index.html>

2.2.1 Working Group Public-Key Infrastructure (X.509) (pkix)

RFC 2560 - X.509 Internet Public-Key Infrastructure Online Certificate Status Protocol – OCSP

RFC 2797 - Certificate Management Messages over CMS

RFC 3161 – Internet X.509 Public-Key Infrastructure Time Stamp Protocols (TSP)

RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile

RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile

RFC 3628 – Policy Requirements for Time-Stamping Authorities

(derivuar nga ETSI TS 102 023)

RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

RFC 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocols

RFC 4211 – Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

RFC 4325 – Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension

2.2.2 Working Group S/ MIME Mail Security

RFC 3125 – Electronic Signature Policies (derivuar nga ETSI TS 101 733)

RFC 3126 – Electronic Signature Formats for long term electronic signatures(derivuar nga ETSI TS 101 733)

RFC 3370 – Cryptographic Message Syntax (CMS) Algorithms

RFC 3852 – Cryptographic Message Syntax (CMS)

2.3 EESSI

Në fund të vitit 1998, ndërkohë që akoma ishte duke u punuar mbi atë që më vonë u bë Direktiva 1999/93/CE, Komisioni Evropian i kërkoi ICTSB (Information and Communication Technology Standards Board) të vlerësonte nëse standardet ekzistuese ishin të mjaftueshme për të krijuar një bazë teknologjike për Direktivën që po përpunohej dhe për të siguruar përdorimin e saj në fushën e nënshkrimeve elektronike.

Më 24/02/1999 u krijua European Electronic Signature Standardization Initiative, e cila pas një analize të zhvillimeve më të fundit teknologjike-shkencore, rekomandoi zhvillimin e standardeve të pajtueshëm me ISO dhe IETF, me qëllim përbushjen e kërkesave që kërkonte Direktiva.

Në këtë mënyrë për të formuluar këto standarde, ICTSB krijoi ETSI (European Telecommunications Standards Institute) dhe CEN (Comité Européen de Normalisation). Në tetor të vitit 2004 pasi EESSI përfundoi mandatin e saj dhe arriti qëllimet e zhvillimit të këtyre standardeve, nevoja për të cilët kishte lindur në 1999, ICTSB vendosi ta mbyllë atë.

Më 17/7/2003 Komisioni Evropian vendosi që disa nga standardet e zhvilluara nga EESSI, dhe më saktësisht ato lidhur me pajisjet e nënshkrimit dhe karakteristikave të besueshmërisë së sistemeve të përdorura nga Ofruesit e Shërbimit, të merreshin si “norma përgjithësisht të njohura lidhur me produktet e nënshkrimit elektronik në pajtim të Direktivës 1999/93/CE të Parlamentit dhe Këshillit Evropian”. Ky vendim u publikua më 15.07.2003 në fletoren zyrtare të Komunitetit Evropian.

Grupi i punës E-sign i CEN përfundoi aktivitetin në 2003, siç kishte qenë e planifikuar, por komitete teknike të tjera të CEN vazhdojnë mirëmbajtjen e dokumenteve, të prodhuar nga ky grup pune, dhe vazhdimësinë e përpunimit të disa të tjerëve me qëllim fitimin e statusit European Norm (EN).

Grupi Teknik (Technical Body Electronic Signature and Infrastructure) i ETSI në anën tjetër vazhdon akoma zhvillimin e specifikimeve të mëtejshme, që gjithmonë e më shumë po drejtohen në aspektin e aplikimit të nënshkrimit elektronik, në mirëmbajtjen e dokumenteve të publikuara nga ai vetë për të arritur në njohje të dyanshme me dokumente të publikuara nga organizma të tjerë (si p.sh. USA Federal PKI).

2.3.1 CEN E-Sign WS

CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

CWA 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)

CWA 14167-3: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

CWA 14167-4: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

CWA 14169: Secure Signature-creation devices "EAL 3+"

CWA 14170: Security requirements for signature creation applications

CWA 14171: General guidelines for electronic signature verification

CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

CWA 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

Lista e plotë e publikimeve të nxjerra nga ky Workshop mund të gjehet në adresën e mëposhtëme:

<http://www.cenorm.be/cenorm/businessdomains/businessdomains/iss/cwa/electronic+signatures.asp>

2.3.2 ETSI ESI

ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates

ETSI TS 101 733: CMS Advanced Electronic Signatures (CAAdES)

ETSI TS 101 861: Time stamping profile

ETSI TS 101 862: Qualified certificate profile

ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

ETSI TS 102 023: Electronic Signatures and Infrastructures (ESI);Policy requirements for time-stamping authorities

ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates

ETSI TS 102 176-1: Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms

ETSI TS 102 176-2: Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel proto-cols and algorithms for signature creation devices

ETSI TS 102 231: Provision of harmonized Trust-service status information

ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

ETSI TR 102 437: Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)

Lista e plotë e publikimeve të nxjerra nga ky Grup Teknik mund të gjendet në adresën e mëposhtme:

<http://pda.etsi.org/pda/queryform.asp>, duke pasur parasysh të vini ESI në fushën “**Search for**” dhe duke zgjedhur **Technical Body Name** në opsjonin: “**Search in...**”

2.4 ISO / IEC 17799 dhe 27001

British Standards Institute ishte i pari që parashikoi nevojën e krijimit të një kornize sigurie për sistemet informatike dhe që më vonë e përmblodhi në atë që u bë një standard, BS 7799. Në 1995 u publikua versioni i parë, i cili bazohej në normative juridike britanike dhe që parashikonte si të krijohej ajo që quhet Information Security Management System – ISMS. Pas krijimit të BS 7799, ishte e nevojshme publikimi i disa kriterëve për vlerësimin e plotësimin të këtyre parametrave të sigurisë në një Information Security Management System. Më 1998 u publikua BS 7799-2 jo vetëm për të vlerësuar një ISMS, por edhe për të certifikuar nga ana formale një të tillë, pasi specifikonte kontrollet e sigurisë për t’u përfshirë sipas nevojës së tipit të ISMS-së. BS 7799 në 2000 u njoh akoma më tej në nivel ndërkombëtar duke u bërë standardi ISO / IEC 17799, i cili më pas në 2007 hyri në familjen 27000 duke u bërë standardi ISO / IEC 27002, ndërsa BS 7799-2 u transformua në ISO / IEC 27001. Botërisht, këto dy standarde janë bërë pika absolute referimi për të krijuar sigurinë dhe më pas për ta vlerësuar atë për një ISMS, duke bërë të mundur në këtë mënyrë dhe certifikimin e pajtueshmërisë me këto standarde.

Kapitulli 3

Shkurtime dhe përkufizime

Përkufizime:

“**Autoriteti Kombëtar për Certifikimin Elektronik**” është përgjegjës për regjistrimin dhe kontrollin e OSHC-ve.

“**Nënshkrim elektronik**” janë të gjitha të dhënat në formën elektronike, të cilat u bashkëlidhen ose shoqërojnë logjikisht të dhëna të tjera elektronike, që shërbejnë si një mënyrë e vërtetimit të identitetit të nënshkruesit dhe e vërtetësisë së dokumentit të nënshkruar.

“**Nënshkrimet elektronike të avancuara**” janë nënshkrimet elektronike, të cilat:

- a) i jepen ekskluzivisht një zotëruesi specifik të kodit të nënshkrimit;
- b) mundësojnë identifikimin e zotëruesit të kodit të nënshkrimit;
- c) prodhohen me mjete të sigurta;
- ç) lidhen me të dhënat, në mënyrë të tillë që të mundësojnë dallimin lehtësisht të çdo ndryshimi të mëpasshëm të këtyre të dhënave.

“**Nënshkrimet elektronike të kualifikuara**” janë nënshkrimet elektronike të avancuara, të cilat:

- a) mbështeten në një certifikatë të kualifikuar, që është e vlefshme në çastin e krijimit të nënshkrimit;
- b) janë prodhuar me një mjet të sigurt për krijimin e nënshkrimeve.

“**Kode të nënshkrimeve**” janë të dhënat elektronike unike, të tilla si kode ose algoritme kriptografie privatë, të cilat përdoren për të krijuar një nënshkrim elektronik.

“**Kode kontrolluese të nënshkrimeve**” janë të dhënat elektronike, të tilla si kode ose algoritme kriptografie publike, të cilat përdoren për të kontrolluar dhe verifikuar një nënshkrim elektronik.

“**Certifikata**” është çelësi publik i një përdoruesi bashkë me disa informacione të tjera, të cilat bëhen të padeshifrueshme, pasi enkriptohet me çelësin privat të ofruesit të shërbimit. (ITU-T Recommendation X.509)

“**Certifikatat e kualifikuara**” janë certifikatat e lëshuara nga ofruesit e shërbimeve të certifikimit, në përputhje me këtë ligj, që përmbushin kërkesat e përcaktuara në këtë ligj dhe në aktet nënligjore të nxjerra në zbatim të tij.

“**Çifti i Çelësave**” është një çelës nënshkrimi dhe një çelës i bashkëngjitur i verifikimit të nënshkrimit të lidhura me një algoritëm asimetric matematikor me njëri-tjetrin.

“**Ofruesit e shërbimeve të certifikimit**” janë personat fizikë ose juridikë, të cilët lëshojnë certifikata të kualifikuara ose vula kohore të kualifikuara.

“**Lëshimi e certifikatave**” është një shërbim i OSHC-së, i cili pas krijimit të certifikatës mundëson përdorimin nga mbajtësi dhe përdorues të tjerë, pasi autorizohet nga ky i fundit.

“Gjenerimi i Certifikatës” quhet shërbimi kur OSHC krijon një certifikatë të bazuar në emrin e zotëruesit të saj, dhe detajeve të tjera atëherë kur është e nevojshme, që verifikohen në momentin e regjistrimit.

“Zotëruesit e Certifikatës së Kualifikuar” janë personat fizikë, të cilët zotërojnë kode nënshkrimesh. Në rastin e nënshkrimeve elektronike të kualifikuara, atyre u caktohen kodet verifikuese përkatëse të nënshkrimeve në certifikatat e kualifikuara.

“Regjistrimi” - është një shërbim i OSHC-së, i cili konsiston në verifikimin e identitetit dhe kur është e nevojshme, detaje të tjera të zotëruesit të certifikatës para krijimit të certifikatës së tij ose lëshimin e të dhënave të aktivizimit, që mundësojnë fillimin e përdorimit të çelësve të nënshkrimit.

“Mjete të sigurta të krijimit të nënshkrimeve” - janë produkte hardware dhe software, të krijuara posaçërisht për nënshkrimet elektronike të kualifikuara, që përdoren për të ruajtur dhe aplikuar kodet përkatëse të nënshkrimeve, sipas kërkesave të këtij ligji dhe të akteve nënligjore të nxjerra në zbatim të tij.

“Produktet për nënshkrimet elektronike të kualifikuara” - janë mjete të sigurta për krijimin e nënshkrimeve, përbërësve të aplikimit të nënshkrimeve dhe përbërësve teknikë për shërbimet e certifikimit.

“Vula kohore të kualifikuara”- janë certifikata elektronike, të lëshuara nga një ofrues i shërbimeve të certifikimit, që konfirmojnë se të dhëna të caktuara elektronike janë paraqitur në një kohë të caktuar.

“Lista e Certifikatave të Revokuara” - është një listë e publikuar nga OSHC, e cila përmban të gjithë numrat e serisë të certifikatave, që janë shfuqizuar përpara datës së skadimit të certifikatës.

“Certifikata të certifikimit” – certifikata të kualifikuara që zotërohen nga një ofrues shërbimi, çelësi privat i të cilit shërben për të gjeneruar çelësat e certifikata të kualifikuara të subjekteve.

“Policat e Sigurisë” - një sërë rregullash dhe direktivash, të nxjerra si rrjedhojë e analizës së rrezikut për të zvogëluar mundësinë e incidenteve (masa parandaluese) dhe zbutjen e efekteve të mëvonshme, për të mbrojtur burimet e cilësuara si të ndjeshme për OSHC-në. Specifikimi i një strategjie sigurie bën të mundur përcaktimin e qartë të nivelit të përgjithshëm të sigurisë, që duhet arritur për një sistem informativ dhe në mënyrë specifike për çdo element të arkitekturës së sigurisë.

“Hardware Security Module” - Module kriptografike hardware, që mund të krijojnë, mirëmbajnë dhe përdorin çelësa privatë të nënshkrimeve të ofruesve të shërbimeve, për t'ia bashkangjitur nënshkrimin e tyre certifikatave të kualifikuara dhe vulave kohore, me qëllim sigurimin në vazhdimësi të vërtetësisë dhe integritetit.

“Incident sigurie” – Një ngjarje e vetme e papritur ose e padëshiruar, ose një seri ngjarjesh të tilla të ndërlydhura me sigurinë e informacioneve dhe që kanë një probabilitet të lartë për të kompromentuar operacionet e biznesit dhe për të vënë në rrezik sigurinë e informacioneve. (ISO / IEC TR 18044: 2004)

“Information Security Management System” – Pjesa e sistemit të brendshëm të menaxhimit, që në bazë të një vlerësimi të rrezikut, përcakton, realizon, bën operacionale proceset dhe burimet.

“**Key Escrow**” – Vend ruajtjeje i çelësit privat pranë ofruesit të shërbimit, ose enteve të tjera të besueshme, nga i cili në mënyrë të qartë është e mundur që personat e autorizuar të marrin informacion mbi një ose me shumë palëve.

“**Vulë Kohore**” – Provë elektronike, që lejon vlefshmërinë kohore.

“**Time-Stamp Token**” – Vulë kohore, TST

“**Time Stamping Authority**” – TSA, palë e besueshme që lëshon TST nëpërmjet sistemeve të ashtuquajtura TSS

“**Time-Stamp Server**” – Sisteme ku bazohet një ofrues shërbimi, i cili operon si TSA për të lëshuar TST

“**Time-Stamping Unit**” – Bashkësia e hardware dhe software, që janë pjesë e një Time-stamp Server dhe i përdorur nga ky i fundit vetëm për të nënshkruar TST dhe që ka vetëm një aparaturë nënshkrimi, i cili përdor vetëm një herë të njëjtën kopje çelësash nënshkrimi.

“**Vlefshmëria kohore**” – Rezultati i një procedure informatike me të cilën i bashkëngjiten një ose me shumë dokumenteve elektronike, një datë dhe një orë ekzakte për informacion të një palë të tretë.

Shkurtime:

HSM	Hardware Security Module
ISMS	Information Security Management System
TSA	Time Stamping Authority
TSS	Time Stamp Server
TST	Time Stamp Token
TSU	Time Stamping Unit

Kapitulli 4

Referime

Direktiva 1999/93/ CE - Direktiva 1999/93/ CE e Parlamentit dhe e Këshillit Evropian e datës 13 Dhjetor 1999, lidhur me kornizën e komunitetit mbi nënshkrimet elektronike.

ETSI TS 101 456 - Electronic Signatures and Infrastructures (ESI), Policy requirements for certification authorities issuing qualified certificates.

ETSI TS 101 861 Time stamping profile.

ETSI TS 101 862 Qualified Certificate Profile

ETSI TS 102 176-1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

ETSI TR 102 437 Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)

ETSI TR 102 438 Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)

ETSI TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

IETF RFC 2119 Key words for use in RFCs to Indicate Requirement Levels

IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

IETF RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocols (CMP)

ISO/IEC 9594-8: 2001 Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks – Fourth edition 2001-08-01

ISO/IEC 17799: 2005 Information technology — Security techniques — Code of practice for information security management

ISO/IEC 27001: 2005 Information technology — Security techniques — Information security management systems — Requirements

NIST SP 800-57 NIST Special Publication 800-57; May, 2006; Recommendation for Key Management – Part 1: General

Kapitulli 5

Modaliteti i kontrollit

5.1 Ofruesi i shërbimit

Ofruesi i shërbimit paraqet dokumente (aty ku është e nevojshme edhe “log”-et e sistemit dhe të aplikacioneve) për të treguar përmbushjen e kërkesave ligjore dhe kërkesat e tjera të sigurisë, në pajtim me standardet e adoptuara dhe në veçanti standardet e ETSI dhe ISO/IEC, pranë Autoritetit, për tu regjistruar si i tillë. Në rastet kur, OSHC ka filluar aktivitetin, pa bërë më parë regjistrimin pranë Autoritetit, atëherë përveç procedurave të mësipërme, duhet të paraqesë regjistrat e inspektimeve të kryera nga ai me frekuencën e duhur, në pajtim të procedurave të tij të brendshme dhe këtë procedurë duhet ta ndjekë deri në përfundimin e aktivitetit të tij.

Konsiderohet e nevojshme të kryhen kontrole me frekuencë mujore për:

- a) Integritetin e përmbajtjes së regjistrit të kontrollit;
- b) Saktësinë e inventarit të pajisjeve të nënshkrimit.

Konsiderohet e nevojshme të kryhen kontrole me frekuencë semestrale për:

- a) Përputhshmërinë e konfigurimit të sistemeve hardware, software, PKI, firewall
- b) Procedurat e kryera nga personeli për sa i përket operacioneve të:
 - 1. Kontrollit të aksesit fizik, kudo që nuk janë përdorur mjete të regjistrimit automatik në regjistrin e kontrollit.
 - 2. Konservimit dhe ruajtjes së dokumentacionit të regjistrimit të subjekteve, të Shfuqizimit dhe Pezullimit të certifikatave të këtyre të fundit
 - 3. Respektimi i masave të sigurisë mbi privatësinë.
 - 4. Përputhshmëria e të dhënave të ruajtura në selinë qendrore dhe atyre të “disaster recovery”, ose të ruajtjes së kopjeve të sigurisë.

Konsiderohet nevojshme të kryhen kontrole vjetore për:

- a) Respektimin e procedurave të tjera të përdorura në aktivitetin e certifikimit.
- b) Funkcionimin e procedurave të *disaster recovery*.

Ofruesi i Shërbimit paraqet prova të restartimit të sistemit dhe të rikuperimit të të dhënave nga qendra e backup-it.

Nëse kërkohet nga Organizmi i Testimit dhe Konfirmimit, OSHC zbaton procedura të tjera.

5.2 Organizmi i testimit dhe konfirmimit

Në analizën e masave të sigurisë dhe të procedurave operative të adoptuara nga OSHC, OTK duhet të marrë si të vërtetë që këto të jenë vendosur me bazë standardin ISO/IEC 17799. Në çdo rast që një OSHC adopton kritere të ndryshme është përgjegjësia e tij të informojë Autoritetin.

OTK-ja:

1. Përpara se të kryejë kontrollin:

- a) Duhet të njihet paraprakisht me dokumentacionin e depozituar pranë Autoritetit nga Ofruesi i Shërbimit të Certifikimit, përfshirë këtu edhe dokumentacionin e mundshëm të dorëzuar pas regjistrimit të këtij të fundit, përveç pikës 1 a, b, c të planit mbi sigurinë, të cilat shqyrtohen vetëm në rast kontestimesh.
- b) Verifikon, që manuali operativ i publikuar pranë faqes së internetit të OSHC apo në forma të tjera publikimi, është i njëjti me atë të dorëzuar pranë Autoritetit dhe i publikuar në faqen zyrtare të këtij të fundit.
- c) Njihet me *Certificate Policy, Certification Practice Statement, Disclosure Statement*, përdorimi i të cilave përcaktohet në certifikatat e lëshuara nga OSHC.
- d) Njihet paraprakisht me autorizimet e mundshme të lëshuara nga Autoriteti për përdorimin e çelësave të certifikimit, të certifikatave të kualifikuara për qëllime të tjera përveç atyre të përcaktuara nga ky dokument.
- e) Njihet me selitë e përdorura nga OSHC: për konservimin e kopjeve rezervë të çelësave, selinë e *disaster recovery* dhe seli të tjera të mundshme të transferimit të shërbimeve të certifikimit.

2. Gjatë inspektimit, bazuar në sa thuhet në këtë dokument OTK-ja:

- a) Verifikon në regjistër, që OSHC ka kryer inspektime të brendshme për procedurat e tij dhe këto inspektime kanë qenë periodike. Gjithashtu, nëse nga këto inspektime të kenë rezultuar situata në kundërshtim me rregullat e përcaktuara nga Autoriteti dhe jo në pajtim të procedurave të përcaktuara nga ai, që OSHC të ketë marrë masat e nevojshme për të korrigjuar këto probleme.
- b) Verifikon pajtueshmërinë me përcaktimet e këtij dokumenti, sidomos për ato specifikime që janë thelbësore. Gjithashtu, mund të kryejë teste dhe kontrole të tjera, që nuk përcaktohen nga ky dokument, për atë kohë sa këto shërbejnë për arritjen e përfundimit të testimit/kontrollit.
- c) Mund të kërkojë, për të kryer verifikimet që përcaktojnë si të nevojshme, ekzekutimin e procedurave lidhur me lëshimin e certifikatave të kualifikuara dhe pajisjeve të sigurta për krijimin e nënshkrimeve. Këto certifikata dhe pajisje të nënshkrimeve, mund të përdoren vetëm për qëllimet e vlerësimit dhe kontrollit. Pasi OTK kryen të gjithë inspektimet e nevojshme, pajisjet e sigurta të krijimit të nënshkrimeve, kthehen në gjendjen e mëparshme dhe certifikatat e krijuara gjatë këtij procesi revokohen menjëherë.

Verifikon raportet e kontrollit, qofshin këto të jashtme ose të brendshme. Në rastin që një raport konstaton probleme teknike, pika të dobëta, ose mungesë vëmendjeje në ndjekjen e përpiktë të procedurave, etj, verifikon që një problem i tillë që është zbuluar nga auditi të jetë korrigjuar.

Shënim: Vlerësimi i verifikimeve, mbi masat e sigurisë dhe masat operative, mbi konsistencën dhe përgatitjen e personelit dhe mbi mjetet e sigurisë së vendosura do të bëhen duke marrë për bazë dokumentacionin që OSHC ka depozituar pranë Autoritetit, edhe në rastin kur versione më të fundit janë publikuar nga OSHC më vonë se versioni i dorëzuar pranë Autoritetit .

5.3 Modaliteti i inspektimit

Data e inspektimit nga Autoriteti i komunikohet personit përgjegjës të OSHC-së të paktën 48 orë para.

Data e fillimit të inspektimit, do të jetë ajo e takimit të vlerësuesve të OTK me personin përgjegjës për inspektimet dhe verifikimet të OSHC, ose me një person të ngarkuar nga ky i fundit në mungesë të tij. Kjo datë dhe orë shënohet në raportin e inspektimit nga OTK dhe nënshkruhet nga përgjegjësi i inspektimeve dhe verifikimeve ose nga personi i caktuar në mungesë të tij.

Grupi i vlerësimit të OTK, bazohet në inspektimet e tij sidomos për sa paraqitet në Manualin Operativ dhe në Planin mbi Sigurinë të OSHC përveç pikës 1, b, c, d, të cilat do ekzaminohen vetëm në rast kontestimesh.

Dokumente të tjera, që do merren parasysh në zhvillimin e vlerësimit janë të poshtëshënuara dhe të cituara në kapitullin 4 – Referime:

- ISO/IEC 17799
- ISO/IEC 27001
- ETSI TS 101 456

1. Karakteristika të përgjithshme për krijimin dhe verifikimin e nënshkrimit.

1. Për krijimin e nënshkrimit, një kopje çelësash mund t'i jepet vetëm një subjekti.
2. N.q.s. subjekti bashkëngjitet nënshkrimit nëpërmjet një procesi automatik, duhet të përdorë një kopje çelësash të ndryshme nga gjithë të tjerat në posedim të tij.
3. Nëse procedura automatike përdor më shumë se një pajisje për të bashkëngjitur nënshkrimin, duhet të përdorët një kopje e veçantë çelësash për çdo pajisje.
4. Çelësat ndahen në grupet e mëposhtme:
 - a. Çelësa nënshkrimi, të destinuar për gjenerimin dhe verifikimin e nënshkrimeve të bashkëngjitura ndaj dokumenteve.
 - b. Çelësa certifikimi, të destinuar për gjenerimin dhe verifikimin e nënshkrimeve të bashkëngjitura në certifikatat e kualifikuara, listave të revokimit dhe listave të pezullimeve, ose nënshkrimit të certifikatave me nënshkrim vulash kohore.
 - c. Çelësa të vulave kohore, destinuar për gjenerimin dhe verifikimin e vulave kohore.
5. Nuk është i lejuar përdorimi një çifti çelësash për funksione të ndryshme nga ato të parashikuara, për secilën kategori, në pikën 4 me lart.
6. Në rrjedhim të pikës 5 me lart çelësat e pikës 4/b mund të përdoren për qëllime të tjera vetëm me autorizim nga Autoriteti.
7. Fortësia e çelësave duhet të jetë e tillë që të garantojë një nivel sigurie që të jetë në raport të drejtë me njohjet më të fundit shkencore dhe teknologjike.

2. Gjenerimi i çelësave.

1. Gjenerimi i kopjes së çelësave duhet të bëhet nëpërmjet pajisjeve dhe procedurave, të cilat sigurojnë në raport me njohjet e fundit shkencore-teknologjike, veçantinë dhe fortësinë e çiftit të krijuar, si dhe fshehtësinë e çelësit privat.
2. Sistemi i gjenerimit të kopjes së çelësave duhet të sigurojë:
 - a. Lidhjen e çiftit të çelësave me kërkesat e algoritmeve të gjenerimit dhe të verifikimit të përdorur;
 - b. Probabiliteti i njëjtë i gjenerimit të të gjithë çifteve të mundshme;
 - c. Identifikimi i subjektit që aktivizon procedurën e gjenerimit.

3. Modaliteti i gjenerimit të çelësave

1. Çelësat e certifikimit mund të krijohen ekskluzivisht nga ofruesi i shërbimit të certifikimit.
2. Çelësat e nënshkrimit mund të krijohen nga subjekti ose nga ofruesi i shërbimit.

3. Gjenerimi i çelësave të nënshkrimit që kryhet në mënyrë autonome nga subjekti, duhet të ndodhë në brendësi të pajisjeve të sigurta të gjenerimit të nënshkrimeve, që duhet të jenë lëshuar ose njohur nga ofruesi i shërbimit.
4. Subjekti është i detyruar të përdorë një pajisje të ofruar nga ofruesi i shërbimit ose të zgjedhë një nga pajisjet e këshilluara prej tij.

4. Ruajtja e çelësave

1. Është i ndaluar shumëfishimi i çelësit privat dhe i mjeteve që e përmbajnë atë.
2. Për arsye të veçanta sigurie është e lejuar që çelësat e certifikimit të eksportohen ose lëvizjen në mënyrë të tillë që gjatë këtij procesi të mos të ulet niveli minimal i sigurisë.
3. Mbajtësi i kopjes së çelësave:
 - a. Konservon me kujdesin më të madh çelësin privat ose mjetin që e përmban atë me qëllim që të garantojë integritetin dhe fshehtësinë më të madhe.
 - b. Të ruajë informacionet mbi vënien në punë të çelësit privat jo në një të njëjtin mjet si ai që ruan çelësin privat.
 - c. Bën kërkesë për revokimin e menjëhershëm të certifikatës së kualifikuar, e cila lidhet me çelësa të cilat janë ruajtura në një mjet me probleme ose një mjet, që ky i fundit të ketë humbur posedimin.

5. Gjenerimi i çelësave jashtë pajisjeve të krijimit të nënshkrimit

1. Nëse gjenerimi i çelësave ndodh në një sistem të ndryshëm nga ai i destinuar për krijimin e nënshkrimit, atëherë ky sistem duhet të sigurojë:
 - a. Pamundësinë e interceptimit ose rikuperimit të çfarëdo informacioni, qoftë ai i përkohshëm e që prodhohet gjatë ekzekutimit të kësaj procedure;
 - b. Transferimin i çelësit privat në kushte sigurie maksimale deri në pajisjen e nënshkrimit në të cilën do përdoret më vonë.
2. Sistemi i gjenerimit duhet të jetë i izoluar, i dedikuar ekskluzivisht për këtë aktivitet dhe i mbrojtur posaçërisht kundër rreziqeve të nderhyrjes dhe interceptimit.
3. Hyrja në sistem duhet të ndodhë duke kontrolluar dhe identifikuar më parë çdo përdorues (subjekt). Çdo sesion pune duhet të ruhet në regjistrin e kontrollit.
4. Përpara gjenerimit të një kopjeje çelësash, i gjithë sistemi duhet të verifikohet për konfigurimin e tij, autenticitetin dhe integritetin e programeve të instaluar dhe mungesës së programeve të paparashikuara nga procedura.

6. Pajisjet e sigurta dhe procedurat për gjenerimin e nënshkrimit.

1. Gjenerimi i nënshkrimit duhet të ndodhë në brendësi të një pajisje të sigurtë të nënshkrimit në mënyrë të tillë që mos të jetë e mundur interceptimi i çelësit privat të përdorur.

2. Pajisja e sigurve e nënshkrimit duhet të jetë aktivizuar ekskluzivisht nga subjekti përpara fillimit të gjenerimit të firmës.
3. Nëse pajisja e sigurt e nënshkrimit personalizohet ajo duhet të paktën të garantojë që ofruesi i shërbimit të ketë marrë informacion mbi të dhënat identifikuese të pajisjes së përdorur dhe lidhjen e saj me subjektin; regjistrimin në pajisje të certifikatës së kualifikuar që është e lidhur me çelësat e nënshkrimit të subjektit.

7. Verifikimi i nënshkrimit elektronik

1. Ofruesit e shërbimit të certifikimit, që lëshojnë certifikata të kualifikuara duhet të ofrojnë ose të paktën të tregojnë një sistem, që bën të mundur verifikimin e nënshkrimeve elektronike.

8. Gjenerimi i çelësve të certifikimit

1. Për çdo çelës të certifikimit, Ofruesi i Shërbimit duhet të krijojë një certifikatë të nënshkruar me çelësin privat të kopjes së çelësve tek të cilat certifikata referohet.
2. Vlerat e përmbajtura në fushat e njëjta të certifikatës së çelësve të certifikimit duhet të kodifikohen në mënyrë që të mos të ketë mundësi të ndodhin ngatërresa në lidhje me emrin, rajonin dhe të dhëna të tjera të ofruesit të shërbimit.

9. Gjenerimi i certifikatave të kualifikuara

1. Përpara gjenerimit të certifikatës ofruesi i shërbimit duhet të :
 - a. Kontrollon vërtetësinë dhe korrektësinë e kërkesës.
 - b. Verifikon zotërimin e çelësit privat dhe funksionimin e duhur të kopjes së çelësve.
2. Lëshimi i certifikatave të kualifikuara duhet të shkruhet në regjistrin e kontrollit, me datën dhe orën ekzakte të gjenerimit. Ky moment duhet të vërtetohet nëpërmjet një sistemi të referimit kohor.

10. Informacionet e përmbajtura në certifikatat e kualifikuara.

1. Certifikatat e kualifikuara përveç informacionit që parashikohet në pikat e tjera të këtij dokumenti duhet të përmbajnë:
 - a. Kodin e subjektit pranë ofruesit të shërbimit.
 - b. Tipologjinë e kopjes së çelësve në bazë të përdorimit për të cilën janë destinuar.
2. Informacionet personale të përfshira në certifikatë, janë të përdorura me të vetmin qëllim për të identifikuar subjektin zotëruar të nënshkrimit elektronik, për të legjitimuar nënshkrimin e një dokumenti elektronik dhe për të treguar funksionet e subjektit.
3. Ofruesi i shërbimit përcakton periudhën e vlefshmërisë së certifikatave në funksion të fortësisë të çelësve të krijimit dhe verifikimit të përmbajtura dhe të shërbimeve për të cilat ato janë destinuar.

4. Certifikuesi ruan informacionet për një periudhë jo më të vogël se 10 vjet që nga koha e skadimit ose e revokimit të certifikatës së kualifikuar.

11. Shfuqizimi i certifikatës së kualifikuar

1. OSHC duhet të shfuqizojë një certifikatë të kualifikuar, kur ka informacion për komprometimin e çelësit privat ose të mjetit të krijimit të nënshkrimit.
2. Nëse shfuqizimi është bërë për shkak të komprometimit të fshehtësisë së çelësit privat, ofruesi në mënyrë urgjente, duhet ta publikojë dhe të plotësojë listën e revokimeve.
3. Shfuqizimi i certifikatave shënohet në regjistrin e kontrollit me datë dhe orë të saktë.
4. Përveç rasteve që gjykohet urgjente, ofruesi i shërbimit lajmëron më parë zotëruesin e certifikatës për shfuqizimin e saj, duke i bërë të ditur datën dhe orën e saktë pas të cilës ajo nuk do të jetë më e vlefshme.
5. Nëse subjekti bën kërkesë për shfuqizim të certifikatës së tij, specifikat e kërkesës dhe mënyra e paraqitjes së saj, duhet të përcaktohen nga ofruesi i shërbimit në manualin e përdorimit.
6. Në rastet kur, ofruesi i shërbimit verifikon origjinalitetin e kërkesës vazhdon me procesin e shfuqizimit të certifikatës brenda afatit të kërkuar. Nëse nuk ka mundësi verifikimi deri në afatin e caktuar, ofruesi e pezullon certifikatën.
7. Kërkesa për shfuqizim nga ana e një pale të tretë të interesuar, e cila është përfaqësuese e një subjekti, duhet t'i dorëzohet ofruesit, bashkangjitur me nënshkrimin e subjektit dhe një autorizim të tij. Pas kësaj, ofruesi duhet të njoftojë subjektin zotërues për shfuqizimin e certifikatës.
8. Nëse dokumentet dhe kërkesat, nuk verifikohen brenda afatit, atëherë ofruesi procedon në pezullimin e certifikatës, deri në përmbushjen e kriterëve.

12. Pezullimi i certifikatës së kualifikuar.

1. Pezullimi nga ana e ofruesit kryhet duke e futur certifikatën në listën e certifikatave të pezulluara (CSL).
2. Përveç rasteve urgjente, ofruesi i shërbimit duhet të lajmërojë paraprakisht subjektin zotërues për pezullimin e certifikatës duke specifikuar arsyet dhe kohëzgjatjen e saj.
3. Lajmërimi duhet t'i specifikojë subjektit datën dhe orën e saktë prej së cilës certifikata do të ndryshojë në statusin "pezulluar".
4. Kërkesa për pezullim nga ana e subjektit duhet t'i paraqitet ofruesit të shërbimit bashkangjitur me nënshkrimin e tij dhe me hollesira të zgjatjes së saj.
5. Kërkesa për pezullim nga një palë e tretë e interesuar, e cila ka të drejtën e përfaqësimit të subjektit, duhet të dorëzohet tek ofruesi e firmosur me nënshkrimin e këtij e subjektit dhe me specifikimet mbi zgjatjen e pezullimit.

13. Zëvendësimi i çelësve të certifikimit

1. Zëvendësimi i çelësve të certifikimit bëhet nga ofruesi i shërbimit të paktën 90 ditë përpara skadimit të certifikatës së certifikimit. Gjenerimi i çelësve bëhet sipas modalitetit dhe rregullave të parashikuara në këtë dokument.
2. Pas gjenerimit të çelësve ofruesi i shërbimit duhet të krijojë një certifikatë, që përmban çelësin e ri publik të nënshkruar me çelësin e vjetër privat, dhe një certifikatë, që përmban çelësin e vjetër publik të nënshkruar me çelësin e ri privat. Këto certifikata duhet t'i dërgohen Autoritetit.

14. Shfuqizimi i certifikatave që përmbajnë çelësa certifikimi.

1. Shfuqizimi i certifikatave me kopje çelësash certifikimi, lejohet në rastet e mëposhtme:
 - a. Komprometim i çelësit privat, në kuptimin e zvogëlimit të besueshmërisë në karakteristikat e sigurisë të çelësit privat.
 - b. Defekt teknik në pajisjen e nënshkrimit.
 - c. Ndërprerjen e aktivitetit.
2. Shfuqizimi duhet t'i njoftohet brenda 24 orësh Autoritetit dhe gjithë subjekteve certifikatat e kualifikuara, të cilëve janë nënshkruar me çelësin privat të kësaj certifikate.
3. Nëse shfuqizimi ndodh për shkak të komprometimit të çelësit privat siç parashikohet në pikën 1 më lart, atëherë të gjitha certifikatat e kualifikuara të nënshkruara me këtë çelës privat, duhet të shfuqizohen menjëherë dhe të njoftohen të gjithë subjektet përkatëse.

15. Kërkesat e sigurisë për sistemet operative.

Sistemi operativ kompjuterik i sistemeve të përpunimit në aktivitetin e certifikimit për gjenerimin e çelësve, gjenerimin e certifikatave të kualifikuara dhe menaxhimin e regjistrimit të certifikatave të kualifikuara duhet të jenë në pajtim me sa përcaktohet në specifikimet ITSEC F-C2/ të nivelit E 2 ose me tepër. Këto nuk aplikohen për sistemin operativ të pajisjes së nënshkrimit.

16. Sistemi i gjenerimit të certifikatave të kualifikuara.

1. Gjenerimi i certifikatave të kualifikuara duhet të ndodhë në një sistem që përdoret ekskluzivisht për gjenerimin e certifikatave, i ndodhur në një seli lokale me sigurinë e nevojshme.
2. Hyrja dhe dalja nga zona rrotull duhet të regjistrohet në regjistrin e kontrollit.
3. Hyrja në sistemin e përpunimit duhet t'i lejohet vetëm personelit të autorizuar dhe kjo të jetë e kufizuar vetëm në funksionet e përcaktuara të secilit. Hyrja duhet të identifikohet nëpërmjet një procedure njohjeje nga sistemi në momentin e fillimit të çdo sesioni.
4. Fillimi dhe përfundimi i çdo sesioni duhet të regjistrohet në regjistrin e kontrollit.

9. Përdorimi i certifikatave nga publiku.

1. Listat e certifikatave të vlefshme, të shfuqizuara dhe të revokuara duhet të bëhen publike.
2. Certifikatat e kualifikuara, me kërkesë të subjektit mund të bëhen të hapura për konsultim publik ose ju komunikohen palëve të treta vetëm në rastet e lejuara nga zotëruesi i certifikatës.
3. Listat e publikuara me certifikatat të shfuqizuara dhe të revokuara, si dhe certifikatat e vlefshme të publikuara janë të përdorshme vetëm për qëllimin e aplikimit të normave që bashkërendojnë verifikimin dhe vlefshmërinë e nënshkrimeve elektronike.

10. Plani mbi sigurinë

1. Ofruesi i shërbimit duhet të formulojë një plan mbi sigurinë në të cilin duhet të jenë të përmbajtura elementet e mëposhtëm:
 - a. struktura e përgjithshme, modalitet e veprimit dhe struktura e logjistikës;
 - b. përshkrim i infrastrukturës së sigurisë për çdo aset të patundshëm me rëndësi për qëllimet e sigurisë;
 - c. shpërndarja e zyrave dhe shërbimeve nëpër ndërtesë/a;
 - d. lista e personelit dhe shpërndarja e tyre nëpër zyrat përkatëse;
 - e. shpërndarja e përgjegjësive;
 - f. algoritmet kriptografike dhe sisteme të tjera të përdorura;
 - g. përshkrim i procedurave të përdorura në aktivitetin e certifikimit;
 - h. përshkrim i pajisjeve të instaluara;
 - i. përshkrim i fluksit të të dhënave;
 - j. procedura e menaxhimit të kopjeve të sigurisë së të dhënave;
 - k. analiza e rrezikut;
 - l. përshkrim të kundërmasave;
 - m. specifikime të kontrollit;
2. Plani i sigurisë, i nënshkruar nga përfaqësuesi ligjor i ofruesit të shërbimit, duhet të dorëzohet në zarf të vulosur tek Autoriteti.
3. Informacioni i detajuar mbi pikat b, c dhe d duhet gjithashtu të dorëzohet në një zarf të vulosur, i ndryshëm nga i sipërpërmenduri, pranë Autoritetit, zarf i cili do të hapet vetëm në rastin e kontestimeve.

11. Sistemi i cilësisë të ofruesit të shërbimit.

1. Brenda një viti pas fillimit të aktivitetit, OSHC duhet të deklarojë pajtueshmërinë e sistemit të tij të cilësisë me normat e standardit ISO 9000 dhe evoluime të mëvonshme, ose të normave të njëvlershme.
2. Manuali i cilësisë duhet të depozitohet pranë Autoritetit dhe të mbahet edhe pranë zyrave të ofruesit të shërbimit.

12. Organizimi i personelit të ofruesit të shërbimit.

1. Organizimi i personelit që punon në fushën e shërbimit të certifikimit, duhet të parashikojë të paktën funksionet e mëposhtme:
 - a. Përgjegjësin e sigurisë.
 - b. Përgjegjësin e gjenerimit dhe ruajtjes së çelësave.
 - c. Përgjegjësin e personalizimit të pajisjes së nënshkrimit.
 - d. Përgjegjësin e gjenerimit të certifikatave.
 - e. Përgjegjësin e mirëmbajtjes të regjistrit të certifikatave.
 - f. Përgjegjësin e regjistrimit të subjekteve (klientëve).
 - g. Përgjegjësin e sigurisë së të dhënave;
 - h. Përgjegjësin e kriptografisë dhe të sistemit kriptografik të përdorur;
 - i. Përgjegjësin e shërbimeve teknike;
 - j. Përgjegjësin e verifikimeve dhe të inspektimeve (kontrolli);
 - k. Përgjegjësin e sistemit të referimit kohor.
2. Të njëjtit individ mund t'i caktohen më shumë funksione seç parashikohet në pikën më lart për sa kohë ato janë në pajtim; funksionet në pajtim midis tyre janë siç vijohet për secilin grup:
 - a. Gjenerimi dhe ruajtja e çelësave, gjenerimi i certifikatave, personalizimi i pajisjes së nënshkrimit, kriptografia, siguria e të dhënave;
 - b. Regjistrimi i subjekteve, mirëmbajtja e regjistrit të certifikatave, kriptografia, siguria e të dhënave, sistemi i referimit kohor.

13. Kodi i emergjencës

1. Për çdo certifikatë të kualifikuar ofruesi i shërbimit duhet të furnizojë subjektin zotëruar të certifikatës me të paktën një kod të emergjencës për të vërtetuar identitetin në rastet e mundshme të një kërkesë për shfuqizim të certifikatës.
2. Në raste emergjence subjekti mund të kërkojë shfuqizimin e menjëhershëm të certifikatës së tij vetëm duke përdorur kodin e rezervuar. Më vonë subjekti është i detyruar të bëjë kërkesën e plotë siç parashikohet nga normativa dhe rregullat e ofruesit të shërbimit.
3. Është përgjegjësi e ofruesit të shërbimit të adoptojë masa sigurie për të siguruar fshehtësinë e kodit të emergjencës.

14. Manuali operativ

1. Manuali operativ përcakton procedurat e aplikuara nga një ofrues shërbimi që lëshon certifikata të kualifikuara në zhvillimin e aktivitetit të tij.
2. Manuali operativ duhet të dorëzohet pranë Autoritetit dhe të publikohet në faqen e internetit të OSHC.

3. Manuali duhet të përmbajë të paktën informacionet e mëposhtme:
- a. të dhënat identifikuese të OSHC;
 - b. të dhënat identifikuese të versionit të manualit operativ;
 - c. përgjegjësin e manualit operativ;
 - d. përgjegjësitë dhe detyrimet e OSHC, të subjekteve zotërues dhe të atyre që aplikojnë për certifikatë të kualifikuar;
 - e. përcaktimet e përgjegjësive dhe kufizimet e mundshme të drejtave;
 - f. adresa e faqes së internetit, ku përveç të tjerash janë të publikuara edhe tarifatat e shërbimit;
 - g. modaliteti i identifikimit dhe regjistrimit të abonentëve;
 - h. modaliteti i gjenerimit të çelësave të krijimit dhe verifikimit të nënshkrimit;
 - i. modaliteti i lëshimit të certifikatave;
 - j. modaliteti i përjashtimit nga shërbimi;
 - k. modaliteti i zëvendësimit të çelësave;
 - l. modaliteti i shfuqizimit dhe revokimit të certifikatave;
 - m. modaliteti i mirëmbajtjes së regjistrimit të certifikatave;
 - n. modaliteti i aksesit së regjistrimit të certifikatave;
 - o. modaliteti i mbrojtjes së fshehtësisë;
 - p. modaliteti i vendosjes së vulave kohore;
 - q. modaliteti operativ për përdorimin e sistemit të verifikimit të nënshkrimit;
 - r. modaliteti operativ për gjenerimin e nënshkrimit elektronik.

15. Detyrimet e ofruesit të shërbimit.

1. Ofruesi i shërbimit të certifikimit duhet të mbajë një kopje të listës së certifikatave të lidhura me çelësat e certifikimit, kjo listë duhet të dorëzohet pranë Autoriteti dhe duhet të jetë e aksesueshme në faqen e tij të internetit.
2. Ofruesit e shërbimit të certifikimit për t'u regjistruar dhe më vonë për ta mbajtur këtë status, duhet të kryejnë aktivitetin e tyre në pajtim me rregulloren, specifikimet teknike të nxjerra Autoriteti dhe ligjin mbi nënshkrimin elektronik.

16. Lista publike e ofruesve të shërbimit të regjistruar

1. Lista publike e ofruesve të shërbimit të certifikimit, të regjistruar në vendin tonë mbahet nga Autoriteti dhe për çdo ofrues përmban informacionin e mëposhtëm:
 - a. Emrin ;
 - b. Selinë ligjore;
 - c. Përfaqësuesin ligjor;
 - d. Emrin X.500;
 - e. Adresën në internet;
 - f. Listën e certifikatave të çelësave të certifikimit;
 - g. Manualin operativ;
 - h. Datën e regjistrimit;
 - i. Datën e ndërprerjes së veprimtarisë dhe zëvendësuesi i mundshëm.
2. Lista publike nënshkruhet dhe bëhet e përdorshme publikisht nga Autoriteti.
3. Autoriteti përditëson listën e certifikatave të çelësave të certifikimit dhe bën të mundur publikimin e tyre.
4. Kjo listë publike, nënshkruhet nga titullari i Autoritetit ose nga një punonjës tjetër i caktuar nga ai, me anë të një nënshkrimi elektronik të avancuar, i cili është krijuar në një pajisje të sigurt të krijimit të nënshkrimeve.

17. Kufizimet e përdorimit.

1. Ofruesi i shërbimit të certifikimit, me kërkesë të subjektit ose të një pale të tretë ka të drejtën e përfshirjes në certifikatën e kualifikuar kufizime të përdorimit të saj.

Rregulla për vlerësimin kohor dhe për mbrojtjen e dokumenteve elektronike

18. Vlerësimi kohor

1. Një provë elektronike i nënshtrohet vlerësimit kohor me gjenerimin e një vulë kohore që vendoset mbi të.
2. Vulat kohore krijohen me anë të një sistemi të posaçëm që është në gjendje të:
 - a. Mbajë datën dhe orën siç parashikohet në standardet ndërkombëtare.
 - b. Krijojë strukturën e të dhënave, siç specifikohet në dy pikat vijuese të këtij dokumenti dhe e nënshkruan në mënyrë elektronike atë.

19. Informacione të përmbajtura në vulën kohore.

1. Një vulë kohore duhet të paktën të përmbajë informacionet e mëposhtme:
 - b. Emrin e lëshuesit (kompanisë, në rastin tonë mund të jetë vetë OSHC)
 - c. Numrin e serisë të vulës kohore.
 - d. Algoritmin e nënshkrimit të vulës kohore.
 - e. Identifikuesin e certifikatës që përmban çelësin e verifikimit të vulës.
 - f. Datën dhe orën e gjenerimit të vulës.
 - g. Identifikuesin e algoritmit HASH të përdorur për të krijuar gjurmën elektronike të dokumentit që i nënshtrohet vlerësimit kohor.
 - h. Vlerën e gjurmës së dokumentit elektronik.
2. Ndër të tjera, vula kohore mund të përmbajë edhe një identifikues të objektit, të cilit i përket gjurma.

20. Precizoni i sistemeve të vlerësimit kohor.

1. Ora e vendosur në një vulë kohore duhet të korrespondojë, me një diferencë prej jo më shumë se një minutë me orën e saktë të sistemit UTC (në momentin e gjenerimit).
2. Data dhe ora e përmbajtur në një vulë kohore janë të specifikuara me referime të Coordinated Universal Time UTC (Koha universale e koordinuar).

Shënim: UTC është sistem kohor i bazuar në sekonda siç është përcaktuar në rekomandimin ITU-R TF .460-5. UTC është ekuivalentja e kohës diellore mesatare në meridianin fillestar (0°). Me specifikisht UTC është një kompromis midis kohës atomike të qëndrueshme (Temps Atomique International – TAI) dhe kohës diellore të derivuar

nga lëvizja e çrregullt e tokës (Greenwich Mean Sidereal Time – GMST). Një sistem më i avancuar mund të jetë UTC(k) një sistem kohor i llogaritur në laborator me marrëveshje të ngushtë me UTC me qëllim arritjen e ± 100 ms.(Rekomandimi ITU-T TF.536-1. Një listë e laboratorëve UTC(k) mund të gjenden në <http://www.bimp.org/>.

Specifikimet e plota të mënyrës së operimit të një TSA (time-spampling authority mund të gjenden në dokumentin ETSI TS 102 023).

21. Çelësat e vulave kohore

1. Çdo kopje çelësash të përdorura për vlerësimin kohor duhet të jetë në mënyre unike e lidhur me një sistem vlerësimi kohor.
2. Për qëllime kufizimi të numrit të vulave kohore të lidhura me të njëjtën kopje çelësash, çelësat e vulosjes kohore duhet të zëvendësohen dhe një certifikatë e re duhet të lëshohet jo më rrallë se një herë në muaj, pavarësisht kohës kur skadon certifikata e vjetër dhe pa revokuar këtë të fundit.
3. Për nënshkrimin e certifikatave të vulosjes kohore duhen përdorur çelësa posaçërisht të krijuar, d.m.th. jo të njëjtat çelësa që përdoren për nënshkrimin e një lloji tjetër certifikate.
4. Çelësat e certifikimit të vulosjes kohore mund të krijohen ekskluzivisht vetëm nga personat përgjegjës të shërbimeve përkatëse.

22. Mirëmbajtja e certifikatave dhe çelësave të vulosjes kohore.

1. Për çelësat e certifikimit të përdorura për nënshkrimin e certifikatave të vulosjes kohore aplikohen të njëjtat rregulla, siç parashikohet për ato që nënshkruajnë certifikata të çelësave të nënshkrimit.
2. Certifikatat përkatëse të çelësave të vulosjes kohore, përveçse të jenë në pajtim me standardin ISO/IEC 9594-8:2001 dhe ndryshime të mëvonshme, duhet të përmbajnë identifikuesin e sistemit të vulosjes kohore që përdor këto çelësa.

23. Siguria e sistemeve të vlefshmërisë kohore.

1. Çdo sistem i vlefshmërisë kohore duhet të krijojë një regjistër operativ jo të rishkrueshëm në të cilin janë automatikisht të regjistruara të gjitha ngjarjet. Çdo anomali ose tentative për të ndërhyrë, që mund të modifikojë funksionimin e saktë të aparatit duke e bërë jo kompatibël me kriteret bazë të operimit, duhet të shënohet në regjistër dhe të shkaktojë bllokimin e sistemit.
2. Zhblokimi i sistemit të vlefshmërisë kohore mund të kryhet ekskluzivisht me ndërhyrjen e personave posaçërisht të autorizuar.

3. Pajtueshmëria me kërkesat e sigurisë të specifikuara në këtë dokument, duhet të verifikohet përmes kriterëve të sigurisë ekuivalente me të paktën ato të përcaktuara nga niveli i vlerësimit E2 dhe fortësia e mekanizmave HIGH të ITSEC , ose nga niveli EAL 3+ të standardit ISO/IEC 15408. Janë të pranueshme nivele të tjera botërisht të njohura që janë ekuivalente me këto të dyja.

24. Regjistrimi i vulave të gjeneruara.

1. Të gjithë vulat e lëshuara nga një sistem vlefshmërie, ruhen në një arkiv digjital të pa modifikueshëm për një periudhë kohore jo më të vogël se 5 vjet.
2. Vula kohore është e vlefshme për të gjithë periudhën e kohës gjatë se cilës vula ruhet në regjistër nga ofruesi i shërbimit.

25. Kërkesa për vlefshmërinë kohore.

1. Ofruesi i shërbimit vendos, duke publikuar në manualin operativ, procedurat e kërkesës për vlefshmërinë kohore.
2. Kërkesa duhet të përmbajë provën elektronike (dokumentin) së cilës vulat kohore duhet t'i referohet.
3. Kjo provë elektronike mund të zëvendësohet nga një ose më shumë gjurmë elektronike, të llogaritura me funksione HASH të parashikuara nga ofruesi i shërbimit në manualin e tij operativ. Megjithatë duhet të pranohen funksione hash të bazuara në algoritmet “dedicated hash-function 3”, që korrespondojnë me funksionin SHA-1 dhe “dedicated hash-function 1”, që korrespondojnë me RIPEMD-160, të përcaktuara në ISO/IEC 10118-3.
4. Ofruesi i shërbimit ka zgjedhjen e implementimit të një sistemi vlefshmërisë kohore në mënyrë që të jetë e mundur lëshimi i më shumë se një vulë kohore për të njëjtën provë elektronike. Në këtë rast, këto vula duhet të krijohen me çelësa të ndryshëm.
5. Gjenerimi i vulave kohore duhet të garantojë një kohë përgjigjeje, e matur si diferenca e kohës së marrjes së kërkesës dhe koha e raportuar në vulën kohore, që nuk duhet të jetë më e madhe se një minutë.

26. Zgjatja e vlefshmërisë të një dokumenti elektronik.

1. Vlefshmëria i një dokumenti elektronik, efektet e të cilit shtrihen përtej limitit të vlefshmërisë të çelësit të nënshkrimit, mund të shtyhet duke e bashkëlidhur me një vulë kohore.

Mbi algoritmet

27. Algoritmet e gjenerimit dhe verifikimit të nënshkrimit.

1. Deri në publikimin e specifikimeve më të reja nga Komisioni Evropian, ofruesit e shërbimit të regjistruar në Shqipëri duhet të përdorin algoritmin RSA (Rivest-Shamir-Adelman) me një gjatësi çelësash jo më të vogël se 1024 bit, e këshillueshme është 2048 bit.
2. Deri në pritje që Komisioni Evropian sipas procedurës së art. 9 të direktivës 1999/93/CE, të publikojë nivelet e reja të vlerësimit për certifikimin e sigurisë së pajisjeve të sigurta të krijimit të nënshkrimit, vlerësimi bëhet me kritere jo më të ulëta se ato të parashikuara nga niveli i vlerësimit E2 dhe fortësia HIGH të ITSEC, ose nga niveli EAL3 e standardit ISO/IEC 15408, ose me të larta. Janë të pranueshme nivele vlerësimi të njohura botërisht si të barasvlershme.
3. Autoriteti ruan të drejtën e ndryshimit të niveleve të vlerësimit të sigurisë krahas evoluimit të teknologjisë dhe të direktivave evropiane që publikohen në të ardhmen.

Profili i certifikatave të kualifikuara

28. Norma të përgjithshme

Profili i certifikatave, nëse nuk është përcaktuar tjetërsoj, duhet të jetë në pajtim të specifikimit RFC 3280, kapitulli 4 “Profili i certifikatave dhe listave të revokimit të ofruesve të certifikatave në infrastrukturën me çelësa publike”, dhe nëse nuk cilësohet ndryshe në përputhje me ETSI TS 101 862 “Profili i certifikatave të kualifikuara”

29. Profili i certifikatave të kualifikuara.

Shënim: OID – Object Identifier – kod numerik standard për identifikimin unik të provave elektronike të përdorura në ri-prezantimin e strukturave të të dhënave në kuadrin e standardeve ndërkombëtare, që kanë të bëjnë me ndërlidhjen e sistemeve të hapura.

1. Nëse nuk përcaktohet ndryshe nga normativa e Autoritetit, certifikatave të kualifikuara i aplikohen specifikime e ETSI 102 280, “Profili i certifikatave X.509 V.3, për certifikata lëshuar personave fizikë”.
2. Fusha **Issuer** (lëshuesi i certifikatës) duhet të përmbajë të paktën atributet e mëposhtme:
 - a. **organizationName** (OID: 2.5.4.10), që përmban emërtimin e organizatës e cila lëshon certifikatën e kualifikuar;
 - b. **countryName** (OID: 2.5.4.6), e cila përmban kodin e shtetit, – country code – siç përcaktohet në ISO 3166, në të cilin organizata e **organizationName** është e regjistruar.
3. Fusha **SubjectDN** (të dhëna identifikuese të subjektit) e certifikatës përmban këto të dhëna:
 - a. **givenName** dhe **surname** (OID: 2.5.4.42 dhe 2.5.4.4) të cilat përmbajnë respektivisht emrin dhe mbiemrin e subjektit zotërues të certifikatës;
 - b. **countryName** (OID: 2.5.4.6) e cila, në rastin që **organizationName** përmban vlerën “jo e pranishme”, përmban kodin, sipas ISO 3166, të shtetit të rezidencës të subjektit. Në rastin që **organizationName** përmban një vlerë të ndryshme nga “jo e pranishme”, përmban kodin e shtetit, sipas ISO 3166, i cili i ka caktuar organizatën kodin identifikues të gjendur në fushën **organizationName**.
 - c. **organizationName** (OID: 2.5.4.10) përmban, nëse është e aplikueshme, statusin social ose emërtimin dhe kodin identifikues të organizatës që ka kërkuar ose ka autorizuar lëshimin e certifikatës për subjektin, kodin identifikues është një kod i cili lëshohet nga autoriteti shtetëror përcaktuar nga

shteti në fushën **countryName**. Nëse kjo fushë nuk është e aplikueshme ath merr vlerën “jo e pranishme”;

- d. **serialNumber** (OID: 2.5.4.5) që përmban numrin e identifikimit personal të subjektit ose numrin e regjistrimit NIPT në rastin e një kompanie. Çdokush nga këto numra paraprihet nga kodi i shtetit sipas ISO 3166 dhe nga karakteri “:”(në heksadecimal “0x3A”);
 - e. në alternativë të attributeve të pikës a), certifikata mund të përmbajë atributin **pseudonym** (OID: 2.5.4.65), që mund të përmbajë çfarëdo “string” unik të zgjedhur nga subjekti. Ky “string” nuk lejon nxjerrjen e të dhënave identifikuese të subjektit. Nëse atributi **pseudonym** është i pranishëm, atributi **countryName** merr vlerën “IT”, atributi **organizationName** merr vlerën “jo e pranishme”, atributi **serialNumber** merr vlerën “pseudonym” dhe atributet e tjera **title** dhe **localityName** nuk janë të pranishëm;
 - f. **dnQualifier** (OID: 2.5.4.46) përmban kodin identifikues të subjektit prapë ofruesit të shërbimit. Ky i ashtuquajtur kod vihet nga ofruesi i shërbimit dhe është unik.
4. Fusha **subjectDN** (të dhëna identifikuese të subjektit) e certifikatës mund të përmbajë attribute të tjera për aq kohë sa nuk është në konflikt mesa përcaktohet në dokumentin ETSI TS 102 280. Kodifikimi i mundshëm i attributeve **title**, **localityName**, **commonName** dhe **organizationalUnitName** duhet të respektojë rregullat e mëposhtme:
- a. **title** (OID: 2.5.4.12), përmban një indikacion të kualifikimit specifik të subjektit, për sa i përket përkatësisë së tij në ndonjë urdhër apo ndonjë lidhje profesionale, mund të përmbajë përmbajtjen e fuqive të tjera profesionale, ose fuqinë për të përfaqësuar një organizatë të specifikuar në **organizationName** ose një titull shkencor a profesional . Në rastin kur fusha **organizationName** përmban një vlerë të ndryshme nga “jo e pranishme”, vendosja e informacioneve në **title** kërkohet nga organizata vetë. Në rastin e kundërt përmban informacione të marra nga vetë-certifikimi i subjektit me ndonjë titull të mundshëm.
 - b. **localityName** (OID: 2.5.4.7), përmban, në rastin që **organizationName** ka një vlerë të ndryshme nga “jo e pranishme”, informacione përkatëse të organizatës së specifikuar.
 - c. **commonName** (OID: 2.5.4.3), në shtesë të **givenName** dhe **surname** mund të përmbajë një emër tjetër të mundshëm me të cilin subjekti njihet zakonisht.
 - d. **organizationalUnitName** (OID: 2.5.4.11), përmban informacione të mëtejshme përkatëse të kompanisë. Ky atribut mund të shfaqet maksimalisht 5 herë.
5. Certifikata përmban shtesat e mëposhtme (extensions):
- a. **keyUsage** (OID: 2.5.29.15) e cila përmban ekskluzivisht vlerën **nonRepudiation** (bit 1 i vënë 1). Kjo shtesë është e shënuar kritike;

- b. **certifikatePolicies** (OID: 2.5.29.32) e cila përmban OID'në e Certificate Policy (CP) dhe Uniform Resource Locator (URL) e cila drejton të Certificate Practice Statement (CPS) në kuadrin e të cilës ofruesi i shërbimit ka lëshuar certifikatën. Nëse një CP nuk adoptohet nga ato të përcaktuara në nivel evropian dhe ndërkombëtar ofruesi i shërbimit përcakton një CP të tijën dhe kjo OID përcaktohet dhe publikohet nga ky i fundit. Mund të ketë të dhëna për më shumë se një CP. URL'ja konfiguron një rrugëkalim absolut për hyrjen e CRL (listën e revokimeve të certifikatave). Kjo shtesë nuk shënohet kritike;
- c. **CRLDistributionPoints** (OID: 2.5.29.31), e cila përmban URL'në që drejton tek CRL/CLS'të (lista e revokimeve ose lista e pezullimeve) të publikuara nga ofruesi i shërbimit ku eventualisht janë të shfaqura informacionet në lidhje me revokimet dhe pezullimet e certifikatave në fjale. URL'ja përshkon një rrugëkalim absolute për hyrjen e CRL'së. Skema për t'u përdorur për URL'në është HTTP ose LDAP dhe lejon shkarkimin anonim të CRL'së. Në rastin që vihen vlera për më shumë se një URL për shtesë, të tilla URL përshkojnë rrugëkalime koherente me CRL-në/CLS-në e fundit të publikuar. Kjo shtesë nuk shënohet kritike
- d. **authorityKeyIdentifier** (OID: 2.5.29.35); që përmban të paktën atributin **keyIdentifier**. Shtesa nuk shënohet kritike;
- e. **subjectKeyIdentifier** (OID: 2.5.29.14); që përmban të paktën atributin **keyIdentifier**. Shtesa nuk shënohet kritike.
- f. **QcStatements**, të përcaktuara në dokumentin ETSI TS 101 862 siç vijon:
 - **id-etsi-qcs-QcCompliance** (OID:0.4.0.1862.1.1);
 - **id-etsi-qcs-qcLimitValue** (OID: 0.4.0.1862.1.2);
 - **id-etsi-qcs-QcRetentionPeriod** (OID: 0.4.0.1862.1.3), vlera e shënuar këtu është e barabartë ose më e madhe se "10";
 - **id-etsi-qcs-QcSSCD** (OID: 0.4.0.1862.1.4);

Kjo shtesë nuk shënohet kritike.

6. Certifikata e nënshkrimit mund të përmbajë shtesat e mëposhtme:

- a. **SubjectDirectoryAttributes** (OID: 2.5.29.9) Kjo nuk përmban asnjë nga fushat e cituara në pikat 3 dhe 4 me lart. Atributi **dateOfBirth** (OID: 1.3.6.1.5.5.7.9.1), nëse i pranishëm kodifikohet në formatin **GeneralizedTime**. Kjo shtesë nuk është e shënuar kritike;
- b. **authorityInfoAccess** (OID: 1.3.6.1.5.5.7.1.1)

Nëse ofruesi i shërbimit vë në dispozicion një sistem OCSP për verifikimin e vlefshmërisë së certifikatës, shtesa **authorityInfoAccess** përmban një fushë **accessDescription** me përshkrimet e modalitetit të hyrjes në shërbimin OCSP, dhe përmban atributet e mëposhtme:

- **accessMethod**, që përmban identifikuesin **id-ad-ocsp** (OID: 1.3.6.1.5.5.7.48.1);
- **accessLocation**, që përmban URL'në e cila drejton OCSP Responder-it të ofruesit të shërbimit, e cila shërben për të kryer verifikimin e të njëjtës

certifikatë. URL konfiguron një rrugëkalim absolut për hyrjen e OCSP Responder-it. Në rastin kur specifikohen më shumë fusha përshkrimi të aksesit, këto të dhëna konfigurojnë rrugëkalime alternative për verifikimin e certifikatës nëpërmjet OCSP.

Kjo shtesë nuk është e shënuar kritike.

- c. Limitet e mundshme të mëtejshme të përdorimit vihen në atributin **explicitText** të fushës **userNotice** të shtesës **certificatePolicies**;

Shtesa të mëtejshme mund të aplikohen në certifikatë, për aq kohe sa janë komform me standardet e përmendura në këtë dokument, dhe nuk shënohen kritike.

Kapitulli 10

Profili i certifikatave të certifikimit dhe certifikatave të vulosjes kohore

30. Profili i certifikatave të certifikimit dhe atyre të vulosjes kohore.

Nëse nuk parashikohet tjetërsoj, profili i këtyre certifikatave është në pajtim të specifikimit RFC 3280.

31. Përdorimi i shtesave në certifikatat e certifikimit.

Certifikatat e certifikimit përmbajnë shtesat e mëposhtme (extensions);

- a. **keyUsage** (OID: 2.5.29.15), përmban vlerat **keyCertSign** dhe **cRLSign** (bit 5 dhe bit 6 të caktuara në 1), kjo shtesë është e shënuar kritike;
- b. **basicConstraints** (OID: 2.5.29.19), përmban vlerën **CA=true**. Shtesa është e shënuar kritike.
- c. **certificatePolicies** (OID: 2.5.29.32), përmban një ose me shumë identifikues të **policyIdentifier** dhe URL-të e CPS relative. Mund të përmbajë OID-në e parashikuar nga RFC 3280 (2.5.29.32.0). Shtesa nuk shënohet kritike.
- d. **CRLDistributionPoints** (OID 2.5.29.31), përmban një ose me shumë URL për akses të CRL/ CLS-ve (listave të revokimit dhe të Pezullimit). URL-ja përcakton rrugëkalimin për aksesimin e këtyre listave. Shtesa nuk shënohet kritike.
- e. **subjectKeyIdentifier** (OID 2.5.29.14) përmban vleren **keyIdentifier**. Shtesa nuk shënohet kritike.

Shtesa të mëtejshme mund të aplikohen në certifikatë, për aq kohë sa janë në pajtim me standardet e përmendura në këtë dokument, dhe nuk shënohen kritike.

Kapitulli 11

Përdorimi i shtesave në certifikatat e vulosjes kohore

32. Profili i certifikatave të vulosjes kohore

Certifikatat e vulosjes kohore përmbajnë shtesat e mëposhtme:

- a. **keyUsage** (OID: 2.5.29.15), përmban vlerën **digitalSignature** (bit 0 i vendosur në 1). Shtesa shënohet kritike.
- b. **extendedKeyUsage** (OID: 2.5.29.37), përmban vlerën **keyPurposeId = timeStamping**. Shtesa shënohet kritike.
- c. **certificatePolicies** (OID: 2.5.29.32), përmban një ose më shumë identifikues të **policyIdentifier** dhe URL-të relative të CPS. Shtesa nuk është e shënuar kritike.
- d. **authorityKeyIdentifier** (OID: 2.5.29.35), përmban të paktën një **keyIdentifier**. Shtesa nuk shënohet kritike.
- e. **subjectKeyIdentifier** (OID: 2.5.29.14), përmban të paktën një **keyIdentifier**. Shtesa nuk shënohet kritike.

Shtesa të mëtejshme mund të aplikohen në certifikatë, për aq kohë sa janë në pajtim me standardet e përmendura në këtë dokument, dhe nuk shënohen kritike.

Kapitulli 12

Rregulla për shërbimet e vlefshmërisë kohore

33. Aksesit në shërbimit e vlefshmërisë kohore të mundësuar nga ofruesi i shërbimit bëhet nëpërmjet protokollit dhe formateve të përcaktuara nga specifikimi ETSI TS 101 861 “Profili i vlerësimit kohor” dhe specifikimi RFC 3161 dhe modifikime të mëtejshme. Vulat kohore, që i dërgohen si përgjigje kërkuarit të vlerësimit kohor ndjekin të njëjtat standarde.
34. Ofruesit e shërbimit mundësojnë ose tregojnë një sistem që lejon hapjen, analizën dhe vizualizimin e vulave kohore. Ky sistem menaxhon me korrektësi strukturat **TimeStampToken** dhe **TimeStampRep** të paktën në formatin “detached”, me verifikimin korrekt të nënshkrimit të sistemit të vlerësimit kohor dhe së të ashtuquajturës asociim, të kryer nëpërmjet funksionit HASH, me dokumentin për të cilin është krijuar vetë vula kohore.
35. Shtesa (ekstensioni) asociuar strukturës **TimeStampToken** dhe **TimeStampRep** nuk duhet të influencojë në funksionimin e sistemit të mësipërm të pikës 2.
36. **TimeStampToken**-at duhet të përfshijnë një identifikues unik të policave të sigurisë në bazë të të cilit janë gjeneruar. Ky identifikues nëse nuk është përcaktuar në nivel evropian ose kombëtar, vendoset vetë nga ofruesi i shërbimit dhe bëhet publik nga po ai.

Kapitulli 13

Informacione mbi revokimin dhe pezullimin e certifikatave

37. Verifikimi i certifikatave – lista e revokimit të certifikatave (CRL)

Informacioni mbi revokimin dhe pezullimin e certifikatave që publikohen nga ofruesi i shërbimit në mënyrë publike nëpërmjet listave të revokimit dhe listave të pezullimit, duhet të jenë të formatit të përcaktuar në specifikimin RFC 3280, kapitulli 5, përveç paragrafëve 5.2.4 dhe 5.2.6.

Listat e certifikatave të revokuara dhe atyre të pezulluara mundësohen për përdorim publik nëpërmjet protokollit HTTP ose LDAP.

38. Verifikimi në kohe reale i certifikatave – OCSP

Në vazhdim të sa u tha në pikën e më lart mbi verifikimin e certifikatave, ofruesi i shërbimit ka opsionin e mundësimin të informacionit edhe nëpërmjet shërbimeve OCSP. Në një rast të tillë këto shërbime duhet të jenë në pajtim me specifikimin RFC 2560 dhe modifikime të mëtejshme.

Kapitulli 14

Formatet dhe aplikimet e nënshkrimit

39. Zarfi kriptografik i nënshkrimit

1. Zarfi kriptografik që ka për qëllim të përmbajë brenda dokumentin e nënshkruar duhet të jetë konform specifikimit RFC 2315 (PKCS7)
2. Zarfi kriptografik i mësipërm është i tipit **signedData** (OID: 1.2.840.113549.1.7.2)
3. Për kodimin e zarfit kriptografik mund të përdoren formatet ASN.1-DER (ISO 8824, 8825) ose BASE64 (RFC 1421).
4. Pasi krijohet zarfi kriptografik ai "file" merr ekstensionin "p7m".
5. Një zarf kriptografik mund të përmbajë një ose më shumë nënshkrime elektronike. Këto të fundit mund të jenë:
 - a. "nënshkrime paralele", në këtë rast nënshkruesi nënshkruan të dhënat e përmbajtura në vetë zarf. (OID: 1.2.840.113549.1.7.1)
 - b. "kundër-nënshkrime", në këtë rast nënshkruesi nënshkruan një nënshkrim tjetër që është vendosur nga një subjekt tjetër. (OID: 1.2.840.113549.1.9.6)
6. Formatet e nënshkrimeve të shumëfishta përcaktohet në specifikimin RFC 2315

40. Kërkesa të shërbimeve të verifikimit

Programet për verifikimin e nënshkrimit të shpërndara nga ofruesi i shërbimit ose të këshilluara nga ai, duhet të veprojnë në mënyrë korrekte me formatin e certifikatave të kualifikuara dhe të njohin këto elemente:

- a. atributin **DateOfBirth** të shtesës **SubjectDirectoryAttributes**;
- b. **qcStatements**-at e mëposhtme:
 1. **id-etsi-qcs-QcCompliance** (OID: 0.4.0.1862.1.1)
 2. **id-etsi-qcs-QcLimitValue** (OID: 0.4.0.1862.1.2)
 3. **id-etsi-QcRetentionPeriod** (OID: 0.4.0.1862.1.3)
 4. **id-etsi-QcSSCD** (OID: 0.4.0.1862.1.4)