Handtekeningbeleid Publicatieblad

Versie 4

(1.3.171.4.1.1.4)

Datum inwerkingtreding: 1 oktober 2023

Inhoudsopgave

1 Inleiding

In dit document wordt het handtekeningbeleid gespecificeerd voor de handtekening Publicatieblad (PB-handtekening) en het zegel Publicatieblad (PB-zegel), die gebruikt worden om de elektronische versie van het Publicatieblad van de Europese Unie (PB) te authenticeren overeenkomstig Verordening (EU) nr. 216/2013 van de Raad van 7 maart 2013 betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie[1].

Een handtekeningbeleid is een geheel van regels voor het aanmaken, valideren en uitbreiden van een of meer onderling verbonden elektronische handtekeningen en/of zegels die de technische en procedurele vereisten vaststellen voor het aanmaken, valideren en beheren op lange termijn daarvan om bepaalde bedrijfsbehoeften (business needs) te vervullen en te bepalen wanneer zij geldig zijn. Een handtekeningbeleid dient ook om alle aspecten van een bepaalde handtekening- of zegelworkflow transparant te maken voor alle betrokkenen, dat wil zeggen de ondertekenaars, ontvangers en arbiters, zodat elektronische handtekeningen en zegels die voldoen aan de voorschriften van het beleid een groter vertrouwen in de toepasbaarheid en de aanvaarding ervan wekken.

De gedetailleerde concepten van een handtekeningbeleid worden beschreven in [ETSI 2015], waarin ook de richtsnoeren en de opzet voor dit document worden vastgesteld. De trefwoorden "MOET/MOETEN" ("MUST" of "SHALL"), "MAG/MOGEN NIET" ("MUST NOT" of "SHALL NOT"), "VERPLICHT" ("REQUIRED"), "MOET/MOETEN NORMAAL GESPROKEN" ("SHOULD"), "MAG/MOGEN NORMAAL GESPROKEN NIET" ("SHOULD NOT"), "AANBEVOLEN" ("RECOMMENDED"), "KAN/KUNNEN" ("MAY") en "FACULTATIEF" ("OPTIONAL") in dit document moeten worden geïnterpreteerd zoals beschreven in RFC 2911 [Bradner 1997].

Het PB wordt gepubliceerd door het Bureau voor publicaties van de Europese Unie (OP, Office des publications) op de EUR-Lex-website (zie punt 1.2.4) en dient als de enige authentieke bron van EU-wetgeving. Het PB verschijnt van maandag tot en met vrijdag, en eventueel in het weekend, in alle officiële talen van de Europese Unie (EU). *In het vervolg wordt de afkorting "PB" gebruikt om dit specifieke toepassingsgebied aan te duiden.*

1.1 Overzicht

Het PB-handtekeningbeleid formaliseert de voornaamste elementen van de implementatie van het aanmaken, valideren en op lange termijn bewaren van elektronische handtekeningen en elektronische zegels, zoals toegepast op het PB als een middel om door het OP gepubliceerde uitgaven van het PB te authenticeren.
Het bestaat uit:

- een inleiding waarin de titel/identificatie van het beleid, de gegevens over de uitgever van het beleid, het beleidsbeheer, de definities en afkortingen enz. zijn opgenomen;
- de verklaringen over handtekeningpraktijken, waarin de daarmee verband houdende beleidsmatige en wettelijke vereisten worden omschreven, alsmede de toepasselijke beveiligingsoverwegingen;

[1] Zie PB L 69 van 13.3.2013, blz. 1.

- de afbakeningsparameters voor bedrijfsprocessen, die een gedetailleerde beschrijving geven van de workflows in verband met het genereren van de elektronische handtekeningen en zegels waarmee de door het OP gepubliceerde PB-uitgaven worden geauthenticeerd;
- de eisen en verklaringen over de toepassing van technische mechanismen en normen, en bijlagen.

1.2 Bedrijfsdomein

1.2.1 Toepassingsgebied en grenzen van het handtekeningbeleid

Het PB-handtekeningbeleid heeft betrekking op elektronische handtekeningen en zegels die door bevoegde PB-ondertekenaars voor afzonderlijke PB-uitgaven worden gegenereerd overeenkomstig de verordening van de Raad betreffende elektronische publicatie van het Publicatieblad van de Europese Unie nadat de validering van elke te ondertekenen uitgave is geslaagd.

1.2.2 Toepassingsdomein

Onder het PB-handtekeningbeleid vallen uitsluitend de in punt 3.1 beschreven elektronische handtekeningen en zegels.

1.2.3 Transactiekader

Niet van toepassing.

1.3 Naam, identificatie en conformiteitsregels van het handtekeningbeleid

1.3.1 Beleidsnaam

De naam van het PB-handtekeningbeleid luidt:

Handtekeningbeleid Publicatieblad

1.3.2 Beleidsidentificatiecode

Aangezien er slechts één Publicatieblad van de Europese Unie is en de publicatie ervan een welbekend proces van de Europese Unie is, kan het PB-handtekeningbeleid door elke partij impliciet worden geïdentificeerd. Een beschrijving van de algemene bedrijfsworkflow is te vinden in punt 3.1.1.1.

Om uitdrukkelijk naar het beleid te verwijzen, *KAN* elke PB-handtekening of elk PB-zegel een expliciete aanduiding van het handtekeningbeleid omvatten, zoals gedefinieerd in punt 5.2.9 van [ETSI 2022-XAdES]. Indien het handtekeningbeleid expliciet wordt aangeduid, MOET deze aanduiding verwijzen naar objectidentificatienummer 1.3.171.4.1.1.4 volgens de coderingsvoorschriften in punt 5.2.9 van [ETSI 2022-XAdES] en [Mealling 2010].

Het wereldwijd unieke objectidentificatienummer 1.3.171.4.1.1.4 identificeert eenduidig de huidige versie van dit beleid. Het voorvoegsel 1.3.171.4 is geregistreerd als het basis-OID voor *Handtekeningbeleid en andere toepassingen van het Bureau voor publicaties van de Europese Unie* (zie http://www.oid-info.com/get/1.3.171.4). Het achtervoegsel 1.1.4 duidt de huidige versie van het PB-handtekeningbeleid aan en de ASN.1-waardenotatie daarvan met namen MOET als volgt luiden: {oj(1) signature-policy(1) version(4)}. Met deze versie wordt versie 1.1.3 van dit beleid overbodig.

1.3.3 Conformiteitsregels van het beleid

Dit beleid maakt geen aanspraak op enige overeenstemming met een ander beleid.

1.3.4 Distributiepunten van het beleid

Het PB-handtekeningbeleidsdocument wordt op de EUR-Lex-website gepubliceerd. Het kan worden opgezocht via de website https://eur-lex.europa.eu/ van het Publicatiebureau.

1.3.5 Geldigheidsduur van het beleid

De huidige versie van het beleid is vanaf 1 oktober 2023 van kracht.

1.3.6 Toepassingsgebied van het beleid

Dit handtekeningbeleid geldt voor alle uitgaven van het PB die zijn gepubliceerd na de datum van inwerkingtreding van de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie. Dit beleid is niet van toepassing op het supplement bij het Publicatieblad van de Europese Unie (S-serie, Publicatieblad S of PB S).

> OPMERKING: Elke versie van dit beleid is geldig tijdens de in elke versie vastgestelde geldigheidsduur. De versies bestrijken samen alle uitgaven van het PB.

1.4 Documentbeheer inzake het handtekeningbeleid

De uitgever van het PB-handtekeningbeleid is het Bureau voor publicaties van de Europese Unie, dat dit document heeft goedgekeurd en het op de EUR-Lex-website heeft gepubliceerd.

Het PB-handtekeningbeleid, zoals gepubliceerd, MOET automatisch rechtskracht hebben en MOET gelden voor het aanmaken, verifiëren en op lange termijn beheren van PB-handtekeningen en -zegels.

De uitgever van het PB-handtekeningbeleid is verantwoordelijk voor:

- de vaststelling en goedkeuring van het PB-handtekeningbeleid;
- de vaststelling van de herzieningsprocedure voor het PB-handtekeningbeleid;
- de vaststelling van de beoordelingscriteria en het proces om ervoor te zorgen dat het PB-handtekeningbeleid voldoet aan Verordening (EU) nr. 216/2013 van de Raad van 7 maart 2013 betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie en Verordening (EU) 2018/2056 van de Raad van 6 december 2018 tot wijziging van Verordening (EU) nr. 216/2013 betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie;
- de vaststelling van de beoordelingscriteria en de beoordelingsprocedure waarmee wordt gewaarborgd dat aanvragen die aanspraak maken op overeenstemming met het PB-handtekeningbeleid daadwerkelijk aan de geldende regels daarvan voldoen;
- de bekendmaking op EUR-Lex van het PB-handtekeningbeleid en gewijzigde versies daarvan.

1.4.1 Beleidsautoriteit

Het PB-handtekeningbeleid wordt beheerd door het Bureau voor publicaties van de Europese Unie.

1.4.2 Contactpersoon

De contactgegevens van de uitgever van dit beleid zijn:

Contactpersoon:	Hoofd administratieve eenheid Publicatieblad en Jurisprudentie
Postadres:	2, rue Mercier, L-2985 Luxembourg
Telefoonnummer:	+352 29291
Fax	+352 292944620
E-mailadres:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Goedkeuringsprocedures

De beleidsgoedkeuringsautoriteit binnen het Bureau voor publicaties van de Europese Unie is de directeur-generaal van het Bureau voor publicaties van de Europese Unie.

1.4.4 Versies van het beleid

In de oorspronkelijke en gewijzigde versies van het beleid *KAN* een minimale datum van inwerkingtreding worden vastgesteld. Een gepubliceerde versie van het beleid MOET per een van de volgende drie data in werking treden:

1. indien van toepassing, de minimale datum van inwerkingtreding zoals vastgesteld in de versie van het beleid;
2. de dag na de datum van de vroegste handtekeningtijdstempel op de PB-handtekening of het PB-zegel van de PB-uitgave met vermelding van de versie van het beleid die wordt gepubliceerd, volgens de plaatselijke tijd in Luxemburg;
3. de dag na de datum van bekendmaking van de versie van het beleid.

Een gewijzigde versie van het beleid MOET automatisch komen te vervallen wanneer de desbetreffende latere gewijzigde versie in werking treedt. In een latere gewijzigde versie van het beleid MOET bovendien de versie die zij overbodig maakt NORMAAL GESPROKEN worden aangegeven.

Bovenstaande regels hebben tot doel te waarborgen dat de handtekening van een bepaalde versie van het beleid niet rechtstreeks of onrechtstreeks onder dezelfde versie van het beleid valt, om cirkelredeneringen te voorkomen. Verder verdient het de voorkeur de overbodige versie op alle mogelijke manieren te bewaren.

1.5 Definities en afkortingen

De in dit document gebruikte definities en acroniemen staan vermeld in tabel 1.

Afkorting	**Definitie (EN-NL)**
CA	Certificate Authority (certificaatautoriteit)
DTBS	Data to Be Signed (te ondertekenen gegevens)
LTV	Long Term Validity (geldigheid op de lange termijn)
OID	Object Identifier (objectidentificatiecode)
PB	Publicatieblad van de Europese Unie
PIN	Personal Identification Number (persoonlijk identificatienummer)
OP	Bureau voor publicaties van de Europese Unie
QC	Qualified Certificate (gekwalificeerd certificaat)
QESig	Qualified Electronic Signature (gekwalificeerde elektronische handtekening)
QESeal	Qualified Electronic Seal (gekwalificeerd elektronisch zegel)
QSCD	Qualified Signature/Seal Creation Device (gekwalificeerd middel voor het aanmaken van handtekeningen/zegels)
SAA	Signature Augmentation Application (toepassing voor het verlengen van de geldigheid van handtekeningen)
SCA	Signature Creation Application (toepassing voor het aanmaken van handtekeningen)
SSCD	Secure Signature Creation Device (veilig middel voor het aanmaken van handtekeningen)
SVA	Signature Validation Application (toepassing voor het valideren van handtekeningen)
TSP	Trust Service Provider (verlener van vertrouwensdiensten)
QTSP	Qualified Trust Service Provider (gekwalificeerd verlener van vertrouwensdiensten)
Wipiwis	What Is Presented Is What Is Signed (ondertekend zoals gepresenteerd)

Tabel 1: Definities en afkortingen

2 Verklaringen over handtekeningpraktijken

2.1 Relevante beleidsvereisten

Uitgaven van het PB vallen onder de artikelen 1 en 2 van de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie, waarin onder andere is bepaald dat de elektronische editie van het Publicatieblad voorzien MOET zijn van een gekwalificeerde elektronische handtekening zoals gedefinieerd overeenkomstig Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad, of van een gekwalificeerd elektronisch zegel zoals gedefinieerd overeenkomstig diezelfde verordening.

Het elektronisch ondertekenen en verzegelen van PB-uitgaven valt onder de implementatie van een handtekening als een wezenlijke formaliteit zoals bedoeld in punt III.2.1 van de UITVOERINGSBEPALINGEN VAN DE EUROPESE COMMISSIE VOOR BESLUIT 2002/47/EG, EGKS, EURATOM INZAKE DOCUMENTENBEHEER EN VOOR BESLUIT 2004/563/EG, EURATOM INZAKE ELEKTRONISCHE EN GEDIGITALISEERDE DOCUMENTEN van 30 november 2009[2], waarin tevens wordt bepaald dat voor elektronische handtekeningen voor het PB een gekwalificeerde elektronische handtekening zoals gedefinieerd in [eIDAS] vereist is.

Krachtens artikel III.2.3 van de UITVOERINGSBEPALINGEN VOOR BESLUIT 2002/47/EG EN VOOR BESLUIT 2004/563/EG[2] is het de taak van de PB-SCA de ondertekenende autoriteit te verifiëren wanneer een ambtenaar van het OP in staat wordt gesteld PB-uitgaven elektronisch te ondertekenen of wanneer het OP als rechtspersoon in staat wordt gesteld om PB-uitgaven elektronisch te verzegelen.

Hoewel PB-uitgaven in elektronische vorm geen rechtsgevolgen kunnen hebben zonder te zijn ondertekend of verzegeld, bepaalt het PB-handtekeningbeleid tevens dat de PB-SCA MOET waarborgen dat slechts de bevoegde PB-ondertekenaars PB-uitgaven kunnen afwijzen, met het oog op een doeltreffende preventie van aanvallen op het publicatieproces van het PB.

Aangezien bevoegde PB-ondertekenaars namens het OP optreden, behoort het tot de verantwoordelijkheid van de directeur-generaal van het OP om (door middel van delegatie) zorg te dragen voor deugdelijke goedkeuring van de respectieve QC's voor ondertekening van het PB. Daartoe geldt dat machtiging van QC's voor ondertekening van het PB:

- correct *MOET* worden geconfigureerd in het gebruikersbeheer van de PB-SCA;
- *NORMAAL GESPROKEN* beperkt *MOET* worden tot bedrijfscertificaten (beroepsmatige certificaten) die waarborgen dat de betrokken persoon aan het OP verbonden is[3];
- transparant *MOET* worden gemaakt door de gemachtigde QC's op de EUR-Lex-website te publiceren, in overeenstemming met artikel 2 van de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie.

2.2 Relevante juridische vereisten

Voor de implementatie van elektronische handtekeningen en elektronische zegels zoals bedoeld in het PB-handtekeningbeleid MOETEN de volgende wettelijke bepalingen gelden:

[2] Zie SEC(2009) 1643.

[3] Bedrijfscertificaten waarborgen dat de betrokken persoon aan een bepaalde organisatie verbonden is. Een grotere mate van zekerheid wordt bereikt doordat de uitgevende QTSP van de desbetreffende certificaathouder verlangt te bewijzen daartoe gerechtigd te zijn.

- Verordening (EU) nr. 216/2013 van de Raad van 7 maart 2013 betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie;
- Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG[4];
- 2009/767/EG: Beschikking van de Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het "één-loket" in het kader van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt[5];
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)[6];
- Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)[7];
- Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming[8];
- 2010/425/EU: Besluit van de Commissie van 28 juli 2010 tot wijziging van Beschikking 2009/767/EG wat betreft het opstellen, bijwerken en publiceren van vertrouwenslijsten van certificatiedienstverleners die onder toezicht staan of zijn geaccrediteerd in een lidstaat[9];
- 2009/496/EG, EURATOM: Besluit van het Europees Parlement, de Raad, de Commissie, het Hof van Justitie, de Rekenkamer, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 26 juni 2009 betreffende de organisatie en de werking van het Bureau voor publicaties van de Europese Unie[10];
- 2011/130/EU: Besluit van de Commissie van 25 februari 2011 tot vaststelling van minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt[3].

[4] Zie PB L 257 van 28.8.2014, blz. 73.

[5] Zie PB L 274 van 20.10.2009, blz. 36.

[6] Zie PB L 119 van 4.5.2016, blz. 1.

[7] Zie PB L 201 van 31.7.2002, blz. 37.

[8] Zie PB L 337 van 18.12.2009, blz. 11.

[9] Zie PB L 199 van 31.7.2010, blz. 30.

[10] Zie PB L 168 van 30.6.2009, blz. 41.

2.3 Technische beveiligingsoverwegingen

Cryptografische instrumenten die in aanmerking komen voor de implementatie van PB-handtekeningen en -zegels MOETEN voldoen aan de vereisten voor gekwalificeerde elektronische handtekeningen als omschreven in [eIDAS], in [ETSI 2016] en in het kader van de meest geavanceerde praktijken op dit gebied.

2.4 Juridische verklaringen

Elektronische handtekeningen en zegels op PB-uitgaven moeten namens het OP op grond van de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie worden gegenereerd.

3 Afbakeningsparameters voor bedrijfsprocessen (BSP's, Business Scoping Parameters)

3.1 BSP's die voornamelijk verband houden met de betrokken toepassing/het betrokken bedrijfsproces

3.1.1 BSP (a): workflow (opeenvolging en timing) van handtekeningen

3.1.1.1 Algemene beschrijving van de bedrijfsworkflow

Het PB wordt door het OP van maandag tot en met vrijdag, en eventueel tijdens het weekend gepubliceerd. Deze publicatie van het PB kan een uitgave van een PB of van een PB-handeling zijn. Een uitgave van een PB is een meertalige bekendmaking van een of meer documenten. Elke taalversie van een uitgave bestaat uit de volledige tekst van elk document in één enkel bestand. Een uitgave van een PB-handeling is een meertalige publicatie van één enkel document dat op zichzelf wordt gepubliceerd. Elke taalversie van een uitgave van een PB-handeling bestaat uit de volledige tekst van elk document in één enkel bestand.

De afzonderlijke uitgaven van het PB en van PB-handelingen worden gecategoriseerd volgens de serie waartoe zij behoren, waarbij de categoriecode onderdeel uitmaakt van de identificatie van het PB. Voor het toepassingsgebied waar het hier om gaat, zijn twee series van belang: L (wetgeving) en C (mededelingen en bekendmakingen). Een serie kan eventueel ook subseries en classificatiesystemen omvatten (zie http://publications.europa.eu/code/en/en-10000.htm voor uitgebreidere informatie over het toepassingsgebied, de documentstructuur en aanvullende achtergrondinformatie).

Naast de L- en C-series van het PB worden ook bijzondere uitgaven met secundaire EU-wetgeving gepubliceerd in de taal van een toetredend land of nieuwe lidstaat. Deze bijzondere uitgaven vallen ook onder het toepassingsgebied.

Zodra een uitgave van een PB of van een PB-handeling volledig is (d.w.z. alle taalversies van de uitgave van een PB of van een PB-handeling zijn in PDF/A beschikbaar) en klaar voor publicatie, wordt de workflow voortgezet met een elektronisch verzegelingsproces (zie punt 3.1.1.2) of een elektronisch ondertekeningsproces (zie punt 3.1.1.3). In geval van elektronische verzegeling wordt automatisch een gekwalificeerd elektronisch zegel gegenereerd met behulp van een gekwalificeerd elektronisch verzegelingscertificaat dat aan het OP als entiteit van de Europese Commissie is afgegeven. In geval van elektronische ondertekening wordt een gekwalificeerde elektronische handtekening gegenereerd door een bevoegd persoon met behulp van een gekwalificeerd elektronisch ondertekeningscertificaat.

De elektronische verzegeling is de door de SCA geselecteerde standaardworkflow, d.w.z. uitgaven van een PB of van een PB-handeling die volledig zijn, zullen het geautomatiseerde verzegelingsproces doorlopen, tenzij het verzegelingsproces niet beschikbaar is. In het laatste geval wordt het ondertekeningsproces gebruikt.

Aangezien voor de ondertekening van elke uitgave een los(se) XAdES-handtekening of -zegel met een manifest (zie [Bartel 2008], [ETSI 2022-XAdES] en Besluit 2011/130/EU van de Commissie van 25 februari 2011 tot vaststelling van minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt[11]) wordt gebruikt, moet bij de verificatie van een handtekening of zegel van een PB of een PB-handeling tijdens de validering volgens [ETSI

[11] PB L 53 van 26.2.2011, blz. 66.

2022-XAdES] ook het manifest worden gevalideerd, in aanvulling op de validering van de XML-kernhandtekening (zie [Bartel 2008]).

In de volgende punten worden de elektronische verzegelings- en ondertekeningsworkflows op hoog niveau beschreven zoals die geïmplementeerd zijn in de PB-SCA, -SAA en -SVA (zie [ETSI 2016]).

3.1.1.2 Aanmaken van een zegel PB en zegel PB-handeling

1. Een volledige uitgave van een PB of van een PB-handeling wordt gedetecteerd voor verzegeling.
2. De SCA voert eerste verificaties uit van de ingediende bestanden:
    a. of er qua omvang inconsistenties zijn tussen de taalversies van de uitgave van een PB of van een PB-handeling en of deze binnen configureerbare grenzen blijven;
    b. of alle verstrekte taalversies voor publicatie waren voorzien.
3. Als de verificatie mislukt, wordt het verzegelingsproces onderbroken. Om het verzegelingsproces te hervatten, is een manuele interventie van bevoegd OP-personeel vereist.
4. Na succesvolle validering door de SCA wordt een manifest gegenereerd met verwijzingen naar elke taalversie van de volledige uitgave. Bovendien komt elke taalversie overeen met een enkele EU-taal; de taalversie krijgt de vorm van een PDF/A-document dat voor de berekening van de hashwaarde van het bericht (“message digest”) als een binaire octetstroom wordt beschouwd.
5. De SCA authenticeert zich bij het centrale portaal voor elektronische handtekeningen van de Europese Commissie en stuurt het gegenereerde manifest voor geautomatiseerde verzegeling.
6. Het portaal voor elektronische handtekeningen verzegelt het verstrekte manifest met behulp van een gekwalificeerd verzegelingscertificaat, dat is afgegeven door een geaccrediteerde Europese QTSP (zie [eIDAS]). De privésleutel voor dit verzegelingscertificaat wordt opgeslagen op een QSCD dat een interface heeft met het portaal voor elektronische handtekeningen.
7. Het aldus gecreëerde XAdES-zegel (zie [ETSI 2022-XAdES]) wordt vervolgens teruggestuurd naar de SCA, die de geldigheid van onder andere de gebruikte algoritmen controleert en zich ervan vergewist dat het verzegelingscertificaat van het desbetreffende zegel goedgekeurd is en eigendom is van dezelfde rechtspersoon die als bevoegde ondertekenaar is geauthenticeerd.
8. Na een succesvolle verificatie wordt de geldigheid van het elektronische zegel verlengd door middel van een door een erkende QTSP afgegeven handtekeningtijdstempel (zie [eIDAS]).
9. Het in de vorige bewerkingsstap verlengde elektronische zegel wordt overgebracht voor bekendmaking op de EUR-Lex-website. Tegelijkertijd wordt een identieke kopie van het zegel door de SCA bewaard.
10. Wanneer de vereiste respijtperiode van 24 uur voor een zegel dat het resultaat is van de vorige verwerkingsstap is verstreken, wordt dit verder verlengd tot een zelfstandige vorm zodat de handtekening lange tijd geldig is, met gebruikmaking van de vertrouwde tijdstempeldienst van een geaccrediteerde Europese QTSP (zie [eIDAS]).

11. Het in de vorige bewerkingsstap verlengde zegel wordt overgebracht voor bekendmaking op de EUR-Lex-website en vervangt daarbij het nog niet tot een zelfstandige vorm uitgebreide zegel van stap 9.
12. Naast de bekendmaking op de EUR-Lex-website worden identieke kopieën van de documenten die samen een uitgave van een PB of van een PB-handeling vormen, samen met het bijbehorende zegel in zelfstandige vorm overgebracht naar het systeem voor digitale bewaring op lange termijn, dat door het OP wordt beheerd en waarin de officiële documenten van de EU-instellingen op lange termijn worden bewaard. Uitvoeringsaspecten met betrekking tot de bewaring op lange termijn vallen NIET onder dit handtekeningbeleid.

3.1.1.3 Aanmaken van een handtekening PB of PB-handeling

1. Een volledige uitgave van een PB of van een PB-handeling wordt gedetecteerd voor ondertekening.
2. Er wordt een manifest gegenereerd met verwijzingen naar elke taalversie van de volledige uitgave. Bovendien komt elke taalversie overeen met een enkele EU-taal; de taalversie krijgt de vorm van een PDF/A-document dat voor de berekening van de hashwaarde van het bericht ("message digest") als een binaire octetstroom wordt beschouwd.

   Complete uitgaven worden tijdens het genereren van het manifest uitsluitend door de SCA beheerd en vergrendeld met het oog op een consistente berekening van de hashwaarde, aangezien dit voor het slagen van dat proces van essentieel belang is.
3. Na succesvolle authenticatie door de SCA kan een bevoegde ondertekenaar een complete uitgave selecteren voor ondertekening, op voorwaarde dat bij de vorige stap het bijbehorende manifest is gegenereerd.
4. Na met succes een te ondertekenen uitgave te hebben geselecteerd, begint de bevoegde ondertekenaar de ondertekeningsprocedure voor deze specifieke uitgave:
   a. om het Wipiwis-beginsel naar behoren na te leven, moet de bevoegde ondertekenaar, alvorens de uitgave te kunnen ondertekenen, ten minste drie verschillende taalversies bekijken met behulp van een conforme PDF/A-viewer. Als de uitgave van een PB of van een PB-handeling minder dan drie taalversies omvat, is de bevoegde ondertekenaar verplicht alle beschikbare taalversies te bekijken.

      De SCA stelt de ondertekenaar in staat elk van de taalversies van de te ondertekenen uitgave te bekijken. De ondertekenaar KAN derhalve desgewenst de gehele te ondertekenen inhoud bekijken;
   b. de bevoegde ondertekenaar kan er bewust voor kiezen de uitgave te verwerpen, waardoor de ondertekeningsprocedure wordt afgebroken, dan wel door middel van de knop Ondertekenen door te gaan met de ondertekening;
   c. wanneer op de knop Ondertekenen wordt gedrukt:
      i. genereert de SCA een verzoek om ondertekening, gericht aan het centrale portaal voor elektronische handtekeningen van de Europese Commissie, waarbij het te ondertekenen manifest wordt gestuurd en de bevoegde ondertekenaar naar het portaal wordt verwezen;
      ii. authenticeert de bevoegde ondertekenaar zichzelf op het portaal voor elektronische handtekeningen en wordt hem het te ondertekenen manifest getoond overeenkomstig de Wipiwis-beginselen;

iii. maakt het portaal voor elektronische handtekeningen verbinding met de middleware die op het werkstation van de bevoegde ondertekenaar geïnstalleerd is en vraagt het gekwalificeerde ondertekeningscertificaat van de ondertekenaar op, dat is afgegeven door een geaccrediteerde Europese QTSP (zie [eIDAS]). Dit certificaat wordt voorgelegd aan de bevoegde ondertekenaar, die op zijn beurt wordt verzocht de overeenkomstige PIN waarmee het QSCD is beveiligd in te voeren om het QSCD te machtigen de handtekening aan te maken met behulp van de privésleutel die overeenkomt met het geselecteerde ondertekeningscertificaat, waarmee het ondertekeningsproces wordt afgerond;

d. De middleware zendt de waarde van de gegenereerde handtekening naar het portaal voor elektronische handtekeningen, dat op zijn beurt een overeenkomstige XAdES-handtekening genereert (zie [ETSI 2022-XAdES]).

5. Deze XAdES-handtekening wordt vervolgens teruggestuurd naar de SCA, die – via het portaal voor elektronische handtekeningen – de geldigheid van onder andere de gebruikte algoritmen controleert en zich ervan vergewist dat het verzegelingscertificaat van de desbetreffende handtekening goedgekeurd is en eigendom is van dezelfde persoon die als bevoegde ondertekenaar is geauthenticeerd.
6. Na een succesvolle verificatie wordt de geldigheid van de handtekening – via het portaal voor elektronische handtekeningen – verlengd door middel van een door een erkende QTSP afgegeven handtekeningtijdstempel (zie [eIDAS]).
7. De in de vorige bewerkingsstap uitgebreide handtekening wordt overgebracht voor bekendmaking op de EUR-Lex-website. Tegelijkertijd wordt een identieke kopie van de handtekening door de SCA bewaard.
8. Wanneer de vereiste respijtperiode van 24 uur voor een handtekening die het resultaat is van de vorige verwerkingsstap is verstreken, wordt deze verder verlengd tot een zelfstandige vorm zodat de handtekening lange tijd geldig is, met gebruikmaking van de vertrouwde tijdstempeldienst van een geaccrediteerde Europese QTSP (zie [eIDAS]).
9. De in de vorige bewerkingsstap uitgebreide handtekening wordt overgebracht voor bekendmaking op de EUR-Lex-website en vervangt daarbij de nog niet tot een zelfstandige vorm uitgebreide handtekening van stap 7.
10. Naast de bekendmaking op de EUR-Lex-website worden identieke kopieën van de documenten die samen een uitgave van een PB of van een PB-handeling vormen, samen met de bijbehorende handtekening in zelfstandige vorm overgebracht naar het systeem voor digitale bewaring op lange termijn, dat door het OP wordt beheerd en waarin de officiële documenten van de EU-instellingen op lange termijn worden bewaard. Uitvoeringsaspecten met betrekking tot de bewaring op lange termijn vallen NIET onder dit handtekeningbeleid.

3.1.1.4 Noodsituatie

Wanneer het als gevolg van een onvoorziene en uitzonderlijke onbeschikbaarheid van het PB-SCA niet mogelijk is om het zegel of de handtekening van een PB of een PB-handeling aan te maken zoals beschreven in de punten 3.1.1.2 of 3.1.1.3, past het Publicatiebureau een QESeal of QESig toe op elk PDF/A-document dat overeenkomt met elke taalversie van de uitgave van het PB of de PB-handeling. Alle verzegelde/ondertekende PDF/A-documenten worden overgebracht voor publicatie op de EUR-Lex-website.

3.1.2 BSP (b): te ondertekenen gegevens

- Handtekeningen en zegels van een PB of een PB-handeling baseren hun vertrouwen op een XML-manifest (zie [Bartel 2008] en [ETSI 2022-XAdES]) waarin alle in PDF/A-formaat beschikbare taalversies die verband houden met een uitgave van een PB of een PB-handeling tot één enkele handtekening zijn gecombineerd en die aan de volgende eisen moet voldoen: elke taalversie die logisch verband houdt met een uitgave van een PB of een PB-handeling *MOET* een eigen hashwaarde hebben;
- alle taalversies die logisch verband houden met een uitgave van een PB of een PB-handeling *MOETEN* tijdens het aanmaken van de handtekening aan de ondertekenaar ter controle worden aangeboden, zodat de inhoud van de handtekening naar inzicht van de ondertekenaar kan worden geverifieerd, zoals beschreven in punt 3.1.1.3, en het Wipiwis-beginsel zodoende wordt nageleefd;
- een correcte visualisatie *MOET* worden gegarandeerd door het gebruik van een conforme PDF/A-lezer;
- de tijdens het ondertekeningsproces aan de ondertekenaar voorgelegde taalversies MOETEN betrekking hebben op de specifieke uitgave die wordt ondertekend;
- om de consistentie te waarborgen, *MOETEN* de technische kenmerken van alle taalversies die logisch verband houden met een uitgave van een PB of een PB-handeling tijdens het aanmaken van het zegel en de handtekening worden geverifieerd.

In het geval van een noodsituatie als beschreven in punt 3.1.1.4 zijn de volgende eisen van toepassing:

- elke taalversie van een uitgave van een PB of een PB-handeling *MOET* een eigen QESeal of QESig hebben;
- alle taalversies die logisch verband houden met een uitgave van een PB of een PB-handeling *MOETEN* tijdens het aanmaken van de handtekening aan de ondertekenaar worden gecontroleerd, zodat de inhoud van de handtekening naar inzicht van de ondertekenaar kan worden geverifieerd en het Wipiwis-beginsel zodoende wordt nageleefd;
- een correcte visualisatie *MOET* worden gegarandeerd door het gebruik van een conforme PDF/A-lezer.

3.1.3 BSP (c): het verband tussen de ondertekende gegevens en de handtekening(en) en zegel(s)

Een handtekening of zegel van een PB of een PB-handeling is van toepassing op alle taalversies van een uitgave van een PB of een PB-handeling, die elk afzonderlijk als PDF/A-document zijn opgemaakt.

Bij het aanmaken van een handtekening of zegel van een PB of een PB-handeling wordt de digitale inhoud van een te ondertekenen of te verzegelen document gecodeerd tot een binaire octetstring met behulp van het sterkste ondersteunde hashing-algoritme dat aan punt 7.3 van [ETSI 2022-Crypto] voldoet.

De hashwaarden van de afzonderlijke documenten worden met de URI's van de oorspronkelijke bestandsnamen tot een XML-manifest gecombineerd, zonder toepassing van aanvullende omzettingen (zie [Bartel 2008]).

Het manifest, met inbegrip van de ondertekende attributen, wordt door middel van XAdES (zie [ETSI 2022-XAdES]) ondertekend of verzegeld voor het in Besluit 2011/130/EU van de Commissie van 25 februari 2013 vastgestelde profiel.

In het geval van een noodsituatie als beschreven in punt 3.1.1.4 wordt elk PDF/A-document dat elke taalversie van het PB of de PB-handeling vertegenwoordigt, ondertekend of verzegeld met behulp van PAdES (zie [ETSI 2016-PAdES] [eIDAS]).

3.1.4 BSP (d): doelgemeenschap

De doelgemeenschap is elke partij die vertrouwt op de authenticiteit van het PB en deze moet verifiëren, alsook alle partijen die verantwoordelijk zijn voor de implementatie van de SCA en SAA die worden gebruikt om elektronische handtekeningen of elektronische zegels aan te maken en de geldigheid ervan te verlengen voor uitgaven van een PB of een PB-handeling.

3.1.5 BSP (e): toewijzing van de verantwoordelijkheid voor de validering en verlenging van handtekeningen

3.1.5.1 Verificatie van handtekeningen en zegels van een PB of een PB-handeling

Elke vertrouwende partij, en met name elke Europese burger, kan een op de website EUR-Lex gepubliceerde uitgave van een PB of een PB-handeling en de bijbehorende losse XAdES-handtekening of het desbetreffende zegel (zie [ETSI 2022-XAdES]) voor verificatie downloaden.

Aangezien voor het aanmaken van een handtekening of een zegel een interoperabele Europese handtekeningnorm en diensten van een geaccrediteerde Europese QTSP (zie [eIDAS]) worden gebruikt, kan de verificatie worden uitgevoerd door gebruik te maken van elk door derden aangeboden verificatiemiddel dat aan de toegepaste normen voldoet, voor zover het manifest op grond van het PB-handtekeningbeleid kan worden gevalideerd.

In het geval van een noodsituatie als beschreven in punt 3.1.1.4 wordt elk PDF/A-document dat elke taalversie van het PB of de PB-handeling vertegenwoordigt, ondertekend of verzegeld met behulp van PAdES (zie [ETSI 2016-PAdES]). De verificatie hiervan kan worden uitgevoerd door gebruik te maken van elk door derden aangeboden verificatiemiddel dat aan de toegepaste normen voldoet.

3.1.5.1.1 Verificatie aan serverzijde

Ter vergemakkelijking van de verificatie van handtekeningen en zegels KAN het OP een gratis PB-SVA aan serverzijde aanbieden, die werkt volgens de onderstaande verificatieworkflow:

1. de verificateur uploadt het te verifiëren PDF/A-bestand samen met het bijbehorende handtekening- of zegelbestand met behulp van de SVA-functie voor het uploaden van bestanden;
2. de SVA berekent de hashwaarde van het geüploade PDF/A-bestand en verifieert of de berekende hashwaarde in het manifestgedeelte van de geüploade handtekening aanwezig is;
3. als de verificatie van de hashwaarde geslaagd is, wordt de XAdES-standaardverificatie van de geüploade kandidaathandtekening of het geüploade kandidaatzegel uitgevoerd, op voorwaarde dat het ondertekenings- of verzegelingscertificaat een bevoegde PB-ondertekenaar aanwijst voor de door het handtekeningtijdstempel bepaalde periode. De SVA verifieert ook of de ondertekenaar tot ondertekening bevoegd was op het moment dat de handtekening volgens het handtekeningtijdstempel werd aangemaakt;
4. de verificatie is geslaagd wanneer alle voorgaande stappen met succes zijn beëindigd. Is dit niet het geval, dan is de uitkomst van de verificatie negatief. In elk geval wordt een volledig verslag van het verificatieproces aan de verificateur voorgelegd.

3.1.5.1.2 Verificatie aan clientzijde

Ter vergemakkelijking van de verificatie van handtekeningen en zegels KAN het OP een gratis PB-SVA aan clientzijde aanbieden, die werkt volgens de onderstaande verificatieworkflow:

1. de verificateur start de gedownloade SVA op, de elektronische handtekening van de programmacode ervan wordt automatisch door de runtime-omgeving geverifieerd en de uitvoering ervan wordt door de verificateur toegestaan wanneer die verificatie is geslaagd;
2. de verificateur selecteert met behulp van de SVA-dialoog voor het selecteren van bestanden een PDF/A-bestand in een bepaalde te verifiëren taalversie samen met het bijbehorende kandidaathandtekening- of kandidaatzegelbestand in het bestandssysteem van de lokale pc;
3. de SVA berekent de hashwaarde van het geselecteerde document en verifieert of de berekende hashwaarde in het manifest van de geselecteerde kandidaathandtekening of het geselecteerde kandidaatzegel aanwezig is;
4. als de verificatie van de hashwaarde geslaagd is, wordt de XAdES-standaardverificatie van de geselecteerde kandidaathandtekening of het geselecteerde kandidaatzegel uitgevoerd;
5. de verificatie is geslaagd wanneer alle voorgaande stappen met succes zijn beëindigd en het ondertekenings- of verzegelingscertificaat een bevoegde PB-ondertekenaar aanwijst voor de door het handtekeningtijdstempel bepaalde periode.

   De gegevens betreffende de bevoegde ondertekenaar KUNNEN bij de SVA bekend zijn op basis van een (standaard-)configuratie. De hashwaarde van het ondertekenings- of verzegelingscertificaat wordt echter ook in het SVA-resultaat vermeld, zodat de verificateur deze handmatig kan vergelijken met de gepubliceerde gegevens over de bevoegde ondertekenaar voor de periode waarin de handtekening of het zegel is aangemaakt, die ook in de SVA vermeld is.

3.2 BSP's die voornamelijk worden beïnvloed door de wettelijke/bestuursrechtelijke bepalingen in verband met de betrokken toepassing/het betrokken bedrijfsproces

3.2.1 BSP (f): Juridisch type van de handtekeningen

Elektronische handtekeningen en zegels op een PB of een PB-handeling MOETEN QESig en QESeal zijn in de zin van [eIDAS].

Bovengenoemd vereiste berust met name op de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie (zie punt 2.2).

Elke ondertekenaar moet een QC verkrijgen om gebruik te kunnen maken van het ondertekeningssysteem.

De kwaliteit van bepaalde elementen van de vereiste QESig en QESeal MOET voldoen aan de volgende kwaliteitseisen:

- middel voor ondertekening en verzegeling: QSCD's die voldoen aan bijlage II van [eIDAS];
- certificaatverlening: QC dat voldoet aan bijlage I van [eIDAS];
- onafhankelijke waarborg voor certificaatlevering: QC afgegeven door een onder toezicht staande of geaccrediteerde QTSP-certificatiedienst die is geaccrediteerd in een land waar [eIDAS] van toepassing is;

- softwarepakket voor handtekeningversleuteling: alleen softwarepakketten voor handtekeningen vermeld in punt 7.3 van [ETSI 2022-Crypto] mogen worden gebruikt;
- LTV-oplossingen: XAdES-handtekeningen en zegels van een PB of PB-handeling (zie [ETSI 2022-XAdES]) MOETEN worden verlengd tot de vorm met -LTA, hetgeen onder meer de vernieuwing van de archiveringstijdstempels dan wel een ander mechanisme inhoudt (externe beveiligde archiveringsmechanismen KUNNEN als alternatief voor de vernieuwing van de archiveringstijdstempels worden beschouwd, op voorwaarde dat zij van dezelfde of een hogere kwaliteit zijn);
- toepassing voor het aanmaken van handtekeningen: de kwaliteit van de PB-SCA MOET aan de door EC-beleid gestelde kwaliteitseisen voldoen en in overeenstemming zijn met de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie.

3.2.2 BSP (g): verbintenis van de ondertekenaar

Elektronische handtekeningen en zegels op uitgaven van een PB of PB-handeling MOETEN namens het OP overeenkomstig de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie worden gegenereerd.

De verbintenis die een bevoegde PB-ondertekenaar aangaat, houdt in dat hij of zij verklaart dat de ondertekende gegevens een authentieke uitgave van een PB of PB-handeling vormen die naar behoren is gevalideerd met inachtneming van de regels met betrekking tot het toepassingsgebied van de bedrijfstoepassing (zie punt 3.1.1) en die door het OP is bekendgemaakt in overeenstemming met de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie, zodat deze als authentieke bron van EU-wetgeving kan dienen.

Een expliciete aanduiding van het verbintenistype MOET ontbreken in een PB-handtekening (zie punt 5.2.3 van [ETSI 2022-XAdES]).

3.2.3 BSP (h): mate van zekerheid over tijdsgegevens

Aan handtekeningen of zegels van een PB of PB-handeling die zijn aangemaakt zoals beschreven in de punten 3.1.1.2 of 3.1.1.3 MOET een handtekeningtijdstempel worden toegevoegd op dezelfde dag (plaatselijke tijd in Luxemburg) als de datum van ondertekening of verzegeling van de uitgave van het PB of de PB-handeling, om te bevestigen dat de handtekening of het zegel niet na de datum van bekendmaking is aangemaakt. Hierdoor wordt gewaarborgd dat de groep van bevoegde ondertekenaars die geldt op de datum van bekendmaking ook geldt voor de handtekening of het zegel.

De PB-SCA MOET ervoor zorgen dat alle gegenereerde XAdES-B-T-handtekeningen aan deze eis voldoen.

De tijdstempels die worden gebruikt voor het aanmaken van handtekeningtijdstempels in XAdES-B-T-handtekeningen MOETEN gekwalificeerde tijdstempels zijn.

PAdES-handtekeningen die worden aangemaakt in een noodsituatie zoals beschreven in punt 3.1.1.4 KUNNEN zonder handtekeningtijdstempel worden aangemaakt.

Indien PAdES-handtekeningen die worden aangemaakt in een noodsituatie zoals beschreven in punt 3.1.1.4, worden aangemaakt met een handtekeningtijdstempel, MOET het handtekeningtijdstempel NORMAAL GESPROKEN een gekwalificeerd tijdstempel zijn dat op dezelfde dag (plaatselijke tijd in Luxemburg) wordt aangebracht als de datum van de ondertekening of het zegel van de uitgave van het PB of de PB-handeling, om te bevestigen dat de handtekening of het zegel niet na de datum van bekendmaking is aangemaakt.

OPMERKING: Dit betekent dat indien in een noodsituaties in de handtekening een handtekeningtijdstempel is opgenomen, dit een niet-gekwalificeerd tijdstempel kan zijn.

Alle andere tijdstempels, met inbegrip van eventuele archiveringstijdstempels en inhoudstijdstempels, MOETEN NORMAAL GESPROKEN gekwalificeerde tijdstempels zijn.

3.2.4 BSP (i): formaliteiten voor ondertekening

Het is de taak van de PB-SCA te voorzien in een interface voor ondertekenaars die, voor zover mogelijk, een geschikte omgeving voor het aanmaken van rechtsgeldige handtekeningen en zegels waarborgt. Deze interface moet:

- gepast advies en informatie bieden over het ondertekenings- en verzegelingsproces van de toepassing;
- zorgen voor samenhang tussen het gebruik van de juiste gegevens voor het aanmaken en verifiëren van handtekeningen en zegels, de middelen voor het aanmaken van handtekeningen en zegels, de te ondertekenen gegevens en de verwachte reikwijdte en het verwachte doel van de handtekening en zegel (of van de ondertekenings- of verzegelingshandeling);
- een duidelijke uitdrukking van de wil tot ondertekenen en de intentie van de gebruiker gebonden te zijn door de handtekening of het zegel mogelijk maken en aantonen;
- geïnformeerde toestemming mogelijk maken en aantonen.

De PB-SVA MOET de vertrouwende partijen (met inbegrip van de ondertekenaar) correcte procedures bieden voor de verificatie en archivering van de elektronische handtekening of het elektronische zegel en van de verificatiegegevens.

3.2.5 BSP (j): levensduur en bestendigheid tegen veranderingen

De ondertekende uitgaven van PB's en PB-handelingen en de handtekeningen daarvan MOETEN voor onbepaalde tijd worden bewaard. Het behoud van de geldigheid van de handtekeningen van PB's en PB-handelingen MOET voor een dergelijke periode worden gewaarborgd (zie artikel 2 van de verordening van de Raad betreffende de elektronische publicatie van het Publicatieblad van de Europese Unie).

3.2.6 BSP (k): archivering

Niet van toepassing.

3.3 BSP's die voornamelijk verband houden met de actoren die betrokken zijn bij het aanmaken/verlengen/valideren van handtekeningen

3.3.1 BSP (l): identiteit (en rollen/attributen) van de ondertekenaars

3.3.1.1 Regels voor voorgestelde ondertekenaars en hun identificatie

Handtekeningen van een PB en PB-handelingen MOETEN door bevoegde ondertekenaars worden toegepast, die meer in het bijzonder ambtenaren van het OP MOETEN zijn die over de nodige deskundigheid beschikken voor de validering van uitgaven van een PB en PB-handelingen volgens de regels met betrekking tot het toepassingsgebied van de bedrijfstoepassing (zie punt 3.1.1.3). In het geval van zegels van een PB en PB-handelingen MOET de bevoegde ondertekenaar het OP zelf zijn als entiteit van de Europese Commissie.

Bevoegde ondertekenaars MOETEN zich ook van hun verantwoordelijkheid bewust zijn en MOETEN te goeder trouw handelen bij de authenticatie van juridische teksten waarin EU-wetgeving is vastgelegd.

Het verband tussen deze ondertekenaars als natuurlijke personen enerzijds en hun handtekeningverificatiegegevens anderzijds MOET worden vastgelegd in een QC in de zin van [eIDAS], waarin hun identiteit en hun verbondenheid met het OP worden bevestigd.

Een PB-ondertekenaar MOET door de directeur-generaal van het OP (eventueel door middel van delegatie) worden gemachtigd

3.3.1.2 Rollen en attributen van de ondertekenaar

De verbondenheid van de ondertekenaar met het OP MOET het enige attribuut voor rollen, functies of kwalificaties zijn waarvoor certificatie in het QC van de ondertekenaar vereist is.

Het MOET de verantwoordelijkheid van de PB-SCA zijn te zorgen voor een gedegen toegangscontrole en machtiging van ondertekenaars alvorens ondertekenaars toegang te verlenen tot de handtekeningfuncties van het authentieke PB.

Toegangscontrole en machtiging van ondertekenaars MOETEN geschieden op basis van een in de SCA geïmplementeerd sterk authenticatiemechanisme en met inachtneming van de machtigingen die zijn geregistreerd met de publiekesleutelcertificaten die bij de bevoegde ondertekenaars in de SCA-gebruikersbeheerdatabank horen.

Vertrouwende partijen *KUNNEN* de gepubliceerde certificaten van PB-ondertekenaars gebruiken om hun wettelijke bevoegdheid te verifiëren.

3.3.1.3 Relevant bewijs van bevoegdheid

Geen verdere bepalingen naast die van punt 3.3.1.2.

3.3.2 BSP (m): vereist betrouwbaarheidsniveau voor authenticatie van de ondertekenaar

Het vereiste betrouwbaarheidsniveau voor de authenticatie van de ondertekenaar wordt gewaarborgd door zijn gekwalificeerd certificaat en het middel waarmee hij zijn handtekening aanmaakt, dat een gekwalificeerd middel voor het aanmaken van handtekeningen/zegels, zoals gedefinieerd in [eIDAS] MOET zijn.

3.4 Andere BSP's

3.4.1 BSP (o): andere informatie die aan de handtekening of het zegel moet worden gekoppeld

3.4.1.1 Gemachtigde PB-ondertekenaars en tijdstempelautoriteiten

Verificatie van de bevoegdheid van ondertekenaars is een essentieel vertrouwensaspect van het authentieke PB.

De bevoegdheid MOET uitdrukkelijk worden bekendgemaakt door de elektronische certificaten van alle bevoegde ondertekenaars via een betrouwbaar medium buiten de SCA/SVA te publiceren.

Bij de publicatie van bevoegde PB-ondertekenaars MOET worden vermeld dat de toezichtstatus van de ondertekenaarscertificaten voor de huidige ondertekeningsperiode voor PB's en PB-handelingen gewaarborgd is.

De bevoegde PB-ondertekenaars en tijdstempelautoriteiten MOGEN NIET in het PB worden gepubliceerd, omdat deze aanpak zou leiden tot cirkelredeneringen, met name met betrekking tot de validering op lange termijn.

Wanneer bevoegde PB-ondertekenaars in de loop van de tijd worden vervangen, MOET de eerdere groep ondertekenaars als historische vertrouwensinformatie worden gepubliceerd. Dit is vereist voor het verifiëren van door deze ondertekenaars ondertekende uitgaven van PB's of PB-handelingen.

Bij de bekendmaking van bevoegde ondertekenaars MOET de periode worden aangeven waarvoor de vermelde ondertekenaars bevoegd waren of zijn; deze vermelding moet daarbij in overeenstemming zijn met de tijdsbeperkingen van deze versie van het beleid.

3.4.1.2 Regels voor attributen, toepassingsgebied en doel van elektronische handtekeningen en zegels

Het proces van het aanmaken van handtekeningen en zegels MOET op de juiste wijze gebruikmaken van handtekeningattributen, met name de ondertekende attributen die informatie bevatten ter ondersteuning van de elektronische handtekening/het elektronische zegel en die samen met de DTBS door de handtekening gedekt worden, waarbij het volgende geldt:

- de identificatiecode van het ondertekeningscertificaat MOET worden gebruikt. Dit is de identificatiecode van of een verwijzing naar het certificaat met de handtekeningverificatiegegevens die overeenstemmen met de gegevens voor het aanmaken van de handtekening of het zegel die de ondertekenaar bij het aanmaken van de elektronische handtekening of het elektronische zegel heeft gebruikt;
- een aanduiding van het handtekeningbeleid KAN worden gebruikt (zie punt 1.2.2);
- het opgegeven tijdstip van ondertekening MOET worden gebruikt. Dit geeft het tijdstip aan waarop de ondertekenaar stelt de handtekening of het zegel te hebben aangemaakt.

  Dit tijdstip is gelijk aan de huidige systeemtijd van het werkstation van de ondertekenaar. Het is GEEN betrouwbaar tijdstip.

  De eigenaar van de PB-SCA MOET er (hiertoe gedelegeerd door de directeur-generaal van het OP) voor zorgen dat de huidige systeemtijd van alle werkstations van de ondertekenaars juist is.

  Dit kan worden bereikt met behulp van NTP met een geschikte tijdsbron (zie [Mills 2010]);
- de aanduiding van het verbintenistype MOET achterwege blijven;
- Andere ondertekende attributen KUNNEN worden gebruikt.

Het gebruik van handtekeningattributen MOET overeenstemmen met [ETSI 2010] en Besluit 2011/130/EU van de Commissie van 25 februari 2013.

3.4.2 BSP (p): cryptografische softwarepakketten

Zie punt 3.2.1.

4 Eisen / verklaringen over de toepassing van technische mechanismen en normen

4.1 Regels voor betrouwbare tijdstempels

De XAdES-B-LTA-handtekening (zie [ETSI 2022-XAdES]) vereist meerdere tijdstempels die MOETEN worden verkregen van een gevalideerde tijdstempeldienst die in een lidstaat of EER-land geaccrediteerd is.

De eigenaar van de PB-SCA MOET er (hiertoe gedelegeerd door de directeur-generaal van het OP) voor zorgen dat de SCA voor het gebruik van geschikte cryptografische algoritmen wordt geconfigureerd.

4.2 Regels voor de geldigheid op lange termijn

Het behoud van de geldigheid van handtekeningen van PB's en PB-handelingen gedurende de verwachte bewaringsduur wordt gewaarborgd door de toepassing van het XAdES-B-LTA-formaat (zie [ETSI 2022-XAdES]) en door vervolgens de handtekening met een aanvullend gekwalificeerd archiveringstijdstempel uit te breiden om de geldigheid ervan zoveel als nodig te verlengen of een geschikte archiveringsoplossing te gebruiken die garanties biedt voor het behoud van de geldigheid van de handtekening.

4.3 Andere bedrijfsmatige en juridische kwesties

Aangezien het PB elke dag van maandag tot en met vrijdag, en mogelijk ook in het weekend, verschijnt, MOET de eigenaar van de PB-SCA er (hiertoe gedelegeerd door de directeur-generaal van het OP) voor zorgen dat de SCA voortdurend bedrijfsklaar is.

Hiertoe MOETEN NORMAAL GESPROKEN overeenkomsten inzake het dienstverleningsniveau worden vastgesteld.

Hoewel handtekeningen en -zegels van PB's of PB-handelingen door elke SVA die in overeenstemming is met de door het PB-handtekeningbeleid omschreven normen en regels (waarbij onder meer manifestvalidering is voorgeschreven) kunnen worden geverifieerd, KAN het OP op de EUR-Lex-website een openbaar toegankelijke SVA ter beschikking stellen om vertrouwende partijen, met name Europese burgers, in staat te stellen handtekeningen van PB's of PB-handelingen te verifiëren zonder een door derden aangeboden hulpprogramma te hoeven aanschaffen.

Het OP KAN als alternatief een SVA ter beschikking stellen als algemeen te downloaden hulpprogramma dat zelfstandig op de computer van de gebruiker kan draaien en alleen vereist dat verificateurs de software vertrouwen wanneer zij op de resultaten ervan vertrouwen.

5 Aanhangsel

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* W3C-aanbeveling, 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]	*Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG* Publicatieblad L 257
[ETSI 2015]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 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; Part 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; Part 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)