2025/1943

30.9.2025

REGOLAMENT TA' IMPLIMENTAZZJONI TAL-KUMMISSJONI (UE) 2025/1943

tad-29 ta' Settembru 2025

li jistabbilixxi regoli għall-applikazzjoni tar-Regolament (UE) Nru 910/2014 tal-Parlament Ewropew u tal-Kunsill fir-rigward ta' standards ta' referenza għal ċertifikati kwalifikati għall-firem elettroniċi u ċertifikati kwalifikati għas-siġilli elettroniċi

IL-KUMMISSJONI EWROPEA,

Wara li kkunsidrat it-Trattat dwar il-Funzjonament tal-Unjoni Ewropea,

Wara li kkunsidrat ir-Regolament (UE) Nru 910/2014 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Lulju 2014 dwar l-identifikazzjoni elettronika u s-servizzi fiduċjarji għal tranżazzjonijiet elettroniċi fis-suq intern u li jħassar id-Direttiva 1999/93/KE ([1]), u b'mod partikolari l-Artikoli 28(6) u 38(6) tiegħu,

Billi:

(1) Iċ-ċertifikati kwalifikati għall-firem elettroniċi u ċ-ċertifikati kwalifikati għas-siġilli elettroniċi jaqdu rwol kruċjali fl-ambjent diġitali tan-negozju għax jippromwovu t-tranżizzjoni minn proċessi tradizzjonali bbażati fuq il-karta lejn proċessi elettroniċi ekwivalenti. Iċ-ċertifikati kwalifikati jsaħħu ċ-ċertezza fir-rigward tal-identità tal-firmatarju u tal-kreatur tas-siġill billi jorbtu d-data tal-validazzjoni ta' firma elettronika jew id-data tal-validazzjoni ta' siġill elettroniku ma' persuna fiżika jew ġuridika rispettivament u billi jikkonfermaw l-isem ta' dik il-persuna.

(2) Il-preżunzjoni tal-konformità stabbilita fl-Artikolu 28(6) u fl-Artikolu 38(6) tar-Regolament (UE) Nru 910/2014 jenħtieġ li tapplika biss meta s-servizzi fiduċjarji kwalifikati għall-ħruġ ta' ċertifikati kwalifikati għall-firem elettroniċi, u s-servizzi fiduċjarji kwalifikati għall-ħruġ ta' ċertifikati kwalifikati għas-siġilli elettroniċi, ikunu konformi mal-istandards stabbiliti f'dan ir-Regolament. Dawn l-istandards jenħtieġ li jkunu jirriflettu prattiki stabbiliti u jiġu rikonoxxuti b'mod wiesa' fis-setturi rilevanti. Jenħtieġ li dawn jiġu adattati biex ikollhom kontrolli addizzjonali li jiżguraw is-sigurtà u l-affidabbiltà tas-servizzi fiduċjarji kwalifikati u tal-kontenut taċ-ċertifikati kwalifikati.

(3) Jekk fornitur tas-servizzi fiduċjarju josserva r-rekwiżiti stabbiliti fl-Anness ta' dan ir-Regolament, il-korpi superviżorji jenħtieġ li jassumu l-konformità mar-rekwiżiti rilevanti tar-Regolament (UE) Nru 910/2014 u jqisu kif xieraq dik il-preżunzjoni waqt l-għoti jew il-konferma tal-istatus kwalifikat tas-servizz fiduċjarju. Iżda fornitur kwalifikat tas-servizzi fiduċjarji xorta jista' jistrieħ fuq prattiki oħra biex juri l-konformità mar-rekwiżiti tar-Regolament (UE) Nru 910/2014.

(4) Il-Kummissjoni tivvaluta regolarment teknoloġiji, prattiki, standards jew speċifikazzjonijiet tekniċi ġodda. F'konformità mal-Premessa 75 tar-Regolament (UE) 2024/1183 tal-Parlament Ewropew u tal-Kunsill ([2]), il-Kummissjoni jenħtieġ li tirrieżamina u taġġorna dan ir-Regolament, jekk ikun meħtieġ, biex iżżommu konformi mal-iżviluppi globali, teknoloġiji, standards jew speċifikazzjonijiet tekniċi ġodda, u biex issegwi l-aqwa prattiki fis-suq intern.

(5) Ir-Regolament (UE) 2016/679 tal-Parlament Ewropew u tal-Kunsill ([3]) u, meta rilevanti, id-Direttiva 2002/58/KE tal-Parlament Ewropew u tal-Kunsill ([4]) japplikaw għall-attivitajiet tal-ipproċessar tad-data personali skont dan ir-Regolament.

([1]) ĠU L 257, 28.8.2014, p. 73, ELI: https://data.europa.eu/eli/reg/2014/910/oj.

([2]) Ir-Regolament (UE) 2024/1183 tal-Parlament Ewropew u tal-Kunsill tal-11 ta' April 2024 li jemenda r-Regolament (UE) Nru 910/2014 fir-rigward tal-istabbiliment tal-Qafas Ewropew għall-Identità Diġitali (ĠU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Ir-Regolament (EU) 2016/679 tal-Parlament Ewropew u tal-Kunsill tas-27 ta' April 2016 dwar il-protezzjoni tal-persuni fiżiċi fir-rigward tal-ipproċessar ta' data personali u dwar il-moviment liberu ta' tali data, u li jħassar id-Direttiva 95/46/KE (Regolament Ġenerali dwar il-Protezzjoni tad-Data) (ĠU L 119, 4.5.2016, p. 1, ELI: https://data.europa.eu/eli/reg/2016/679/oj).

([4]) Id-Direttiva 2002/58/KE tal-Parlament Ewropew u tal-Kunsill tat-12 ta' Lulju 2002 dwar l-ipproċessar tad-data personali u l-protezzjoni tal-privatezza fis-settur tal-komunikazzjoni elettronika (Direttiva dwar il-privatezza u l-komunikazzjoni elettronika) (ĠU L 201, 31.7.2002, p. 37, ELI: https://data.europa.eu/eli/dir/2002/58/oj).

(6) Il-Kontrollur Ewropew għall-Protezzjoni tad-Data ġie kkonsultat f'konformità mal-Artikolu 42(1) tar-Regolament (UE) 2018/1725 tal-Parlament Ewropew u tal-Kunsill ([5]) u ta l-opinjoni tiegħu fis-6 ta' Ġunju 2025.

(7) Il-miżuri previsti f'dan ir-Regolament huma f'konformità mal-opinjoni tal-kumitat stabbilit bl-Artikolu 48 tar-Regolament (UE) Nru 910/2014,

ADOTTAT DAN IR-REGOLAMENT:

Artikolu 1

Standards ta' referenza u speċifikazzjonijiet għal ċertifikati kwalifikati għall-firem elettroniċi u għas-siġilli elettroniċi

1. L-istandards ta' referenza u l-ispeċifikazzjonijiet imsemmija fl-Artikolu 28(6) tar-Regolament (UE) Nru 910/2014 huma stabbiliti fl-Anness I ta' dan ir-Regolament.

2. L-istandards ta' referenza u l-ispeċifikazzjonijiet imsemmija fl-Artikolu 38(6) tar-Regolament (UE) Nru 910/2014 huma stabbiliti fl-Anness II ta' dan ir-Regolament.

Artikolu 2

Dħul fis-seħħ

Dan ir-Regolament għandu jidħol fis-seħħ fl-għoxrin jum wara dak tal-pubblikazzjoni tiegħu f'*Il-Ġurnal Uffiċjali tal-Unjoni Ewropea*.

Dan ir-Regolament għandu jorbot fl-intier tiegħu u japplika direttament fl-Istati Membri kollha.

Magħmul fi Brussell, id-29 ta' Settembru 2025.

Għall-Kummissjoni
Il-President
Ursula VON DER LEYEN

([5]) Ir-Regolament (UE) 2018/1725 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Ottubru 2018 dwar il-protezzjoni ta' persuni fiżiċi fir-rigward tal-ipproċessar ta' data personali mill-istituzzjonijiet, korpi, uffiċċji u aġenziji tal-Unjoni u dwar il-moviment liberu ta' tali data, u li jħassar ir-Regolament (KE) Nru 45/2001 u d-Deċiżjoni Nru 1247/2002/KE (ĠU L 295, 21.11.2018, p. 39, ELI: https://data.europa.eu/eli/reg/2018/1725/oj).

ANNESS I

Lista ta' standards ta' referenza u speċifikazzjonijiet għal ċertifikati kwalifikati għall-firem elettroniċi

L-istandards ETSI EN 319 411-2 V2.6.1 ("ETSI EN 319 411-2"), ETSI EN 319 412-1 V1.6.1 ("ETSI EN 319 412-1"), ETSI EN 319 412-2 V2.4.1 ("ETSI EN 319 412-2"), u ETSI EN 319 412-5 V2.5.1 ("ETSI EN 319 412-5") japplikaw bl-adattamenti li ġejjin:

1. Għal ETSI EN 319 411-2:

(1) 2.1 Referenzi normattivi

— [1] ETSI EN 319 401 V3.1.1 (2024-06) "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Rekwiżiti ta' Politika Ġenerali għall-Forniturі tas-Servizzi Fiduċjarji".

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Rekwiżiti ta' politika u tas-sigurtà għall-forniturі tas-servizzi fiduċjarji li joħorġu ċ-ċertifikati; Parti 1: Rekwiżiti ġenerali", bl-adattamenti li ġejjin:

Klawżola 2.1 Referenzi normattivi ta' ETSI EN 319 411-1 V1.5.1 għandhom jiġu emendati kif ġej:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Rekwiżiti ta' Politika Ġenerali għall-Forniturі tas-Servizzi Fiduċjarji".

— [10] ETSI EN 319 412-2 V2.4.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 2: Profil taċ-ċertifikat għal ċertifikati maħruġa lil persuni fiżiċi".

— [14] ETSI EN 319 412-1 V1.6.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 1: Ħarsa ġenerali u strutturi komuni tad-data".

— [3] ETSI EN 319 412-5 V2.5.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 5: QCStatements".

— [5] ETSI EN 319 412-1 V1.6.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 1: Ħarsa ġenerali u strutturi komuni tad-data".

— [6] CEN/TS 419261:2015 "Rekwiżiti tas-sigurtà għal sistemi affidabbli li jimmaniġġaw iċ-ċertifikati u t-timbri tal-ħin".

— [7] Il-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà, Sottogrupp dwar il-Kriptografija: "Agreed Cryptographic Mechanisms" ippubblikati mill-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà ("ENISA") ([1]).

— [8] Ir-Regolament ta' Implimentazzjoni tal-Kummissjoni (UE) 2024/482 ([2]) li jistabbilixxi r-regoli għall-applikazzjoni tar-Regolament (UE) 2019/881 tal-Parlament Ewropew u tal-Kunsill fir-rigward tal-adozzjoni tal-iskema Ewropea taċ-ċertifikazzjoni taċ-ċibersigurtà bbażata fuq il-Kriterji Komuni (EUCC).

— [9] Ir-Regolament ta' Implimentazzjoni tal-Kummissjoni (UE) 2024/3144 ([3]) li jemenda r-Regolament ta' Implimentazzjoni (UE) 2024/482 fir-rigward tal-istandards internazzjonali applikabbli u li jikkoreġi dak ir-Regolament ta' Implimentazzjoni.

— [10] ISO/IEC 15408:2022 (Partijiet 1 sa 5): "Is-sigurtà tal-informazzjoni, iċ-ċibersigurtà u l-protezzjoni tal-privatezza – Kriterji tal-evalwazzjoni għas-sigurtà tal-IT".

— [11] FIPS PUB 140-3 (2019) "Rekwiżiti tas-Sigurtà għall-Moduli Kriptografiċi".

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) ĠU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) ĠU L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(2) 5.2 Rekwiżiti tad-Dikjarazzjoni tal-Prattika taċ-Ċertifikazzjoni

— OVR-5.2-02 Is-CP(s) identifikati mid-dokumentazzjoni tat-TSP għandhom jispeċifikaw ir-rekwiżiti tal-profili taċ-ċertifikati li jridu jintużaw.

(3) 5.3 Isem u identifikazzjoni tal-Politika taċ-Ċertifikat

— OVR-5.3-01 Jekk issir xi bidla fis-CP kif deskritt fil-klawżola 4.2.2 li taffettwa l-applikabbiltà, għandu jinbidel l-identifikatur tal-politika.

(4) 6.1 Responsabbiltajiet ta' pubblikazzjoni u repożitorju

— OVR-6.1-02 L-informazzjoni identifikata f'DIS-6.1-04 of ETSI EN 319 411-1 [2] għandha tkun disponibbli pubblikament u internazzjonalment.

(5) 6.2.2 Validazzjoni inizjali tal-identità

— REG-6.2.2-01A Il-ġbir ta' attributi u evidenza dwar l-identità tas-suġġett kif ukoll il-validazzjoni tagħhom għandhom ikunu kif speċifikat f'konformità mal-atti ta' implimentazzjoni adottati skont l-Artikolu 24(1c) tar-Regolament (UE) Nru 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] u [QCP-n-qscd] L-identità tal-persuna fiżika u, jekk applikabbli, kwalunkwe attribut speċifiku tal-persuna, għandhom jiġu vverifikati f'konformità mal-atti ta' implimentazzjoni adottati skont l-Artikolu 24(1c) tar-Regolament (UE) Nru 910/2014 [i.1].

— NOTA 1 null.

(6) 6.3.3 Ħruġ ta' ċertifikat

— GEN-6.3.3-01 Għandhom japplikaw ir-rekwiżiti GEN-6.3.3-01 sa GEN-6.3.3-10 identifikati f'ETSI EN 319 411-1 [2], il-klawżola 6.3.3.

— GEN-6.3.3-02 [KUNDIZZJONALI] Jekk jinħareġ ċertifikat lil persuna fiżika identifikata b'rabta mal-persuna ġuridika, l-attributi tas-suġġett li jidentifikaw lill-organizzazzjoni fiċ-ċertifikat għandhom jirrappreżentaw lill-persuna ġuridika jew lil subentità ta' dik il-persuna ġuridika u l-identifikatur tas-suġġett fiċ-ċertifikat għandu jkun il-persuna fiżika.

— GEN-6.3.3-03 L-identifikatur tas-CP għandu jkun [GĦAŻLA]:

(a) [QCP-n]

— kif speċifikat fil-klawżola 5.3, l-entrata (a), u/jew

— OID, allokat mit-TSP, minn parti kkonċernata rilevanti oħra jew minn standardizzazzjoni ulterjuri għal politika taċ-ċertifikat li ttejjeb ir-rekwiżiti korrispondenti tal-politika applikabbli definiti f'dan id-dokument.

(b) [QCP-n-qscd]

— kif speċifikat fil-klawżola 5.3, l-entrata (c), u/jew

— OID, allokat mit-TSP, parti kkonċernata rilevanti oħra jew standardizzazzjoni ulterjuri għal politika taċ-ċertifikat li ttejjeb ir-rekwiżiti korrispondenti tal-politika applikabbli definiti f'dan id-dokument.

(7) 6.3.5 Par Kjavi u Użu taċ-Ċerifikat

— SDP-6.3.5-02A [KUNDIZZJONALI] Jekk it-TSP jimmaniġġa l-QSCD għas-suġġett, it-TSP għandu jkun fornitur kwalifikat tas-servizzi fiduċjarji li jipprovdi servizz fiduċjarju kwalifikat għall-immaniġġar ta' apparat kwalifikat għall-holqien ta' firem elettroniċi mill-bogħod, f'konformità mar-Regolament (UE) Nru 910/2014 [i.1]

— SDP-6.3.5-11A L-obbligi tal-abbonat (ara l-klawżola 6.3.4) għandhom jinkludu, jekk l-abbonat jew is-suġġett jiġġenera l-kjavijiet tas-suġġett:

(a) obbligu li jiġġenera l-kjavijiet tas-suġġetti b'algoritmu konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà [7] u ppubblikati mill-ENISA għall-użi tal-kjavi ċċertifikata kif identifikata fis-CP;

(b) obbligu li juża tul u algoritmu tal-kjavi konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà [7] u ppubblikati mill-ENISA għall-użi tal-kjavi ċċertifikata kif identifikata fis-CP waqt il-perjodu tal-validità taċ-ċertifikat.

(8) 6.3.10 Servizzi tal-Istatus taċ-Ċertifikat

— CSS-6.3.10-08 [KUNDIZZJONALI] Jekk jiġu pprovduti CRLs, it-TSP għandu jħares l-integrità u d-disponibbiltà tal-aħħar CRL imqar għall-perjodu speċifikat fis-CPS kif mitlub f'CSS-6.3.10-12.

(9) 6.4.4 Kontrolli tal-Persunal

— OVR-6.4.4-02 Il-persunal tat-TSP bi rwoli ta' fiduċja, u jekk applikabbli s-subkuntratturi tiegħu bi rwoli fdati, għandu jkun jista' jissodisfa r-rekwiżit ta' "għarfien espert, esperjenza u kwalifiki" b'taħriġ u kredenzjali formali, jew b'esperjenza reali, jew b'taħlita tat-tnejn.

— OVR-6.4.4-03 Il-konformità ma' OVR-6.4.4-02 għandha tinkludi aġġornamenti regolari (imqar kull 12-il xahar) dwar theddid ġdid u prattiki attwali tas-sigurtà.

— OVR-6.4.4-04 Minbarra r-rwoli fdati identifikati f'ETSI EN 319 401 [1], (il-klawżola 7.2-15), għandhom jiġu appoġġati r-rwoli fdati tal-uffiċjali tar-reġistrazzjoni u tar-revoka b'responsabbiltajiet kif definiti f'TS 419261 [6]. Meta l-QTSP ikun immaniġġat direttament minn Stat Membru jew korp tas-settur pubbliku jew operat f'ismu, dawk ir-rwoli fdati addizzjonali jista' jissodisfahom rappreżentant formali wieħed jew aktar li jaġixxu għal u f'isem uffiċjali tar-reġistrazzjoni u tar-revoka li jaqdu dmirhom f'amministrazzjonijiet lokali jew reġjonali.

(10) 6.4.9 Terminazzjoni ta' CA jew RA

— OVR-6.4.9-02 Il-pjan tat-terminazzjoni tat-TSP għandu jikkonforma mar-rekwiżiti stabbiliti fl-atti ta' implimentazzjoni adottati skont l-Artikolu 24(5) tar-Regolament (UE) Nru 910/2014 [i.1].

(11) 6.5.1 Ġenerazzjoni u Installazzjoni ta' Par Kjavi

— OVR-6.5.1-01A Il-ġenerazzjoni ta' par kjavi tas-CA għandha ssir b'algoritmu konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-finijiet tal-iffirmar tas-CA.

— OVR-6.5.1-01B It-tul u l-algoritmu tal-kjavi magħżula għall-kjavi tal-iffirmar tas-CA għandhom ikunu konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-finijiet tal-iffirmar tas-CA.

— OVR-6.5.1-01C [KUNDIZZJONALI] Jekk is-CA tiġġenera l-kjavijiet tas-suġġett, il-kjavijiet tas-suġġett iġġenerati mis-CA għandhom jikkonformaw mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-finijiet iddikjarati fis-CP waqt il-perjodu tal-validità taċ-ċertifikat.

(12) 6.5.2 Protezzjoni tal-materjal tal-kjavi u kontrolli tal-inġinerija tal-modulu kriptografiku

— GEN-6.5.2-01 Għandhom japplikaw ir-rekwiżiti kollha identifikati f'ETSI EN 319 411-1 [2], il-klawżola 6.5.2, ħlief ir-rekwiżiti OVR-6.5.2-01, OVR-6.5.2-03 u OVR-6.5.2-04.

— GEN-6.5.2-02 Il-ġenerazzjoni tal-par kjavi tat-TSP, inkluż il-kjavijiet użati mis-servizzi tar-revoka u tar-reġistrazzjoni, għandha ssir f'apparat kriptografiku sigur li jkun sistema affidabbli ċċertifikata f'konformità ma':

— Il-Kriterji Komuni għall-Evalwazzjoni tas-Sigurtà tat-Teknoloġija tal-Informazzjoni, kif stabbiliti fl-ISO/IEC 15408 [10] jew il-Kriterji Komuni għall-Evalwazzjoni tas-Sigurtà tat-Teknoloġija tal-Informazzjoni, il-verżjoni CC:2002, il-Partijiet 1 sa 5, ippubblikati mill-parteċipanti tal-Arranġament dwar ir-Rikonoxximent taċ-Ċertifikati tal-Kriterji Komuni fil-qasam tas-Sigurtà tal-IT, u ċċertifikati għal EAL 4 jew ogħla; jew

— l-iskema Ewropea taċ-ċertifikazzjoni taċ-ċibersigurtà bbażata fuq Kriterji Komuni (EUCC) [8][9] u ċċertifikata għal EAL 4 jew ogħla; jew

— sal-31.12.2030, FIPS PUB 140-3 [11] il-livell 3.

Din iċ-ċertifikazzjoni għandha tkun għal mira tas-sigurtà jew profil tal-protezzjoni, jew għal dokumentazzjoni tad-disinn u tas-sigurtà tal-modulu, li tissodisfa r-rekwiżiti ta' dan id-dokument, abbażi ta' analiżi tar-riskju u b'kunsiderazzjoni ta' miżuri tas-sigurtà fiżiċi u miżuri tas-sigurtà mhux tekniċi oħrajn.

Jekk l-apparat kriptografiku sigur jibbenefika minn ċertifikazzjoni tal-EUCC [8][9], dak l-apparat għandu jiġi kkonfigurat u użat f'konformità ma' dik iċ-ċertifikazzjoni.

— GEN-6.5.2-03 Il-kjavi tal-iffirmar privata tas-CA għandha tinżamm u tintuża f'apparat kriptografiku sigur li jissodisfa r-rekwiżiti ta' GEN-6.5.2-01 u GEN-6.5.2-02.

(13) 6.5.7 Kontrolli tas-Sigurtà tan-Networks

— OVR-6.5.7-02 L-iskennjar għall-vulnerabbiltajiet mitlub minn REQ-7.8-13 ta' ETSI EN 319 401 [1] għandu jsir imqar darba kull trimestru.

— OVR-6.5.7-03 It-test tal-penetrazzjoni mitlub minn REQ-7.8-17X ta' ETSI EN 319 401 [1] għandu jsir imqar darba fis-sena.

— OVR-6.5.7-04 Il-firewalls għandhom jiġu kkonfigurati biex iwaqqfu l-protokolli u l-aċċessi kollha mhux meħtieġa għall-operazzjoni tat-TSP.

(14) 6.6.1 Profil taċ-Ċertifikat

— GEN-6.6.1-05 Iċ-ċertifikat għandu jinkludi wieħed mill-identifikaturi ta' politika identifikati f'GEN-6.3.3-03 [GĦAŻLA]. Iċ-ċertifikat jista' jinkludi OIDs oħrajn allokati mit-TSP.

2. Għal ETSI EN 319 412-2:

(1) 2.1 Referenzi normattivi

— [2] ETSI EN 319 412-5 V2.5.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 5: QCStatements".

— [9] Il-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà, Sottogrupp dwar il-Kriptografija "Agreed Cryptographic Mechanisms" ippubblikati mill-ENISA.

(2) 4.2.2 Firma

— GEN-4.2.2-2 L-algoritmu tal-firma għandu jintgħażel f'konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [9].

— NOTA null.

(3) 4.2.3.1 Emittenti ta' persuni ġuridiċi

— GEN-4.2.3.1-3 Jekk ikun magħruf li jeżisti numru tar-reġistrazzjoni xieraq, l-identità tal-emittent għandu jkun fiha organizationIdentifier b'valur ta' dak in-numru tar-reġistrazzjoni kif dikjarat fir-rekord uffiċjali korrispondenti li jistabbilixxi dak in-numru tar-reġistrazzjoni.

(4) 4.2.5 Informazzjoni dwar il-kjavi pubblika tas-suġġett

— GEN-4.2.5-2 Il-kjavi pubblika tas-suġġett għandha tintgħażel f'konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [9].

— NOTA null.

(5) 4.2.6 Numru tas-serje

— GEN-4.2.6-01 In-numru tas-serje taċ-ċertifikat (kif speċifikat fl-IETF RFC 5280 [1] il-klawżola 4.1.2.2) għandu jkun uniku għal kull ċertifikat maħruġ mit-TSP.

ANNESS II

Lista ta' standards ta' referenza u speċifikazzjonijiet għal ċertifikati kwalifikati għas-siġilli elettroniċi

L-istandards ETSI EN 319 411-2 V2.6.1 ("ETSI EN 319 411-2"), ETSI EN 319 412-1 V1.6.1 ("ETSI EN 319 412-1"), ETSI EN 319 412-3 V1.3.1 ("ETSI EN 319 412-3"), ETSI EN 319 412-2 V2.4.1 ("ETSI EN 319 412-2"), u ETSI EN 319 412-5 V2.5.1 ("ETSI EN 319 412-5") japplikaw bl-adattamenti li ġejjin:

1. Għal ETSI EN 319 411-2:

(1) 2.1 Referenzi normattivi

— [1] ETSI EN 319 401 V3.1.1 (2024-06) "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Rekwiżiti ta' Politika Ġenerali għall-Forniturі tas-Servizzi Fiduċjarji".

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Rekwiżiti ta' politika u tas-sigurtà għall-forniturі tas-servizzi fiduċjarji li joħorġu ċ-ċertifikati; Parti 1: Rekwiżiti ġenerali", bl-adattamenti li ġejjin:

Klawżola 2.1 Referenzi normattivi ta' ETSI EN 319 411-1 V1.5.1 għandhom jiġu emendati kif ġej:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Rekwiżiti ta' Politika Ġenerali għall-Forniturі tas-Servizzi Fiduċjarji".

— [10] ETSI EN 319 412-2 V2.4.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 2: Profil taċ-ċertifikat għal ċertifikati maħruġa lil persuni fiżiċi".

— [14] ETSI EN 319 412-1 V1.6.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 1: Ħarsa ġenerali u strutturi komuni tad-data".

— [3] ETSI EN 319 412-5 V2.5.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 5: QCStatements".

— [5] ETSI EN 319 412-1 V1.6.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 1: Ħarsa ġenerali u strutturi komuni tad-data".

— [6] CEN/TS 419261:2015 "Rekwiżiti tas-sigurtà għal sistemi affidabbli li jimmaniġġaw iċ-ċertifikati u t-timbri tal-ħin", (prodotti mis-CEN).

— [7] Il-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà, Sottogrupp dwar il-Kriptografija: "Agreed Cryptographic Mechanisms" ippubblikati mill-ENISA.

— [8] Ir-Regolament ta' Implimentazzjoni (UE) 2024/482 li jistabbilixxi r-regoli għall-applikazzjoni tar-Regolament (UE) 2019/881 tal-Parlament Ewropew u tal-Kunsill fir-rigward tal-adozzjoni tal-iskema Ewropea taċ-ċertifikazzjoni taċ-ċibersigurtà bbażata fuq il-Kriterji Komuni (EUCC).

— [9] Ir-Regolament ta' Implimentazzjoni (UE) 2024/3144 li jemenda r-Regolament ta' Implimentazzjoni (UE) 2024/482 fir-rigward tal-istandards internazzjonali applikabbli u li jikkoreġi dak ir-Regolament ta' Implimentazzjoni.

— [10] ISO/IEC 15408:2022 (Partijiet 1 sa 5) "Informazzjoni, iċ-ċibersigurtà u l-protezzjoni tal-privatezza – Kriterji tal-evalwazzjoni għas-sigurtà tal-IT".

— [11] FIPS PUB 140-3 (2019) "Rekwiżiti tas-Sigurtà għall-Moduli Kriptografiċi".

(2) 5.2 Rekwiżiti tad-Dikjarazzjoni tal-Prattika taċ-Ċertifikazzjoni

— OVR-5.2-02 Is-CP(s) identifikati mid-dokumentazzjoni tat-TSP għandhom jispeċifikaw ir-rekwiżiti tal-profili taċ-ċertifikati li jridu jintużaw.

(3) 5.3 Isem u identifikazzjoni tal-Politika taċ-Ċertifikat

— OVR-5.3-01 Jekk issir xi bidla fis-CP kif deskritt fil-klawżola 4.2.2 li taffettwa l-applikabbiltà, għandu jinbidel l-identifikatur tal-politika.

(4) 6.1 Responsabbiltajiet ta' pubblikazzjoni u repożitorju

— OVR-6.1-02 L-informazzjoni identifikata f'DIS-6.1-04 of ETSI EN 319 411-1 [2] għandha tkun disponibbli pubblikament u internazzjonalment.

(5) 6.2.2 Validazzjoni inizjali tal-identità

— REG-6.2.2-01A Il-ġbir ta' attributi u evidenza dwar l-identità tas-suġġett kif ukoll il-validazzjoni tagħhom għandhom ikunu kif speċifikat f'konformità mal-atti ta' implimentazzjoni adottati skont l-Artikolu 24(1c) tar-Regolament (UE) Nru 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] u [QCP-l-qscd] L-identità tal-persuna ġuridika u, jekk applikabbli, kwalunkwe attribut speċifiku tal-persuna, għandhom jiġu vverifikati f'konformità mal-atti ta' implimentazzjoni adottati skont l-Artikolu 24(1c) tar-Regolament (UE) Nru 910/2014 [i.1].

— NOTA 3, Ara n-Nota 2.

(6) 6.3.3 Ħruġ ta' ċertifikat

— GEN-6.3.3-01 Għandhom japplikaw ir-rekwiżiti GEN-6.3.3-01 sa GEN-6.3.3-10 identifikati f'ETSI EN 319 411-1 [2], il-klawżola 6.3.3.

— GEN-6.3.3-02 L-identifikatur tas-CP għandu jkun [GĦAŻLA]:

(a) [QCP-l]

— kif speċifikat fil-klawżola 5.3, l-entrata (b), u/jew

— OID, allokat mit-TSP, minn parti kkonċernata rilevanti oħra jew minn standardizzazzjoni ulterjuri għal politika taċ-ċertifikat li ttejjeb ir-rekwiżiti korrispondenti tal-politika applikabbli definiti f'dan id-dokument.

(b) [QCP-l-qscd]

— kif speċifikat fil-klawżola 5.3, l-entrata (d), u/jew

— OID, allokat mit-TSP, minn parti kkonċernata rilevanti oħra jew minn standardizzazzjoni ulterjuri għal politika taċ-ċertifikat li ttejjeb ir-rekwiżiti tal-politika applikabbli definiti f'dan id-dokument.

(7) 6.3.5 Par Kjavi u Użu taċ-Ċerifikat

— SDP-6.3.5-02A [KUNDIZZJONALI] Jekk it-TSP jimmaniġġa l-QSCD għas-suġġett, it-TSP għandu jkun fornitur kwalifikat tas-servizzi fiduċjarji li jipprovdi servizz fiduċjarju kwalifikat għall-immaniġġar ta' apparat kwalifikat għall-ħolqien ta' siġilli elettroniċi mill-bogħod, f'konformità mar-Regolament (UE) Nru 910/2014 [i.1]

— SDP-6.3.5-11A L-obbligi tal-abbonat (ara l-klawżola 6.3.4) għandhom jinkludu, jekk l-abbonat jew is-suġġett jiġġenera l-kjavijiet tas-suġġett:

(a) obbligu li jiġġenera l-kjavijiet tas-suġġetti b'algoritmu konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-użi tal-kjavi ċċertifikata kif identifikata fis-CP; u

(b) obbligu li juża tul u algoritmu tal-kjavi konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-użi tal-kjavi ċċertifikata kif identifikata fis-CP waqt il-perjodu tal-validità taċ-ċertifikat.

(8) 6.3.10 Servizzi tal-Istatus taċ-Ċertifikat

— CSS-6.3.10-08 [KUNDIZZJONALI] Jekk jiġu pprovduti CRLs, it-TSP għandu jħares l-integrità u d-disponibbiltà tal-aħħar CRL imqar għall-perjodu speċifikat fis-CPS kif mitlub f'CSS-6.3.10-12.

(9) 6.4.4 Kontrolli tal-Persunal

— OVR-6.4.4-02 Il-persunal tat-TSP bi rwoli ta' fiduċja, u jekk applikabbli s-subkuntratturi tiegħu bi rwoli fdati, għandu jkun jista' jissodisfa r-rekwiżit ta' "għarfien espert, esperjenza u kwalifiki" b'taħriġ u kredenzjali formali, jew b'esperjenza reali, jew b'taħlita tat-tnejn.

— OVR-6.4.4-03 Il-konformità ma' OVR-6.4.4-02 għandha tinkludi aġġornamenti regolari (imqar kull 12-il xahar) dwar theddid ġdid u prattiki attwali tas-sigurtà.

— OVR-6.4.4-04 Minbarra r-rwoli fdati identifikati f'ETSI EN 319 401 [1], (il-klawżola 7.2-15), għandhom jiġu appoġġati r-rwoli fdati tal-uffiċjali tar-reġistrazzjoni u tar-revoka b'responsabbiltajiet kif definiti f'TS 419261 [6]. Meta l-QTSP ikun immaniġġat direttament minn Stat Membru jew korp tas-settur pubbliku jew operat f'ismu, dawk ir-rwoli fdati addizzjonali jista' jissodisfahom rappreżentant formali wieħed jew aktar li jaġixxu għal u f'isem uffiċjali tar-reġistrazzjoni u tar-revoka li jaqdu dmirhom f'amministrazzjonijiet lokali jew reġjonali.

(10) 6.4.9 Terminazzjoni ta' CA jew RA

— OVR-6.4.9-02 Il-pjan tat-terminazzjoni tat-TSP għandu jikkonforma mar-rekwiżiti stabbiliti fl-atti ta' implimentazzjoni adottati skont l-Artikolu 24(5) tar-Regolament (UE) Nru 910/2014 [i.1]].

(11) 6.5.1 Ġenerazzjoni u Installazzjoni ta' Par Kjavi

— OVR-6.5.1-01A Il-ġenerazzjoni ta' par kjavi tas-CA għandha ssir b'algoritmu konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-finijiet tal-iffirmar tas-CA.

— OVR-6.5.1-01B It-tul u l-algoritmu tal-kjavi magħżula għall-kjavi tal-iffirmar tas-CA għandhom ikunu konformi mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-finijiet tal-iffirmar tas-CA.

— OVR-6.5.1-01C [KUNDIZZJONALI] Jekk is-CA tiġġenera l-kjavijiet tas-suġġett, il-kjavijiet tas-suġġett iġġenerati mis-CA għandhom jikkonformaw mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [7] għall-finijiet iddikjarati fis-CP waqt il-perjodu tal-validità taċ-ċertifikat.

(12) 6.5.2 Protezzjoni tal-materjal tal-kjavi u kontrolli tal-inġinerija tal-modulu kriptografiku

— GEN-6.5.2-01 Għandhom japplikaw ir-rekwiżiti kollha identifikati f'ETSI EN 319 411-1 [2], il-klawżola 6.5.2, ħlief ir-rekwiżiti OVR-6.5.2-01, OVR-6.5.2-03 u OVR-6.5.2-04.

— GEN-6.5.2-02 Il-ġenerazzjoni tal-par kjavi tat-TSP, inkluż il-kjavijiet użati mis-servizzi tar-revoka u tar-reġistrazzjoni, għandha ssir f'apparat kriptografiku sigur li jkun sistema affidabbli ċċertifikata f'konformità ma':

  — Il-Kriterji Komuni għall-Evalwazzjoni tas-Sigurtà tat-Teknoloġija tal-Informazzjoni, kif stabbiliti fl-ISO/IEC 15408 [10] jew il-Kriterji Komuni għall-Evalwazzjoni tas-Sigurtà tat-Teknoloġija tal-Informazzjoni, il-verżjoni CC:2002, il-Partijiet 1 sa 5, ippubblikati mill-parteċipanti tal-Arranġament dwar ir-Rikonoxximent taċ-Ċertifikati tal-Kriterji Komuni fil-qasam tas-Sigurtà tal-IT, u ċċertifikati għal EAL 4 jew ogħla; jew

  — l-iskema Ewropea taċ-ċertifikazzjoni taċ-ċibersigurtà bbażata fuq Kriterji Komuni (EUCC) [8][9] u ċċertifikata għal EAL 4 jew ogħla; jew

  — sal-31.12.2030, FIPS PUB 140-3 [11] il-livell 3.

Din iċ-ċertifikazzjoni għandha tkun għal mira tas-sigurtà jew profil tal-protezzjoni, jew għal dokumentazzjoni tad-disinn u tas-sigurtà tal-modulu, li tissodisfa r-rekwiżiti ta' dan id-dokument, abbażi ta' analiżi tar-riskju u b'kunsiderazzjoni ta' miżuri tas-sigurtà fiżiċi u miżuri tas-sigurtà mhux tekniċi oħrajn.

Jekk l-apparat kriptografiku sigur jibbenefika minn ċertifikazzjoni tal-EUCC [8][9], dak l-apparat għandu jiġi kkonfigurat u użat f'konformità ma' dik iċ-ċertifikazzjoni.

— GEN-6.5.2-03 Il-kjavi tal-iffirmar privata tas-CA għandha tinżamm u tintuża f'apparat kriptografiku sigur li jissodisfa r-rekwiżiti ta' GEN-6.5.2-01 u GEN-6.5.2-02.

(13) 6.5.7 Kontrolli tas-Sigurtà tan-Networks

— OVR-6.5.7-02 L-iskennjar għall-vulnerabbiltajiet mitlub minn REQ-7.8-13 ta' ETSI EN 319 401 [1] għandu jsir imqar darba kull trimestru.

— OVR-6.5.7-03 It-test tal-penetrazzjoni mitlub minn REQ-7.8-17X ta' ETSI EN 319 401 [1] għandu jsir imqar darba fis-sena.

— OVR-6.5.7-04 Il-firewalls għandhom jiġu kkonfigurati biex iwaqqfu l-protokolli u l-aċċessi kollha mhux meħtieġa għall-operazzjoni tat-TSP.

(14) 6.6.1 Profil taċ-Ċertifikat

— GEN-6.6.1-05 Iċ-ċertifikat għandu jinkludi wieħed mill-identifikaturi ta' politika identifikati f'GEN-6.3.3-02 [GĦAŻLA].

2. Għal ETSI EN 319 412-3:

(1) 2.1 Referenzi normattivi

— [2] ETSI EN 319 412-2 V2.4.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 2: Profil taċ-Ċertifikat għal ċertifikati maħruġa lil persuni fiżiċi".

(2) 4.2.1 Suġġett

— LEG-4.2.1-6 L-attribut organizationIdentifier għandu jkun fih identifikazzjoni tal-organizzazzjoni suġġett inkwistjoni li tkun differenti isem l-organizzazzjoni. Jekk ikun magħruf li jeżisti numru tar-reġistrazzjoni xieraq, l-attribut tal-organizationIdentifier għandu jkun fih valur ta' dak in-numru tar-reġistrazzjoni kif dikjarat fir-rekord uffiċjali korrispondenti li jistabbilixxi dak in-numru tar-reġistrazzjoni.

3. Għal ETSI EN 319 412-2:

(1) 2.1 Referenzi normattivi

— [2] ETSI EN 319 412-5 V2.5.1 "Firem u Infrastrutturi Fiduċjarji Elettroniċi (ESI); Profili taċ-Ċertifikati; Parti 5: QCStatements".

— [9] Il-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà, Sottogrupp dwar il-Kriptografija: "Agreed Cryptographic Mechanisms" ippubblikati mill-ENISA.

(2) 2.2 Referenzi informattivi

— [i.7] null.

(3) 4.2.2 Firma

— GEN-4.2.2-2 L-algoritmu tal-firma għandu jintgħażel f'konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [9].

— NOTA null.

(4) 4.2.3.1 Emittenti ta' persuni ġuridiċi

— GEN-4.2.3.1-3 Jekk ikun magħruf li jeżisti numru tar-reġistrazzjoni xieraq, l-identità tal-emittent għandu jkun fiha organizationIdentifier b'valur ta' dak in-numru tar-reġistrazzjoni kif dikjarat fir-rekord uffiċjali korrispondenti li jistabbilixxi dak in-numru tar-reġistrazzjoni.

(5) 4.2.5 Informazzjoni dwar il-kjavi pubblika tas-suġġett

— GEN-4.2.5-2 Il-kjavi pubblika tas-suġġett għandha tintgħażel f'konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-ENISA [9].

— NOTA null.

(6) 4.2.6 Numru tas-serje

— GEN-4.2.6-01 In-numru tas-serje taċ-ċertifikat (kif speċifikat fl-IETF RFC 5280 [1] il-klawżola 4.1.2.2) għandu jkun uniku għal kull ċertifikat maħruġ mit-TSP.