DIGITALISERINGSSTYRELSEN

Offentlig politik for kvalificeret signatur- og seglvalidering

Version 1.1

Oktober 2021

DIGITALISERINGSSTYRELSEN

Indholdsfortegnelse

DIGITALISERINGSSTYRELSEN

DIGITALISERINGSSTYRELSEN

DIGITALISERINGSSTYRELSEN

1. Indledning

1.1 Introduktion

Hvis man ønsker at fæste tillid til elektroniske signaturer eller elektroniske segl, er det væsentligt at have en tillidsfuld proces for validering, der indeholder alle nødvendige kontroller til sikring af, at den elektroniske signatur eller det elektroniske segl var gyldig på underskriftstidspunktet. En modtager af data med elektroniske signaturer eller elektroniske segl kan enten vælge selv at gennemføre en validering eller anvende en tillidstjeneste, der tilbyder validering af elektroniske signaturer og elektroniske segl. Jf. [eIDAS] er en sådan valideringsservice en elektronisk tillidstjeneste og er dermed underlagt eIDAS-reguleringen af tillidstjenester, hvis den ikke er undtaget jf. artikel 2. Det betyder samtidig, at en valideringstjeneste kan opnå status som kvalificeret tillidstjeneste, hvis kravene til kvalificerede tillidstjenester er opfyldt.

Den samlede sikkerhed for validering af elektroniske signaturer og elektroniske segl er afhængig af processerne for validering samt den underliggende forretningsførelse af valideringsservice. Denne valideringspolitik fastlægger krav til udbydere, som ønsker at udbyde en kvalificeret valideringstjeneste for validering af elektroniske signaturer og elektroniske segl jf. [eIDAS]. Dette kan både være kvalificerede elektroniske signaturer og segl samt ikke-kvalificerede elektroniske signaturer og segl. Udbydere kan vælge at anvende alternative valideringspolitikker, hvis disse lever op til kravene i [eIDAS].

Dette dokument er udformet til at leve op til kravene i [ETSI EN 319 401] og [ETSI EN 319 102-1].

Der findes en række tekniske specifikationer fra ETSI som en VA frivilligt kan vælge at indarbejde i VA's valideringstjeneste. Dette vil eventuelt lette arbejdet for VA, hvis disse specifikationer på et senere tidspunkt gøres til europæisk norm inkluderet i fremtidige versioner af denne politik:

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
- ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services
- ETSI TS 119 102-2 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report

1.2 Dokumentnavn

Dette dokument med navnet "Offentlig politik for kvalificeret signatur- og seglvalidering", forkortet OPQV, beskriver en offentlig politik for kvalificeret validering af elektroniske signaturer og elektroniske segl. Den seneste version af denne politik for validering 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.

DIGITALISERINGSSTYRELSEN

1.3.2 Kontaktinformation

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 godkendes af Digitaliseringsstyrelsen efter en offentlig høringsproces.

1.3.4 Offentliggørelse

[KRAV 1.3.4-01] Kvalificerede tillidstjenesteudbydere, der validerer elektroniske signaturer og elektroniske segl efter 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.

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 319 102-1]	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation - Version 1.1.1 (2016-05)
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

DIGITALISERINGSSTYRELSEN

3. Definitioner og forkortelser

3.1 Definitioner

B-signatur: En signatur eller et segl, der kan valideres så længe de korresponderende certifikater ikke er spærrede jf. *Basic Signature* defineret i [ETSI EN 319 102-1] afsnit 4.3.1.

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.

Elektronisk signatur: Data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre data i elektronisk form, og som anvendes af underskriveren til at skrive under med.

Elektronisk segl: Data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre data i elektronisk form, og som giver sikkerhed for disse tilknyttede datas oprindelse og integritet.

LTA-signatur: En signatur eller et segl med langtidstilgængelighed og integritet af valideringsdata jf. *Signature providing Long Term Availability and Integrity of Validation Material* defineret i [ETSI EN 319 102-1] afsnit 4.3.1.

LTV-signatur: En signatur eller et segl med indarbejdet valideringsdata jf. *Signature with Long-Term Validation Material* defineret i [ETSI EN 319 102-1] afsnit 4.3.1.

Signatur med tidsstempel: En signatur eller et segl med indarbejdet tidsstempling jf. *Signature with Time* defineret i [ETSI EN 319 102-1] afsnit 4.3.1.

Valideringspolitik: Et sæt regler, der angiver krav til validering af elektroniske signaturer og/eller elektroniske segl. Nærværende dokument er en valideringspolitik.

Valideringstjenesteudbyder (VA): En udbyder af tillidstjeneste til validering af elektroniske signaturer og/eller elektroniske segl jf. eIDAS artikel 3 litra 16) a).

3.2 Forkortelser

AdES	"Advanced Electronic Signature"
BCP	"Business Continuity Plan"
CA	Certificeringscenter ("Certificate Authority")
ETSI	"European Telecommunications Standards Institute"
TSL	"Trusted Service List"
UTC	Fælles tidsangivelse ("Universal Time Coordinated")
VA	Valideringstjenesteudbyder ("Validation Authority")

DIGITALISERINGSSTYRELSEN

4. Generelt konceptbeskrivelse

4.1 Generelt om krav til tillidstjenesteudbydere, der validerer elektroniske signaturer og elektroniske sejl

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

[ETSI EN 319 401] indeholder generelle krav til tillidstjenesteudbydere, mens [ETSI EN 319 102-1] stiller specifikke krav til signatur- og seglgenerering samt signatur- og seglvalidering for signaturer og segl i AdES-format.

4.2 Valideringstjeneste og valideringsservice

En valideringsservice kan både anvendes internt i en organisation og som en service for eksterne parter. Hvis servicen udbydes generelt, vil udbyderen typisk være en tillidstjenesteudbyder, der er reguleret af [eIDAS]. En valideringstjeneste kan være kvalificeret jf. [eIDAS] artikel 32 og artikel 33.

I det følgende benævnes en kvalificeret tillidstjenesteudbyder, der udbyder en valideringsservice med validering af elektroniske signaturer eller elektroniske segl, for en kvalificeret valideringstjenesteudbyder (forkortet VA).

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

4.3 Abonnent

En abonnent er en fysisk eller en juridisk person, der efter aftale med VA, kan få valideret en elektronisk signatur eller et elektronisk segl.

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 forhold 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 VA's tjenester.

4.4 Valideringspolitik og VA-praksis

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

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

DIGITALISERINGSSTYRELSEN

5. Introduktion til valideringspolitik og Generelle krav

5.1 Generelt krav

[KRAV 5.1-01] VA'er, der validerer elektroniske signaturer eller elektroniske segl under denne politik, skal være en kvalificeret tillidstjenesteudbyder jf. [eIDAS].

[KRAV 5.1-02] VA skal efterleve krav i eIDAS artikel 32, eIDAS artikel 33 og eIDAS artikel 40.

5.2 Identifikation

Denne politik er identificeret som "Offentlig politik for kvalificeret signatur- og seglvalidering - Version 1.0"

6. Politik og implementering

6.1 Risikovurdering

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

[KRAV 6.1-02] VA 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] VA skal fastlægge og dokumentere alle sikkerhedskrav og operationelle procedure, der er nødvendige for overholdelse af denne politik. Dokumentationen skal være en del af VA-praksis jf. afsnit 6.2.

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

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

6.2 VA-praksis

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

[KRAV 6.2-02] VA's ledelse skal have ansvaret for og godkende den samlede VA-praksis og sikre korrekt implementering, herunder at praksissen er i overensstemmelse med denne politik og er kommunikeret til relevante medarbejdere og partnere.

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

DIGITALISERINGSSTYRELSEN

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

[KRAV 6.2-05] VA skal i VA-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] Den offentlige del af VA-praksis skal som minimum indeholde:

a) angivelse af hvilke CA rodcertifikater, der indgår i VA's tillidsanker
b) enhver begrænsning af brugen af valideringstjenesten
c) eventuelle forpligtelser for abonnenten

Note: I forhold til punkt a) i ovenstående kan VA vælge at angive en klasse af rodcertifikater, hvis der samtidig findes en henvisning til, hvilke CA rodcertifikater klassen indeholder. Fx kan VA angive, at VA's tillidsanker består af alle CA rodcertifikater, der findes på EU Kommissionen TSL.

[KRAV 6.2-07] VA-praksis bør indeholde evt. oppetidsbegrænsninger af VA's tjeneste.

6.3 Vilkår og betingelser

[KRAV 6.3-01] VA 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 tjenesten, herunder VA's ansvarsbegrænsning i forhold til forkert brug af tjenesten,
h) lovvalg
i) procedure for tvister,
j) at VA er en kvalificeret tillidstjeneste jf. eIDAS-forordningen,
k) VA'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.

DIGITALISERINGSSTYRELSEN

[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.

[KRAV 6.3-07] VA skal have politikker og procedurer til løsning af klager og tvister modtaget fra kunder eller andre afhængige parter om leveringen af ydelserne eller andre relaterede forhold og skal være i overensstemmelse med VA's vilkår og betingelser.

[KRAV 6.3-08] Kan en tvist ikke løses forligsmæssigt, kan enhver af parterne vælge at indbringe tvisten for de almindelige domstole. Værneting er København. Dansk ret er gældende.

6.4 Informationssikkerhedspolitik

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

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

[KRAV 6.4-03] Ændringer i politik for informationssikkerhed skal kommunikeres til tredjeparter, hvor det er relevant. Dette kan inkludere abonnenter, overensstemmelsesvurderingsorgan, tilsyn og andre myndigheder.

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

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

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

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

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

[KRAV 6.4-08] VA'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 VA's ledelse.

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

DIGITALISERINGSSTYRELSEN

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

7. VA styring og drift

7.1 Introduktion

[KRAV 7.1-01] VA skal have et system eller systemer til kvalitetsstyring og informationssikkerhedsstyring, der er passende for de valideringstjenester som udbydes.

7.2 Intern organisation

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

[KRAV 7.2-02] VA-organisationen skal agere pålideligt og ikke-diskriminerende.

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

Note: VA har mulighed for at begrænse driftsområdet for sine tjenester, og VA bør offentliggøre sit driftsområde i sin praksis. Eksempelvis kan VA angive, at valideringer udelukkende udføres for et fastlagt antal abonnenter og for elektroniske signaturer og elektroniske segl, hvor der er anvendt certifikater fra et antal specificerede CA'er.

[KRAV 7.2-04] VA 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 VA er en privat virksomhed, skal VA 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] VA 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 VA opererer i, herunder men ikke begrænset til antallet af kunder og den finansielle risiko, som VA påtager sig i forhold til de validerede elektroniske signaturer og elektroniske segl.

[KRAV 7.2-07] VA 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] VA skal have skriftlige dokumenterede 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 VA's aktiver.

DIGITALISERINGSSTYRELSEN

7.3 Personalesikkerhed

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

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

[KRAV 7.3-03] Herunder skal VA's personale inklusiv 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] VA 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 personoplysninger, der er relevant for de udbudte tjenester og jobfunktionen.

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

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

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

[KRAV 7.3-08] Betroede roller, hvoraf VA'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 tildeles rollen.

[KRAV 7.3-10] VA's personale (både midlertidigt og permanent) skal have jobbeskrivelser defineret ud fra de roller, som de skal udfylde under hensyntagen til adskillelse af pligter (segregation of duties), mindsteprivilegier (least priviledge), 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 VA-specifikke funktioner. Sidstnævnte bør omfatte krav til færdigheder og erfaring.

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

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

[KRAV 7.3-14] Alle VA's medarbejdere med betroede roller skal være fri for interessekonflikter, der kan skade uafhængigheden af VA'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 VA's kritiske systemer til service management inklusive systemgenskabelse.

c) Systemoperatører: Ansvarlig for driften af VA's kritiske systemer på daglig basis. Autoriseret til at udføre sikkerhedskopi af systemer.

d) Systemrevisorer: Autoriseret til at se lagrede data og audit-logfiler fra VA'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] Personalet 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] VA skal vedligeholde en oversigt over aktiver herunder informationsaktiver. Alle informationsaktiver skal klassificeres i henhold til VA's risikovurdering, og VA skal sikre en tilstrækkelig beskyttelse af alle aktiver.

7.4.2 Håndtering af medier

[KRAV 7.4.2-01] Alle medier i VA'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] VA skal implementere en effektiv adgangskontrol, der beskytter mod uautoriseret fysisk eller logisk adgang til VA's systemer.

Særligt gælder det, at:

- **[KRAV 7.5-02]** VA skal implementere foranstaltninger (fx firewalls), der beskytter VA'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 VA.
- **[KRAV 7.5-04]** VA 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.

DIGITALISERINGSSTYRELSEN

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

7.6 Kryptografiske kontroller

7.6.1 Generelle kontroller

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

7.7 Validering

7.7.1 Generel om validering

[KRAV 7.7.1-01] VA's udbudte tjeneste til validering af elektroniske signaturer og elektroniske segl under denne politik skal validere elektroniske signaturer og elektroniske segl i overensstemmelse med politikken under hensyntagen til eventuelle begrænsninger, som beskrevet herunder eller i den offentlige del af VA-praksis.

Herunder gælder særligt at:

[KRAV 7.7.1-02] VA skal præsentere resultatet af valideringen inklusiv relevante detaljer og eventuelle begrænsninger relevante for den validerende part, der skal fortolke resultatet.

[KRAV 7.7.1-03] Medmindre den validerende part anmoder om andet, skal valideringen indledes med "Validation process for Signature providing Long Term Availability and Integrity of Validation Material" jf. [ETSI EN 319 102-1] afsnit 5.6.3.

[KRAV 7.7.1-04] Status på en validering skal være en af følgende:

TOTAL-PASSED:

Når kryptografiske kontroller af signaturen eller seglet (inklusiv kontroller af hashværdier for dataobjekter, der er signeret indirekte) er gennemført med succes, herunder at alle kontroller beskrevet i denne politik er gennemført med succes.

TOTAL-FAILED:

DIGITALISERINGSSTYRELSEN

Når en kryptografisk kontrol er fejlet (inklusiv kontrol af hashværdier for dataobjekter, der er signeret indirekte), eller det er fastlagt, at generering af signaturen eller seglet er foretaget efter, at signeringscertifikatet blev spærret, eller fordi signaturen eller seglet ikke er i overensstemmelse med basisstandarder, således at det ikke er muligt at processere de kryptografiske elementer i signaturen.

INDETERMINATE:

Når resultatet af de gennemførte kontroller ikke gør det muligt at placere signaturen eller seglet i *TOTAL-PASSED* eller *TOTAL-FAILED*.

Note: Det er tilladt at præsentere status uden anvendelse af termerne TOTAL-PASSED, TOTAL-FAILED og INDETERMINATE, så længe det ikke er muligt at misforstå, hvilken af de tre typer resultatet dækker over.

[KRAV 7.7.1-05] Ovenstående status skal være suppleret med detaljeret information som specificeret i [ETSI EN 319 102-1] afsnit 5.1.3.

Note: Resultatet kan, hvor det er relevant, være præsenteret i niveauer, så det overordnede resultat præsenteres først, mens tekniske detaljer skjules i undermenuer eller lignende.

Note: VA kan implementere validering som en eller flere forskellige løsninger, herunder men ikke nødvendigvis begrænset til:

- En del af softwaren, der afvikles på en PC med grafisk brugergrænseflade,
- En webservice,
- En webapplikation,
- Et kommandolinjeværktøj og
- Et SDK eller middleware for andre applikationer.

7.7.2 Valg af valideringsproces

[KRAV 7.7.2-01] Alle krav i [ETSI EN 319 102-1] afsnit 5.1.2 skal efterleves.

7.7.3 Status af valideringsproces og valideringsrapport

[KRAV 7.7.3-01] Alle krav i [ETSI EN 319 102-1] afsnit 5.1.3 skal efterleves.

7.7.4 Valideringsbegrænsninger

[KRAV 7.7.4-01] Alle krav i [ETSI EN 319 102-1] afsnit 5.1.4 skal efterleves.

7.7.5 Kontrol af format

[KRAV 7.7.5-01] Formatet skal kontrolleres i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.2.

DIGITALISERINGSSTYRELSEN

7.7.6 Identifikation af signerings- eller seglcertifikat

[KRAV 7.7.6-01] Signerings- eller seglcertifikatet skal identificeres i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.3.

7.7.7 Initial kontekst validering

[KRAV 7.7.7-01] Initialisering af valideringskontekst skal ske i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.4.

7.7.8 Kontrol af, at statusinformation er ajourført

[KRAV 7.7.8-01] Kontrol af, at statusinformation er ajourført, skal ske i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.5.

7.7.9 Validering af X.509 certifikat

[KRAV 7.7.9-01] Validering af signerings- eller seglcertifikatet skal ske i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.6. Chain-modellen skal understøttes, og shell-modellen kan understøttes.

[KRAV 7.7.9-02] VA skal angive, hvilke modeller der understøttes i den offentlige del af VA-praksis.

7.7.10 Kryptografiske kontroller

[KRAV 7.7.10-01] Den kryptografiske integritet af de signerede data skal ske i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.7.

7.7.11 Signatur- eller seglaccept validering

[KRAV 7.7.11-01] Ekstra verifikation af signatur eller segl skal ske i overensstemmelse med [ETSI 319 102-1] afsnit 5.2.8.

7.7.12 Visning af valideringsresultat

[KRAV 7.7.12-01] Visning af valideringsresultat skal ske i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.2.9.

7.7.13 Validering af B-signatur

[KRAV 7.7.13-01] Validering af en B-signatur skal være i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.3.

7.7.14 Validering af tidsstempler

[KRAV 7.7.14-01] Validering af tidsstempler skal være i overensstemmelse med [ETSI EN 319 102-1] afsnit 5.4.

DIGITALISERINGSSTYRELSEN

7.7.15 Validering af signaturer med tidsstempler og LTV-signaturer

[KRAV 7.7.15-01] Validering af signaturer med tidsstempler og LTV-signaturer skal være i overensstemmelse med [ETSI 319 102-1] afsnit 5.5.

7.7.16 Validering af LTA-signaturer

[KRAV 7.7.16-01] Validering af LTA-signaturer skal være i overensstemmelse med [ETSI 319 102-1] afsnit 5.6.

7.8 Fysisk og miljømæssig sikkerhed

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

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

[KRAV 7.8-03] VA 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 VA, skal befinde sig inden for en beskyttet sikkerhedsperimeter med fysisk beskyttelse mod indtrængen, adgangskontrol og alarmer for at opdage indtrængen.

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

[KRAV 7.9-04] Integriteten i VA's systemer og data skal beskyttes mod vira, malware og uautoriseret software, herunder skal VA 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 VA'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] VA skal have mediehåndteringsprocesser, der sikrer medier mod forældelse og degenerering i den periode, hvor data skal lagres.

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

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

7.10 Netværkssikkerhed

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

Særligt gælder at:

- **[KRAV 7.10-02]** VA 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]** VA skal sikre, at adgang til og kommunikation mellem zoner begrænses til det nødvendige.
- **[KRAV 7.10-05]** VA skal eksplicit blokere eller deaktivere forbindelser og services, der ikke skal anvendes.
- **[KRAV 7.10-07]** VA skal regelmæssigt gennemgå fastlagte netværks- og firewallregler.
- **[KRAV 7.10-09]** Særligt kritiske systemer skal placeres i særligt sikrede zoner.
- **[KRAV 7.10-10]** VA skal adskille dedikeret netværk til administration af it-systemer og VA's driftsnetværk.
- **[KRAV 7.10-11]** VA må ikke anvende systemer, der anvendes til administration af implementeringen af sikkerhedspolitikken til andre formål.
- **[KRAV 7.10-12]** VA skal holde driftssystemer adskilt fra udviklings- og testsystemer.
- **[KRAV 7.10-13]** VA 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]** VA skal sikre ekstern netværksredundans for systemer med høje krav til tilgængelighed fra eksterne kilder.

DIGITALISERINGSSTYRELSEN

- **[KRAV 7.10-15]** Mindst én gang hvert kvartal skal VA udføre sårbarhedsscanning 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]** Mindst én gang årligt , efter etablering og ved væsentlige ændringer og opdateringer i infrastrukturen eller i de anvendte applikationer skal VA udføre penetrationstest. Penetrationstesten gennemføres af en part med færdigheder, værktøjer, etisk kodeks og uafhængighed, som er nødvendigt for at kunne give en pålidelig rapport. Penetrationstesten skal dokumenteres.

7.11 Hændelseshåndtering

[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 VA's netværk, skal registreres og rapporteres som alarmer.
- **[KRAV 7.11-04]** VA skal overvåge følgende hændelser:
    a) opstart og nedlukning af logfunktionerne og
    b) tilgængelighed og brug af nødvendige tjenester med VA's netværk.
- **[KRAV 7.11-05]** VA skal handle rettidigt og koordineret for at reagere hurtigt på sikkerhedshændelser og begrænse konsekvenserne af sikkerhedsbrud.
- **[KRAV 7.11-06]** VA skal have personale med betroede roller til opfølgning på advarsler om potentielt kritiske sikkerhedshændelser, hvilket sikrer, at relevante hændelser rapporteres i overensstemmelse med VA's procedurer.
- **[KRAV 7.11-07]** VA skal have procedurer og beredskab, der sikrer notifikation af sikkerhedshændelser 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 VA også notificere denne uden unødig forsinkelse.
- **[KRAV 7.11-09]** VA's systemer skal overvåges, hvilket skal omfatte monitorering eller regelmæssig gennemgang af auditlogs for at identificere ondsindet aktivitet med henblik på at alarmere potentielle kritiske sikkerhedshændelser til sikkerhedspersonale.
- **[KRAV 7.11-10]** VA skal håndtere enhver kritisk sårbarhed, som ikke tidligere er håndteret af VA, inden for 48 timer efter at den er identificeret.

- **[KRAV 7.11-11]** For enhver identificeret sårbarhed skal VA i forhold til de potentielle skader enten:
  a) oprette og implementere en plan for mitigering af sårbarheden eller
  b) dokumentere grundlaget for VA'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] VA skal registrere og kunne tilgå alle relevante oplysninger vedrørende data genereret og modtaget af VA i et passende tidsrum, herunder efter ophør af aktiviteterne i VA, navnlig med henblik på at kunne fremlægge bevismateriale i retssager og kunne sikre tjenestens kontinuerte drift.

Særligt gælder at:

- **[KRAV 7.12-02]** VA skal sikre fortroligheden og integriteten af lagrede data relateret til driften af VA's services.
- **[KRAV 7.12-03]** VA skal sikre komplethed, fortroligheden og integriteten af lagrede data relateret til driften af VA's services i henhold til dokumenteret forretningspraksis offentliggjort i VA-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 auditlogning, skal synkroniseres med UTC mindst en gang dagligt.
- **[KRAV 7.12-07]** Data, relateret til VA's services, skal lagres i et passende tidsrum, for at tilvejebringe nødvendige juridiske beviser, og som angivet i VA's vilkår og betingelser.
- **[KRAV 7.12-08]** Hændelser skal logges på en måde, så loggen ikke let kan slettes eller ødelægges i den periode, som loggen skal gemmes (medmindre den er overflyttet sikkert til medie til langtidsopbevaring).

7.13 Business Continuity Plan

[KRAV 7.13-01] VA 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 VA's private signeringsnøgler, hvis sådanne eksisterer, skal driften genoprettes inden for den frist, der er fastlagt i BCP, idet årsagen til katastrofen er håndteret med passende afhjælpende foranstaltninger.

DIGITALISERINGSSTYRELSEN

7.14 Ophør af VA

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

Særligt gælder at:

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

  Inden VA afslutter sine tjenester, skal følgende procedurer efterleves:

  a) **[KRAV 7.14-03]** Som led i at VA ophører med at levere tjenester, skal VA underrette følgende parter om ophøret: Alle abonnenter og andre parter, som VA 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 VA ophører med at levere tjenester, skal VA offentliggøre information om ophør for andre modtagerparter.
  c) **[KRAV 7.14-05]** Som led i at VA ophører med at levere tjenester, skal VA lukke for autorisation for alle eventuelle underleverandører til at handle på vegne af VA ved udførelse af funktioner i forbindelse med processen med validering af elektroniske signaturer og elektroniske segl.
  d) **[KRAV 7.14-06]** Som led i at VA ophører med at levere tjenester, skal VA overføre forpligtelser til en pålidelig part for at opretholde al information, der er nødvendig for at dokumentere driften af VA i en rimelig periode, medmindre VA kan påvise, at VA ikke har sådanne informationer.
  e) **[KRAV 7.14-07]** Som led i at VA ophører med at levere tjenester, skal VA'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 VA forsøge at overdrage leverance af tillidstjenesten for de eksisterende kunder og brugere til en anden VA.

- **[KRAV 7.14-09]** Ved ophør af VA's tjenester skal VA 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 7.14-11]** Hvis VA er en privat virksomhed, skal VA 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 7.14-09.

- **[KRAV 7.14-12]** VA skal i sin VA-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.

DIGITALISERINGSSTYRELSEN

7.15 Overensstemmelse

[KRAV 7.15-01] VA skal sikre, at den agerer lovligt og troværdigt som en kvalificeret tillidstjeneste, der validerer elektroniske signaturer og elektroniske segl .

Særligt gælder at:

- **[KRAV 7.15-02]** VA 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 VA 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]** VA skal træffe passende tekniske og organisatoriske foranstaltninger mod uautoriseret eller ulovlig behandling af personoplysninger og imod utilsigtet tab eller ødelæggelse eller beskadigelse af personoplysninger.

DIGITALISERINGSSTYRELSEN

Bilag A

Denne politiks opfyldelse af krav til kvalificerede valideringstjenester fastlagt i [ETSI EN 319 401] og [ETSI EN 319 102-1].

QVA	ETSI EN 319 401	ETSI EN 319 102-1
KRAV 1.3.4-01		
KRAV 5.1-01		
KRAV 5.1-02		
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		
KRAV 6.2-07		
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 6.3-06	REQ-6.2-06	
KRAV 6.3-07		
KRAV 6.3-08		
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	

DIGITALISERINGSSTYRELSEN

KRAV 6.4-10	REQ-6.3-09	
KRAV 6.4-11	REQ-6.3-10	
KRAV 7.1-01		
KRAV 7.2-01		
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		
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	

DIGITALISERINGSSTYRELSEN

KRAV 7.6.1-01	REQ-7.5-01	
KRAV 7.7.1-01		ETSI EN 319 102-1 afsnit 5.1.1
KRAV 7.7.1-02		ETSI EN 319 102-1 afsnit 5.1.1
KRAV 7.7.1-03		ETSI EN 319 102-1 afsnit 5.1.1
KRAV 7.7.1-04		ETSI EN 319 102-1 afsnit 5.1.1
KRAV 7.7.1-05		ETSI EN 319 102-1 afsnit 5.1.1
KRAV 7.7.2-01		ETSI EN 319 102-1 afsnit 5.1.2
KRAV 7.7.3-01		ETSI EN 319 102-1 afsnit 5.1.3
KRAV 7.7.4-01		ETSI EN 319 102-1 afsnit 5.1.4
KRAV 7.7.5-01		ETSI EN 319 102-1 afsnit 5.2.2
KRAV 7.7.6-01		ETSI EN 319 102-1 afsnit 5.2.3
KRAV 7.7.7-01		ETSI EN 319 102-1 afsnit 5.2.4
KRAV 7.7.8-01		ETSI EN 319 102-1 afsnit 5.2.5
KRAV 7.7.9-01		ETSI EN 319 102-1 afsnit 5.2.6
KRAV 7.7.9-02		
KRAV 7.7.10-01		ETSI EN 319 102-1 afsnit 5.2.7
KRAV 7.7.11-01		ETSI EN 319 102-1 afsnit 5.2.8
KRAV 7.7.12-01		ETSI EN 319 102-1 afsnit 5.2.9
KRAV 7.7.13-01		ETSI EN 319 102-1 afsnit 5.3
KRAV 7.7.14-01		ETSI EN 319 102-1 afsnit 5.4
KRAV 7.7.15-01		ETSI EN 319 102-1 afsnit 5.5
KRAV 7.7.16-01		ETSI EN 319 102-1 afsnit 5.6
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 7.8-11		
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		
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 7.10-07	REQ-7.8-06	
KRAV 7.10-09	REQ-7.8-07	

DIGITALISERINGSSTYRELSEN

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 7.11-01	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 7.13-01	REQ-7.11-01	
KRAV 7.13-02	REQ-7.11-02	
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 7.14-11	REQ-7.12-09	
KRAV 7.14-12	REQ-7.12-10	
KRAV 7.15-01	REQ-7.13-01	

DIGITALISERINGSSTYRELSEN

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	