< Ontwerp Elektronische Handtekening

Datum: 7 oktober 2020
Publicatie: V8.2.0.0

Inhoudsopgave

1 Inleiding

1.1 Doel en scope

Dit document beschrijft het architectuurontwerp van de elektronische handtekening binnen AORTA, met als doel het vastleggen van gemaakte ontwerpbeslissingen zodat die kunnen dienen als kader voor verdere uitwerking en realisatie. Het gaat hierbij om de generieke architectuur van de elektronische handtekening zoals die gebruikt kan worden door zorgtoepassingen binnen AORTA. Dit document beschrijft derhalve geen:

- Aspecten die algemeen gelden voor AORTA. Zie daarvoor [Arch AORTA];
- Aspecten die vallen onder de noemer 'implementatie'. Zie de [IH EH UZI-pas].
- Aspecten die specifiek zijn voor een bepaalde zorgtoepassing. Dergelijke aspecten dienen beschreven te worden in de zorgtoepassingdocumentatie;
- Aspecten over het gebruik van elektronische handtekeningen buiten de scope van AORTA.

1.2 Doelgroep voor dit document

Dit stuk is gericht op de doelgroepen van bij AORTA betrokken ICT-architecten:

- bij Nictiz die zorgtoepassingen ontwikkelen die gebruik gaan maken van de elektronische handtekening;
- bij ICT-leveranciers die deze zorgtoepassingen gaan implementeren in hun software.

1.3 Documenthistorie

Versie	Datum	Omschrijving
6.10.0.0	12-okt-2011	Initiële publicatie voor AORTA v6
6.11.0.0	12-okt-2012	Ongewijzigde herpublicatie als onderdeel van AORTA-Infrastructuur v6·11
8.0.1.0	15-mei-2017	Opgenomen in publicatie 8.0.1.0
8.1.0.0	1-juli-2018	Opgenomen in publicatie 8.1.0.0
8.2.0.0	7-okt-2020	Opgenomen in publicatie 8.2.0.0

2 Kaders en uitgangspunten

2.1 Externe normen en kaders

Hieronder volgt een korte uiteenzetting over de wettelijke eisen aan de elektronische handtekening.

De [Wet Elektronische Handtekeningen] (WEH) definieert de elektronische handtekening als een handtekening die bestaat uit elektronische gegevens die zijn gekoppeld ("vastgehecht of logisch geassocieerd") aan de ondertekende gegevens en die worden gebruikt als middel voor authenticatie ("met zekerheid vaststellen van de identiteit van de gebruiker"). De elektronische handtekening kan worden gebruikt ("is gelijk te stellen aan een gewone handtekening") als de gebruikte methode van authenticatie voldoende betrouwbaar is gelet op het doel en de omstandigheden.

De WEH geeft aan dat de gebruikte methode voor authenticatie voldoende betrouwbaar is (behoudens tegenbewijs) als de elektronische handtekening voldoet aan de eisen:

1. Zij is uniek verbonden aan de ondertekenaar.
2. Zij identificeert[1] de ondertekenaar.
3. Zij komt tot stand met middelen die de ondertekenaar onder zijn exclusieve controle kan houden.
4. De manier waarop de elektronische handtekening aan de gegevens is verbonden, maakt het mogelijk om elke wijziging achteraf van de gegevens te detecteren.
5. Zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in Telecomwet art 1.1.
6. Zij is "gezet" met een "veilig middel" als bedoeld in Telecomwet art 1.1.

De definitie van Veilig Middel staat in de Telecomwet. Daar wordt de verdere inhoudelijke definitie verlegd naar een AMvB (Algemene Maatregel van Bestuur), en er wordt de verplichting vastgelegd om het Veilig Middel te laten goedkeuren. Het Besluit Elektronische Handtekeningen is deze AMvB en legt een aantal (functionele) eisen aan het Veilig Middel vast, die neerkomen op het volgende:

- Het Veilig Middel en het stelsel voor uitgifte moeten garanderen dat de erop uitgegeven sleutels uniek zijn.
- Het moet naar de huidige stand van de techniek bestand zijn tegen afleiden van de sleutels en vervalsen van de elektronische handtekening.
- Het beschermt de sleutels tegen gebruik door anderen.
- Het laat de te ondertekenen gegevens ongewijzigd en belet niet dat die gegevens vóór de ondertekening aan de ondertekenaar worden voorgelegd.

De [Regeling Elektronische Handtekeningen] zegt dat een middel vermoed wordt te voldoen aan de eisen in het Besluit Elektronische Handtekeningen als het voldoet aan technische specificatie van de *CEN Workshop Agreement* 14169. PKIoverheid geeft aan dat voor de Nederlandse overheid is besloten dat een smartcard geldt als Veilig Middel. De UZI-pas voldoet aan de PKIoverheid specificaties en is dus een Veilig Middel.

[1] Volgens de Europese richtlijn mag die identificatie ook zijn in de vorm van een pseudoniem, d.w.z. een aangenomen naam die niet gelijk is aan de echte naam van de ondertekenaar.

De wetgeving biedt een zekere mate van vrijheid voor wat betreft de mate van betrouwbaarheid. Er is de keus tussen:

- De "gewone" elektronische handtekening, d.w.z. een handtekening waarvan door partijen onderling is overeengekomen dat die voldoende betrouwbaar is. Het bestaat uit elektronische gegevens die zijn toegevoegd aan of logisch geassocieerd zijn met andere elektronische gegevens.
- Een "geavanceerde" elektronische handtekening, d.w.z. gebaseerd op PKI. Ten opzichte van de gewone elektronische handtekening biedt de geavanceerde elektronische handtekening extra garanties ten aanzien van de herkomst van die gegevens. Het gaat hierbij om de volgende aspecten:
  - Identificatie; De handtekening is op unieke wijze aan de ondertekenaar verbonden. Hierdoor is het mogelijk om de ondertekenaar te identificeren.
  - Onweerlegbaarheid; De handtekening komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden. Dit betekent dat de verzender niet kan ontkennen dat hij het bericht heeft verzonden.
  - Integriteit; Elke wijziging van de gegevens die na ondertekening zijn gemaakt kan worden opgespoord.
- Een "gekwalificeerde" elektronische handtekening. In de Wet Elektronische Handtekeningen wordt als meest betrouwbaar niveau genoemd: een geavanceerde elektronische handtekening op basis van een Gekwalificeerd Certificaat en een Veilig Middel. NB. De term "gekwalificeerde elektronische handtekening" wordt niet in de wet genoemd maar wordt in literatuur over dit onderwerp veel gebruikt. Ook in dit document zal deze term gehanteerd worden.

De architectuur moet een oplossing bieden voor het toepassen van elektronische handtekeningen binnen de context van AORTA. Daarbij gelden, kort samengevat, de volgende eisen:

- De EH moet generiek bruikbaar zijn in meerdere zorgtoepassingen.
- De EH moet voldoen aan de eisen van de Geneesmiddelenwet (ingegaan 1 juli 2007) [Geneesmiddelenwet].
- De EH moet eindgebruikers de mogelijkheid bieden om door hen te verzenden informatie te voorzien van een 'handtekening', zodanig dat de ontvangers van die informatie voldoende zekerheid wordt geboden dat de betreffende informatie daadwerkelijk van de ondertekenaar en verzender afkomstig is, en dat deze ongewijzigd is.
- De EH moet het mogelijk maken om een vrij te kiezen set van gegevens te ondertekenen. Welke informatie daadwerkelijk ondertekend wordt, zal per zorgtoepassing gedefinieerd worden.
- De EH moet de mogelijkheid bieden om over één patiëntstuk of bericht meerdere elektronische handtekeningen te plaatsen, gezet door één of meer personen, en betrekking hebbende op gelijke dan wel verschillende delen van het patiëntstuk of bericht.
- De EH moet een niveau van betrouwbaarheid bieden dat vergelijkbaar is met de handgeschreven handtekening. Met andere woorden, de EH moet voldoen aan de wet- en regelgeving voor elektronische handtekeningen en het vertrouwensniveau van de Geavanceerde Elektronische Handtekening realiseren.
- De EH moet redelijkerwijs inpasbaar zijn in de omgeving en processen van de grote meerderheid van de zorgaanbieders, zowel vanuit beheers- als vanuit gebruikersperspectief. Dit betekent onder meer:
  1. De EH moet passen in een complexe infrastructuur waarbij functies voor verwerking en opslag van gegevens verdeeld zijn over verschillende systemen (bijv. multi-tier systemen, gedistribueerde systemen).
  2. De EH moet passen bij een op het ASP-model gebaseerd GBZ.

3. De EH moet aansluiten bij toekomstvaste (open) standaarden die breed ondersteund worden door verkrijgbare producten in de markt.
4. De EH moet zo mogelijk gebruik maken van bestaande ervaringen met elektronische handtekeningen.
5. De EH moet compatible zijn met systemen die (nog) niet de elektronische handtekening ondersteunen.

2.1.1 Aanvullende richtlijnen

Zelfs als er de beschikking is over een geavanceerde elektronische handtekening met gekwalificeerd certificaat en veilig middel, blijft de mogelijkheid dat het proces van ondertekenen onvolkomenheden of achterdeurtjes kent. Met deze middelen is de kwaliteit van de cryptografie en de veiligheid van de sleutels geborgd, maar er zijn bij het ondertekenen meer systeemcomponenten betrokken (kaartlezers, drivers, middleware, operating system en applicatie).

Er moet dus gekeken worden naar het hele signing-proces. ETSI heeft specificaties voor dit proces beschreven. De status van de specificaties is echter tamelijk bescheiden, dat wil zeggen dat de specificaties niet de status van officiële standaard hebben. Er is geen proces voor evaluatie of certificering van applicaties tegen deze specificaties beschreven. Eisen aan de elektronische handtekening, aan het gekwalificeerde certificaat en aan het veilig middel ("*secure signature creation device*") zijn gestandaardiseerd. De specificaties voor toepassing ervan in bedrijfsprocessen en applicaties zijn door CEN werkgroepen echter als *adviezen* (CWA - CEN Workshop agreement) neergelegd. Deze CWA documenten hebben in het algemeen niet de status van standaard, met uitzondering van CWA 14169, de specificatie voor het Veilig Middel. Ze kunnen echter in het kader van de AORTA specificaties wel als eis worden gesteld.

Het [CWA-14170] document *(Security Requirements for Signature Creation Systems)* geeft specificaties voor het aanmaken van de elektronische handtekening. Dit CWA-document is geen standaard, maar een "vrijwillige" specificatie voor een *signature creation application*. Het beschrijft een functioneel model, een datamodel en geeft detailspecificaties.

Het [CWA-14171] document "*General guidelines for electronic signature verification*" geeft concrete adviezen ten aanzien van het verifiëren van elektronische handtekeningen.

2.1.2 Organisatorische context

De wet- en regelgeving kent alleen natuurlijke personen als ondertekenaar. Indien een persoon tekent namens een organisatie, zal de relatie tussen de organisatie en de ondertekenaar moeten blijken uit de ondertekende gegevens.

De genoemde normen voor PKI besteden ook aandacht aan de context waarin de certificaten en de middelen voor ondertekenen worden uitgegeven. De ETSI standaarden kennen het begrip "abonnee", een persoon of organisatie die contractant is naar de uitgever van de certificaten en vertrouwd middel. Deze abonnee heeft daardoor ook verantwoordelijkheden bij de betrouwbare uitgifte van die middelen. De pas/certificaathouder maakt gebruik van het abonnement van de abonnee en heeft daarom verplichtingen aan de abonnee. De abonnee kan voorwaarden stellen aan het gebruik van de pas door de pas/certificaathouder. Bij het zetten van de elektronische handtekening is het echter primair de pas/certificaathouder zelf die verantwoordelijk is voor de ondertekende inhoud.

Het normenkader van het UZI-register kent ook een dergelijk abonnee-begrip. Een zorgaanbieder treedt op als abonnee. De zorgaanbieder/abonnee kan een zorginstelling zijn, waaronder vele UZI-pashouders vallen, of een huisartsenpraktijk met alleen de arts zelf als pashouder.

2.2 Relatie met AORTA-principes en –beslissingen

De architectuur moet een oplossing bieden voor het toepassen van elektronische handtekeningen binnen de context van AORTA. Daarbij gelden, kort samengevat, de volgende eisen met betrekking tot AORTA-principes en -beslissingen:

- De EH moet gebaseerd zijn op berichtenuitwisseling via het LSP zoals die beschreven is in [Arch AORTA].
- De EH moet zo zijn opgezet, dat het LSP geen medisch-inhoudelijke informatie verwerkt of opslaat.
- De EH moet gebruik kunnen maken van de UZI-pas en UZI certificaten zoals die door het UZI-register wordt uitgereikt aan zorgverleners en medewerkers.

2.3 Relatie met AORTA-bedrijfsactoren

Deze paragraaf beschrijft de AORTA actoren in de context van het implementeren en gebruiken van elektronische handtekeningen. Zie [Arch AORTA] voor de definitie van de actoren.

2.3.1 Zorgverlener

Op grond van wetten ([WGBO], [WOG]) zijn zorgverleners gerechtigd en/of verplicht om bepaalde medische handelingen te verrichten, dossiers te houden en stukken met medische betekenis te ondertekenen en te versturen.

Zorgverleners hebben belang bij de elektronische handtekening omdat die hun ondersteuning biedt bij het uitoefenen van hun beroep. De elektronische handtekening heeft echter ook tot gevolg dat zorgverleners de ondertekende stukken niet kunnen ontkennen. Het is van belang dat de elektronische handtekening veilig en betrouwbaar is zonder dat al te veel concessies worden gedaan ten aanzien van het gebruiksgemak.

2.3.2 Zorgaanbieder

De verantwoordelijkheid van de zorgaanbieder als abonnee betreft het conform de regels aanvragen en (laten) intrekken van UZI-passen. De verantwoordelijkheid voor de ondertekende berichten ligt bij de persoon van zorgverlener of medewerker als ondertekenaar, niet bij de zorgaanbieder als abonnee.

Zorgaanbieders hebben min of meer dezelfde belangen bij de elektronische handtekening als zorgverleners. In aanvulling daarop spelen ook mogelijke kostenbesparingen als gevolg van verbeterde mogelijkheden tot digitalisering een rol.

2.3.3 Medewerker van de zorgaanbieder

Waarschijnlijk zal het plaatsen van elektronische handtekeningen door medewerkers beperkt blijven tot administratieve en/of logistieke toepassingen.

Medewerkers hebben belang bij de elektronische handtekening omdat die in bepaalde gevallen door hen zou kunnen worden gebruikt. Dit moet nader onderzocht worden voor die specifieke zorgtoepassingen waar dit van toepassing kan zijn. Het is voor medewerkers van belang dat elektronisch ondertekenen ook voor hen mogelijk wordt.

Wanneer een medewerker handelingen uitvoert namens een zorgverlener, dan spreken we van een *gemandateerde medewerker* of, kortweg, een *gemandateerde*. Merk op dat het in de praktijk kan voorkomen dat de medewerker van een zorgverlener zelf ook als zorgverlener geregistreerd staat.

2.3.4 Patiënt

Het gebruik van elektronische handtekeningen dient om de zorgverlening aan patiënten te verbeteren. Patiënten hebben belang bij de elektronische handtekening omdat die het uitwisselen van informatie tussen zorgverleners kan bewerkstelligen omdat het de zorgverlener meer zekerheden biedt. Tegelijk is ook voor hen van belang dat die informatie-uitwisseling door het gebruik van elektronische handtekeningen veilig en betrouwbaar blijft. Het door de patiënt zelf laten controleren van de geldigheid van de betreffende handtekeningen is vooralsnog niet aan de orde. De patiënt krijgt in het kader van deze architectuur niet de rol van ondertekenaar of ontvanger van ondertekende informatie.

2.4 Bedrijfsrollen

De bovenbeschreven belanghebbenden kunnen in een of meerdere rollen betrokken zijn bij het gebruik van de elektronische handtekening.

2.4.1 Ondertekenaar

De ondertekenaar is degene die een samenhangend stuk informatie, bijvoorbeeld een document, wil voorzien van een handtekening, om daarmee voor anderen kenbaar te maken dat het stuk van zijn hand is en dat hij verantwoordelijkheid neemt voor de inhoud ervan. De ondertekenaar als persoon is een zorgverlener of een medewerker die handelt uit naam van een zorgverlener (“gemandateerd”).

Een voorbeeld van een ondertekenaar is een huisarts die een medicatievoorschrift (recept) ondertekent conform de geneesmiddelenwet.

ONTW.BESL.BA·01 In de architectuur wordt het zetten van een (gekwalificeerde) elektronische handtekening door medewerkers met een UZI-pas op naam niet uitgesloten maar een UZI-pas *niet op naam* wel uitgesloten; indien het voor een specifieke zorgtoepassing niet gewenst is dat medewerkers patiëntstukken ondertekenen, dan kan dat in de betreffende zorgtoepassing uitgesloten worden.

In specifieke gevallen is het wenselijk stukken te laten tekenen door een rechtspersoon in plaats van door een natuurlijke persoon. Een voorbeeld is een zorgaanbieder die als organisatie een factuur ondertekent teneinde die naar de zorgverzekeraar of patiënt te sturen. Deze situatie valt niet zonder meer binnen het wettelijk kader voor de elektronische handtekening. In dit architectuurontwerp valt deze mogelijkheid buiten scope.

ONTW.BESL.BA·02 Het zetten van een elektronische handtekening door een zorgaanbieder (organisatie) in plaats van door een zorgverlener (persoon) is in dit architectuurontwerp niet aan de orde. Omdat de elektronische handtekening door een zorgaanbieder geen uitdrukking geeft t.a.v. een waarborg.

2.4.2 Verzender

De verzender is de persoon die een bericht wil verzenden aan een ander. Dit kan een zorgverlener zijn of een medewerker.

Een voorbeeld van een persoon als verzender is de huisartsassistente die een recept rechtstreeks naar een apotheek verstuurt.

Merk op dat wanneer een zorgverlener een document verstuurt *met behulp van* een systeem, dan zien we de zorgverlener als de werkelijke verzender en niet het systeem.

2.4.3 Ontvanger

De ontvanger is de persoon of organisatie die een bericht ontvangt. De ontvanger kan een zorgverlener of diens medewerker zijn, maar ook een organisatie. De ontvanger van informatie hoeft niet de verwerker daarvan te zijn.

Een voorbeeld van een persoon als ontvanger is een apotheker die een recept van een huisarts ontvangt. In veel gevallen echter zal het niet de apotheker zelf zijn, maar zal zijn apotheekinformatiesysteem de ontvangst van ondertekende medicatievoorschriften verzorgen.

2.4.4 Verwerker

De verwerker is de persoon of organisatie die een ontvangen bericht verwerkt. De persoon hoeft niet per se de ontvanger te zijn. Bij het verwerken van een bericht hoort ook het controleren van de juistheid van het bericht, zoals het beoordelen van een eventuele handtekening.

Een voorbeeld van een verwerker is een apothekersassistente die een ontvangen recept verwerkt door onder andere de medicatie aan de patiënt te overhandigen. Het is ook (theoretisch) mogelijk dat de verwerking volledig geautomatiseerd gebeurt. In dat geval is er sprake van een organisatie als verwerker. Er zal echter ook in die gevallen altijd een persoon als verantwoordelijke betrokken zijn.

Een geldige elektronische handtekening betekent voor de verwerker dat hij kan vertrouwen op de inhoud en de echtheid van het ondertekende patiëntstuk. Dat de verwerker besluit het ondertekende patiëntstuk te verwerken, betekent niet dat hij de verantwoordelijkheid op zich neemt voor de juistheid van het patiëntstuk. Die verantwoordelijkheid blijft bij de ondertekenaar. Wel draagt de verwerker de verantwoordelijkheid voor zijn eigen handelen, inclusief de interpretatie van het ondertekende patiëntstuk.

3 Elektronische Handtekening

De elektronische handtekening als uitbreiding op de AORTA-architectuur heeft primair tot doel om zorgverleners en medewerkers een middel te bieden dat vergelijkbaar is met een handtekening op papier. Door het zetten van een elektronische handtekening verklaart de ondertekenaar zich akkoord met de inhoud van het ondertekende. Soms is dit nodig om tot een overeenkomst te komen, in sommige gevallen geldt ook een wettelijk vereiste dat bepaalde gegevens moeten worden ondertekend.

De elektronische handtekening kent, zoals beschreven in hoofdstuk 2.1, drie vormen:

- Gewone elektronische handtekening;
- Geavanceerde elektronische handtekening;
- Gekwalificeerde elektronische handtekening.

Binnen de AORTA architectuur wordt er gebruik gemaakt van de gekwalificeerde elektronische handtekening. In het vervolg zal de term EH worden gebruikt voor gekwalificeerde elektronische handtekening, tenzij anders is vermeld.

Voor de EH wordt een gekwalificeerd certificaat gebruikt, dat vervolgens ook aan het ondertekende bericht wordt toegevoegd. Het certificaat wordt door een certificatiedienstverlener (CSP) uitgegeven. In geval van de AORTA-architectuur is dat het UZI-register. Conform het Certification Practice Statement van het UZI-register [CPS-UZI] is alleen het handtekeningcertificaat (en de bijbehorende private sleutel) toegestaan voor gebruik bij het zetten van elektronische handtekeningen. Alleen zorgverleners en hun medewerkers kunnen met een persoonlijke UZI-pas daadwerkelijk elektronische handtekeningen zetten.

4 Elektronische Handtekening in AORTA-architectuur

Het beschrevene in dit hoofdstuk is een generieke benadering voor het gebruik van de elektronische handtekening. Zorgtoepassing specifieke oplossingen zijn beschreven in de documentatie van de betreffende zorgtoepassing.

4.1 Gekwalificeerde elektronische handtekening

Door het gebruik van een EH bij het uitwisselen van patiëntgegevens kunnen er extra garanties geboden worden. Die extra garanties leiden tot vertrouwensniveau hoog, zoals beschreven in [Ontw Authenticatie], en gelden ten aanzien van de volgende aspecten:

- Identiteit van de ondertekenaar (Het UZI-nummer en een verwijzing naar het certificaat van de ondertekenaar zijn aanwezig, men kan erop vertrouwen dat deze door het UZI-register zijn gecontroleerd)
- Authenticiteit van de identiteit van de ondertekenaar (door gebruik van alleen aan de ondertekenaar beschikbare middelen)
- Integriteit van de ondertekende gegevens (omdat de handtekening cryptografisch is gekoppeld aan de ondertekende gegevens kan een wijziging nadat de handtekening is gezet aan de ondertekende gegevens door controle van de handtekening worden gedetecteerd)
- Wilsuiting (ondertekenaar verklaart zich gebonden aan de inhoud)
- Bevoegdheid (ondertekenaar verklaart bevoegd te zijn tot de uitgevoerde rechtshandeling, de betekenis van die verklaring, en de noodzaak van de bevoegdheid hangen af van de ondertekende gegevens en van de context)
- Plaatsing in de tijd (als het tijdstip van tekenen mede is ondertekend, heeft ontvanger zekerheid over een tijdstip in het verleden waarop de gegevens bestonden en waarop ondertekenaar de wilsuiting deed)
- Onweerlegbaarheid (de ondertekenaar kan door de aanwezigheid van de handtekening niet ontkennen de ondertekende gegevens gezien en/of aangemaakt te hebben).

Er zijn verschillende activiteiten van belang in de procesgang bij het gebruik van de EH binnen de AORTA architectuur, zoals weergegeven in AORTA.STK.d3610.

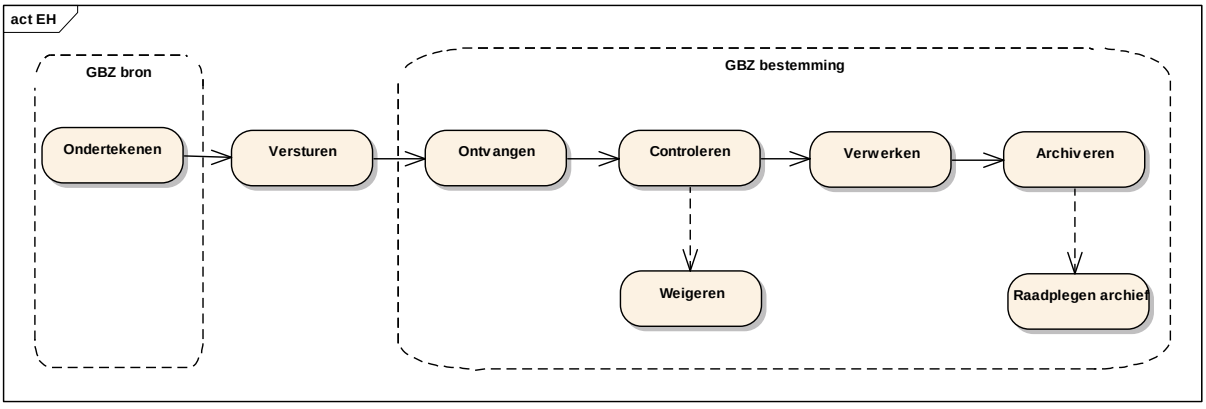

Diagram AORTA.STK.d3610: Processen bij elektronische handtekening

Voor de EH ligt met name de nadruk op de volgende processen:

- Ondertekenen;
- Versturen;

- Controleren;
- Archiveren.

De processen ontvangen en verwerken zijn standaard AORTA processen zoals beschreven in [Arch AORTA].

De EH specifieke activiteiten worden in de volgende paragrafen besproken. Daarnaast is paragraaf 4.1.4 opgenomen met additionele informatie rondom het verwerken.

4.1.1 Ondertekenen

Een EH kan zowel door een zorgverlener als een gemandateerde medewerker worden gezet. De gemandateerde medewerker dient in dat geval wel te bezitten over een UZI-pas op naam. Op de UZI-pas van de zorgverlener en de UZI-pas van de medewerker op naam is onder andere een handtekeningcertificaat opgenomen. Met dit certificaat dient de ondertekenaar de EH te zetten. Een gemandateerde medewerker zet dus zijn eigen EH met het handtekeningcertificaat op zijn persoonlijke pas. Een UZI-pas niet op naam bezit niet over een handtekeningcertificaat en is daarmee uitgesloten voor het zetten van een EH. In het geval het niet gewenst is dat een medewerker met zijn UZI-pas op naam gebruik maakt van een EH, dan kan dat in de betreffende zorgtoepassing uitgesloten worden.

Afhankelijk van de zorgtoepassing moeten de te ondertekenen gegevens kenbaar worden gemaakt aan de ondertekenaar, volgens het "what you see is what you sign"-principe (WYSIWYS). Welke gegevens ondertekend moeten worden, is afhankelijk van de zorgtoepassing. Wel is het van belang dat er alleen ondubbelzinnige gegevens ondertekend worden. Bij gebruik van uniform gangbare codestelsels wordt in de te ondertekenen gegevensset zowel de formele code alsook de corresponderende beschrijvende tekst opgenomen. Hoofdstuk 4.1.1.1 geeft een uitgebreidere beschrijving omtrent codes en identiteitsnummers. Het formaat voor het handtekeningtoken wordt gedetailleerd uitgewerkt in de [IH EH UZI-pas]. Het handtekeningtoken zal minimaal de volgende gegevens bevatten:

- UZI-nummer en naam van de ondertekenaar (voor specifieke zorgtoepassingen kunnen kan ook de UZI rolcode worden vereist).
- Eenduidige identificatie van het handtekeningcertificaat van de ondertekenaar.
- Datum en tijd van tekenen.
- Patiëntgegevens: BSN, naam, geslacht, geboortedatum.
- Overige zorgtoepassingsspecifieke gegevens
- Referentie naar het met het handtekeningtoken overeenkomende deel in het HL7v3-bericht; (zorgtoepassingsspecifiek)

Om het vertrouwensniveau te waarborgen dat beoogd wordt bij gebruik van de EH, dient de ondertekenaar bij het ondertekenen van patiëntgegevens ter bevestiging een niet triviale (bewuste) handeling te verrichten. Deze handeling moet de handtekening aan de ondertekenaar binden, bijvoorbeeld door middel van het ingeven van een pincode.

De ondertekenaar ondertekent een gegevensset (patiëntstuk) en niet het bericht zelf. Op deze manier wordt het mogelijk om ondertekende patiëntstukken te versturen (push) en/of op te vragen (pull). De EH wordt gepresenteerd zoals beschreven in [IH EH UZI-pas].

Het is mogelijk om meerdere handtekeningen te zetten onder dezelfde gegevensset of een gedeelte van dezelfde gegevensset. Een al bestaande handtekening kan in dat geval

worden meegenomen als deel van de gegevensset die ondertekend moet worden. Afhandeling en betekenis van geneste handtekeningen is zorgtoepassing afhankelijk.

4.1.1.1 Codes en identiteitsnummers

Het gebruik van codes in de ondertekende tekst vraagt enige uitleg. Codes zijn voor de mens in het algemeen minder begrijpelijk dan een tekst die de betekenis ervan weergeeft. Automatische verwerking van codes is in veel gevallen echter veel eenvoudiger te realiseren dan automatische verwerking van teksten.

Bij een in de zorg uniform gangbaar codestelsel is de betekenis van de codes, die tussen zorgverleners en hun zorgsystemen worden uitgewisseld, voor beide zijden duidelijk. Bij elke code hoort ook een beschrijvende tekst, die voor de ondertekenaar beter begrijpelijk is dan de code. Voor geautomatiseerde matching en verwerking is de code bruikbaarder. Het opnemen van de code in de ondertekende gegevens is niet zozeer nodig om de wilsuiting van de ondertekenaar duidelijk te maken (daarvoor zou de beschrijvende tekst voldoende zijn) maar dient vooral om verminking of manipulatie van de codes onderweg te voorkomen. Indien de elektronische handtekening alleen de beschrijvende tekst zou bevatten, zou geautomatiseerde verwerking op basis van de niet ondertekende formele code elders in het patiëntbericht riskant zijn. De elektronische handtekening zou dan immers geen garantie bieden dat de code onveranderd is.

Een argument tegen het ondertekenen van de code zou kunnen zijn, dat de zorgverlener deze niet begrijpt. Niet ondertekenen zou echter betekenen dat voor de automatische verwerking van de code niet de elektronische handtekening geen betekenis zou hebben.

Bij het ondertekenen van de code komt de vraag op, of de applicatie van de verwerker ook moet verifiëren of in het ontvangen patiëntbericht de code en toelichtende tekst daadwerkelijk corresponderen. Dat zou echter het probleem van het matchen van de beschrijvende teksten herintroduceren. Omdat de verwerker al beschikt over de code, zou een zekere tolerantie bij het matchen van de teksten gehanteerd kunnen worden. Of matchen van de code nodig en nuttig is en welke toleranties zijn toegestaan, zal per zorgtoepassing en codestelsel moeten worden beoordeeld. Daarom wordt hiervoor geen algemene regel opgenomen.

Bij lokaal gebruikte codestelsels of codestelsels die niet uniform zijn (dat wil zeggen dat er meerdere varianten of versies bestaan en/of dat een code anders geïnterpreteerd kan worden dan de afzender bedoelt) is het niet gewaarborgd dat ondertekenaar en verwerker dezelfde betekenis aan de code zullen hechten. In zo'n geval is het verstandig de code achterwege te laten, teneinde elk mogelijk misverstand uit te sluiten. Denk bijvoorbeeld aan fabrikantartikelnummers van medicijnen. Dit betekent dat de ondertekenaar een tekst ondertekent, die de verwerker moet interpreteren. Daarvoor is in het algemeen menselijke tussenkomst nodig.

Het BSN van de patiënt en het UZI-nummer van de zorgverlener spelen een belangrijke rol bij gegevensuitwisseling in de zorg. Het BSN en het UZI-nummer zijn identiteitsnummers, op te vatten als betrouwbare en uniform gebruikte codestelsels.

- In het geval van het BSN is de zorgverlener verplicht de identiteit van de patiënt te controleren en te zorgen dat het juiste BSN wordt opgenomen in het zorgsysteem. Het BSN kan dus als betrouwbaar gegeven in het patiëntbericht worden opgenomen en mede ondertekend.
  De GBA kent een standaard schrijfwijze voor de naam van de burger/patiënt. Via de SVB-Z kunnen zorgsystemen de naam met de juiste schrijfwijze opvragen. Het is echter nog geen algemene regel dat zorgsystemen deze schrijfwijze toepassen. Er zijn vele oorzaken aan te wijzen die leiden tot verschillende schrijfwijzen.

Betrouwbaar matchen van de naam van de patiënt tussen zorgsystemen op basis van alleen de tekst is dus niet haalbaar. De naam van de patiënt moet echter wel worden ondertekend, omdat de ondertekenaar deze kent.
In geval van twijfel kan de ondertekende tekst worden geraadpleegd. Het valt buiten het kader van dit document om de situaties waarin dit moet gebeuren of de wijze waarop voor te schrijven.
Ondanks dat de wet voorschrijft dat van elke patiënt het BSN wordt opgevraagd en geverifieerd, zijn er in het zorgproces situaties denkbaar waarin (nog) geen BSN bekend is van een patiënt, bijvoorbeeld bij pasgeborenen, bewusteloos binnengebrachte patiënten of buitenlanders. In dergelijke gevallen moeten zo mogelijk vijf identificerende gegevens worden geregistreerd (Voornamen, Achternaam, Geslacht, geboortedatum, geboorteplaats) en aan de ondertekende tekst worden toegevoegd. Voor lokaal gebruik is het in zo'n geval toelaatbaar dat een lokaal patiëntnummer wordt gebruikt in plaats van het BSN. Een consequentie daarvan is dat die informatie binnen het systeem moet blijven omdat patiëntberichten zonder BSN niet over AORTA uitgewisseld kunnen worden. Achteraf aanpassen van het patiënt-ID in een BSN in de ondertekende patiëntstukken is niet mogelijk, wel het koppelen van gegevens lokaal binnen het GBZ.

- In het geval van het UZI-nummer gaat het om een uniek nummer dat aan de zorgverlener wordt toegekend. Daaraan zijn de naam en rol(len) van de zorgverlener gekoppeld. Het UZI-nummer is een betrouwbare code voor de identificatie van de zorgverlener (of medewerker in de zorg). Deze moet daarom worden ondertekend. Het UZI-register kent een standaard schrijfwijze voor de naam van de zorgverlener. Het is in principe mogelijk deze als standaard te hanteren en deze te gebruiken als tweede middel om de zorgverlener te identificeren. Het blijkt dat in de voorkomende gevallen zorgverleners een voorkeur hebben voor een andere schrijfwijze van de eigen naam. Het valt buiten het kader van dit document om het gebruik van de standaard schrijfwijze van de naam voor te schrijven. Daarom wordt toegestaan dat de zorgverlener de schrijfwijze van de eigen naam kiest, en deze mede ondertekent. Matchen van de tekstrepresentatie van de naam van de zorgverlener wordt niet voorgeschreven.

4.1.2 Versturen

Bij het versturen wordt het ondertekende patiëntstuk ingepakt in een bericht. De ondertekende informatie kan hierbij verzonden worden en de verzending mag de inhoud, samenhang en volgorde niet wijzigen. Eventuele wijzigingen die ongedaan kunnen worden gemaakt door canonicalisatie aan de kant van de ontvanger, zijn wel toegestaan. Naast het ondertekende patiëntstuk wordt de bijbehorende EH en het handtekeningcertificaat waarmee de EH is getekend ook opgenomen in het bericht. Per zorgtoepassing kan hiervan worden afgeweken en is het mogelijk om in plaats van het handtekeningcertificaat alleen een referentie naar het handtekeningcertificaat op te nemen.

In een bericht kunnen meerdere handtekeningtokens worden opgenomen. Hierbij kunnen de patiëntstukken met elkaar samenhangen maar apart zijn ondertekend. Een logische samenhang tussen de patiëntstukken kan echter ook ontbreken.

Het versturen kan op een ander tijdstip gedaan worden dan het ondertekenen. Ook het verzenden van het ondertekende patiëntstuk kan gedaan worden door een ander dan de ondertekenaar.

De ZIM negeert eventuele EH's in berichten die gericht zijn aan zorgaanbieders of zorgverleners. De betreffende berichten worden inclusief EH doorgezet naar de eindbestemming, ongeacht de geldigheid van de EH.

4.1.3 Controleren

De aanwezigheid van de EH moet direct zichtbaar zijn voor de ontvanger. De ontvanger van het bericht moet exact kunnen zien welke gegevens en handtekeningattributen de verzender wel en niet heeft ondertekend. Als hiervan wordt afgeweken, moeten de implicaties duidelijk zijn voor ondertekenaar en ontvanger. Zonodig zullen hierover binnen de beroepsgroepen duidelijke afspraken per zorgtoepassing worden gemaakt.

De ontvangstapplicatie moet de geldigheid van de EH controleren. Deze controle behelst verschillende aspecten.

Als eerste moet de XML signature gecontroleerd worden.
Dit wordt beschreven in [IH EH UZI-pas].

Als tweede moet het certificaat gecontroleerd worden op geldigheid, of het gaat om een gekwalificeerd certificaat en of het certificaat afkomstig is van een vertrouwde CSP. Deze controle wordt afgehandeld zoals beschreven in [IH EH UZI-pas] en [UZI-register].

In het handtekeningtoken zijn een aantal velden opgenomen met informatie over het certificaat. Deze velden moeten worden gecontroleerd tegen de gegevens van het meegestuurde certificaat. Het gaat hierbij om de volgende gegevens:

- UZI-nummer van ondertekenaar;
- Referentie naar het certificaat met daarin de uitgevende Certificate Authority en certificaatserienummer.

Door het opnemen van informatie uit het certificaat in het token kunnen na een positieve controle de gegevens als betrouwbaar worden beschouwd.

De volgende controlestap is de controle of er op de juiste manier gebruik is gemaakt van een handtekeningtoken. Het juiste gebruik van het token is zorgtoepassing afhankelijk. Verder wordt in deze controlestap de inhoud van het token gecontroleerd met de inhoud van het bericht. De ondertekende velden die zijn opgenomen in het handtekeningtoken moeten overeenkomen met de velden in het bericht.

Een verdere uitwerking van de controles bij ontvangst zijn weer te vinden in [IH EH UZI-pas].

Het GBZ dient een log bij te houden en daar voldoende informatie in op te nemen om reconstructie van de controle te ondersteunen. In geval van afkeuring dient hier ook de reden van afkeuring in te worden opgenomen.

4.1.4 Verwerken

Bij een positieve uitkomst van de handtekeningcontrole kan het betreffende patiëntstuk verwerkt worden (veelal geautomatiseerd, maar niet altijd). Indien het patiëntstuk handmatig verwerkt wordt, moet het voor de verwerker duidelijk zijn dat het patiëntstuk ondertekend is, dat die ondertekening gecontroleerd is en dat de uitkomst van die controle positief is. Ook bij geautomatiseerde verwerking moet de voor de verwerking verantwoordelijke persoon dit te allen tijde kunnen nagaan.

Bij negatieve uitkomst van de handtekeningcontrole (een uitzondering) dient het GBZ de voor verwerking van het patiëntstuk verantwoordelijke zorgverlener of diens gemandateerde medewerker proactief te informeren. Daarnaast moet het GBZ in dat geval ook terugkoppeling geven aan de afzender van het bericht dat de ongeldige handtekening bevat, door middel van een passende foutmelding.

4.1.5 Archiveren

De AORTA architectuur biedt geen voorzieningen ter ondersteuning van langdurige, veilige archivering van berichten met elektronische handtekening. De inrichting en archivering wordt overgelaten aan de eigenaar van het GBZ. Wel kunnen specifieke eisen omtrent archivering worden vastgelegd in het kader van een bepaalde zorgtoepassing. Als handvat worden er vanuit ETSI wel een aantal aanbevelingen gedaan omtrent het archiveren [CWA-14171].

4.2 Uitzonderingen bij elektronische handtekening

Bij het proces van tekenen, verzenden en verwerken van een EH kunnen uitzonderingen optreden. In [Arch AORTA] en de [Foutentabel] staan de algemene richtlijnen voor de detectie en afhandeling van uitzonderingen beschreven. AORTA.STK.t3610 en AORTA.STK.t3620 beschrijven de uitzonderingen die gedetecteerd worden door de verzendende respectievelijk de ontvangende GBZ.

De uitzonderingen die optreden bij het verzendende GBZ zijn uitzonderingen die optreden bij het ondertekenen en verzenden. De uitzonderingen die optreden bij het ontvangende GBZ treden op bij:

- Controle XML-signature
- Controle certificaat en keten
- Controle certificaatvelden in token
- Controle business rules

Tabel AORTA.STK.t3610: Uitzonderingen gedetecteerd door verzendende GBZ

Uitzonderingen	Maatregel
Getoond handtekeningtoken niet bevestigd door ondertekenaar	Afbreken interactie
UZI-pas heeft geen handtekeningcertifaat	Gebruiker melden dat hij niet bevoegd is tot het zetten van een EH
Pincode onjuist	Melden aan gebruiker

Tabel AORTA.STK.t3620: Uitzonderingen gedetecteerd door ontvangende GBZ

Uitzonderingen	Treedt op bij	Maatregel
Berekende hash-waarde van token ongelijk aan hash-waarde in SignedInfo	Controle XML-signature	Verwerking onderbreken, optreden fout melden.
Berekende hash-waarde van signature ongelijk aan hash-waarde in signature	Controle XML-signature	Verwerking onderbreken, optreden fout melden.
Verificatie van de handtekening	Controle certificaat en	Verwerking onderbreken,

van de CA niet correct	keten	optreden fout melden.
Verkeerde certificaat gebruikt (geen handtekeningcertificaat)	Controle certificaat en keten	Verwerking onderbreken, optreden fout melden.
Geldigheidsduur certificaat verstreken	Controle certificaat en keten	Verwerking onderbreken, optreden fout melden.
Certificaat ingetrokken	Controle certificaat en keten	Verwerking onderbreken, optreden fout melden.
Certificatieketen komt niet uit bij vertrouwd (UZI) CA-certificaat	Controle certificaat en keten	Verwerking onderbreken, optreden fout melden.
Certificatieketen niet correct	Controle certificaat en keten	Verwerking onderbreken, optreden fout melden.
Voorgeschreven velden in token komen niet overeen met certificaat	Controle certificaatvelden in token	Verwerking onderbreken, optreden fout melden.
Signature ontbreekt	Controle business rules	Verwerking onderbreken, optreden fout melden.
Handtekeningtoken ontbreekt	Controle business rules	Verwerking onderbreken, optreden fout melden.
Token stemt niet overeen met bericht	Controle business rules	Verwerking onderbreken, optreden fout melden.

De foutafhandeling wordt beschreven in [IH EH UZI-pas].

5 Gebruikte technieken

Het handtekeningtoken dat wordt ondertekend, is gebaseerd op een specifiek voor AORTA ontwikkeld XML-formaat en dus niet rechtstreeks op HL7 (het uitwisselformaat waarmee de ondertekende gegevens worden verzonden). De specificatie van het handtekeningtoken dient zodanig te zijn dat de gegevensset in het handtekeningtoken eenvoudig kan worden vergeleken met de gegevens in het HL7v3 bericht zodat ook de juistheid van het bericht kan worden geverifieerd.

Nadeel van de keuze voor XML voor het handtekeningtoken is de niet-eenduidigheid van XML (semantisch identieke XML-constructen kunnen syntactisch verschillend zijn). Dit zou kunnen leiden tot het onterecht afwijzen van een correct ondertekend handtekeningtoken. Om dat probleem te vermijden, wordt gebruik gemaakt van de zogenoemde canonieke vorm van XML zoals beschreven in [XML-EXC-C14N].

In het normenkader voor de elektronische handtekening (WSS specificaties en XAdES) wordt aangegeven dat het nodig is om het certificaat van de ondertekenaar te borgen door het certificaat of een ondubbelzinnige verwijzing daarnaar te ondertekenen. Dit is een tegenmaatregel tegen een aanvalsscenario waarbij achteraf het certificaat van de ondertekenaar wordt vervangen door een ander certificaat met dezelfde publieke sleutel, maar met een andere naam, andere attributen en/of uitgegeven door een andere CA. In de AORTA architectuur is een dergelijk aanvalsscenario vrijwel uitgesloten doordat uitsluitend UZI certificaten worden geaccepteerd, en het UZI-register bij elk sleutelpaar slechts één certificaat uitgeeft. Om de specificatie van de elektronische handtekening ongevoelig te maken voor deze uitgangspunten en om te voldoen aan de functionele eis die ETSI in XAdES stelt, is besloten toch het certificaat te borgen. De letterlijke specificatie van XAdES kon niet worden gevolgd, omdat de elektronische handtekening is gebaseerd op WSS.

WSS beschrijft het opnemen van een extra verwijzing in de Signature structuur. Voor GBZ-bouwers die geen WSS toolkit gebruiken, zou dit met name bij ontvangst extra werk opleveren. Om de gebruikte digital signature zo eenvoudig mogelijk te houden, is daarom niet gekozen voor de WSS optie maar voor het opnemen in het handtekeningtoken (dat ook de overige te tekenen gegevens bevat) van een eenduidige identificatie van het certificaat met behulp van de naam van de uitgever en het serienummer van het certificaat. Dit betekent voor de softwarebouwers, dat ze slechts één verwijzing naar een XML structuur in de Signature hoeven op te nemen en slechts één verwijzing hoeven te verifiëren.

Voor het formaat van de elektronische handtekening wordt gebruik gemaakt van XML-signatures, de W3C-standaard voor elektronische handtekeningen geïntegreerd in XML, conform de Web Services Security (WSS) specificaties van het OASIS consortium.

XML-Signatures [XML-DSIG] biedt grote flexibiliteit:

- Het is mogelijk meerdere gegevenselementen met één XML Signature te tekenen, ook als deze niet aaneengesloten in de (gecanonicaliseerde) XML-file staan.
- Het is mogelijk meerdere handtekeningen te plaatsen over één set gegevens of XML-file.

WSS biedt een nadere specificatie van XML signatures en geeft aan hoe XML signatures in SOAP kunnen worden ingepast. Voor WSS is gekozen vanwege de brede acceptatie in

de industrie. Hierdoor is de ondersteuning voor XML Signatures voor een gemiddelde softwareleverancier tegen geringere inspanning te realiseren, dan wanneer wordt uitgegaan van XML signatures met een specifieke invulling voor AORTA. Er zijn twee versies, WSS 1.0 en WSS 1.1, dat upwards compatible is met WSS 1.0. Gekozen is voor WSS 1.0, omdat dit breder wordt ondersteund.

Met XML-Signatures is het dus bijvoorbeeld mogelijk om eerst een set medische gegevens door de zorgverlener te laten ondertekenen met de UZI-pas, en daarna die gegevens bij verzending in de vorm van een HL7v3-bericht opnieuw te laten ondertekenen, bijvoorbeeld met het UZI-servercertificaat van de communicatieserver.

De werking van XML-signatures behelst een aantal stappen waarin de signature tot stand komt. Voor een gedetailleerde beschrijving wordt verwezen naar de [IH EH UZI-pas].

Het ondertekenen dient altijd te gebeuren met de volgende algoritmen:

1. Digest: SHA256.
2. Signing: RSA met 1024 of 2048 bit sleutels (afhankelijk van de UZI-pas).

Referenties

Referentie	Document	Versie
[DO]	Documentatieoverzicht AORTA	8.2.0.0
[Arch AORTA]	Architectuur AORTA	8.2.0.0
[IH EH UZI-pas]	Implementatiehandleiding elektronische handtekening met UZI-pas	8.2.0.0
[Wet Elektronische Handtekeningen]	http://wetten.overheid.nl	
[Richtlijn 1999/93/EG van het Europees Parlement en de Raad]	http://eur-lex.europa.eu/nl/index.htm	
[Regeling Elektronische Handtekeningen]	http://wetten.overheid.nl	
[Geneesmiddelen wet]	http://wetten.overheid.nl	
[CPS-UZI]	Certification Practice Statement (CPS) CIBG UZI-register https://www.uzi-register.nl/cps/cps.html	Zie [DO]
[CWA-14170]	ftp://ftp.cenorm.be/PUBLIC	
[CWA-14171]	ftp://ftp.cenorm.be/PUBLIC	
[XML-EXC-C14N]	http://www.w3.org/TR/xml-exc-c14n/	
[XML-DSIG]	http://www.w3.org/TR/xmldsig-core/	
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc5280.txt	
[WS Security]	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf	1.0 (2004)
[WS Security 1.1]	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf	
[UZI-register]	http://www.uzi-register.nl	
[Ontw TLG]	Ontwerp toegangslog	8.2.0.0
[Ontw Authenticatie]	Ontwerp Authenticatie	8.2.0.0
[Foutentabel]	Foutentabel	8.2.0.0