

Offentlig politik for kvalificeret tidsstempling

Oktober 2019

Version 1.0

Indholdsfortegnelse

1.	Indledning.....	4
1.1	Introduktion	4
1.2	Dokumentnavn.....	4
1.3	Politik administration.....	4
1.3.1	Organisation, der administrerer dokumentet.....	4
1.3.2	Kontakt information.....	4
1.3.3	Godkendelsesprocedure for politik.....	5
1.3.4	Offentliggørelse.....	5
1.4	Intellectuelle rettigheder	5
2.	Referencer	5
3.	Definitioner og forkortelser	6
3.1	Definitioner	6
3.2	Forkortelser	7
4.	Generelt konceptbeskrivelse.....	7
4.1	Generelt om krav til tillidstjenesterudbydere, der udsteder tidsstempler.....	7
4.2	Tidsstemplingservices.....	7
4.3	Tidsstemplingsudsteder (TSA)	8

4.4 Abonnent	8
4.5 Tidsstemplingspolitik og TSA-praksis	8
5. Introduktion til tidsstemplingspolitik og Generelle krav	9
5.1 Generelt krav	9
5.2 Identifikation	9
5.3 Infrastruktur og anvendelse	9
5.3.1 Best practices tidsstemplingspolitik	9
6. Politikker og implementering	10
6.1 Risikovurdering	10
6.2 TSA-praksis	10
6.3 Vilkår og betingelser	11
6.4 Informationssikkerhedspolitik	12
6.5 TSAs forpligtelser	13
6.5.1 Generelle forpligtelser	13
6.5.2 TSAs forpligtelser i forhold til abonnenter	13
6.6 Information til modtagerparter	13
7. TSA styring og drift	13
7.1 Introduktion	13
7.2 Intern organisation	13
7.3 Personalesikkerhed	14
7.4 Styring af aktiver	16
7.4.1 Generelle krav	16
7.4.2 Håndtering af medier	16

7.5 Adgangskontrol.....	16
7.6 Kryptografiske kontroller	17
7.6.1 Generelle kontroller.....	17
7.6.2 TSU nøglegenerering.....	17
7.6.3 Beskyttelse af TSU private nøgler.....	18
7.6.4 TSU certifikat.....	18
7.6.5 Fornyelse af TSU's nøgler.....	19
7.6.6 Livscyklushåndtering af kryptografiske moduler til signering ...	19
7.6.7 Terminering af TSU's private nøgler.....	19
7.7 Tidsstempling.....	20
7.7.1 Udstedelse af tidsstempler	20
7.7.2 UTC-synkronisering af ur	21
7.8 Fysisk og miljømæssig sikkerhed.....	21
7.9 Driftssikkerhed.....	23
7.10 Netværkssikkerhed	23
7.11 Hændelseshåndtering.....	25
7.12 Indsamling af beviser	26
7.13 Business Continuity Plan.....	27
7.14 Ophør af TSA	27
7.15 Overensstemmelse	28
Bilag A.....	30

1. Indledning

1.1 Introduktion

I en række applikation er det nødvendigt at fastslå, at data eksisterende på et givet tidspunkt. Dette gælder blandt andet i forbindelse med opbevaring af elektronisk signerede data, hvor det er væsentligt at kunne dokumentere, at den elektroniske signatur blev genereret på et tidspunkt, hvor det tilhørende certifikat var gyldigt dvs. ikke udløbet eller spærret. Dette løses ved at benytte en tillidstjeneste, som udsteder kryptografiske tidsstempler, hvor en såkaldt hash-værdi af data (herunder signerede data) kædes sammen med et tidspunkt via et elektronisk segl.

Den samlede sikkerhed for tidsstempler er afhængig af underliggende forretningsførelse af tidsstemplings servicen. Denne tidsstemplingspolitik fastlægger krav til udbydere, som ønsker at udstede kvalificerede tidsstempler jf. eIDAS. Udbydere kan vælge at anvende alternative tidsstemplingspolitikker, hvis disse lever op til kravene i [eIDAS] for tillidstjenesteudbydere, der tilbyder tidsstempler.

Dette dokument er udformet til at leve op til kravene i [ETSI EN 319 421]. Afsnit 2 til afsnit 7 følger afsnitsnummerering fra [ETSI EN 319 421]. Specifikke krav relateret til kvalificerede TSA'er fra [ETSI EN 319 421] afsnit 8 er indlejret i afsnit 1 til afsnit 7 i dette dokument.

1.2 Dokumentnavn

Dette dokument med navnet ”Offentlig politik for kvalificeret tidsstempling” forkortet OPQT beskriver en offentlig politik for udstedelse af kvalificerede tidsstempler. Den seneste version af denne politik for udstedelse af tidsstempler kan findes på <https://certifikat.gov.dk>.

1.3 Politik administration

1.3.1 Organisation, der administrerer dokumentet

Denne politik er ejet og vedligeholdt af Digitaliseringsstyrelsen.

1.3.2 Kontakt information

Forespørgsler vedrørende denne politik kan rettes til:

Digitaliseringsstyrelsen

Landgreven 4

1301 København K

Telefon: 3392 5200

E-mail: digst@digst.dk

1.3.3 Godkendelsesprocedure for politik

Denne politik er godkendes af Digitaliseringsstyrelsen efter en offentlig høringsproces.

1.3.4 Offentliggørelse

Kvalificerede tillidstjenesteudbydere, der udsteder tidsstempler under denne politik, skal offentliggøre politikken på udbyderens hjemmeside sammen med EU-tillidsmærket for kvalificerede tillidstjenester på 24/7 basis uden adgangsbegrænsninger.

1.4 Intellektuelle rettigheder

Digitaliseringsstyrelsen har alle rettighederne til denne politik.

Politikken er udgivet under Creative Common licens: "Kreditering 4.0 International" (<http://creativecommons.org/licenses/by/4.0/>)

2. Referencer

[eIDAS]	EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF
[ETSI EN 301 549]	Accessibility requirements suitable for public procurement of ICT products and services in Europe
[ETSI EN 319 122]	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSI EN 319 411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 421]	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamp
[ETSI EN 319 422]	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[ETSI TS 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[FIPS PUB 140-2]	National Institute of Standards and Technology - Federal Information Processing Standard (140-2) - Security Requirements for Cryptographic Modules
[ISO/IEC 15408]	Information technology -- Security techniques -- Evaluation criteria for IT security
[ISO/IEC 19790]	Information technology -- Security techniques -- Security requirements for cryptographic modules

3. Definitioner og forkortelser

3.1 Definitioner

Certifikat ("public key certificate"): En elektronisk attest, som angiver certifikatindehaverens offentlige nøgle sammen med supplerende information, og som entydigt knytter den offentlige nøgle til identifikation af certifikatindehaveren. Et offentligt certifikat skal signeres af et certificeringscenter (CA), som derved bekræfter certifikatets gyldighed.

Tidsstempel: Data i elektronisk form, der binder andre elektroniske data til et givet tidspunkt som bevis for at disse data eksisterede på det givne tidspunkt.

Tidsstemplingsenhed ("TSU"): Se afsnit 4.2.

TSA-praksis: En specifikation af hvilke principper og procedurer, en TSA anvender ved udstedelse af certifikater til opfyldelse af tilhørende tidsstemplingspolitik. Se i øvrigt afsnit 4.5.

Tidsstemplingspolitik: Et sæt regler, der angiver krav til udstedelse og brug af tidsstempler i en eller flere specifikke sammenhænge, hvor der findes fælles sikkerhedskrav. Nærværende dokument er en tidsstemplingspolitik. Se i øvrigt afsnit 4.5.

Tidsstemplingsudsteder (TSA): Se afsnit 4.3.

3.2 Forkortelser

BCP “Business Continuity Plan”

BTSP “Best Practice Time-Stamp Policy”

CA Certificeringscenter (“Certificate Authority”)

ETSI “European Telecommunications Standards Institute”

TSA Tidsstemplingsudsteder (“Time Stamping Authority”)

TSU Tidsstemplingsenhed (“Time Stamping Unit”)

UTC Fælles tidsangivelse (“Universal Time Coordinated”)

4. Generelt konceptbeskrivelse

4.1 Generelt om krav til tillidstjenesterudbydere, der udsteder tidsstempler

For at sikre et ensartet niveau af sikkerhed for udbydere af tillidstjenester, har ETSI offentliggjort en antal standarder, der fastlægger en række krav.

[ETSI EN 319 401] indeholder generelle krav til tillidstjenesteudbydere, mens [ETSI EN 319 421] stiller specifikke krav til tillidstjenesteudbydere, der udsteder elektroniske tidsstempler.

Det vurderes, at efterlevelse af krav i [ETSI EN 319 401] og [ETSI EN 319 421] opfylder krav til tillidstjenesteudbydere, der udsteder elektroniske tidsstempler jf. [eIDAS].

Nærværende politik er yderligere specifikation af ”best practices time-stamp policy (BTSP)” for TSA’er, der udsteder kvalificerede elektroniske tidsstempler jf. [ETSI EN 319 421].

4.2 Tidsstemplingsservices

Leverance af en tidsstemplingsservice er i denne politik brudt ned i følgende servicekomponenter:

- **Tidsstemplingsenhed:** Denne servicekomponent, TSU, genererer og sender tidsstempler. En TSA kan have en eller flere TSU’er til at levere sin service.
- **Styring af tidsstempling:** Denne servicekomponent overvåger og kontrollerer, at tidsstemplingsservicens driftes som specificeret i TSA-praksis.

Denne opdeling har udelukkende til formål at tydeliggøre kravene gennem en klassificering og skal ikke opfattes som arkitekturmæssige krav til en implementering.

4.3 Tidsstemplingsudsteder (TSA)

Kvalificerede tillidstjenesteudbydere, der udsteder kvalificerede elektroniske tidsstempler jf. [eIDAS] artikel 41 og artikel 42 benævnes tidsstemplingsudsteder forkortet TSA (Time Stamping Authority).

TSA kan anvende underleverandører i forbindelse med den tilbudte tjeneste, men det er altid det overordnede ansvar for at sikre, at krav i denne politik er overholdt.

4.4 Abonnent

En abonnent er en fysisk eller en juridisk person, der efter aftale med TSA, kan anmode om kvalificerede elektroniske tidsstempler.

Hvis abonnenten er en fysisk person, er abonnenten direkte ansvarlig i forhold til overholdelse af vilkår og betingelser for anvendelse af tjenesten.

Hvis abonnenten er en juridisk person, er abonnenten ansvarlig i forholdt til overholdelse af vilkår og betingelser for sine slutbrugeres anvendelse af tjenesten. Det er således abonnentens pligt at håndhæve overholdelse af vilkår og betingelser for anvendelse af tjenesten over for sine slutbrugere. Slutbrugere omfatter i denne sammenhæng både fysiske personer, der arbejder under instruks fra abonnenten og systemer hos abonnenten, der anvender TSA's tjenester.

4.5 Tidsstemplingspolitik og TSA-praksis

En tidsstemplingspolitik er en Trust Service Policy som defineret i [ETSI EN 319 401], der fastlægger krav til en tillidstjenesteudbyder, som udsteder elektroniske tidsstempler.

En TSA-praksis er en Trust Service Practice Statement som defineret i [ETSI EN 319 401], der beskriver hvordan en given TSA har implementeret kravene for en eller flere tidsstemplingspolitikker.

5. Introduktion til tidsstemplingspolitik og Generelle krav

5.1 Generelt krav

[KRAV 5.1-01] TSA'er, der udsteder elektroniske tidsstempler under denne politik, skal være en kvalificeret tillidstjenesteudbyder jf. [eIDAS] og udstede tidsstempler med minimum 1 sekunds nøjagtighed.

[KRAV 5.1-02] TSA'er, der udsteder kvalificerede elektroniske tidsstempler under denne politik, skal sikre, at den agerer lovligt og troværdigt.

[KRAV 5.1-03] Hvis TSA tilbyder en nøjagtighed i tidsstempler, der er bedre end 1 sekund, skal den tilbudte nøjagtighed fremgå af den offentliggjorte del af TSA-praksis og af de udstedte tidsstempler.

5.2 Identifikation

[KRAV 5.2-01] Tidsstempler udstedt efter denne politik skal indeholde "object identifier"-værdien:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

i feltet "policy" i svar på en tidsstempelforespørgsel medmindre, der svares med en fejlbesked, hvorved TSA erklærer overensstemmelse med BTSP jf. [ETSI EN 319 421].

5.3 Infrastruktur og anvendelse

5.3.1 Best practices tidsstemplingspolitik

[KRAV 5.3.1-01] Denne politik er rettet mod krav til tidsstempler til anvendelse sikre af gyldighed af elektroniske signaturer over længere tid (fx som defineret i [ETSI EN 319 122]), men kan anvendes generelt, hvor denne politik opfylder krav til sikkerhed og kvalitet af efterspurgte elektroniske tidsstempler i det omfang at TSA vilkår og betingelser tillader det.

[KRAV 5.3.1-02] Denne politik kan anvendes af kvalificerede TSA, der tilbyder tidsstempler som en åben tjeneste og/eller for en lukket gruppe af abonnenter.

6. Politikker og implementering

6.1 Risikovurdering

[KRAV 6.1-01] TSA skal gennemføre risikovurdering for at identificere, analysere og evaluere forretningsmæssige og tekniske risici.

[KRAV 6.1-02] TSA skal implementere passende foranstaltninger til håndtering af risici med udgangspunkt i risikovurderingen. Foranstaltningerne skal sikre, at sikkerhedsniveauet står i forhold til risikoen.

[KRAV 6.1-03] TSA skal fastlægge og dokumentere alle sikkerhedskrav og operationelle procedure, der er nødvendige for overholdelse af denne politik. Dokumentation skal være en del af TSA-praksis jf. afsnit 6.2.

[KRAV 6.1-04] Risikovurderingen skal revideres regelmæssigt og mindst én gang årligt.

[KRAV 6.1-05] TSA's ledelse skal godkende risikovurderingen og acceptere den identificerede restrisiko.

6.2 TSA-praksis

[KRAV 6.2-01] TSA skal udfærdige en TSA-praksis, der adresserer alle krav i denne politik. Denne TSA-praksis skal også omfatte alle eksterne organisationer, der understøtter TSA's tjeneste og skal være i overensstemmelse med denne politik. TSA-praksis kan være delt op i en offentlig og en privat del, hvor den offentlige del af TSA-praksis offentliggøres.

[KRAV 6.2-02] TSA's ledelse skal have ansvaret for og godkende den samlede TSA-praksis og sikre korrekt implementering herunder at praksissen er kommunikeret til relevante medarbejdere og partnere.

[KRAV 6.2-03] TSA skal gøre den offentlige del af TSA's gældende praksis tilgængelig på TSA's hjemmeside på 24/7 basis.

[KRAV 6.2-04] TSA-praksis skal gennemgås og revideres regelmæssigt og mindst én gang årligt. Ansvar for vedligehold af TSA-praksis skal fastlægges og dokumenteres. Ændringer i TSA-praksis skal dokumenteres.

[KRAV 6.2-05] TSA skal i TSA-praksis angive bestemmelser ved ophør af tjenesten. Disse skal som minimum inkludere information om hvem der bliver notificeret ved ophør og hvem, der overtager kunder og brugere, hvis der findes denne type aftaler.

[KRAV 6.2-06] TSA-praksis skal som minimum indeholde

- a) mindst en hash-algoritme, som anvendes til at repræsentere data, der tidsstemples
- b) nøjagtighed af tidsangivelsen i tidsstemplerne i forhold til UTC
- c) synkroniseringskilde eller -kilder
- d) enhver begrænsning af brugen af tidsstemplingstjenesten

- e) eventuelle forpligtelser for abonnenten
- f) forpligtelser for modtagerparter
- g) Oplysninger om, hvordan en modtagerpart skal kontrollere tidsstemplet, for at med rimelighed at kunne have tillid til tidsstemplet (se punkt 6.6) og oplysninger om eventuelle begrænsninger i gyldighedsperioden
- h) ethvert tilkendegivelse om at opfylde kravene til tidsstempling i henhold til national eller europæisk lovgivning

Note: I forhold til punkt h) i ovenstående skal TSA i sin praksis som minimum angive at tidsstemplingstjenesten er en kvalificeret tillidstjeneste jf. eIDAS.

[KRAV 6.2-07] TSA-praksis bør indeholde tilgængelighedsoplysninger af TSA's tjeneste.

6.3 Vilkår og betingelser

[KRAV 6.3-01] TSA skal stille vilkårene for sine tjenester til rådighed for alle abonnenter og modtagerparter.

[KRAV 6.3-02] Vilkår og betingelser skal blandt andet indeholde:

- a) en beskrivelse af tjenesten herunder hvilke politikker, der er omfattet af tjenesten,
- b) eventuelle begrænsninger i anvendelsen af tjenesten,
- c) abonnentens forpligtelser,
- d) information om tillidstjenesten for modtagerparter
- e) tid for opbevaring af hændelseslog,
- f) ansvarsbegrænsninger,
- g) begrænsninger i brugen af tjeneste, herunder TSA's ansvarsbegrænsning i forhold til forkert brug af tjenesten,
- h) lovvalg
- i) procedure for tvister,
- j) at TSA er en kvalificeret tillidstjeneste jf. eIDAS forordningen,
- k) TSA's kontaktinformation og
- l) eventuelle tilsagn om tilgængelighed.

[KRAV 6.3-03] Abonnenter og modtagerparter, der er afhængige af tillidstjenesten, skal informeres om præcise vilkår og betingelser, herunder ovennævnte punkter, inden de indgår et kontraktforhold.

[KRAV 6.3-04] Vilkår og betingelser skal stilles til rådighed via et varigt kommunikationsmedie.

[KRAV-6.3-05] Vilkår og betingelser skal foreligge på et letforståeligt sprog.

[KRAV-6.3-06] Vilkår og betingelser kan overføres elektronisk.

6.4 Informationssikkerhedspolitik

[KRAV 6.4-01] TSA skal leve op til kravene i standard for informationssikkerhed ISO 27001 og kunne dokumentere efterlevelse fx igennem certificering.

[KRAV 6.4-02] TSA skal have en ledelsesgodkendt politik for informationssikkerhed, der fastlægger organisationens informationssikkerhedsledelse.

[KRAV 6.4-03] TSA skal informere relevante parter om ændringer i politik for informationssikkerhed.

[KRAV 6.4-04] TSA's politik for informationssikkerhed skal dokumenteres, implementeres og vedligeholdes herunder sikkerhedskontrol og driftsprocedurer for TSA's faciliteter, systemer og informationsaktiver for leverede tjenester.

[KRAV 6.4-05] TSA skal kommunikere politik for informationssikkerhed til alle medarbejdere herunder medarbejdere hos underleverandører, der udfører arbejde for TSA.

Note: Medarbejdere, der er ansat i TSA's organisation, men som ikke udfører arbejde relateret til organisationens rolle som TSA, er ikke omfattet af ovenstående krav.

[KRAV 6.4-06] TSA har det overordnede ansvar for overholdelse af informationssikkerhedspolitikken uanset anvendelse af eventuelle underleverandører.

[KRAV 6.4-07] TSA skal fastlægge og sikre en effektiv implementering af relevante kontroller hos underleverandører.

[KRAV 6.4-08] TSA's politik og aktiver for informationssikkerhed skal revideres årligt og ved væsentlige ændringer med henblik på at sikre kontinuitet, egnethed, tilstrækkelighed og effektivitet.

[KRAV 6.4-09] Alle ændringer, der kan påvirke det leverede sikkerhedsniveau skal godkendes af TSA's ledelse.

[KRAV 6.4-10] TSA skal gennemgå konfiguration af TSA's systemer med faste intervaller og mindst en gang årligt for ændringer, der ikke lever op til TSA's politik for informationssikkerhed.

[KRAV 6.4-11] Det maksimale interval mellem to af ovenstående gennemgange skal dokumenteres i TSA's praksis.

6.5 TSAs forpligtelser

6.5.1 Generelle forpligtelser

[KRAV 6.5.1-01] TSA skal overholde eventuelle yderligere forpligtelser, der er angivet i tidsstempellet enten direkte eller inkorporeret som reference.

Note: Hvis TSA indsætter elementer i tidsstempler fx i form af extensions og disse indeholder implicitte eller eksplicitte forpligtelser, skal disse overholdes uanset at disse forpligtelser ikke er angivet i nærværende politik.

6.5.2 TSAs forpligtelser i forhold til abonnenter

[KRAV 6.5.2-01] Det foreliggende dokument stiller ingen specifikke forpligtelser til abonnenten. Alle specifikke TSA-specifikke krav til abonnenten, skal være angivet i TSA's vilkår og betingelser.

6.6 Information til modtagerparter

[KRAV 6.6-01] Vilkår og betingelser for modtagerparter skal som minimum inkludere følgende forpligtelser for modtagerparten inden et tidsstempel accepteres:

- a) Modtagerpart skal kontrollere, at tidsstempellet er korrekt signeret, og at den private nøgle, der bruges til at signere tidsstempellet, ikke er blevet markeret som kompromitteret på kontroltidspunktet,
- b) Modtagerpart skal tage hensyn til eventuelle begrænsninger for brugen af tidsstempellet angivet i tidsstempelpolitikken og
- c) Modtagerpart skal tage hensyn til andre forholdsregler, der er angivet i aftaler eller lignende.

Note: Punkt a) i ovenstående krav kan sikres ved, at det er en korrekt signeret og at certifikatet hørende til den anvendte nøgle er gyldig i forhold til gyldighedsperiode samt at certifikatets serinummer ikke findes på den relevante opdaterede spærreliste.

7. TSA styring og drift

7.1 Introduktion

[KRAV 7.1-01] TSA skal have et system eller systemer til kvalitetsstyring og informationssikkerhedsstyring, der er passende for de tidsstemplingstjenester, der leveres jf. KRAV 6.4-01.

7.2 Intern organisation

[KRAV 7.2-01] TSA skal være en juridisk person.

[KRAV 7.2-02] TSA-organisationen skal agere pålidelig og ikke-diskriminerende.

[KRAV 7.2-03] TSA bør gøre sine tjenester tilgængelige for alle, hvis aktiviteter falder inden for det angivne driftsområde, og at de overholder deres forpligtelser som angivet i TSA's vilkår og betingelser.

Note: TSA har mulighed for at begrænse driftsområdet for sine tjenester og TSA bør offentliggøre sit driftsområde i sin praksis. Eksempelvis kan TSA angive, at tidsstempler udelukkende udstedes til én angivet abonnent, men at tidsstempler fra TSA kan verificeres af alle modtagerparter.

[KRAV 7.2-04] TSA skal opretholde tilstrækkelige finansielle ressourcer og/eller tegne en passende ansvarsforsikring i overensstemmelse med gældende lov, herunder eIDAS, til dækning af forpligtelser som følge af dets aktiviteter.

[KRAV 7.2-05] Hvis TSA er en privat virksomhed, skal TSA tegne og opretholde en ansvarsforsikring jf. KRAV 7.2-04. Forsikringen skal som minimum have en dækning på kr. 25 millioner pr. år.

[KRAV 7.2-06] TSA skal have den finansielle stabilitet og ressourcer, der kræves for at fungere i overensstemmelse med denne politik.

Note: Ovenstående krav skal vurderes i forhold til den kontekst TSA opererer, herunder men ikke begrænset til antallet af kunder og den finansielle risiko som TSA påtager sig i forhold til de udstedte tidsstempler.

[KRAV 7.2-07] TSA skal have politikker og procedurer til løsning af klager og tvister modtaget fra kunder eller andre modtagerparter om leveringen af ydelserne eller andre relaterede forhold.

[KRAV 7.2-08] TSA skal have skriftlig dokumenteret aftale- og kontraktforhold på plads, hvor levering af tjenesteydelser omfatter underleverancer, outsourcing eller andre tredjepartsordninger.

[KRAV 7.2-09] Opgaver og ansvarsområder, der kan indeholde konfliktende interesser, skal adskilles for at reducere mulighederne for uautoriseret eller utilsigtet ændring eller misbrug af TSA's aktiver.

7.3 Personalesikkerhed

[KRAV 7.3-01] TSA skal sikre at personale og underleverandører understøtter en tillidsfuld drift af TSA.

[KRAV 7.3-02] TSA skal til stadighed have et tilstrækkeligt antal medarbejdere med den nødvendige uddannelse, træning, teknisk viden og erfaring vedrørende typen, omfanget og omfanget af det arbejde, der er nødvendigt for at levere tidsstemplingstjenester.

[KRAV 7.3-03] Herunder skal TSA's personale inklusive personale ved eventuelle underleverandører være i stand til at opfylde kravet om "ekspertviden, erfaring og kvalifikationer" gennem formelle uddannelser og akkrediteringer eller gennem egentlig erfaring eller en kombination af de to.

[KRAV 7.3-04] TSA skal ansætte personale, og hvor det er relevant, anvende underleverandører, som har den nødvendige ekspertise, pålidelighed, erfaring og kvalifikationer, og som har modtaget uddannelse vedrørende informationssikkerhed og beskyttelse af persondataoplysninger, der er relevant for de udbudte tjenester og jobfunktionen.

[KRAV 7.3-05] Ovenstående uddannelseskrav bør omfatte regelmæssige (mindst hver 12 måneders) opdateringer om nye trusler og nuværende sikkerhedspraksis.

[KRAV 7.3-06] Der skal anvendes passende disciplinære sanktioner for personale, der overtræder TSA's politikker eller procedurer.

[KRAV 7.3-07] Sikkerhedsroller og -ansvar som angivet i TSA's informationssikkerhedspolitik skal dokumenteres i stillingsbeskrivelser eller i dokumenter, der er tilgængelige for alle berørte medarbejdere.

[KRAV 7.3-08] Betroede roller, hvoraf TSA's sikkerhed er afhængig, skal være klart identificeret og ledelsesgodkendte.

[KRAV 7.3-09] Tildeling af en betroet rolle til en medarbejder skal godkendes af ledelsen og accepteres af medarbejderen, der tildes rollen.

[KRAV 7.3-10] TSA's personale (både midlertidigt og permanent) skal have jobbeskrivelser defineret ud fra de roller de skal udfylde under hensyntagen til adskillelse af pligter (segregation of duties), mindsteprivilegier (least privilege), følsomheden af data som kan tilgås, baggrundstjek og medarbejders uddannelse og awareness.

[KRAV 7.3-11] Hvor det er relevant skal jobbeskrivelser skelne mellem generelle funktioner og TSA-specifikke funktioner. Sidstnævnte bør omfatte krav til færdigheder og erfaring.

[KRAV 7.3-12] Personale skal anvende administrative procedurer og processer, der er i overensstemmelse med TSA's informationssikkerhedsstyringsprocedurer.

[KRAV 7.3-13] Ledende medarbejdere skal have erfaring eller træning i forhold til drift af TSA, kendskab til sikkerhedsprocedurer for personale med sikkerhedsansvar og erfaring med informationssikkerhed og risikovurdering, der er tilstrækkelig til at kunne udføre ledelsesfunktioner for TSA.

[KRAV 7.3-14] Alle TSA's medarbejdere med betroede roller skal være fri for interessekonflikter, der kan skade uafhængigheden af TSA's drift.

[KRAV 7.3-15] De betroede roller skal inkludere roller, med følgende ansvar:

- a) Security Officers: Samlet implementeringsansvar for administrationen af sikkerhedspraksis.
- b) System Administrators: Autoriseret til at installere, konfigurere og vedligeholde TSA's kritiske systemer til service management inklusive systemgen-skabelse.
- c) Systemoperatører: Ansvarlig for driften af TSA's kritiske systemer på daglig basis. Autoriseret til at udføre sikkerhedskopi af system.

- d) Systemrevisorer: Autoriseret til at se lagrede data og audit-logfiler fra TSA's kritiske systemer.

[KRAV 7.3-16] Personale, der skal tilgå eller konfigurere rettigheder for betroede roller skal være formelt godkendt af en sikkerhedsansvarlig på øverste ledelsesniveau efter "least privilege"-princippet.

[KRAV 7.3-17] Personale må ikke have adgang til funktioner forbeholdt betroede roller før de nødvendige kontroller er gennemført.

7.4 Styring af aktiver

7.4.1 Generelle krav

[KRAV 7.4.1-01] TSA skal vedligeholde en oversigt over aktiver herunder informationsaktiver. Alle informationsaktiver skal klassificeres i henhold til TSA's risikovurdering og TSA skal sikre en tilstrækkelig beskyttelse af alle aktiver.

7.4.2 Håndtering af medier

[KRAV 7.4.2-01] Alle medier i TSA's driftssystem skal håndteres sikkert i overensstemmelse med klassificering herunder skal

- medier med fortroligt data skal bortskaffes med en sikker metode,
- medier beskyttes mod skade, tyveri og uautoriseret adgang og forældelse og
- fortrolige data beskyttes mod uautoriseret adgang ved genbrug af lagringsmedier.

7.5 Adgangskontrol

[KRAV 7.5-01] TSA skal implementere en effektiv adgangskontrol, der beskytter mod uautoriseret fysisk eller logisk adgang til TSA's systemer.

Særligt gælder det, at:

- **[KRAV 7.5-02]** TSA skal implementere foranstaltninger (fx firewalls), der beskytter TSA's interne netværk mod uautoriseret adgang, herunder adgang fra abonnenter og modtagerparter.
- **[KRAV 7.5-03]** Firewalls skal konfigureres for at forhindre alle protokoller og adgange, der ikke er nødvendige for driften af TSA.
- **[KRAV 7.5-04]** TSA skal implementere en effektiv brugeradministration herunder administration af adgange for operatører, administratorer og systemauditorer.
- **[KRAV 7.5-05]** Brugerkonti skal jævnligt gennemgås for at sikre at brugere til stadighed kun har nødvendige rettigheder jf. politik for adgangsrettigheder.

- **[KRAV 7.5-06]** Adgang til informations- og applikationssystemfunktioner skal begrænses i overensstemmelse med adgangskontrolpolitikken.
- **[KRAV 7.5-07]** TSA's driftssystemer skal implementere en tilstrækkelig IT-sikkerhed til at understøtte adskillelse af betroede roller identificeret i TSA-praksis, herunder adskillelse af sikkerhedsadministration og operationelle roller. Særligt skal anvendelse af utility programmer begrænses og kontrolleres til det nødvendige.
- **[KRAV 7.5-08]** TSA's personale skal identificeres og autentificeres inden der gives adgang til kritiske systemer og applikationer
- **[KRAV 7.5-09]** TSA's personale skal være ansvarlig for deres aktiviteter fx gennem effektiv hændelseslogging.

7.6 Kryptografiske kontroller

7.6.1 Generelle kontroller

[KRAV 7.6.1-01] TSA skal implementere en sikker håndtering af kryptografiske nøgler og kryptografiske moduler. Håndteringen skal dække hele livscyklussen for nøgler og moduler.

7.6.2 TSU nøglegenerering

- a) **[KRAV 7.6.2-01]** Generering af TSU'ens private signeringsnøgler skal ske i et fysisk sikret miljø (jf. afsnit 7.8) af personale med tillid til roller (jf. afsnit 7.3) under dual kontrol. Det personale, der er bemyndiget til at udføre denne funktion, er begrænset til dem, der kræves i henhold til TSA-praksis.
- b) **[KRAV 7.6.2-02]** Generering af TSU'ens private signeringsnøgler skal udføres i et sikkert kryptografisk modul, som:
 - i) er et troværdigt system, der er sikret til EAL 4 eller højere i overensstemmelse med [ISO/IEC 15408] eller tilsvarende nationale eller internationalt anerkendte evalueringskriterier for it-sikkerhed. Dette skal være et sikkerhedsmål eller en beskyttelsesprofil, der opfylder kravene i nærværende dokument på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikke-tekniske sikkerhedsforanstaltninger, eller
 - ii) opfylder kravene i [ISO/IEC 19790] eller [FIPS PUB 140-2] level 3.

Det kryptografiske modul bør være som angivet i i).

- c) **[KRAV 7.6.2-03]** TSU'ens nøglegenereringsalgoritmen, nøglelængden på signeringsnøgle og signaturalgoritmen, der anvendes til signering af tidsstempler, skal være som specificeret i [ETSI TS 119 312]. Anbefalinger til

kryptografiske algoritmer og nøglelængder defineret i [ETSI TS 119 312] kan erstattes af nationale anbefalinger.

- d) **[KRAV 7.6.2-04]** En TSUs signeringsnøgle bør ikke importeres til forskellige kryptografiske moduler.
- e) **[KRAV 7.6.2-05]** Hvis den samme signeringsnøgle anvendes i forskellige kryptografiske moduler, skal nøglen være knyttet til det samme offentlige nøglecertifikat i alle de forskellige kryptografiske moduler.
- f) **[KRAV 7.6.2-06]** En TSU skal have en enkelt privat tidsstempelssigneringsnøgle aktiv ad gangen.

7.6.3 Beskyttelse af TSU private nøgler

[KRAV 7.6.3-01] Fortrolighed og integritet af TSU's private nøgler skal opretholdes.

Særligt gælder at:

- a) **[KRAV 7.6.3-02]** TSU'ens private signeringsnøgle skal opbevares og anvendes i et kryptografisk modul, som:
 - i) er et troværdigt system, der er sikret til EAL 4 eller højere i overensstemmelse med [ISO/IEC 15408] eller tilsvarende nationale eller internationalt anerkendte evalueringskriterier for it-sikkerhed. Dette skal være et sikkerhedsmål eller en beskyttelsesprofil, der opfylder kravene i nærværende dokument på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikke-tekniske sikkerhedsforanstaltninger, eller
 - ii) opfylder kravene i [ISO/IEC 19790] eller [FIPS PUB 140-2] level 3.

Det kryptografiske modul bør være som angivet i i).

- b) **[KRAV 7.6.3-03]** Hvis TSU'ens private nøgler sikkerhedskopieres, skal de kun kopieres, opbevares og genetableres af personale i betroede roller under dual kontrol i et fysisk sikret miljø (jf. afsnit 7.8). Det personale, der er bemyndiget til at udføre denne funktion, skal være begrænset til dem, der kræves i henhold til TSA's praksis.
- c) **[KRAV 7.6.3-04]** Enhver sikkerhedskopi af TSU's private nøgler skal til stadighed beskyttes på minimum det samme niveau som for det kryptografiske modul, hvor nøglen er genereret og anvendes for at sikre dets integritet og fortrolighed.

7.6.4 TSU certifikat

[KRAV 7.6.4-01] TSA skal garantere integriteten og autenticitet af TSU'ens (offentlige) signaturverifikationsnøgler. Som minimum skal følgende opfyldes:

- a) **[KRAV 7.6.4-02]** TSU'ens (offentlige) signaturverifikationsnøgler skal stilles til rådighed for modtagerparter i et certifikat.

- b) **[KRAV 7.6.4-03]** TSU'ens certifikat skal være udstedt af et kvalificeret CA, der efterlever krav i [ETSI EN 319 411-1] og [ETSI EN 319 411-2].
- c) **[KRAV 7.6.4-04]** TSU'en må ikke udstede ikke tidsstempler, før TSU'ens certifikat er indlæst i TSU'en eller dens kryptografiske modul.

[KRAV 7.6.4-05] Ved modtagelse af TSU'ens certifikat, bør TSA kontrollere, at certifikatet er blevet signeret korrekt af CA (herunder verifikation af certifikatkæden til en anerkendt kvalificeret CA).

7.6.5 Fornyelse af TSU's nøgler

[KRAV 7.6.5-01] Gyldighedsperioden for TSU's certifikat må ikke være længere end den periode, hvor den valgte algoritme og nøglelængde er anerkendt som egnet til formål (se afsnit 7.6.2 punkt c)).

7.6.6 Livscyklushåndtering af kryptografiske moduler til signering

[KRAV 7.6.6-01] Kryptografiske moduler, der anvendes i forbindelse med tidsstempling, skal være beskyttet i hele livscyklus. Som minimum skal følgende opfyldes:

- a) **[KRAV 7.6.6-02]** Kryptografiske moduler må ikke være manipuleret under forsendelse.
- b) **[KRAV 7.6.6-03]** Kryptografiske moduler må ikke manipuleres med under opbevaring.
- c) **[KRAV 7.6.6-04]** Installation, aktivering og kopiering af TSU'ens signeringsnøgler i kryptografiske moduler skal kun udføres af personale i betroede roller med mindst dual kontrol i et fysisk sikret miljø (jf. afsnit 7.8).
- d) **[KRAV 7.6.6-05]** TSU'ens signeringsnøgler opbevaret på TSU'ens kryptografisk modul skal slettes på en måde, at det praktisk umuligt at genskabe dem, når det kryptografiske modul ikke længere skal anvendes til signering med TSU'ens signeringsnøgler.

7.6.7 Terminering af TSU's private nøgler

[KRAV 7.6.7-01] TSA skal fastlægge en udløbsdato for TSU's signeringsnøgler.

Bemærk: At udløbsdato for TSU's signeringsnøgle ikke er det samme som udløbsdato for tilhørende certifikat.

[KRAV 7.6.7-02] Udløbsdatoen må ikke overskride gyldighedsperioden for det tilhørende certifikat.

[KRAV 7.6.7-03] Udløbsdatoen skal tage hensyn til levetiden defineret under "recommended key sizes versus time" i [ETSI TS 119 312].

[KRAV 7.6.7-04] For at kunne bekræfte tidsstemplets gyldighed i et tilstrækkeligt tidsrum, bør TSU's signeringsnøgle gyldighed være mindre end certifikatets gyldighed.

Fx kan signeringsnøgler være gyldige i et år, hvis tilhørende certifikat er gyldig i 4 år.

[KRAV 7.6.7-05] Udløbsdatoen for TSU'ens signeringsnøgler kan defineres, når TSU'ens kryptografiske modul initialiseres eller ved at angive en "privateKeyUsagePeriod"-extension i TSU'ens certifikat.

[KRAV 7.6.7-06] TSU'ens signeringsnøgler må ikke anvendes efter udløbet af deres gyldighedsperiode.

Særligt gælder at:

- a) **[KRAV 7.6.7-07]** Der skal være administrative eller tekniske procedurer, der sikrer, at en ny nøgle etableres, når en TSU'ens signeringsnøgle udløber.
- b) **[KRAV 7.6.7-08]** TSU'ens signeringsnøgler og enhver nøgledel, herunder eventuelle kopier, skal destrueres, så nøglerne ikke kan genskabes.

7.7 Tidsstempeling

7.7.1 Udstedelse af tidsstempler

[KRAV 7.7.1-01] Tidsstempler skal være i overensstemmelse med tidsstempelprofilen som defineret i ETSI EN 319 422.

[KRAV 7.7.1-02] Særligt skal tidsstempler markeres som kvalificerede tidsstempler ved at inkludere én qcStatements-extension med værdien "esi4-qtst-Statement-1" jf. [ETSI EN 319 422] afsnit 9.1.

[KRAV 7.7.1-03] Tidsstemplerne udstedes sikkert og skal indeholde den korrekte tid.

Herunder gælder særligt:

- a) **[KRAV 7.7.1-04]** De tidsværdier, som TSU'en bruger i tidsstemplet, skal være sporbar til mindst en af de realtidsværdier, der distribueres af et UTC(k) laboratorium.
- b) **[KRAV 7.7.1-05]** Det tidspunkt, der er angivet i tidsstemplet skal være synkroniseret med UTC inden for den nøjagtighed, der er defineret i denne politik og, hvis den er til stede, inden for den nøjagtighed, der er defineret i selve tidsstemplet.
- c) **[KRAV 7.7.1-06]** Hvis TSA's ur er detekteret (jf. KRAV 7.7.2-04) som ude af den angivne nøjagtighed (jf. KRAV 7.7.1-04), skal tidsstempler ikke udstedes.
- d) **[KRAV 7.7.1-07]** Tidsstemplet skal signeres ved hjælp af en nøgle, der udelukkende er genereret til dette formål.
- e) **[KRAV 7.7.1-08]** Tidsstempelgenereringssystemet skal afvise ethvert forsøg på at udstede tidsstempler, når efter TSU's signeringsnøgles udløbstidspunkt.

[KRAV 7.7.1-09] TSU'er, der udsteder kvalificerede tidsstempler jf [eIDAS] under denne politik, må ikke udstede ikke-kvalificerede tidsstempler.

[KRAV 7.7.1-10] TSA'er, der udsteder kvalificerede tidsstempler jf. [eIDAS] under denne politik fra en TSU og samtidig udsteder ikke-kvalificerede tidsstempler fra andre TSU'er, skal anvende et andet emnenavn (subject distinguishedName) i certifikater for TSU'erne, der udsteder ikke-kvalificerede tidsstempler end certifikatet for TSU, der udsteder kvalificerede tidsstempler under denne politik.

[KRAV 7.7.1-11] Ovenstående ikke-kvalificerede TSU'er skal tilgås via andre serviceinterfaces end for TSU'er, der opererer under denne politik.

7.7.2 UTC-synkronisering af ur

[KRAV 7.7.2-01] TSU's ure skal synkroniseres med UTC inden for den deklarerede nøjagtighed.

Herunder gælder som minimum at:

- a) **[KRAV 7.7.2-02]** Kalibrering af TSU's ure skal opretholdes således, at urene ikke drive uden for den deklarerede nøjagtighed.
- b) **[KRAV 7.7.2-03]** Den deklarerede nøjagtighed skal være på 1 sekund eller bedre.
- c) **[KRAV 7.7.2-04]** TSU's ure skal beskyttes mod trusler, som kan resultere i en ikke-detekteret ændring af urene, der bringer dem uden for dets kalibrering.

Note: Eksempler på trusler kan være ændring foretaget af personale uden autorisation samt manipuleret radiosignal eller elektriske stød.

- d) **[KRAV 7.7.2-05]** TSA skal registrere, om den tid, der skal anvendes i et tidsstempel, driver eller springer ud af synkronisering med UTC.
- e) **[KRAV 7.7.2-06]** Hvis det konstateres, at den tid, der skal anvendes i et tidsstempel, driver eller springer ud af synkronisering med UTC, skal TSU'en stoppe tidsstempeludstedelse.
- f) **[KRAV 7.7.2-07]** Synkroniseringen af ure skal opretholdes, når et skudsekund meddelt af det relevante organ finder sted. Ændringen for at tage højde for skudsekund skal ske inden for sidste minut på dagen, hvor skudsekundet er planlagt. Det præcise tidspunkt for ændringen skal logges (inden for den angivne nøjagtighed).

7.8 Fysisk og miljømæssig sikkerhed

[KRAV 7.8-01] TSA skal sikre den fysiske adgang til elementer i TSA's systemer i forhold til fastlagt politik for klassifikation herunder minimering af risici i forhold til den fysiske sikkerhed.

[KRAV 7.8-02] TSA skal sikre, at adgang til driftslokaler er begrænset til autoriserede personer.

[KRAV 7.8-03] TSA skal implementere en effektiv beskyttelse mod

- tab, skader og kompromittering af aktiver og forretningsaktiviteter samt
- kompromittering eller tyveri af information og driftsudstyr

[KRAV 7.8-04] Komponenter, der er afgørende for sikker drift af TSA, skal befinde sig inden for en beskyttet sikkerhedsperimeter med fysisk beskyttelse mod indtrængen, adgangskontrol og alarmer for at opdage indtrængen.

Følgende skal være opfyldt:

- a) **[KRAV 7.8-05]** Der skal anvendes adgangskontrol på kryptografiske moduler for at opfylde kravene til sikkerhed beskrevet i afsnit 7.6.
- b) Følgende kontroller til styring af tidsstempler skal være opfyldt:
 - **[KRAV 7.8-06]** Udstyr til styring af tidsstempling skal drives i et miljø, der fysisk og logisk beskytter ydelserne mod kompromittering gennem uautoriseret adgang til systemer eller data.
 - **[KRAV 7.8-07]** Al adgang til det fysisk sikre område skal være underlagt uafhængigt audit, og ikke-autoriseret person skal ledsages af en autoriseret person i det sikre område. Hver indgang til og udgang fra det sikre område skal logges.
 - **[KRAV 7.8-08]** Fysisk beskyttelse skal opnås ved at skabe klart definerede perimeter (dvs. fysiske barrierer) omkring styring af tidsstemplingen. Lokalerne, der er delt med andre organisationer, skal være uden for denne perimeter.
 - **[KRAV 7.8-09]** Fysiske og miljømæssige sikkerhedskontroller skal beskytte systemressourcerne, de faciliteter, som indeholder systemressourcer og de faciliteter, der bruges til at understøtte deres drift. TSA's fysiske og miljømæssige sikkerhedspolitik for systemer, der beskæftiger sig med tidsstempling, skal mindst omfatte fysisk adgangskontrol, beskyttelse mod naturkatastrofer, brandsikkerhed, beskyttelse mod manglende støttefunktioner (f.eks. el og telekommunikation), sikring mod struktorkollaps, sikring mod lækager, beskyttelse mod tyveri og indbrud. Der skal være implementeret planer for genskabelse efter driftsmæssige katastrofer (disaster recovery).
 - **[KRAV 7.8-10]** Kontroller skal beskytte mod at udstyr, information, medier og software, der vedrører tidsstemplingstjenesterne, fjernes uden autorisation.

[KRAV 7.8-11] Andre funktioner kan driftes i det sikre område, hvis adgangen er begrænset til det autoriserede personale.

7.9 Driftssikkerhed

[KRAV 7.9-01] TSA skal benytte anerkendte systemer og produkter, som er beskyttet mod ændringer og sikre den tekniske sikkerhed og pålidelighed af de processer, der understøttes af disse systemer og produkter.

[KRAV 7.9-02] TSA skal sikre, at der forud for enhver systemudvikling (dvs. egenudvikling eller udvikling hos tredjepart) foreligger en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne. Planen skal indeholde en analyse af, at sikkerhedskrav er opfyldt for at kunne opretholde et tilstrækkeligt sikkerhedsniveau.

[KRAV 7.9-03] TSA skal implementere dokumenterede processer til release- og ændringshåndtering af software-, hardware- og konfigurationsændringer. TSA skal desuden have dokumenterede processer for sikkerhedsopdatering af egenudviklet og standardsoftware og -firmware. Processerne skal inkludere dokumentation for gennemført ændringer.

[KRAV 7.9-04] Integriteten i TSA's systemer og data skal beskyttes mod vira, malware og uautoriseret software herunder skal TSA implementere processer, der sikrer, at

- sikkerhedsopdateringer installeres i rimelig tid efter at de bliver tilgængelige,
- sikkerhedsopdateringer ikke installeres, hvis det vurderes, at de introducerer nye uacceptable sårbarheder eller ustabilitet, der ikke opvejer fordelene ved opdateringerne og
- årsager til at undlade eller udskyde en sikkerhedsopdatering er dokumenteret.

[KRAV 7.9-05] Alle medier i TSA's driftssystem skal håndteres sikkert i overensstemmelse med klassificering herunder skal medier beskyttes mod skade, tyveri og uautoriseret adgang og forældelse.

[KRAV 7.9-06] TSA skal have mediehåndteringsprocesser, der sikrer medier mod forældelse og degenerering i den periode, hvor data skal lagres.

[KRAV 7.9-07] TSA skal etablere og implementere procedurer for alle betroede og administrative roller som kan have indvirkning på TSA's sikkerhed og drift.

[KRAV 7.9-08] TSA skal planlægge og overvåge kapacitetsbehov for at sikre, at der til stadighed er tilstrækkelige driftsressourcer til rådighed.

7.10 Netværkssikkerhed

[KRAV 7.10-01] TSA's netværk og systemer skal beskyttes mod angreb og uautoriseret adgang.

Særligt gælder at:

- **[KRAV 7.10-02]** TSA skal segmentere sine systemer i netværk eller zoner i forhold til en risikovurdering under hensyntagen til funktionelle, logiske

og fysiske (inkl. placering) sammenhænge mellem de kritiske systemer og services.

- **[KRAV 7.10-03]** Alle systemer i en zone skal underlægges samme sikkerhedskontroller.
- **[KRAV 7.10-04]** TSA skal sikre, at adgang til og kommunikation mellem zoner begrænses til det nødvendige.
- **[KRAV 7.10-05]** TSA skal eksplicit blokere eller deaktivere forbindelser og services, der ikke skal anvendes.
- **[KRAV 7.10-06]** Herunder skal TSA konfigurere alle TSU systemer så alle konti, applikationer, services og porte, der ikke anvendes i TSU'en drift er fjernet eller deaktiveret.
- **[KRAV 7.10-07]** TSA skal regelmæssigt gennemgå fastlagte netværks- og firewallregler.
- **[KRAV 7.10-08]** TSA skal drifte, vedligeholde og beskytte alle TSU systemer i sikre zoner eller særligt sikrede zoner.
- **[KRAV 7.10-09]** Særligt kritiske systemer skal placeres i særligt sikrede zoner.
- **[KRAV 7.10-10]** TSA skal adskille dedikeret netværk til administration af it-systemer og TSA's driftsnetværk.
- **[KRAV 7.10-11]** TSA må ikke anvende systemer, der anvendes til administration af implementeringen af sikkerhedspolitikken til andre formål.
- **[KRAV 7.10-12]** TSA skal holde driftssystemer adskilt fra udviklings- og testsystemer.
- **[KRAV 7.10-13]** TSA skal sikre at kommunikation mellem kritiske systemer udelukkende sker gennem sikrede kanaler, der er fysisk eller logisk adskilt fra andre kommunikationskanaler og giver fortrolighed, integritet og autenticitet mellem systemerne.
- **[KRAV 7.10-14]** TSA skal sikre ekstern netværksredundans for systemer med høje krav til tilgængelighed fra eksterne kilder.
- **[KRAV 7.10-15]** TSA skal udføre regelmæssige sårbarhedsscanninger fra eksterne og interne IP-adresser. Scanningerne gennemføres af en part med færdigheder, værktøjer, etisk kodeks og uafhængighed, som er nødvendig for at kunne give en pålidelig rapport. Scanninger skal dokumenteres.
- **[KRAV 7.10-16]** TSA skal udføre penetrationstest efter etablering og ved væsentlige ændringer og opdateringer i infrastrukturen eller i de anvendte applikationer. Penetrationstesten gennemføres af en part med færdigheder, værktøjer, etisk kodeks og uafhængighed, som er nødvendig for at kunne give en pålidelig rapport. Penetrationstesten skal dokumenteres.

- **[KRAV 7.10-17]** TSA skal sikre, at kun betroede roller har adgang til sikre zoner og særligt sikre zoner.

7.11 Hændeshåndtering

[KRAV 7.11-01] Systemaktiviteter som adgang til it-systemer, brug af it-systemer og kald af services skal overvåges.

Særligt gælder at:

- **[KRAV 7.11-02]** Overvågningen skal tage højde for følsomheden af de data, der indsamles eller analyseres.
- **[KRAV 7.11-03]** Unormale systemaktiviteter, der udgør et potentiel sikkerhedsbrud, herunder indtrængen i TSA's netværk skal registreres og rapporteres som alarmer.
- **[KRAV 7.11-04]** TSA skal overvåge følgende hændelser:
 - a) opstart og nedlukning af logfunktionerne og
 - b) tilgængelighed og brug af nødvendige tjenester med TSA's netværk.
- **[KRAV 7.11-05]** TSA skal handle rettidigt og koordineret for at reagere hurtigt på sikkerhedshændelser og begrænse konsekvenserne af sikkerhedsbrud.
- **[KRAV 7.11-06]** TSA skal have personale med betroet rolle til opfølgning på advarsler om potentielt kritiske sikkerhedshændelser og sikrer, at relevante hændelser rapporteres i overensstemmelse med TSA's procedurer.
- **[KRAV 7.11-07]** TSA skal have procedurer og beredskab, der sikre notifikation af sikkerhedshændelse eller tab af integritet til relevante parter jf. gældende regulering fx databeskyttelsesmyndigheder og/eller eIDAS tilsynsorgan senest 24 timer efter, at hændelsen er identificeret.
- **[KRAV 7.11-08]** Hvis der er en sandsynlighed for, at en sikkerhedshændelse eller tab af integritet kan påvirke en fysisk eller juridisk person negativt, skal TSA også notificere denne uden unødigt forsinkelse.
- **[KRAV 7.11-09]** TSA's systemer skal overvåges, hvilket skal omfatte monitorering eller regelmæssige gennemgang af auditlogs for at identificere ondsindet aktivitet med henblik på at alarmere potentielle kritiske sikkerhedshændelser til sikkerhedspersonale.
- **[KRAV 7.11-10]** TSA skal håndtere enhver kritisk sårbarhed, som ikke tidligere er håndteret af TSA, inden for 48 timer efter at den er identificeret.
- **[KRAV 7.11-11]** For enhver identificeret sårbarhed skal TSA i forhold til de potentielle skader enten
 - a) oprette og implementere en plan for mitigering af sårbarheden eller

- b) dokumentere grundlaget for TSA's beslutning om, at sårbarheden ikke kræver mitigering.
- **[KRAV 7.11-12]** Hændelsesrapporterings- og responsprocedurer skal etableres på en sådan måde, at skader fra sikkerhedshændelser og funktionsfejl minimeres.

7.12 Indsamling af beviser

[KRAV 7.12-01] TSA skal registrere og kunne tilgå alle relevante oplysninger vedrørende data genereret og modtaget af TSA i et passende tidsrum, herunder efter ophør af aktiviteterne i TSA, navnlig med henblik på at kunne fremlægge bevismateriale i retssager og kunne sikre tjenestens kontinuerede drift.

Særligt gælder at:

- **[KRAV 7.12-02]** TSA skal sikre fortroligheden og integriteten af lagrede data relateret til driften af TSA's services.
- **[KRAV 7.12-03]** TSA skal sikre kompletthed, fortroligheden og integriteten af lagrede data relateret til driften af TSA's services i henhold til dokumenteret forretningspraksis offentliggjort i TSA-praksis.
- **[KRAV 7.12-04]** Data herunder auditlog skal kunne fremfindes og stilles til rådighed som bevis i en retssag.
- **[KRAV 7.12-05]** Det nøjagtige tidspunkt for væsentlige hændelser i forhold til driftsmiljø, nøglehåndtering og tidssynkronisering skal registreres.
- **[KRAV 7.12-06]** Tiden, som anvendes til i forbindelse med auditlogging, skal synkroniseres med UTC mindst en gang dagligt.
- **[KRAV 7.12-07]** Data relateret til TSA's services skal lagres i et passende tidsrum for at tilvejebringe nødvendige juridiske beviser og som angivet i TSA's vilkår og betingelser.
- **[KRAV 7.12-08]** Hændelser skal logges på en måde, så log ikke let kan slettes eller ødelægges i den periode, som loggen skal gemmes (medmindre den er overflyttet sikkert til medie til langtidsopbevaring).

TSU nøglehåndtering

- a) **[KRAV 7.12-09]** Data relateret til alle hændelser vedrørende TSU-nøglerens livscyklus skal logges.
- b) **[KRAV 7.12-10]** Data relateret til alle hændelser vedrørende TSU-certifikatets livscyklus (hvis relevant) skal logges.

Synkronisering af ure

- c) **[KRAV 7.12-11]** Data relateret til alle hændelser vedrørende synkronisering af en TSUs ur til UTC skal logges. Dette skal indeholde oplysninger om normal omkalibrering eller synkronisering af ure anvendt til tidsstempling.

- d) **[KRAV 7.12-12]** Data relateret til alle hændelser vedrørende detektering af manglende synkronisering skal logges.

7.13 Business Continuity Plan

[KRAV 7.13-01] TSA skal fastlægge, teste og vedligeholde en Business Continuity Plan (BCP), der skal aktiveres i forbindelse med en driftsmæssig katastrofe.

[KRAV 7.13-02] I tilfælde af en driftsmæssig katastrofe herunder kompromittering af en af TSA's private signeringsnøgler skal driftens genoprettes inden for den frist, der er fastlagt i BCP, idet årsagen til katastrofen er håndteret med passende afhjælpende foranstaltninger.

Særligt gælder at:

- a) **[KRAV 7.13-03]** TSA's katastrofeplan skal omfatte kompromittering eller mistanke om kompromittering af TSU's private signeringsnøgler eller manglende kalibrering af et TSU-ur, som kan have påvirket udstedte tidsstempler.
- b) **[KRAV 7.13-04]** I tilfælde af kompromittering, mistanke om kompromittering eller manglende kalibrering ved udstedelse af tidsstempel skal TSA gøre beskrivelse af hændelsen til tilgængelig for alle abonnenter og modtagerparter.
- c) **[KRAV 7.13-05]** I tilfælde af en driftsmæssig kompromittering, mistanke om en driftsmæssig kompromittering eller manglende kalibrering af TSU, må TSU'en ikke udstede tidsstempler før der er iværksat foranstaltninger, der genopretter TSU'en.
- d) **[KRAV 7.13-06]** I tilfælde af kritisk kompromittering af TSA's drift eller manglende kalibrering skal TSA gøre beskrivelse af hændelsen til tilgængelig for alle abonnenter og modtagerparter. Beskrivelsen skal indeholde informationer, der gør det muligt at identificere de tidsstempler, der måtte være berørt, medmindre dette tilsidesætter TSA brugere privatlivsbeskyttelse eller sikkerheden for TSA's tjenester.

7.14 Ophør af TSA

[KRAV 7.14-01] Potentielle forstyrrelser for abonnenter og modtagerparter skal minimeres som følge af ophør af TSA's tjenester herunder skal oplysninger, der kræves for at verificere rigtigheden af tillidstjenesten, vedligeholdelse.

Særligt gælder at:

- **[KRAV 7.14-02]** TSA skal løbende vedligeholde en plan for ophør af TSA-tjenesterne.

Inden TSA afslutter sine tjenester, gælder skal følgende procedurer efterleves:

- a) **[KRAV 7.14-03]** Som led i at TSA ophører med at levere tjenester, skal TSA underrette følgende parter om ophøret: Alle abonnenter og andre parter, som TSP har aftaler med eller anden form for etablerede relationer, herunder eventuelle modtagerparter, andre relevante TSP'er samt relevante myndigheder herunder tilsynsmyndigheder.
 - b) **[KRAV 7.14-04]** Som led i at TSA ophører med at levere tjenester, skal TSA offentliggøre information om ophør for andre modtagerparter.
 - c) **[KRAV 7.14-05]** Som led i at TSA ophører med at levere tjenester, skal TSA lukke for autorisation for alle eventuelle underleverandører til at handle på vegne af TSA ved udførelse af funktioner i forbindelse med processen med udstedelse af tidsstempler.
 - d) **[KRAV 7.14-06]** Som led i at TSA ophører med at levere tjenester, skal TSA overføre forpligtelser til en pålidelig part for at opretholde al information, der er nødvendig for at dokumentere driften af TSA i en rimelig periode, medmindre TSA kan påvise, at TSA ikke har sådanne informationer.
 - e) **[KRAV 7.14-07]** Som led i at TSA ophører med at levere tjenester, skal TSA's private nøgler, herunder sikkerhedskopier, destrueres eller gøres utilgængelige for brug på en sådan måde, at de private nøgler ikke kan genskabes.
 - f) **[KRAV 7.14-08]** Hvis det er muligt, skal TSA forsøge at overdrage leverance af tillidstjenesten for de eksisterende kunder og brugere til en anden TSA.
- **[KRAV 7.14-09]** Ved ophør af TSA's tjenester skal TSA opretholde sine forpligtelser til at stille sine offentlige nøgler til rådighed for modtagerparter i en rimelig periode eller overføre disse forpligtelser til en anden pålidelig part.
 - **[KRAV 7.14-10]** Ved ophør af TSA's tjenester skal TSA sikre spærring af alle TSU'ers certifikater.
 - **[KRAV 7.14-11]** Hvis TSA er en privat virksomhed eller en fysisk person, skal CA stille en uigenkaldelig anfordringsgaranti eller lignende i et godkendt institut til sikring af betaling af sine økonomiske forpligtelser i henhold til KRAV 7.14-1 til KRAV 7.14-10.
 - **[KRAV 7.14-12]** TSA skal i sin TSA-praksis angive bestemmelser ved ophør af tjenesten. Disse skal som minimum inkludere
 - a) information om hvem der bliver notificeret ved ophør og
 - b) hvem, der overtager kunder og brugere, hvis der findes denne type aftaler.

7.15 Overensstemmelse

[KRAV 7.15-01] TSA skal sikre, at den agerer lovligt og troværdigt som en kvalificeret tillidstjeneste, der udsteder tidsstempler.

Særligt gælder at:

- **[KRAV 7.15-02]** TSA skal kunne dokumentere opfyldelse af gældende lovgivning. Herunder særligt eIDAS' regulering af kvalificerede tillidstjenester inklusiv eventuelle standarder som Kommissionen måtte pege på jf. [eIDAS] artikel 19 4.a).
- **[KRAV 7.15-03]** Tjenester og slutbrugerprodukter leveret af TSA skal være tilgængelige for personer med handicap, når det er muligt og der bør tages hensyn til gældende standarder for tilgængelighed som fx [ETSI EN 301 549].
- **[KRAV 7.15-04]** TSA skal træffes passende tekniske og organisatoriske foranstaltninger mod uautoriseret eller ulovlig behandling af personoplysninger og imod utilsigtet tab eller ødelæggelse eller beskadigelse af personoplysninger.

Bilag A

Denne politiks opfyldelse af krav til kvalificerede tidsstempler fastlagt i [ETSI EN 319 401] samt [ETSI EN 319 421] og [ETSI EN 319 422].

OPQT	ETSI EN 319 401	ETSI EN 319 421 + ETSI EN 319 422
KRAV 5.1-01		
KRAV 5.1-02	REQ-7.13-01	
KRAV 5.1-03		ETSI EN 319 421 afsnit 5.1
KRAV 5.2-01		ETSI EN 319 421 afsnit 5.2
KRAV 5.3.1-01		ETSI EN 319 421 afsnit 5.3.1
KRAV 5.3.1-02		ETSI EN 319 421 afsnit 5.3.1
KRAV 6.1-01	REQ-5-01	
KRAV 6.1-02	REQ-5-02	
KRAV 6.1-03	REQ-5-03	
KRAV 6.1-04	REQ-5-04	
KRAV 6.1-05	REQ-5-05	
KRAV 6.2-01	REQ-6.1-01 REQ-6.1-03 REQ-6.1-04 REQ-6.1-05	
KRAV 6.2-02	REQ-6.1-02 REQ-6.1-06 REQ-6.1-07	
KRAV 6.2-03	REQ-6.1-02 REQ-6.1-10	
KRAV 6.2-04	REQ-6.1-08	

	REQ-6.1-09	
KRAV 6.2-05	REQ-6.1-11 REQ-7.12-10	
KRAV 6.2-06		ETSI EN 319 421 afsnit 6.2
KRAV 6.2-07		ETSI EN 319 421 afsnit 6.2
KRAV 6.3-01	REQ-6.2-01	
KRAV 6.3-02	REQ-6.2-02	
KRAV 6.3-03	REQ-6.2-03	
KRAV 6.3-04	REQ-6.2-04	
KRAV 6.3-05	REQ-6.2-05	
KRAV 6.3-05	REQ-6.2-06	
KRAV 6.4-01		
KRAV 6.4-02	REQ-6.3-01	
KRAV 6.4-03	REQ-6.3-02	
KRAV 6.4-04	REQ-6.3-03	
KRAV 6.4-05	REQ-6.3-04	
KRAV 6.4-06	REQ-6.3-05	
KRAV 6.4-07	REQ-6.3-06	
KRAV 6.4-08	REQ-6.3-07	
KRAV 6.4-09	REQ-6.3-08	
KRAV 6.4-10	REQ-6.3-09	
KRAV 6.4-11	REQ-6.3-10	
KRAV 6.5.1-01		ETSI EN 319 421 afsnit 6.5.1
KRAV 6.5.2-01		ETSI EN 319 421 afsnit 6.5.2

KRAV 6.6-01		ETSI EN 319 421 afsnit 6.6
KRAV 7.1-01		ETSI EN 319 421 afsnit 7.2 b)
KRAV 7.2-01		ETSI EN 319 421 afsnit 7.2 a)
KRAV 7.2-02	REQ-7.1.1-01 REQ-7.1.1-02	
KRAV 7.2-03	REQ-7.1.1-03	
KRAV 7.2-04	REQ-7.1.1-04	
KRAV 7.2-05		
KRAV 7.2-06	REQ-7.1.1-05	
KRAV 7.2-07	REQ-7.1.1-06	
KRAV 7.2-08	REQ-7.1.1-07	
KRAV 7.2-09	REQ-7.1.2-01	
KRAV 7.3-01	REQ-7.2-01	
KRAV 7.3-02		ETSI EN 319 421 afsnit 7.2 c)
KRAV 7.3-03	REQ-7.2-03	
KRAV 7.3-04	REQ-7.2-02	
KRAV 7.3-05	REQ-7.2-04	
KRAV 7.3-06	REQ-7.2-05	
KRAV 7.3-07	REQ-7.2-06	
KRAV 7.3-08	REQ-7.2-07 REQ-7.2-08	
KRAV 7.3-09	REQ-7.2-09	
KRAV 7.3-10	REQ-7.2-10	
KRAV 7.3-11	REQ-7.2-11	

KRAV 7.3-12	REQ-7.2-12	
KRAV 7.3-13	REQ-7.2-13	
KRAV 7.3-14	REQ-7.2-14	
KRAV 7.3-15	REQ-7.2-15	
KRAV 7.3-16	REQ-7.2-16	
KRAV 7.3-17	REQ-7.2-17	
KRAV 7.4.1-01	REQ-7.3.1-01 REQ-7.3.1-02	
KRAV 7.4.2-01	REQ-7.3.2-01 REQ-7.4-10 REQ-7.7-06	
KRAV 7.5-01	REQ-7.4-01	
KRAV 7.5-02	REQ-7.4-02	
KRAV 7.5-03	REQ-7.4-03	
KRAV 7.5-04	REQ-7.4-04	
KRAV 7.5-05	REQ-7.4-05	
KRAV 7.5-06	REQ-7.4-06	
KRAV 7.5-07	REQ-7.4-07	
KRAV 7.5-08	REQ-7.4-08	
KRAV 7.5-09	REQ-7.4-09	
KRAV 7.6.1-01	REQ-7.5-01	
KRAV 7.6.2-01		ETSI EN 319 421 afsnit 7.6.2 a)
KRAV 7.6.2-02		ETSI EN 319 421 afsnit 7.6.2 b)
KRAV 7.6.2-03		ETSI EN 319 421 afsnit 7.6.2 c)

KRAV 7.6.2-04		ETSI EN 319 421 afsnit 7.6.2 d)
KRAV 7.6.2-05		ETSI EN 319 421 afsnit 7.6.2 e)
KRAV 7.6.2-06		ETSI EN 319 421 afsnit 7.6.2 f)
KRAV 7.6.3-01		ETSI EN 319 421 afsnit 7.6.3
KRAV 7.6.3-02		ETSI EN 319 421 afsnit 7.6.3 a)
KRAV 7.6.3-03		ETSI EN 319 421 afsnit 7.6.3 b)
KRAV 7.6.3-04		ETSI EN 319 421 afsnit 7.6.3 c)
KRAV 7.6.4-01		ETSI EN 319 421 afsnit 7.6.4
KRAV 7.6.4-02		ETSI EN 319 421 afsnit 7.6.4 a)
KRAV 7.6.4-03		ETSI EN 319 421 afsnit 7.6.4 b) ETSI EN 319 421 afsnit 8.1
KRAV 7.6.4-04		ETSI EN 319 421 afsnit 7.6.4 c)
KRAV 7.6.4-05		ETSI EN 319 421 afsnit 7.6.4
KRAV 7.6.5-01		ETSI EN 319 421 afsnit 7.6.5
KRAV 7.6.6-01		ETSI EN 319 421 afsnit 7.6.6
KRAV 7.6.6-02		ETSI EN 319 421 afsnit 7.6.6 a)
KRAV 7.6.6-03		ETSI EN 319 421 afsnit 7.6.6 b)
KRAV 7.6.6-04		ETSI EN 319 421 afsnit 7.6.6 c)
KRAV 7.6.6-05		ETSI EN 319 421 afsnit 7.6.6 d)
KRAV 7.6.7-01		ETSI EN 319 421 afsnit 7.6.7
KRAV 7.6.7-02		ETSI EN 319 421 afsnit 7.6.7
KRAV 7.6.7-03		ETSI EN 319 421 afsnit 7.6.7
KRAV 7.6.7-04		ETSI EN 319 421 afsnit 7.6.7
KRAV 7.6.7-05		ETSI EN 319 421 afsnit 7.6.7

KRAV 7.6.7-06		ETSI EN 319 421 afsnit 7.6.7
KRAV 7.6.7-07		ETSI EN 319 421 afsnit 7.6.7 a)
KRAV 7.6.7-08		ETSI EN 319 421 afsnit 7.6.7 b)
KRAV 7.7.1-01		ETSI EN 319 421 afsnit 7.7.1
KRAV 7.7.1-02		ETSI EN 319 422 afsnit 9.1
KRAV 7.7.1-03		ETSI EN 319 421 afsnit 7.7.1
KRAV 7.7.1-04		ETSI EN 319 421 afsnit 7.7.1 a)
KRAV 7.7.1-05		ETSI EN 319 421 afsnit 7.7.1 b)
KRAV 7.7.1-06		ETSI EN 319 421 afsnit 7.7.1 c)
KRAV 7.7.1-07		ETSI EN 319 421 afsnit 7.7.1 d)
KRAV 7.7.1-08		ETSI EN 319 421 afsnit 7.7.1 e)
KRAV 7.7.1-09		ETSI EN 319 421 afsnit 7.7.1
KRAV 7.7.1-10		ETSI EN 319 421 afsnit 7.7.1
KRAV 7.7.1-11		ETSI EN 319 421 afsnit 7.7.1
KRAV 7.7.2-01		ETSI EN 319 421 afsnit 7.7.2
KRAV 7.7.2-02		ETSI EN 319 421 afsnit 7.7.2 a)
KRAV 7.7.2-03		ETSI EN 319 421 afsnit 7.7.2 b)
KRAV 7.7.2-04		ETSI EN 319 421 afsnit 7.7.2 c)
KRAV 7.7.2-05		ETSI EN 319 421 afsnit 7.7.2 d)
KRAV 7.7.2-06		ETSI EN 319 421 afsnit 7.7.2 e)
KRAV 7.7.2-07		ETSI EN 319 421 afsnit 7.7.2 f)
KRAV 7.8-01	REQ-7.6-01	
KRAV 7.8-02	REQ-7.6-02	
KRAV 7.8-03	REQ-7.6-03	

	REQ-7.6-04	
KRAV 7.8-04	REQ-7.6-05	
KRAV 7.8-05		ETSI EN 319 421 afsnit 7.8 a)
KRAV 7.8-06		ETSI EN 319 421 afsnit 7.8 b)
KRAV 7.8-07		ETSI EN 319 421 afsnit 7.8 b)
KRAV 7.8-08		ETSI EN 319 421 afsnit 7.8 b)
KRAV 7.8-09		ETSI EN 319 421 afsnit 7.8 b)
KRAV 7.8-10		ETSI EN 319 421 afsnit 7.8 b)
KRAV 7.8-11		ETSI EN 319 421 afsnit 7.8
KRAV 7.9-01	REQ-7.7-01	
KRAV 7.9-02	REQ-7.7-02	
KRAV 7.9-03	REQ-7.7-03 REQ-7.7-04	
KRAV 7.9-04	REQ-7.7-05 REQ-7.7-09	
KRAV 7.9-05	REQ-7.7-06	
KRAV 7.9-06	REQ-7.7-07	
KRAV 7.9-07	REQ-7.7-08	
KRAV 7.9-08		ETSI EN 319 421 afsnit 7.9
KRAV 7.10-01	REQ-7.8-01	
KRAV 7.10-02	REQ-7.8-02	
KRAV 7.10-03	REQ-7.8-03	
KRAV 7.10-04	REQ-7.8-04	
KRAV 7.10-05	REQ-7.8-05	

KRAV 7.10-06		ETSI EN 319 421 afsnit 7.10 b)
KRAV 7.10-07	REQ-7.8-06	
KRAV 7.10-08		ETSI EN 319 421 afsnit 7.10 a)
KRAV 7.10-09	REQ-7.8-07	
KRAV 7.10-10	REQ-7.8-08	
KRAV 7.10-11	REQ-7.8-09	
KRAV 7.10-12	REQ-7.8-10	
KRAV 7.10-13	REQ-7.8-11	
KRAV 7.10-14	REQ-7.8-12	
KRAV 7.10-15	REQ-7.8-13	
KRAV 7.10-16	REQ-7.8-14 REQ-7.8-15	
KRAV 7.10-17		ETSI EN 319 421 afsnit 7.10 c)
KRAV 7.11-01	REQ-7.9-01	
KRAV 7.11-02	REQ-7.9-02	
KRAV 7.11-03	REQ-7.9-03	
KRAV 7.11-04	REQ-7.9-04	
KRAV 7.11-05	REQ-7.9-05	
KRAV 7.11-06	REQ-7.9-06	
KRAV 7.11-07	REQ-7.9-07	
KRAV 7.11-08	REQ-7.9-08	
KRAV 7.11-09	REQ-7.9-09	
KRAV 7.11-10	REQ-7.9-10	
KRAV 7.11-11	REQ-7.9-11	

KRAV 7.11-12	REQ-7.9-12	
KRAV 7.12-01	REQ-7.10-01	
KRAV 7.12-02	REQ-7.10-02 REQ-7.10-08	
KRAV 7.12-03	REQ-7.10-02 REQ-7.10-03	
KRAV 7.12-04	REQ-7.10-04	
KRAV 7.12-05	REQ-7.10-05	
KRAV 7.12-06	REQ-7.10-06	
KRAV 7.12-07	REQ-7.10-07	
KRAV 7.12-08	REQ-7.10-02 REQ-7.10-08	
KRAV 7.12-09		ETSI EN 319 421 afsnit 7.12 a)
KRAV 7.12-10		ETSI EN 319 421 afsnit 7.12 b)
KRAV 7.12-11		ETSI EN 319 421 afsnit 7.12 c)
KRAV 7.12-12		ETSI EN 319 421 afsnit 7.12 d)
KRAV 7.13-01	REQ-7.11-01	
KRAV 7.13-02	REQ-7.11-02	
KRAV 7.13-03		ETSI EN 319 421 afsnit 7.13 a)
KRAV 7.13-04		ETSI EN 319 421 afsnit 7.13 b)
KRAV 7.13-05		ETSI EN 319 421 afsnit 7.13 c)
KRAV 7.13-06		ETSI EN 319 421 afsnit 7.13 d)
KRAV 7.14-01	REQ-7.12-01	
KRAV 7.14-02	REQ-7.12-02	

KRAV 7.14-03	REQ-7.12-03	
KRAV 7.14-04	REQ-7.12-04	
KRAV 7.14-05	REQ-7.12-05	
KRAV 7.14-06	REQ-7.12-06	
KRAV 7.14-07	REQ-7.12-07	
KRAV 7.14-08	REQ-7.12-08	
KRAV 7.14-09	REQ-7.12-11	
KRAV 7.14-10		ETSI EN 319 421 afsnit 7.14 a)
KRAV 7.14-11	REQ-7.12-09	
KRAV 7.14-12	REQ-7.12-10	
KRAV 7.15-01	REQ-7.13-01	
KRAV 7.15-02	REQ-7.13-02	
KRAV 7.15-03	REQ-7.13-03 REQ-7.13-04	
KRAV 7.15-04	REQ-7.13-05	