Signaturpolitik vedrørende Official Journal-signatur

Version 4

(1.3.171.4.1.1.4)

Gældende pr. 1. oktober 2023

Indholdsfortegnelse

1 Indledning

Dette dokument beskriver signaturpolitikken for Official Journal-signaturen (OJ-signatur) og Official Journal-seglet (OJ-segl), som anvendes til at autentificere den elektroniske udgave af Den Europæiske Unions Tidende (EUT = OJ) i henhold til Rådets forordning (EU) nr. 216/2013 om elektronisk offentliggørelse af Den Europæiske Unions Tidende[1].

En signaturpolitik er et regelsæt, der vedrører genereringen, valideringen og udvidelsen af én eller flere sammenhørende elektroniske signaturer og/eller segl, og som fastsætter tekniske og proceduremæssige krav til generering, validering og langsigtet administration af sådanne signaturer for at imødekomme særlige forretningsmæssige krav og for at fastlægge, hvornår de er gyldige. Formålet med en signaturpolitik er også at synliggøre alle aspekter af en given signatur- og/eller seglarbejdsgang for alle involverede parter, nemlig underskrivere, modtagere og voldgiftsmænd, således at elektroniske signaturer og segl, der opfylder politikkens krav, kan skabe øget tillid ved anvendelse og accept af disse signaturer og segl.

De nærmere begreber i forbindelse med en signaturpolitik er forklaret i [ETSI 2015], der også fastlægger retningslinjerne og strukturen for dette dokument. Nøgleordene "SKAL", "MÅ", "MÅ IKKE", "PÅKRÆVET", "BØR", "BØR IKKE", "ANBEFALET", "KAN" og "VALGFRI" skal i dette dokument fortolkes som beskrevet i RFC 2911 [Bradner 1997].

OJ offentliggøres af Den Europæiske Unions Publikationskontor (OP) på EUR-Lex-webstedet (se afsnit 1.2.4) som den eneste autentiske kilde til EU-lovgivning. OJ offentliggøres fra mandag til fredag og eventuelt i weekenden på alle Den Europæiske Unions (EU's) officielle sprog. *I det følgende anvendes akronymet "OJ" som en samlet betegnelse for dette særlige anvendelsesområde.*

1.1 Oversigt

OJ-signaturpolitikken formaliserer hovedelementerne i implementeringen af genereringen, valideringen og den langsigtede bevarelse af elektroniske signaturer og segl, når den anvendes i forbindelse med OJ som et middel til autentificering af OJ-numre, der offentliggøres af OP. Den består af:

- en indledning, der omfatter titel på og identifikation af politikken, oplysninger om udstederen af politikken, administration af politikken, definitioner og akronymer mv.
- erklæringer om praksis for signaturanvendelse, som fastlægger de tilknyttede politiske og juridiske krav, samt de relevante sikkerhedsovervejelser
- parametrene for forretningsanvendelsesområde, som beskriver de arbejdsgange, der er involveret i generering af elektroniske signaturer og segl, som autentificerer de OJ-numre, der offentliggøres af OP
- krav til og erklæringer om tekniske mekanismer og implementering af standarder samt bilag.

[1] Se EUT L 69 af 13.3.2013, s. 1.

1.2 Forretningsområde

1.2.1 Anvendelsesområde for og afgrænsning af signaturpolitikken

OJ-signaturpolitikken omfatter elektroniske signaturer og segl, der genereres for hvert enkelt OJ-nummer af bemyndigede OJ-underskrivere i overensstemmelse med Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende efter validering af hvert nummer, der skal signeres.

1.2.2 Anvendelsesområde

De elektroniske signaturer og segl, der er omfattet af OJ-signaturpolitikken, er udelukkende dem, der er beskrevet i afsnit 3.1.

1.2.3 Transaktionskontekst

Ikke relevant.

1.3 Signaturpolitikkens navn, identifikations- og overensstemmelsesregler

1.3.1 Politikkens titel

OJ-signaturpolitikkens titel er som følger:

Signaturpolitik vedrørende Official Journal-signatur

1.3.2 Politikkens identifikation

Da der kun er én udgave af Den Europæiske Unions Tidende, og offentliggørelsen er en velkendt proces i Den Europæiske Union, kan OJ-signaturpolitikken identificeres implicit af en hvilken som helst part. En beskrivelse af den generelle arbejdsgang findes i afsnit 3.1.1.1.

Når politikken skal angives eksplicit, *KAN* hver enkelt OJ-signatur og hvert enkelt OJ-segl indeholde en eksplicit signaturpolitikangivelse som fastlagt i afsnit 5.2.9 i [ETSI 2022-XAdES]. Såfremt den eksplicitte signaturpolitikangivelse medtages, SKAL den angive objektidentifikatoren 1.3.171.4.1.1.4 under anvendelse af de grundformater, der er fastsat i afsnit 5.2.9 i [ETSI 2022-XAdES] og i [Mealling 2010].

Den globalt unikke objektidentifikator 1.3.171.4.1.1.4 identificerer entydigt denne version af signaturpolitikken. Præfikset 1.3.171.4 er registreret som grund-OID for *signaturpolitikker og til EU's Publikationskontors andre formål* (se http://www.oid-info.com/get/1.3.171.4). Suffikset 1.1.4 identificerer den nuværende version af OJ-signaturpolitikken, og dens ASN.1-værdinotation med navne SKAL være oj(1) signature-policy(1) version(4). Med denne version forældes version 1.1.3 af denne politik.

1.3.3 Politikkens konformitetsbestemmelser

Den nuværende politik kræver ikke konformitet med nogen anden signaturpolitik.

1.3.4 Politikkens distributionspunkter

OJ-signaturpolitikken offentliggøres på EUR-Lex-webstedet. Den findes på Publikationskontorets websted på https://eur-lex.europa.eu/.

1.3.5 Politikens gyldighedsperiode

Denne politikversion træder i kraft den 1. oktober 2023.

1.3.6 Politikkens anvendelsesområde

Denne politik gælder for alle OJ-numre, der er offentliggjort og signeret elektronisk efter ikrafttrædelsen af Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende. Denne politik finder ikke anvendelse på supplementet til Den Europæiske Unions Tidende (S-serien eller EU-Tidende S eller OJ S).

> BEMÆRK: Hver version af denne politik er gyldig inden for den gyldighedsperiode, der er fastsat i hver version. Sættet af alle udgaver dækker alle OJ-numre.

1.4 Administration af signaturpolitikdokumenter

Udstederen af OJ-signaturpolitikken er Den Europæiske Unions Publikationskontor, som tager dette dokument i brug og offentliggør det på EUR-Lex-webstedet.

OJ-signaturpolitikken, som den er offentliggjort, SKAL automatisk have retslig gyldighed og SKAL finde anvendelse på genereringen, verificeringen og den langsigtede administration af OJ-signaturer og -segl.

Udstederen af OJ-signaturpolitikken har ansvaret for:

- at specificere og godkende OJ-signaturpolitikken,
- at fastlægge revideringsprocessen for OJ-signaturpolitikken,
- at fastlægge vurderingskriterierne og den proces, der sikrer, at OJ-signaturpolitikken overholder Rådets forordning (EU) nr. 216/2013 af 7. marts 2013 om elektronisk offentliggørelse af Den Europæiske Unions Tidende og Rådets forordning (EU) 2018/2056 af 6. december 2018 om ændring af forordning (EU) nr. 216/2013 om elektronisk offentliggørelse af Den Europæiske Unions Tidende,
- at fastlægge vurderingskriterierne og den proces, der sikrer, at de programmer, der kræver konformitet med OJ-signaturpolitikken, rent faktisk overholder dens nuværende bestemmelser,
- offentliggørelse på EUR-Lex af OJ-signaturpolitikken og ændrede udgaver af denne.

1.4.1 Politikmyndighed

OJ-signaturpolitikken administreres af Den Europæiske Unions Publikationskontor.

1.4.2 Kontaktperson

Udstederen af denne politik kan kontaktes ved hjælp af følgende adresseoplysninger:

Kontaktperson:	Kontorchefen for EU-Tidende og retspraksis
Postadresse:	2, rue Mercier, L-2985 Luxembourg
Telefonnummer:	+352 29291
Faxnummer:	+352 292944620
E-mailadresse:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Godkendelsesprocedurer

Den godkendende myndighed i Den Europæiske Unions Publikationskontor er generaldirektøren for Den Europæiske Unions Publikationskontor.

1.4.4 Politikudgaver

Den første udgave og senere ændrede udgaver af politikken *KAN* angive en dato for seneste ikrafttrædelse. Når en udgave af politikken offentliggøres, SKAL den træde i kraft senest på én af følgende tre datoer:

1. Den seneste ikrafttrædelsesdato, der måtte være angivet i politikudgaven.
2. Den dag, der følger efter datoen for det tidligste signaturtidsstempel på OJ-signaturen eller segl på det OJ-nummer, der angiver den politikversion, der er offentliggjort, i henhold til lokal tid i Luxembourg
3. Den dag, der følger efter datoen for offentliggørelsen af politikudgaven.

Enhver givet ændret version af politikken SKAL automatisk bortfalde, når den respektive efterfølgende ændrede version træder i kraft. En efterfølgende ændret udgave af politikken BØR desuden angive den udgave, som den afløser.

Ovenstående regler har til formål at sikre, at signaturen for en given version af politikken ikke, hverken direkte eller indirekte, er underlagt den samme udgave af politikken for at forhindre en cirkelslutning. Desuden er det at foretrække at bevare den forældede version på en hvilken som helst måde.

1.5 Definitioner og akronymer

De definitioner og akronymer, der er anvendt i dette dokument, er anført i Table 1.

Akronym	**Definition:**
CA	Nøglecenter
DTBS	Data til underskrivning
LTV	Langsigtet gyldighed
OID	Objektidentifikator
OJ	Den Europæiske Unions Tidende (EUT)
PIN	Personligt identifikationsnummer
OP	Den Europæiske Unions Publikationskontor
QC	Kvalificeret certifikat
QESig	Kvalificeret elektronisk signatur
QESeal	Kvalificeret elektronisk segl
QSCD	Kvalificeret signatur-/seglgenereringssystem
SAA	Signaturudvidelsessystem
SCA	Signaturgenereringssystem
SSCD	Sikkert signaturgenereringssystem
SVA	Signaturvalideringssystem
TSP	Tillidstjenesteudbyder
QTSP	Kvalificeret tillidstjenesteudbyder
WIPIWIS	Det viste er det, der underskrives

Tabel 1: Definitioner og akronymer

2 Erklæringer om praksis for signaturanvendelse

2.1 Tilknyttede politikkrav

OJ-numre reguleres af artikel 1 og 2 i Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende, som bl.a. fastlægger, at den elektroniske udgave af Official Journal (EU-Tidende) SKAL bære en kvalificeret elektronisk signatur, der er defineret i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014, eller et kvalificeret elektronisk segl, der er defineret i overensstemmelse med forordning (EU) nr. 910/2014.

Elektronisk underskrivning og forsegling af OJ-numre hører under implementering af en signatur som en væsentlig formalitet, som anført i artikel III.2.1 i Europa-Kommissionens GENNEMFØRELSESBESTEMMELSER TIL AFGØRELSE 2002/47/EF, EKSF, EURATOM OM DOKUMENTHÅNDTERING OG AFGØRELSE 2004/563/EF, EURATOM OM ELEKTRONISKE OG DIGITALISEREDE DOKUMENTER af 30. november 2009[2], som også fastlægger, at elektroniske signaturer, som anvendes til OJ, kræver en kvalificeret elektronisk signatur som angivet i [eIDAS].

I henhold til artikel III.2.3 i GENNEMFØRELSESBESTEMMELSER TIL AFGØRELSE 2002/47/EF OG AFGØRELSE 2004/563/EF[2] varetages verificeringen af den underskrivende myndighed af OJ-SCA-systemet, når en embedsmand fra OP får adgang til elektronisk at underskrive OJ-numre, eller når OP som juridisk person får adgang til at forsegle OJ-numre elektronisk.

Selv om OJ-numre i elektronisk format ikke kan have retsvirkning uden at være underskrevet eller forseglet, fastlægger OJ-signaturpolitikken også, at OJ-SCA-systemet SKAL garantere, at kun de bemyndigede OJ-underskrivere kan afvise OJ-numre, således at angreb på OJ-offentliggørelsesprocessen effektivt undgås.

Da bemyndigede OJ-underskrivere handler på vegne af OP, er det generaldirektøren for OP's ansvar at garantere (ved uddelegering) behørig godkendelse af de respektive kvalificerede certifikater til OJ-underskrift. Godkendelse af kvalificerede certifikater til OJ-underskrift

- *SKAL* derfor være korrekt konfigureret i OJ-SCA-systemets brugeradministration,
- *BØR* være begrænset til fælles certifikater (professionelle), der garanterer indholdets tilknytning til OP[3],
- SKAL gøres gennemskuelige via offentliggørelse af de godkendte kvalificerede certifikater på EUR-Lex-webstedet, i overensstemmelse med artikel 2 i Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende.

2.2 Tilknyttede juridiske krav

Implementeringen af elektroniske signaturer og elektroniske segl som omhandlet i OJ-signaturpolitikken SKAL reguleres af følgende lovbestemmelser:

- Rådets forordning (EU) nr. 216/2013 af 7. marts 2013 om elektronisk offentliggørelse af Den Europæiske Unions Tidende

[2] Se SEC(2009) 1643.

[3]Fælles certifikater, der garanterer indholdets tilknytning til en specifik organisation. Sikkerheden øges, fordi den udstedende CSP håndhæver beviset for den respektive certifikatejers adkomst.

- 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[4]
- 2009/767/EF: Kommissionens beslutning af 16. oktober 2009 om fastlæggelse af foranstaltninger, der skal lette anvendelsen af elektroniske procedurer ved hjælp af "kvikskranker" i henhold til Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked[5]
- Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)[6]
- Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation)[7]
- Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse[8]
- 2010/425/EU: Kommissionens afgørelse af 28. juli 2010 om ændring af beslutning 2009/767/EF for så vidt angår oprettelse, vedligeholdelse og offentliggørelse af positivlister over certificeringstjenesteudbydere, der overvåges af/er akkrediteret af medlemsstaterne[9]
- 2009/496/EF, EURATOM: Europa-Parlamentets, Rådets, Kommissionens, Domstolens, Revisionsrettens, Det Europæiske Økonomiske og Sociale Udvalgs og Regionsudvalgets afgørelse af 26. juni 2009 om organisationen og driften af Kontoret for Den Europæiske Unions Publikationer[10]
- 2011/130/EU: Kommissionens afgørelse af 25. februar 2011 om fastsættelse af mindstekrav ved behandling af elektronisk underskrevne dokumenter på tværs af grænserne foretaget af de kompetente myndigheder som omhandlet i Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked[3.]

2.3 Tekniske sikkerhedshensyn

Kryptografiske værktøjer, der kan anvendes til implementering af OJ-signaturer og -segl SKAL opfylde kravene til kvalificerede elektroniske signaturer som defineret i [eIDAS], i [ETSI 2016] og i den relevante nyeste praksis.

[4] Se EUT L 257 af 28.8.2014, s. 73.

[5] Se EUT L 274 af 20.10.2009, s. 36.

[6] Se EUT L 119 af 4.5.2016, s. 1.

[7] Se EFT L 201 af 31.7.2002, s. 37.

[8] Se EUT L 337 af 18.12.2009, s. 11.

[9] Se EUT L 199 af 31.7.2010, s. 30.

[10] Se EUT L 168 af 30.6.2009, s. 41.

2.4 Juridiske erklæringer

Elektroniske signaturer og segl på OJ-numre skal genereres på vegne af OP på grundlag af Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende.

3 Parametre for forretningsanvendelsesområde (PFA)

3.1 PFA'er, der hovedsageligt er knyttet til den pågældende anvendelse/forretningsproces

3.1.1 PFA (a): Arbejdsgang (rækkefølge og timing) for signaturer

3.1.1.1 Beskrivelse af generel forretningsgang

OP offentliggør OJ fra mandag til fredag og eventuelt i weekenden. Denne OJ-offentliggørelse kan være et OJ-nummer eller et OJ-dokument. Et OJ-nummer repræsenterer en offentliggørelse af et eller flere dokumenter på flere sprog Hver sprogudgave af et nummer består af hele teksten i hvert dokument i én enkelt fil. Et OJ-dokument er en flersproget offentliggørelse af ét dokument, der offentliggøres særskilt. Hver sprogudgave af et OJ-dokument består af hele teksten i hvert dokument i én enkelt fil.

De enkelte OJ-numre og OJ-dokumenter kategoriseres efter den udgave, de hører under, med kategorien som en identificerende del af OJ. Der er to udgaver, der er relevante for det nuværende anvendelsesområde, nemlig L (Retsforskrifter) og C (Meddelelser og oplysninger). En udgave kan eventuelt have underudgaver og klassificeringssystemer (se http://publications.europa.eu/code/da/da-10000.htm for en nærmere forklaring på anvendelsesområdet, dokumentstrukturen og supplerende baggrundsoplysninger).

Foruden OJ-L- og C-udgaverne er der også specialudgaver, som offentliggøres på sproget i et kandidatland/ny medlemsstat, og som indeholder afledt EU-ret. Disse specialudgaver indgår også i anvendelsesområdet.

Når et OJ-nummer eller OJ-dokument er færdigt (dvs. alle sprogudgaver af OJ-nummeret eller OJ-dokumentet er tilgængelige i PDF/A) og klart til offentliggørelse, fortsætter arbejdsgangen enten med en elektronisk forsegling (se afsnit 3.1.1.2) eller en elektronisk signering (se afsnit 3.1.1.3). I tilfælde af elektronisk forsegling genereres der automatisk et kvalificeret elektronisk segl ved hjælp af et kvalificeret elektronisk forseglingscertifikat, der udstedes til OP som en enhed i Europa-Kommissionen. I tilfælde af elektronisk signering genererer en bemyndiget person en kvalificeret elektronisk signatur ved hjælp af et kvalificeret elektronisk signaturcertifikat.

Den elektroniske forsegling er den standardarbejdsgang, der vælges af SCA-systemet, dvs. færdige OJ-numre eller OJ-dokumenter gennemgår den automatiske forseglingsproces, medmindre forseglingsprocessen ikke er tilgængelig. I sidstnævnte tilfælde anvendes underskrivningsprocessen.

Eftersom der anvendes en/et separat XAdES-signatur/-segl med et manifest (se [Bartel 2008], [ETSI 2022] og 2011/130/EU: Kommissionens afgørelse af 25. februar 2011 om fastsættelse af mindstekrav ved behandling af elektronisk underskrevne dokumenter på tværs af grænserne foretaget af de kompetente myndigheder som omhandlet i Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked[11]) til underskrivning af hvert enkelt nummer, når en/et signatur/-segl for et OJ-nummer eller OJ-dokument skal verificeres, er det også nødvendigt at gennemføre en validering af manifestet ud over XML-signaturens kerne (se [Bartel 2008]) under [ETSI 2022] valideringen med henblik på verificering af en signatur eller et segl for et OJ-nummer eller OJ-dokument.

Følgende trin beskriver arbejdsgangen for elektronisk højniveauforsegling og -signering, som den er implementeret i OJ-SCA, -SAA og -SVA (se [ETSI 2016]).

[11] EUT L 53 af 26.2.2011, s. 66.

3.1.1.2 Generering af segl for OJ-nummer og OJ-dokument

1. Der spores et komplet OJ-nummer eller OJ-dokument til forsegling.
2. SCA-systemet udfører foreløbige verificeringskontroller af de leverede filer:
    a. Det kontrollerer, om der er størrelsesuoverensstemmelser mellem sprogudgaverne af OJ-nummeret/OJ-dokumentet, og om de holder sig inden for de konfigurerbare størrelsesgrænser.
    b. Det kontrollerer, om alle de leverede sprogudgaver er planlagt til offentliggørelse.
3. I tilfælde af verificeringsfejl afbrydes forseglingsprocessen. Genoptagelse af forseglingsprocessen kræver manuel indgriben fra en bemyndiget OP-medarbejder.
4. Efter gennemført validering af SCA-systemet genereres der et manifest med henvisning til hver sprogudgave af det komplette nummer. Desuden svarer hver sprogudgave til et individuelt EU-sprog og repræsenteres som et PDF/A-dokument, der behandles som en binær oktetstrøm under beregningen af fingeraftrykket (message digest).
5. SCA-systemet autentificerer i forhold til Kommissionens centrale elektroniske signaturportal og sender det genererede manifest til automatiseret forsegling.
6. Den elektroniske signaturportal forsegler det leverede manifest ved hjælp af et kvalificeret forseglingscertifikat udstedt af en akkrediteret europæisk QTSP (se. [eIDAS]). Den private nøgle, der er knyttet til dette forseglingscertifikat, gemmes i en QSCD, der er forbundet med den elektroniske signatur-portal.
7. XAdES-seglet (jf. [ETSI 2022-XAdES]), der genereres på denne måde, sendes derefter tilbage til SCA-systemet, som bl.a. kontrollerer gyldigheden af de anvendte algoritmer og verificerer, at det respektive segls forseglingscertifikat er godkendt og ejes af den juridiske person, der er autentificeret som bemyndiget underskriver.
8. Når verificeringen er gennemført, udvides det elektroniske segl med et signaturtidsstempel fra en akkrediteret QTSP (jf. [eIDAS]).
9. Det elektroniske segl, der blev udvidet på det foregående trin i processen, overføres til offentliggørelse på EUR-Lex-webstedet. En identisk kopi af seglet lagres samtidig i SCA-systemet.
10. Når den krævede frist på 24 timer for et segl, der er genereret på det foregående trin, udløber, udvides det igen til en selvbærende form med henblik på at gøre signaturen gyldig i en lang periode ved hjælp af et sikkert tidsstempel fra en akkrediteret europæisk QTSP (se [eIDAS]).
11. Det segl, der blev udvidet på det foregående trin i processen, overføres til offentliggørelse på EUR-Lex-webstedet og erstatter seglet fra trin 9, som ikke var blevet udvidet til en selvbærende form.
12. Foruden offentliggørelsen på EUR-Lex-webstedet overgives identiske kopier af de dokumenter, der udgør et OJ-nummer eller OJ-dokument, sammen med det tilsvarende segl i selvbærende form, til det digitale langtidsarkivsystem, som forvaltes af OP, med henblik på langtidsopbevaring af EU-institutionernes officielle dokumenter. Implementeringsaspekter vedrørende langtidsopbevaring er dog IKKE behandlet i denne signaturpolitik.

3.1.1.3 Generering af signatur for OJ-nummer og OJ-dokument

1. Der spores et komplet OJ-nummer eller OJ-dokument til signering.
2. Der genereres et manifest med henvisning til hver sprogudgave af det komplette nummer. Desuden svarer hver sprogudgave til et individuelt EU-sprog og repræsenteres som et

PDF/A-dokument, der behandles som en binær oktetstrøm under beregningen af fingeraftrykket (message digest).

Bemærk, at komplette numre udelukkende styres og låses af SCA-systemet under manifestgenereringen for at sikre en konsekvent beregning af fingeraftrykket, som er afgørende for processen.

3. Når nummeret er autentificeret af SCA-systemet, kan en bemyndiget underskriver vælge et komplet nummer til underskrivning, forudsat at det tilsvarende manifest er udarbejdet på det foregående trin.
4. Når et nummer er valgt til underskrivning, påbegynder den bemyndigede underskriver underskrivningsproceduren for det pågældende nummer:
    a. For at overholde WIPIWIS-princippet er den bemyndigede underskriver tvunget til at gennemgå mindst tre forskellige sprogudgaver ved hjælp af en konform PDF/A-fremviser, inden vedkommende kan underskrive nummeret. Hvis OJ-nummeret eller OJ-dokumentet foreligger i mindre end tre sprogudgaver, er den bemyndigede underskriver tvunget til at gennemgå alle disponible sprogudgaver.

        Bemærk, at SCA-systemet giver underskriveren mulighed for at gennemgå hver enkelt sprogudgave i det nummer, der skal underskrives. Underskriveren KAN derfor gennemgå hele det indhold, der skal underskrives, såfremt han eller hun ønsker det.

    b. Den bemyndigede underskriver kan bevidst vælge enten at afvise nummeret, hvilket stopper underskrivningsprocessen, eller fortsætte med at underskrive ved at trykke på knappen Sign (Underskriv).
    c. Når der trykkes på Sign-knappen:
        i. SCA-systemet genererer en underskriftsanmodning til Kommissionens centrale elektroniske signaturportal, der sender manifestet til underskrift og omdirigerer den bemyndigede underskriver til portalen.
        ii. Den bemyndigede underskriver autentificerer sig på den elektroniske signaturportal og får vist det manifest, der skal underskrives, i overensstemmelse med WIPIWIS-principperne.
        iii. Den elektroniske signaturportal opretter forbindelse til den middleware, der er installeret på den bemyndigede underskrivers arbejdsstation, og henter det kvalificerede underskriftscertifikat, der er udstedt af en akkrediteret europæisk QTSP (jf. [eIDAS]). Dette certifikat fremvises for den bemyndigede underskriver, som derefter bliver bedt om at indtaste den tilsvarende pin-kode, der beskytter QSCD for at bemyndige QSCD-systemet til at generere signaturen ved hjælp af den private nøgle, som svarer til det valgte underskriftscertifikat, hvorved underskrivningsprocessen er gennemført.
    d. Middlewaren sender den signaturværdi, der blev genereret, til den elektroniske signaturportal, som igen genererer en tilsvarende XAdES-signatur (jf. [ETSI 2022-XAdES])
5. XAdES-signaturen sendes derefter tilbage til SCA-systemet, som — via den elektroniske signaturportal — bl.a. kontrollerer gyldigheden af de anvendte algoritmer og verificerer, at den respektive signaturs signaturcertifikat er godkendt og ejes af den samme person, der er autentificeret som bemyndiget underskriver.

6. Når verificeringen er gennemført, udvides signaturen — via den elektroniske signaturportal — med et signaturtidsstempel fra en akkrediteret europæisk QTSP (jf. [eIDAS]).
7. Den signatur, der blev udvidet på det foregående trin i processen, overføres til offentliggørelse på EUR-Lex-webstedet. En identisk kopi af underskriften lagres samtidig i SCA-systemet.
8. Når den krævede frist på 24 timer for en signatur, der er genereret på det foregående trin, udløber, udvides det igen til en selvbærende form med henblik på at gøre signaturen gyldig i en lang periode ved hjælp af et sikkert tidsstempel fra en akkrediteret europæisk QTSP (se [eIDAS]).
9. Den signatur, der blev udvidet på det foregående trin i processen, overføres til offentliggørelse på EUR-Lex-webstedet og erstatter signaturen fra trin 7, som endnu ikke var blevet udvidet til en selvbærende form.
10. Foruden offentliggørelsen på EUR-Lex-webstedet overgives identiske kopier af de dokumenter, der udgør et OJ-nummer eller OJ-dokument, sammen med den tilsvarende signatur i selvbærende form, til det digitale langtidsarkivsystem, som forvaltes af OP, med henblik på langtidsopbevaring af EU-institutionernes officielle dokumenter. Implementeringsaspekter vedrørende langtidsopbevaring er dog IKKE behandlet i denne signaturpolitik.

3.1.1.4 Nødsituation

Hvis det ikke er muligt at generere OJ-nummerets eller OJ-dokumentets segl eller signatur som beskrevet i afsnit 3.1.1.2 eller 3.1.1.3 på grund af en uforudset og ekstraordinær manglende tilgængelighed af OJ-SCA-systemet, vil Publikationskontoret anvende et QESeal eller QESig på hvert enkelt PDF/A-dokument, der svarer til hver sprogudgave af OJ-nummeret eller OJ-dokumentet. Alle forseglede/signerede PDF/A-dokumenter vil blive overført til offentliggørelse på EUR-Lex-webstedet.

3.1.2 PFA (b): Data til underskrivning

- OJ-signaturer og -segl afhænger af et XML-manifest (jf. [Bartel 2008] og [ETSI 2022-XAdES]), som samler alle sprogudgaver, der er gjort tilgængelige i PDF/A-format tilhørende et OJ-nummer eller OJ-dokument, i én enkelt signatur, som skal overholde følgende krav: Hver sprogudgave, der logisk vedrører et OJ-nummer eller OJ-dokument, *SKAL* have sin egen fingeraftryksværdi.
- Alle sprogudgaver, der logisk tilhører et OJ-nummer eller OJ-dokument, SKAL vises til underskriveren under signaturgenereringen med henblik på kontrol, så signaturindholdet kan verificeres efter underskriverens ønske som beskrevet i afsnit 3.1.1.3, i overensstemmelse med WIPIWIS-princippet.
- Behørig visualisering *SKAL* sikres ved anvendelse af en PDF/A-konform læser.
- Kun de sprogudgaver, der vedrører det nummer, der underskrives, *MÅ* vises til underskriveren under underskrivningsprocessen.
- De tekniske karakteristika for alle de sprogudgaver, der logisk er knyttet til et OJ-nummer eller OJ-dokument, SKAL kontrolleres under genereringen af seglet og signaturen for at sikre ensartethed.

I tilfælde af en nødsituation som beskrevet i afsnit 3.1.1.4 ovenfor gælder følgende krav:

- Hver sprogudgave af et OJ-nummer eller OJ-dokument, *SKAL* have sin egen QESeal eller QESig.

- Alle sprogudgaver, der logisk tilhører et OJ-nummer eller OJ-dokument, SKAL gennemgås af underskriveren under signaturgenereringen, så signaturindholdet kan verificeres efter underskriverens ønske i overensstemmelse med WIPIWIS-princippet.
- Behørig visualisering *SKAL* sikres ved anvendelse af en PDF/A-konform læser.

3.1.3 PFA (c): Forholdet mellem underskrevne data og signatur(er) og segl

En signatur eller et segl for et OJ-nummer eller OJ-dokument gælder for alle sprogudgaver af et OJ-nummer eller OJ-dokument, der hver især er formateret som et PDF/A-dokument.

Under genereringen af en signatur eller et segl for et OJ-nummer eller OJ-dokument laves et fingeraftryk på filindholdet i et dokument, der skal underskrives/forsegles, i form af en binær oktetstreng ved hjælp af den stærkeste understøttede "digest"-algoritme, der overholder afsnit 7.3 i [ETSI 2022-Crypto].

De enkelte dokumentfingeraftryksværdier sættes sammen med URI'erne for de originale filnavne i et XML-manifest uden anvendelse af yderligere transformationer (jf. [Bartel 2008]).

Manifestet med de underskrevne attributter underskrives eller forsegles ved hjælp af XAdES (jf. [ETSI 2022-XAdES]) med hensyn til den profil, der er beskrevet i Kommissionens afgørelse 2011/130/EU af 25. februar 2013.

I tilfælde af en nødsituation som beskrevet i afsnit 3.1.1.4 ovenfor vil hvert PDF/A-dokument, der repræsenterer hver enkelt sprogudgave af EFS- eller OJ-aktudstedelserne, blive underskrevet eller forseglet med anvendelse af PAdES (jf. [ETSI 2016-PAdES] [eIDAS]).

3.1.4 PFA (d): Målfællesskab

Målfællesskabet er enhver part, der er afhængig af og skal verificere ægtheden af OJ, og alle parter, der er ansvarlige for gennemførelsen af den SCA og SAA, der anvendes til at oprette e-signaturer eller e-segl, og som udvider dem til OJ-numre eller OJ-dokumenter.

3.1.5 PFA (e): Fordeling af ansvar for signaturvalidering og -udvidelse

3.1.5.1 Verificering af signatur eller segl for et OJ-nummer eller OJ-dokument

Enhver signaturmodtager, særligt EU-borgere, kan downloade et OJ-nummer eller OJ-dokument, der er offentliggjort på EUR-Lex-webstedet, og den/det tilsvarende separate XAdES-signatur eller -segl (jf. [ETSI 2022-XAdES]) til verificering.

Da en interoperabel europæisk signaturstandard og tjenesterne fra en akkrediteret europæisk QTSP (jf. [eIDAS]) anvendes ved signatur- og seglgenereringen, kan verificering foretages ved hjælp af et hvilken som helst tredjepartsverificeringssystem, der overholder de anvendte standarder, forudsat at valideringen kan gennemføres på basis af OJ-signaturpolitikken.

I tilfælde af en nødsituation som beskrevet i afsnit 3.1.1.4 ovenfor vil hvert PDF/A-dokument, der repræsenterer hver enkelt sprogudgave af EFS- eller OJ-aktudstedelserne, blive underskrevet eller forseglet med anvendelse af PAdES (jf. [ETSI 2016-PAdES]). Verificeringen af disse kan foretages ved hjælp af et hvilken som helst tredjepartsverificeringssystem, der overholder den anvendte standard.

3.1.5.1.1 Verificering på serversiden

For at lette signatur- og seglverificeringen KAN OP VÆLGE at tilbyde et gratis OJ-server-SVA-system, som fungerer efter følgende verificeringsprocedure:

1. Verifikatoren uploader den PDF/A-fil, der skal verificeres, sammen med den tilhørende signatur- eller seglfil ved at anvende filuploadfunktionaliteten i SVA-systemet.
2. SVA-systemet beregner fingeraftrykket (digest) til den uploadede PDF/A-fil og verificerer, at det beregnede fingeraftryk er indeholdt i den uploadede signatur.

3. Når fingeraftrykket er verificeret, udføres standard XAdES-verificeringen af den uploadede signatur- eller seglkandidat, forudsat at underskrifts- eller forseglingscertifikatet identificerer en bemyndiget OJ-underskriver for den periode, der er bestemt af signaturtidsstemplet. SVA-systemet verificerer også, at underskriveren havde bemyndigelse til at underskrive på det tidspunkt, hvor signaturen ifølge signaturtidsstemplet blev genereret.
4. Verificeringen kan gennemføres, når alle forudgående trin er gennemført korrekt. I modsat fald mislykkes signaturverificeringen. Under alle omstændigheder får verifikatoren vist en forståelig rapport over verificeringsprocessen.

3.1.5.1.2 Verificering på klientsiden

For at lette signatur- og seglverificeringen KAN OP VÆLGE at tilbyde et gratis OJ-klient-SVA-system, som fungerer efter følgende verificeringsprocedure:

1. Verifikatoren starter det downloadede SVA-system, dets kodesignatur verificeres automatisk af run-time-miljøet, og gennemførelsen godkendes af verifikatoren, når kodesignaturen er verificeret.
2. Verifikatoren vælger en PDF/A-fil i en bestemt sprogudgave, som skal verificeres, sammen med den tilhørende kandidatsignatur- eller seglfil på den lokale PC's filsystem ved hjælp af filvalgsdialogen i SVA-systemet.
3. SVA-systemet beregner fingeraftrykket til det valgte dokument og verificerer, at det beregnede fingeraftryk er indeholdt i manifestet til den valgte signatur- eller seglkandidat.
4. Når verificeringen af fingeraftrykket er gennemført, sker der en standard XAdES-verificering af den valgte signatur- eller seglkandidat.
5. Verificeringen er gennemført korrekt, når alle forudgående trin er gennemført korrekt, og når underskrifts- eller forseglingscertifikatet har identificeret en bemyndiget OJ-underskriver for den periode, der er bestemt af signaturtidsstemplet.

   Bemærk, at SVA-systemet muligvis KAN kende oplysninger om den bemyndigede underskriver på basis af en (standard) konfiguration. Certifikatets fingeraftryk på underskrifts- eller forseglingscertifikatet er dog også angivet i SVA-resultatet, så verifikatoren manuelt kan sammenholde det med de offentliggjorte oplysninger om den juridiske underskriver for signatur- eller seglgenereringsperioden, som også er angivet i SVA-resultatet.

3.2 PFA'er, der hovedsagelig påvirkes af de retlige/reguleringsmæssige bestemmelser, der er knyttet til den pågældende anvendelse/forretningsproces

3.2.1 PFA (f): Signaturernes juridiske form

Elektroniske signaturer og segl, der anbringes på et OJ-nummer eller OJ-dokument, SKAL være QESig og QESeal som omhandlet i [eIDAS].

Ovenstående krav er især baseret på Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende (jf. afsnit 2.2).

Et kvalificeret certifikat skal opnås af hver enkelt underskriver som en betingelse for anvendelse af signatursystemet.

Kvaliteten af de specifikke elementer i de nødvendige QESig og QESeal SKAL opfylde følgende kvalitetskrav:

- Udstyr til underskrivning og forsegling: QSCD'er, der overholder bilag II til [eIDAS]
- Certifikatfremskaffelse: QC, der overholder bilag I til [eIDAS]
- Uafhængigt tilsagn om fremskaffelse af certifikat: QC udstedes af en overvåget eller akkrediteret QTSP-certificeringstjeneste, som er akkrediteret i ethvert land, hvor [eIDAS] finder anvendelse
- Signaturkrypteringspakke: Der må kun anvendes signaturprogrammer, der er anført i afsnit 7.3 i [ETSI 2022-Crypto]
- LTV-løsninger: XAdES-signatur- og seglformer for OJ-numre eller OJ-dokumenter (jf. [ETSI 2022-XAdES]) SKAL udvides til LTA-formen, der omfatter fornyelse af arkiveringstidsstempler eller andet (eksterne sikre arkiveringsmekanismer KAN overvejes som et alternativ til fornyelse af arkivtidsstempel, forudsat at de er af tilsvarende eller højere kvalitet).
- Signaturgenereringssystem: Kvaliteten af OJ-SCA-systemet SKAL opfylde de kvalitetskrav, der pålægges af Kommissionens politikker, og skal overholde kravene i Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende

3.2.2 PFA (g): Underskriverens forpligtelser

Elektroniske signaturer og segl på OJ-numre eller OJ-dokumenter SKAL genereres på vegne af OP på grundlag af Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende.

Denne forpligtelse, som en bemyndiget OJ-underskriver påtager sig, er udtryk for, at de underskrevne data udgør et autentisk OJ-nummer eller OJ-dokument, der er behørigt valideret med hensyn til reglerne for forretningsanvendelsesområdet (jf. afsnit 3.1.1) og offentliggjort af OP i overensstemmelse med Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende, således at udgaven kan tjene som en autentisk kilde til EU-lovgivning.

Ingen eksplicit angivelse af forpligtelsestype MÅ derfor være indeholdt i en OJ-signatur (jf. afsnit 5.2.3 i [ETSI 2022-XAdES]).

3.2.3 PFA (h): Sikringsniveau for tidsdokumentation

Et signaturtidsstempel SKAL tilføjes til signaturer eller segl for OJ-numre eller OJ-dokumenter, der genereres som beskrevet i afsnit 3.1.1.2 eller 3.1.1.3, samme dag (lokal tid i Luxembourg) som datoen for underskrivning eller forsegling af OJ-nummeret eller OJ-dokumentet for at godtgøre, at signaturen eller seglet ikke blev genereret efter datoen for offentliggørelsen. Dermed sikres det, at den gruppe bemyndigede underskrivere, der er relevante på offentliggørelsesdatoen, også er relevante for signaturen eller seglet.

OJ-SCA-systemet SKAL sikre, at alle XAdES-B-T-signaturer, der genereres, opfylder dette krav.

Det tidsstempel, der anvendes til at generere signaturtidsstempler i XAdES-B-T-signaturer SKAL være kvalificerede tidsstempler.

PAdES-signaturer, der er genereret i tilfælde af en nødsituation som beskrevet i afsnit 3.1.1.4 KAN genereres uden et signaturtidsstempel.

Hvis PAdES-signaturer, der er genereret i tilfælde af en nødsituation som beskrevet i afsnit 3.1.1.4, genereres med et signaturtidsstempel, BØR signaturtidsstemplet være et kvalificeret tidsstempel og anvendes samme dag (lokal tid i Luxembourg) som datoen for signaturen eller seglet for OJ-nummeret eller OJ-dokumentet for at attestere, at signaturen eller seglet ikke blev genereret efter datoen for offentliggørelsen.

BEMÆRK: Det betyder, at hvis der i en nødsituation indgår et signaturtidsstempel i signaturen, kan det være et ikke-kvalificeret tidsstempel.

Alle andre tidsstempler, herunder arkiveringstidsstempler og eventuelle indholdstidsstempler, SKAL være kvalificerede tidsstempler.

3.2.4 PFA (i): Underskriftsformaliteter

Det er OJ-SCA-systemets opgave at tilvejebringe en underskrivergrænseflade på en sådan måde, at der i videst muligt omfang sikres et gyldigt juridisk signatur- og seglmiljø. Grænsefladen skal:

- indeholde passende råd og oplysninger om systemets signatur- og seglproces
- sikre konsistens mellem anvendelsen af den behørige signatur- og seglgenerering og verificeringsdataene, signatur- og seglgenereringssystemet, de data, der skal underskrives, og det forventede anvendelsesområde for og formål med signaturen og seglet (eller underskrivnings- eller forseglingshandlingen)
- muliggøre og påvise et klart udtryk for viljen til at underskrive og brugerens hensigt om at blive bundet af signaturen eller seglet
- muliggøre og fremvise informeret samtykke.

OJ-SVA-systemet SKAL sikre, at signaturmodtagerne (herunder underskriveren) har korrekte procedurer til verificering og arkivering af den elektroniske signatur eller det elektroniske segl og verificeringsdataene.

3.2.5 PFA (j): Levetid og modstandsdygtighed over for forandring

De underskrevne OJ-numre og OJ-dokumenter og deres signaturer SKAL opbevares på ubestemt tid. Bevarelsen af OJ-numrenes eller OJ-dokumenternes signaturers gyldighed SKAL sikres i en sådan periode (jf. artikel 2 i Rådets forordning om elektronisk offentliggørelse af Den Europæiske Unions Tidende).

3.2.6 PFA (k): Arkivering

Ikke relevant.

3.3 PFA'er, der hovedsagelig er knyttet til de aktører, der er involveret i at generere/udvide/validere signaturer

3.3.1 PFA (l): Underskrivernes identitet (og roller/attributter)

3.3.1.1 Foreslået underskriver og identifikationsregler

Signaturer for OJ-numre eller OJ-dokumenter SKAL anvendes af bemyndigede underskrivere, som især SKAL være OP-embedsmænd, som har den fornødne ekspertise til at validere OJ-numre eller OJ-dokumenter i overensstemmelse med reglerne for forretningsanvendelsesområdet (jf. afsnit 3.1.1.3). For så vidt angår segl for OJ-numre eller OJ-dokumenter SKAL den bemyndigede underskriver være selve OP som en enhed under Europa-Kommissionen.

Bemyndigede underskrivere SKAL også være bevidste om deres ansvar og SKAL handle loyalt ved autentificeringen af lovtekster, der repræsenterer EU-lovgivning.

Forbindelsen mellem disse fysiske underskrivere og deres signaturverificeringsdata SKAL attesteres i et kvalificeret certifikat med hensyn til [eIDAS] som bekræfter deres identitet og deres tilknytning til OP.

Bemyndigelse af en OJ-underskriver SKAL foretages af generaldirektøren for OP (evt. ved delegering).

3.3.1.2 Underskriverens roller og attributter

Ingen rolle, funktion eller kvalificering MÅ kræve attestering i underskriverens kvalificerede certifikat ud over underskriverens tilknytning til OP.

Det SKAL være OJ-SCA-systemets opgave at sikre behørig adgangskontrol og underskriverbemyndigelse, inden underskrivere får adgang til AOJ's signaturfunktioner.

Adgangskontrol og underskriverbemyndigelse SKAL gennemføres på basis af en stærk autentificeringsmekanisme, der er implementeret i SCA-systemet, og de tilladelser, der er registreret med offentlige nøglecertifikater, som svarer til de bemyndigede underskrivere i SCA-systemets brugeradministrationsdatabase.

Signaturmodtagere *KAN* bruge OJ-underskriveres offentliggjorte certifikater til verificering af deres lovmæssige adkomst.

3.3.1.3 Tilknyttet bevis på bemyndigelse

Ingen yderligere bestemmelser ud over afsnit 3.3.1.2.

3.3.2 PFA (m): Det sikringsniveau, der kræves til autentificering af underskriveren

Det sikringsniveau, der kræves til autentificering af underskriveren, sikres ved hjælp af dennes kvalificerede certifikat og midler til generering af signaturen, som SKAL være et kvalificeret signatur-/seglgenereringssystem som defineret i [eIDAS].

3.4 Andre PFA'er

3.4.1 PFA (o): Andre oplysninger, der skal knyttes til signaturen eller seglet

3.4.1.1 Bemyndigede OJ-underskrivere og tidsstemplingsbemyndigelser

Verificering af underskrivernes bemyndigelse er et vigtigt tillidsaspekt af AOJ.

Bemyndigelse SKAL ske eksplicit ved offentliggørelse af de elektroniske certifikater for alle bemyndigede underskrivere via et medie, der anses for sikkert, eksternt fra SCA/SVA.

Ved offentliggørelsen af bemyndigede OJ-underskrivere SKAL det angives, at overvågningsstatus for underskrivercertifikater er garanteret for den aktuelle underskrivningsperiode for OJ-numre eller OJ-dokumenter.

Bemyndigede OJ-underskrivere og tidsstemplingsbemyndigede MÅ IKKE offentliggøres i OJ, da denne metode ville skabe cirkelslutningsproblemer, især med hensyn til langsigtet validering.

Når bemyndigede OJ-underskrivere ændres over tid, SKAL den tidligere gruppe af underskrivere offentliggøres som historiske tillidsoplysninger. Dette kræves ved verificering af OJ-numre eller OJ-dokumenter, der er underskrevet af disse underskrivere.

Ved offentliggørelsen af bemyndigede underskrivere SKAL den periode angives, som de angivne underskrivere var eller er bemyndigede for, og denne angivelse skal være i overensstemmelse med tidsbegrænsningen i denne politikversion.

3.4.1.2 Regler for attributter, anvendelsesområde og formål vedrørende elektronisk signatur og segl

Signatur- og seglgenereringsprocessen SKAL gøre behørig brug af signaturattributter, særligt de underskrevne attributter, som er oplysninger, der understøtter den/det elektroniske signatur/segl og som dækkes af signaturen/seglet sammen med data, der skal underskrives i overensstemmelse med følgende:

- Den underskrivende certifikatidentifikator SKAL benyttes. Det er identifikatoren for, eller en henvisning til, det certifikat, der indeholder signaturverificeringsdataene, som

svarer til de signatur- eller seglgenereringsdata, der anvendes af underskriveren til at generere den/det elektroniske signatur/segl.

- En angivelse af signaturpolitikken KAN anvendes (jf. afsnit 1.2.2).
- Det påståede underskrivningstidspunkt SKAL benyttes. Det angiver det tidspunkt, hvor underskriveren påstår at have genereret signaturen eller seglet.

  Bemærk, at dette tidspunkt er det aktuelle systemtidspunkt på underskriverens PC. Det er IKKE et sikkert tidspunkt.

  Ejeren af OJ-SCA-systemet SKAL (ved delegering, som foretages af generaldirektøren for OP) sørge for, at den aktuelle systemtidsangivelse på alle underskriver-PC'er er præcis.

  Dette kan opnås ved at anvende NTP med en egnet tidskilde (jf. [Mills 2010]).
- INGEN angivelse af forpligtelsestype MÅ anvendes.
- Andre underskrevne attributter KAN anvendes.

Brugen af signaturattributter SKAL være i overensstemmelse med [ETSI 2010] og Kommissionens afgørelse 2011/130/EU af 25. februar 2013.

3.4.2 PFA (p): Kryptografiske pakker

Se afsnit 3.2.1.

4 Krav til/erklæringer om tekniske mekanismer og implementering af standarder

4.1 Regler for sikkert tidsstempel

XAdES-B-LTA-signaturformen (jf. [ETSI 2022-XAdES]) kræver flere tidsstempler, som SKAL indhentes fra en tidsstempeltjeneste, der er akkrediteret i en medlemsstat eller et EØS-land.

Ejeren af OJ-SCA-systemet SKAL (ved delegering, som foretages af generaldirektøren for OP) sørge for, at SCA-systemet er konfigureret til brug af egnede kryptografiske algoritmer.

4.2 Regler for langsigtet gyldighed

Bevarelse af gyldigheden af signaturer for OJ-numre eller OJ-dokumenter i den forventede bevarelsesperiode er sikret i kraft af implementeringen af XAdES-B-LTA-formen (jf. [ETSI 2022-XAdES]) og derefter ved udvidelse af signaturen med et supplerende kvalificeret arkivtidsstempel med henblik på at forlænge gyldigheden efter behov eller en egnet arkiveringsløsning, der giver garanti for bevarelse af signaturens gyldighed.

4.3 Eventuelt og juridiske anliggender

Da OJ offentliggøres fra mandag til fredag og evt. i weekenden, SKAL OJ-SCA-systemejeren (ved delegering, der foretages af generaldirektøren for OP) sikre, at SCA-systemet fungerer uden afbrydelser.

Til dette formål BØR der etableres serviceleveranceaftaler.

Selv om signaturer og segl for OJ-numre eller OJ-dokumenter kan verificeres ved hjælp af et hvilket som helst SVA-system, der overholder de standarder og regler, der er fastlagt i OJ-signaturpolitikken, som også kræver validering af manifestet, KAN OP lægge et offentligt tilgængeligt SVA-system på EUR-Lex-webstedet, så signaturmodtagere, særligt EU-borgere, kan verificere signaturer for OJ-numre eller OJ-dokumenter uden at være nødt til at købe et system fra tredjepart.

OP KAN, som en alternativ mulighed, stille et SVA-system til rådighed som et offentligt tilgængeligt program, der kan downloades, og som kører uafhængigt på brugerens desktop og kun kræver, at verifikatoren har tillid til softwaren, når vedkommende er afhængig af de resultater, programmet leverer.

5 Tillæg

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* W3C-anbefaling, 2008
[Bradner 1997]	Bradner S. *Key words for use in RFCs to indicate requirement levels* RFC 2119, Network Working Group, 1997
[Mealling 2010]	Mealling M. *A URN Namespace of Object Identifiers* RFC 3061, Network Working Group, 2001
[Mills 2010]	Mills D., Delaware U., Martin J., ISC Ed., Burbank J., Kasch W. *Network Time Protocol Version 4: Protocol and Algorithms Specification* RFC 5905, IETF, 2010
[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* EU-Tidende L 257
[ETSI 2015]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Signature Policies; Del 1: Building blocks and table of contents for human readable signature policy documents* TS 119 172-1, v1.1.1, ETSI, 2015
[ETSI 2016]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI);* *Policy and security requirements for applications for signature creation and signature validation* TS 119 101, v1.1.1, ETSI, 2016
[ETSI 2016-PAdES]	ETSI-ESI PAdES digital signatures; Del 1: Building blocks and PAdES baseline signatures ETSI EN 319 142-1 V1.1.1 (2016-04)
[ETSI 2022-XAdES]	ETSI-ESI XAdES digital signatures; Del 1: Building blocks and XAdES baseline signatures ETSI EN 319 132-1 V1.2.1 (2022-02)
[ETSI 2022-Crypto]	ETSI-ESI Cryptographic Suites ETSI TS 119 312 V1.4.2 (2022-02)