1. Inleiding

1.1. Inhoud

Dit document bevat de regels van de policy die gebruikt worden om vast te leggen onder welke voorwaarden het aanmaken van elektronische handtekeningen en de validatiemethodes geldig zijn wanneer gebruikt binnen de context van eBesluitvorming met de 'Certipost e-Signing Integrated' dienst .

Bovendien legt dit document de rollen en verplichtingen vast van alle actoren die betrokken zijn bij transacties met elektronische handtekeningen. De rechten en de verplichtingen voor de entiteiten die hierbij betrokken zijn, worden vernoemd in de vorm van zowel contractuele verplichtingen als technische vereisten.

Ten slotte geeft dit document ook een overzicht van de technische standaarden en de handelingen die gebruikt worden om elektronische handtekeningen aan te maken met deze dients.

1.2. Indeling van het document

De structuur van dit document is gebaseerd op het 'signature policy framework' volgens ETSI TR 102 041 v1.1.1: "Signature Policy report" [1].

1.3. Definities

Advanced Electronic Signature: dit betekent een elektronische handtekening die aan volgende vereisten voldoet:

- Is uniek verbonden met de ondertekenaar;
- Is in staat om de ondertekenaar te identificeren;
- Is aangemaakt met middelen welke de ondertekenaar volledig kan behouden onder zijn / haar eigen controle; en
- Is verbonden met de gegevens tot welke het gerelateerd is op zulke wijze dat elke toekomstige wijziging op te sporen is.

Attributen van de handtekening: Additionele informatie die eventueel mede getekend is met het document van de ondertekenaar.

Auteurschap en attributie: Is een vorm van aangegane verplichting bij het plaatsen van een elektronische handtekening die het auteurschap of co-auteurschap van de inhoud van het ondertekende document erkent maar verder geen impliciete verplichtingen van juridische aard (zoals deze bij het ondertekenen van een bepaalde overeenkomst) inhoudt.

Certification Authority (CA): Een autoriteit die het vertrouwen heeft van een of meerdere gebruikers om certificaten aan te maken en toe te wijzen. Eventueel kan deze autoriteit ook de sleutels van de gebruikers aanmaken.

Certificaatpolicy: Een verzameling regels met benaming die aangeven welke de toepasbaarheid is van een certificaat voor een bepaalde gemeenschap en/of een bepaalde klasse van toepassing met gemeenschappelijke veligheidsvereisten.

Certificate revocation list (CRL): Een lijst met serienummers van herroepen of geschorste certificaten van een gegeven CA samen met de infromatie betreffende de herroeping of schorsing.

Elektronische handtekening: betekent de elektronisch gegevens die verbonden worden of logisch geassocieerd zijn met andere elektronische gegevens met als doel de authenticiteit en integriteit van de gegevens te verzekeren.

Gekwalificeerd certificaat: Een certificaat dat voldoet aan de vereisten vastgelegd in Annex I en welke ter beschikking gessteld is door een certificatiedienstverlener welke voldoet aan de vereisten in Annex II van de Richtlijn EC 1999/93 [3]

Hash: Een functie die een rij van bits mapt met een andere rij van bits met een (beperkte) vaste lengte. Hierdoor wordt er aan de volgende eigenschappen voldaan:
- Het is rekenkundig niet uitvoerbaar om bij een bepaalde output een passende input af te leiden
- Het is rekenkundig niet uitvoerbaar om bij een bepaalde input een andere input te vinden die tot dezelfde output leidt.

Online certificate status protocol (OCSP): Een online dienst die in 'real time' statusinformatie van certificaten ter beschikking stelt.

Public key: De sleutel van het asymetrische sleutelpaar van een entiteit die openbaar gemaakt mag worden.

Private key: De sleutel van het asymetrische sleutelpaar van een entiteit die nooit openbaar gemaakt mag worden en enkel door deze entiteit aangewend mag worden.

Signature Policy: Een verzameling van technische en procedurele vereisten voor de aanmaak en de controle op de geldigheid van een elektronische handtekening.

Signature Policy identifier: Een object dat de indentificatie van een Signature Policy op een ondubbelzinnige manier vastlegt.

Timestamp: Een bewijs van het bestaan van gegevens op een bepaald moment in de tijd in de vorm van een gegevensstructuur getekend door een een bepaalde autoriteit (Time Stamping Authority). Deze structuur bevat een betrouwbare tijdsindicatie, een unieke identificate voor elke nieuw aangemaakte timestamp, een identificatie die op een unieke wijze verwijst naar een timestamp policy waaronder de timestamp is aangemaakt, en een hash.

Time stamp authority: Een autoriteit die vertrouwd wordt door een of meerder gebruikers om een Time Stamping Service aan te bieden.

Time stamp service: Een dienst die een betrouwbare timestamp kan aanmaken.

2. 'Certipost e-Signing Integrated' dienst voor eBesluitvorming

2.1. Actoren

Ondertekenaar: Entiteit (natuurlijke persoon) die een document via de eBesluitvorming toepassing elektronisch ondertekent.

Digipolis eBesluitvorming: Deze toepassing wordt gebruikt door o.a. ondertekenaars van elektronische documenten en doet daarvoor beroep op de 'Certipost e-Signing Intergrated' dienst.

Certipost e-Signing Integrated: Dit is een dienst die door de Digipolis eBesluitvormingsapplicatie wordt opgeroepen om de ondertekenaar toe te laten om documenten in eBesluitvorming elektronisch te ondertekenen.

Verificateur: Entiteit welke de elektronische handtekening valideert of bevestigt. Dit kan een betrokken partij zijn die hierop steunt of een andere partij voor welke de geldigheid van de elektronische handtekening van belang is.

2.2. 'Certipost e-Signing Integrated' dienst

Het doel van de integratie van de 'Certipost e-Signing Integrated' dienst binnen eBesluitvorming is het mogelijk maken om documenten – van verschillende aard – elektronisch te ondertekenen.

Deze dienst wordt opgeroepen op een eenduidig vastgelegde en beveiligde wijze en voldoet aan de voorwaarden gespecificeerd in artikel 5.1 van de Europese richtlijn en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot de elektronische handtekeningen (Wet van 9 juli 2001).

2.3. Ondersteunde standaarden

Verschillende documenttypes worden ondersteund vermits ze in base-64 gecodeerde (gecanonicalizeerde) bitstromen worden omgezet. De toegepaste elektronisch handtekening heeft een XAdES-T formaat volgens de ETSI norm [1] met het handtekeningscertificaat in de getekende attributen. Een 'signature timestamp' is ook toegevoegd als een niet getekend attribuut.

2.4. Aanmaak van de handtekening

De ondertekenaar kan een elektronisch handtekening aanmaken volgens deze Signature Policy door gebruik te maken van eBesluitvorming.

Op vraag van deze applicatie geeft de 'Certipost e-Signing Integrated' dienst de mogelijkheid om een elektronische handtekening te plaatsen op een document met een gekwalificeerd certificaat welk zich bevindt op een beveiligde drager: een elektronisch professioneel certificaat uitgegeven door Certipost op een USB-token of smartcard.

De Gekwalificeerde Certificaten uitgegeven in het kader van de betreffende certificaatpolicies komen tegemoet aan de vereisten van bijlage I van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). Ze kunnen worden gebruikt om de elektronische handtekeningen te ondersteunen die equivalent zijn aan handtekeningen op papier, zoals gespecificeerd in artikel 5.1 van de Europese richtlijn en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001).

2.5. Nagaan van de geldigheid van een handtekening

De verificateur kan gebruik maken van eender welke methode om de geldigheid van een handtekening na te gaan volgens deze Policy.

Echter, opdat deze verificatie zou in overeenstemming zijn met de hier beschreven Signature Policy moet er minimaal aan volgende voorwaarden worden voldaan:

1. De cryptografische geldigheid van de handtekening moet aangetoond worden.
2. De geldigheid van het certificaat gebruikt door de ondertekenaar op het moment van de ondertekening moet getoetst worden: het mocht niet herroepen of geschorst zijn op het moment dat de handtekening geplaatst werd. Het certificaat mocht ook nog niet vervallen zijn en moest reeds geldig zijn. Een volledige controle van de geldigheid van de certificaatketen (certificate chain) moet ook uitgevoerd worden met inbegrip van de geldigheid van alle certificaten in die ketting. Er moet bovendien rekening gehouden worden met de periode tussen het eventuele melden van een certificaat dat b.v. herroepen moet worden en de eigenlijke opname van deze informatie zodat ze beschikbaar is tijdens de verificatie (Zie 3.3.4.2: 'Grace period')
3. Er moet nagegaan worden dat het certificaat gebruikt door de ondertekenaar op het moment van de ondertekening voldoet aan de aanvaarde Certificaatpolicy.
4. De geldigheid van de tijdsmarkering (timestamp) in de handtekening moet ook worden nagegaan.

Voor de details van de verificatieprocedure dient men de 'Signature Policy informatie' met daarin de 'algemene regels' te raadplegen.

Het nagaan van de geldigheid van een elektronisch handtekening kan ook gebeuren met behulp van de Certipost online verificatiedienst welke voldoet aan de bovenstaande criteria.

3. Signature Policy informatie

3.1. Algemeen

In overeenstemming met de ETSI vereisten[i] bevat deze Signature Policy de volgende gegevens:

3.1.1. Signature Policy Identifier:

- Signature Policy Name: **Digipolis eBesluitvorming elektronische handtekening**
- Signature Policy OID: **0.3.2062.7.2.1.5.1.0**
- Signature Policy URL: http://www.certipost.com/showpolicy?OID=0.3.2062.7.2.1.5.1.0

3.1.2. Datum van uitgave

20/01/2012

3.1.3. Naam van de uitgever van de Signature Policy:

Certipost

- Contact details:
  Hoofdzetel: Certipost s.a/n.v. • Centre Monnaie / MuntCentrum • B-1000 Bruxelles / Brussel
  TVA/BTW BE 0475.396.406

[i] Zie het document [1] ETSI TR 102 041 (V1.1.1) : « Signature Policy report »

Operationeel adres: Ninovesteenweg 196, B-9320 Erembodegem
Phone: +32 53 60 11 11 - Fax: +32 53 60 11 01

- OID van de uitgever van de Signature Policy : **0.3.2062.7.2.1.5**

3.2. Periode van toepasbaarheid

Deze Signature Policy is geldig vanaf de datum van publicatie totdat deze wordt vervangen door een volgende versie.

3.3. Algemene regels

3.3.1. Regels voor de ondertekenaar / eBesluitvorming

3.3.1.1. Afwezigheid van tijdsgebaseerde dynamische inhoud

De ondertekenaar en/of eBesluitvorming zijn ervoor verantwoordelijk dat het bestand dat ondertekend gaat worden geen dynamische inhoud bevat welke het gevisualizeerde resultaat van het bestand zou kunnen wijzigen over een bepaalde tijd. (b.v. zinnen of delen ervan die veranderen na een bepaalde datum). De ondertekenaar en/of eBesluitvorming moeten er op toezien dat er niet zo'n dynamische inhoud vervat zit in het bestand welke zal ondertekend worden door de 'Certipost e-Signing Integrated' dienst.

Voor die reden is het sterk af te raden om documenten te laten ondertekenen die macro's of andere uitvoerbare code bevatten. We raden aan om in zulk geval deze eerst om te zetten naar een formaat welke geen dynamische inhoud bevat, zoals TIFF, PDF/A, JPEG, …

3.3.1.2. Formaat van de ondertekende data is impliciet af te leiden

De ondertekenaar en/of eBesluitvorming zorgen ervoor dat – indien er bij latere verificatie dubbelzinnigheid zou kunnen optreden over het originele formaat – het formaat van het bestand voor een eventuele verificateur, welke visueel de ondertekende data wordt aangeboden tijdens het verificatieproces, impliciet vast te stellen is.

3.3.1.3. Aard van verplichting is af te leiden uit context

Vermits eBesluitvorming de 'Certipost e-Signing Intergated' dienst voor verschillende doeleinden kan gebruiken en de eventuele verplichting die aangegaan kan worden bij het zetten van en dus de functie van een (elektronische) handtekening kan verschillen, moeten deze eventuele verplichting en functie ondubbelzinnig uit de context af te leiden zijn. In ieder ander geval moet de minimale verplichting verondersteld worden, namelijk die van "Auteurschap of Attributie", in welke de ondertekenaar zijn / haar verantwoordelijkheid erkent betreffende het ondertekende document, zonder in dat geval enige andere juridische verplichting aan te gaan.

3.3.1.4. Plaats van de ondertekening

De ondertekenaar en/of eBesluitvorming zorgen ervoor dat de plaats van de ondertekening ondubbelzinning vast te stellen is uit de context van het te ondertekenen document. Indien dit niet het geval is, wordt automatisch aangenomen dat deze plaats zich binnen het rechtsgebied van België / de Vlaamse Gemeenschap bevindt.

3.3.1.5. Rol of hoedanigheid van de ondertekenaar

De ondertekenaar en/of eBesluitvorming zorgen ervoor dat de rol of hoedanigheid van de ondertekenaar ondubbelzinning vast te stellen in uit de context van het te ondertekenen document. Indien dit niet het geval is, wordt automatisch aangenomen dat deze rol beperkt is door hetgeen eventueel aangegeven is door het certificaat waarmee de handtekening geplaatst werd.

3.3.1.6. Tijdstip van de ondertekening

Vermits de ondertekening interactief gebeurt en de elektronische handtekening in de XAdES-T vorm met een 'timestamp' kort daarna beschikbaar is, doet deze 'timestamp' dienst als tijdstip van de ondertekening. Er kan

geen tijd van ondertekening worden doorgegeven vanuit de eBesluitvorming toepassing (in de vorm van het attribuut "SigningTime"). Deze aangeleverde tijd zou toch enkel een informatieve en niet bewijsbare waarde hebben.

3.3.2. Regels voor de 'Certipost e-Signing Integrated' dienst

3.3.2.1. Ondertekende attributen

De 'Certipost e-Signing Integrated' dienst zorgt ervoor dat bij de ondertekende attributen het handtekeningscertificaat (SigningCertificate), het certificaat waarmee de handtekening geplaatst werd (met inbegrip van het volledige certificatiepad), vervat zit. Hiermee wordt een eenvoudige vervanging van het certificaat van de ondertekenaar tegengegaan.

Andere optionele attributen worden in deze context niet ondersteund.

3.3.2.2. Ongetekende attributen

De 'Certipost e-Signing Integrated' dienst zorgt voor de tijdsmarkering (SignatureTimeStamp) als een ongetekend attribuut.

Andere optionele attributen worden in deze context niet ondersteund.

3.3.3. Regels voor de verificateur

3.3.3.1. Ondertekende attributen

Certificaat waarmee ondertekend is (SigningCertificate). De geldigheid van het certificaat gebruikt door de ondertekenaar op het moment van de ondertekening moet getoetst worden: het mocht niet herroepen of geschorst zijn op het moment dat de handtekening geplaatst werd. Het certificaat mocht ook nog niet vervallen zijn en moest reeds geldig zijn. Een volledige controle van de geldigheid van de certificaatketen (certificate chain) moet ook uitgevoerd worden met inbegrip van de geldigheid van alle certificaten in die ketting. Er moet bovendien rekeningschap gegeven worden aan de periode tussen het eventuele melden van een certificaat dat b.v. herroepen moet worden en de eigenlijke opname van deze informatie zodat ze beschilkbaar is tijdens de verificatie (Zie 3.3.4.2: 'Grace period')

- Als de verificatie wordt uitgevoerd voor het verstrijken van het handtekeningscertificaat: De verificateur moet een online certificaat status verificatie uitvoeren indien mogelijk. Indien hieruit blijkt dat het certificaat herroepen of geschorst is en de datum van herroeping of schorsing voor het tijdstip van de ondertekening plaatsvond mag de handtekening niet als geldig beschouwd worden. Het alternatief is om de CRLs (Certificate Revocation Lists) te gebruiken enkel en alleen indien men rekening houdt met de 'grace period': de herroepingsinformatie moet de werkelijke status aangeven. Dit wil zeggen dat in dit geval mogelijk gewacht moet worden op de publicatie van een nieuwe CRL.
- Indien de verzekerde statusinformatie (nog) niet beschikbaar is moet de verificatie van de handtekening als onvolledig beschouwd worden en moet deze later opnieuw uitgevoerd worden.
- Als de verificatie wordt uitgevoerd na het verstrijken van het handtekeningscertificaat: De verificatie kan niet meer met zekerheid worden uitgevoerd binnen deze context. Voor het verstrijken moet de elektronische handtekening uitgebreid worden opdat verificatie op lange termijn mogelijk is, of alternatieve methods moeten aangewend worden.

3.3.3.2. Ongetekende attributen

De tijdsmarkering (SignatureTimestamp) moet gecontroleerd worden. De verificateur moet de geldigheid van deze 'timestamp' en dat van het handtekeningscertificaat van deze 'timestamp' nakijken. Deze 'timestamp' mag echter niet gebruikt worden als onweerlegbaarheidsbewijs voor lange periodes (na vervallen van de geldigheidsperiode van het timestamp certificaat). Voor bewijskracht lang na ondertekening is uitbreiding van de handtekening naar een ander formaat nodig aangezien het gebruikte beveiligingsalgoritme mogelijks achterhaal is.

3.3.3.3. Certificaatpolicy

Er moet ook nagegaan worden dat het certificaat gebruikt door de ondertekenaar op het moment van de ondertekening voldoet aan de aanvaarde Certificaatpolicy.

3.3.4. Voorwaarden van vertrouwen

3.3.4.1. Handtekeningscertificaat

3.3.4.1.1. Vereisten

Het certificaat moet gekwalificeerd zijn en op een beveiligde drager beschikbaar zijn.

Lengte van het certificatenpad

Er zijn geen beperkingen.

Aanvaarde certificaatpolicies

Enkel certificaatpolicies die in verband staan met gekwalificeerde certificaten voor natuurlijke personen in een bepaalde professionele hoedanigheid en die op een beveiligde drager beschikbaar zijn (namelijk: een elektronisch professioneel certificaat uitgegeven door Certipost op een USB-token of smartcard) zijn toegestaan.

De OID is:

- 0.3.2062.7.1.1.101.1 (Gekwalificeerd professioneel certificaat uitgegeven door Certipost)

Benaming

Er zijn geen beperkingen.

3.3.4.1.2. Vereisten voor herroeping

Statusinformatie i.v.m. herroeping van het certificaat van de ondertekenaar en de CA certificaten die hier betrekking op hebben (namelijk deze in de certificaatketting), moet bekomen worden via OCSP of via volledige CRLs.

3.3.4.2. Timestamping

Public Key Regels van de Time Stamping authoriteiten

Het certificaat van de timestamping authoriteit moet de ExtendedKeyUsage (OID: 1.3.6.1.5.5.7.3.8) bevatten.

De aangewende time stamping service beperkt zich tot deze aangewend door Certipost voor het aanbieden van de ´Certipost e-Signing Integrated´ dienst.

Benaming

Er zijn geen beperkingen.

Grace Period

Op het tijdstip van het aanmaken van de elektronische handtekening door de 'Certipost e-Signing Integrated' dienst zal er een validatie plaatsvinden van het certificaat dat gebruikt wordt om te ondertekenen. Dit is met inbegrip van het nagaan van de status op gebied van herroeping of schorsing van het gegeven certificaat. Die verificatie wordt uitgevoerd door informatie aan te vragen (via CRL of OCSP) van de uitgever van het certificaat. Er is echter een periode tussen de aanvraag tot herroeping of schorsing en het publiceren van die informatie (via CRL of OCSP). Voor CRLs is er het bijkomend

probleem dat er ook een bijkomende periode is tussen de publicatie van nieuwe CRLs en die periodiciteit kan aanleiding geven tot een langere vertraging tussen het melden van een herroeping of schorsing en het opnemen en beschikbaar stellen van de nieuwe aangepaste status.

Het gevolg daarvan is dat er een klein risico bestaat dat de statusinformatie gedurende een bepaalde periode niet correct is. B.v. het certificaat wordt geldig beschouwd maar was in feite al herroepen. Dit heeft natuurlijk gevolgen voor de verificatie van de handtekening zelf.

Daarom is het nodig om de verificatie later opnieuw uit te voeren na een tijdsinterval waarbij dit risico wordt geminimalizeerd of zelfs uitgesloten.

Na een verificatie die uitgevoerd wordt, rekeninghoudend met dit tijdsinterval ('grace period'), kan de handtekening eventueel uitgebreid worden naar een XAdES-C formaat (zie [1]) welke een validatie op langere termijn toelaat.

Deze extensie is echter niet opgenomen als onderdeel van deze policy of de besproken oplossing.

Maximale Aanvaardingstijd

Niet van toepassing.

3.3.4.2.1. Vereisten voor herroeping

Statusinformatie i.v.m. herroeping van het certificaat van de ondertekenaar en de CA certificaten die hier betrekking op hebben (namelijk deze in de certificaatketting), moet bekomen worden via OCSP of via volledige CRLs.

3.3.4.3. Attributen

Het elektronisch ondertekenen van bijkomende attributen maakt geen onderdeel uit van deze Signature Policy.

3.3.4.4. Beperkingen van de algorithmes

De volgende beperkingen bij het ondertekenen zijn van toepassing m.b.t. deze Signature Policy:

- De **Handtekeningsalgorithmes:** Maken gebruik van RSA / SHA1.
- **Minimale Sleutel Lengte**: Bedraagt minimaal 1024 bits.

Deze Signature Policy legt verder geen beperkingen op voor de algorithmes voor certificaten of de timestamping authoriteiten.

3.3.4.5. Algemene Extensies

Er zijn er geen gedefinieerd in deze Signature Policy.

3.4. Signature Validation Policy Extensie

De validatie van een elektronische handtekening onder deze Signature Policy kan aangevuld worden met bijkomende stappen zoals:

- De extensie van de handtekening (naar een formaat met volledige, uitgebreide of archiveerbare validatiedata) zoals gedefinieerd door ETSI [4].
- De beveiligde archivering en het onderhouden van auditsporen in elke andere vorm die de geldigheid van de elektronische handtekening op lange termijn ondersteunen.
- Het ondertekenen van de ondertekende documenten door een andere partij – eventueel op een later tijdstip – (b.v. Certipost of een archief) als een vorm van 'e-notary' handtekening. Dit betekent een 'trusted third party' dienst welke de authenticiteit en de integriteit van de gegeven data verzekert op

een gegeven ogenblik (b.v. ontvangst of stockage) en dus mogelijke bewijsstukken archiveert voor toekomstig gebruik.

De bovestaande uitbreidingen maken geen onderdeel uit van deze Signature Policy en kunnen eventueel aanleiding zijn tot een bijkomende of gewijzigde Signature Policy.

3.5. Toepassingsgebied, domein van gebruik, context van de transacties

De handtekeningen, die gezet en gevalideerd zullen worden, liggen binnen de context van eBesluitvorming. De betrokken partijen zijn Digipolis en haar klanten. Ze zijn dus beperkt tot een omgeving van overheidsinstellingen of organisaties gebonden aan die overheden.

De eBesluitvormingsapplicatie zal de 'Certipost e-Signing Integrated' dienst voor verschillende doeleinden gebruiken. De eventuele verplichtingstypes (commitment types) die aangegaan kunnen worden bij het zetten van een (elektronisch) handtekening kunnen dus verschillen. In dit geval, waar de verplichtingstypes niet expliciet opgenomen zijn in de elektronische handtekening zelf, moeten de toepassingsgebieden en de eventuele verplichtingen ondubbelzinnig uit de context van het ondertekend document af te leiden zijn. In ieder ander geval moet de minimale verplichting verondersteld worden, namelijk die van "Auteurschap of Attributie", in welke de ondertekenaar zijn / haar verantwoordelijkheid betreffende het document erkent, zonder in dat geval enige andere juridische verplichting aan te gaan.

Vermits de elektronische handtekening onder deze Signature Policy voor diverse doeleinden binnen het kader van e-Besluitvorming kan worden gebruikt, dienen ondertekenaar, verificateur en al wie vertrouwt op dergelijke handtekening en/of die handtekening dient te waarderen telkens rekening te houden met de betrokken functie van de handtekening in de concrete situatie. Deze functie en concrete situatie waarin de handtekening wordt gebruikt, kan voor een deel ook blijken uit enige bijkomende verwerking (b.v. archivering) die toegepast kan worden met het oog op het verzekeren van de geldigheid op lange termijn van deze elektronische handtekening.
Certipost is niet aansprakelijk voor het gebruik dat de ondertekenaar en anderen zouden maken van de elektronische handtekening, noch voor de functie die de ondertekenaar toekent aan de handtekening, noch voor de ondertekende gegevens zelf (o.m. het gebruik, de semantiek, de inhoud, de vorm, de geldigheid, de wettelijkheid, volledigheid of juistheid van deze ondertekende gegevens).

3.6. Expliciete en impliciet Signature Policy

Men kan zowel een expliciete als een impliciete verwijzing hebben naar de Signature Policy binnenin het ondertekend document. Vermits de handtekeningen, die gezet en gevalideerd zullen worden, binnen de context van eBesluitvorming vallen, en de betrokken partijen Digipolis en haar klanten zijn, is Digipolis de beheerder van deze Signature Policy. Bovendien is deze context niet open en beperkt deze zich tot een omgeving van overheidsinstellingen of organisaties gebonden aan die overheden. Daarom werd verkozen om de verwijzing naar deze Signature Policy niet expliciet in de handtekeningen zelf op te nemen.

Door de mogelijke ondertekenaars te kennen te geven van het bestaan van een Signature Policy die gebonden is aan het gebruik van eBesluitvorming voor het aanmaken van elektronische handtekeningen, en door die ondertekenaars de mogelijkheid te geven de beschrijving van die Signature Policy te raadplegen, legt men impliciet vast in welke context het aanmaken van de elektronische handtekeningen gebeurt en op welke wijze het ondertekenen en de validatie moet gebeuren.
De hier beschreven Signature Policy heeft een unieke identificatie, namelijk een OID (Object Identifier).

3.7. Publicatie van deze Signature Policy

Voor dat een ondertekenaar een elektronische handtekening zet moet hij in staat zijn om te weten welke Signature Policy er van toepassing is. Ook de verificateur moet hiervan op de hoogte zijn opdat de verificatie correct zou zijn.

Digipolis voorziet via de eBesluitvorming toepassing in het informeren van de ondertekenaars en de verificateurs omtrent de inhoud van deze Signature Policy en publiceert dit document op haar web site.

3.8. Archivering van deze Signature Policy

Het is de verantwoordelijkheid van Digipolis om deze Signature Policy te archiveren en eventuele nieuwe versies bij te voegen tot dit archief.

3.9. Signature Policy conformiteitsverklaring

Deze Signature Policy beweert conform te zijn met ETSI TR 102 041 [1].

4. Referenties

[1] ETSI TR 102 041 (v1.1.1): “Signature Policy report”.
[2] RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.
[3] EC 1999/93: European Community (EC) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES

[4] ETSI TS 101 903 V1.4.1 (2009-06) " XML Advanced Electronic Signatures (XAdES)"