Justitiestandaard Asynchrone Berichtenuitwisseling 2.0.1

Technische Standaarden ebXML Configuratiegids

Directie Informatisering

Standaardisatiecommissie Justitie

Versie: 2.0.1

Status: Definitief

Editors:

Pim van der Eijk, Sonnenglanz Consulting BV

Albert Kappe, Capgemini

Abstract:

De specificatie Justitiestandaard Asynchroon Berichtenuitwisseling (JAB) is een standaard voor berichtenuitwisseling tussen organisaties in Justitie en Politie in Nederland. De ebXML Messaging v2.0 standaard is een complexe specificatie die veel configuratieopties biedt. Dit document specificeert een drietal *profielen* van de ebMS 2.0 standaard die interoperabiliteit verbeteren door de configuratieopties te beperken en die aansluiten op het gehanteerde beleid in de ketens waarin Politie en Justitie-organisaties samenwerken. In het kader van het toepassen van deze standaard voor specifieke ketenprocessen kunnen deze profielen verder worden uitgewerkt door aanvullende beperkingen vast te stellen.

Dit document is in de vorm van een *deployment specificatie* voor het gebruik van ebXML Messaging, afgeleid van een sjabloon ontwikkeld door het OASIS Implementation, Interoperability and Conformance Technical Committee (IIC TC).

Inhoudsopgave

1 Inleiding

Dit document specificeert een Technische Standaard voor Asynchrone Berichtenuitwisseling tussen organisaties in het Justitie- en Politiedomein als een toepassing van de ebXML Message Service Specification 2.0 **[ISO 15000-2]** voor de ketens waarin Justitie- en Politieorganisaties samenwerken. Deze specificatie kan nader gespecialiseerd worden voor specifieke koppelvlaken, zoals de uitwisseling tussen Politie en OM rond Routinezaken **[EPV-TA-2]**, of het bevragen van de Verwijsindex Personen.

EbXML Messaging **[ISO 15000-2]** is bedoeld voor uiteenlopende toepassingen en faciliteert die diversiteit door een scala aan configureerbare feature en opties te bieden. Elk gebruik van ebXML Messaging in een bepaalde keten of binnen een bepaalde gemeenschap vereist in de praktijk een bepaalde mate van aanvullende standaardisatie. Aangezien veel van de configuratiefeatures in de standaard optioneel zijn, moet precies gedocumenteerd worden welke onderdelen ervan toegepast worden en op welke manier, om op de verschillende relevante niveaus interoperabiliteit tussen applicaties te realiseren. Die informatie kan verzameld en gepubliceerd worden als gebruikshandleiding of configuratiegids voor de keten. Het legt de overeengekomen conventies voor het gebruik van ebXML message service handlers in de keten vast, de functionaliteit die van een implementatie verwacht wordt en de details van het gebruik van de standaard. Een deployment specificatie is niet hetzelfde als een ebXML samenwerkings-protocol overeenkomst (CPA, **[ISO 15000-1]**), al hebben sommige onderdelen van een deployment specificatie gevolgen voor de specifieke invulling van CPA XML documenten.

Het OASIS Implementation, Interoperability en Conformance (IIC) Technical Committee (TC) heeft voor dit soort deployment specificaties een sjabloon opgesteld **[Deployment Guide 1.1]**. Dit sjabloon is al eerder toegepast door bepaalde sectoren zoals de detailhandel en de gezondheidszorg, en is daarmee een standaard manier van configureren geworden. Dit document is opgesteld aan de hand van deze sjabloon. Het is slechts een summiere beschrijving van het specifieke gebruik van ebXML Messaging en bevat geen achtergrondinformatie, motivatie, voorbeelden en andere informatie die nuttig is voor het in de praktijk toepassen van deze specificatie.

1.1 Doel van dit document

Het doel van dit document is om Justitie- en Politie-organisaties die met behulp van ebXML Messaging informatie willen uitwisselen, een handvat te geven om generieke ebXML Messaging 2.0 software te configureren zodat berichten uitgewisseld kunnen worden.

Dit document is direct afgeleid van **[Deployment Guide 1.1]** en is om praktische redenen niet volledig vertaald. Leveranciers van producten en diensten rond ebXML Messaging zijn bekend met deze sjabloon doordat deze ook in andere sectoren elders in de wereld wordt gebruikt. Dit vereenvoudigt implementatie van ebXML messaging software bij Justitie, Politie en hun partners.

Als op een bepaald onderdeel geen specifieke richtlijn is gegeven, is een van de volgende waarden aangegeven:

Niet van toepassing. Dit is voor onderdelen die niet relevant zijn voor het Justitie- en Politie-domein, of voor features die niet gebruikt worden.

Nader in te vullen: geeft aan dat er geen wijziging of voorkeur voor een bepaalde invulling van het onderdeel is op het algemene niveau waar dit document zich op richt. Specifieke toepassingen van deze specificatie, zoals berichtenuitwisseling in de strafrechtsketen (EBV), zullen hier in veel gevallen wel nog aanvullende eisen voor stellen.

In onderzoek: voor onderdelen die nog nader onderzocht worden en mogelijk in toekomstige versies nader uitgewerkt worden.

1.2 Ondersteunde varianten

De ebXML Messaging standaard waarop deze specificatie is gebaseerd biedt een hogere mate van configureerbaarheid dan in de praktijk wenselijk is. Om redenen van interoperabiliteit, eenvoud en overzichtelijkheid onderscheidt deze specificatie een drietal varianten van uitwisselingen. Elke variant veronderstelt bepaalde voorgedefinieerde keuzen voor parameters als synchroniciteit, beveiliging en betrouwbaarheid en is daarmee een “profiel” voor ebXML Messaging.

Elke uitwisseling zal moeten voldoen aan één van deze profielen:

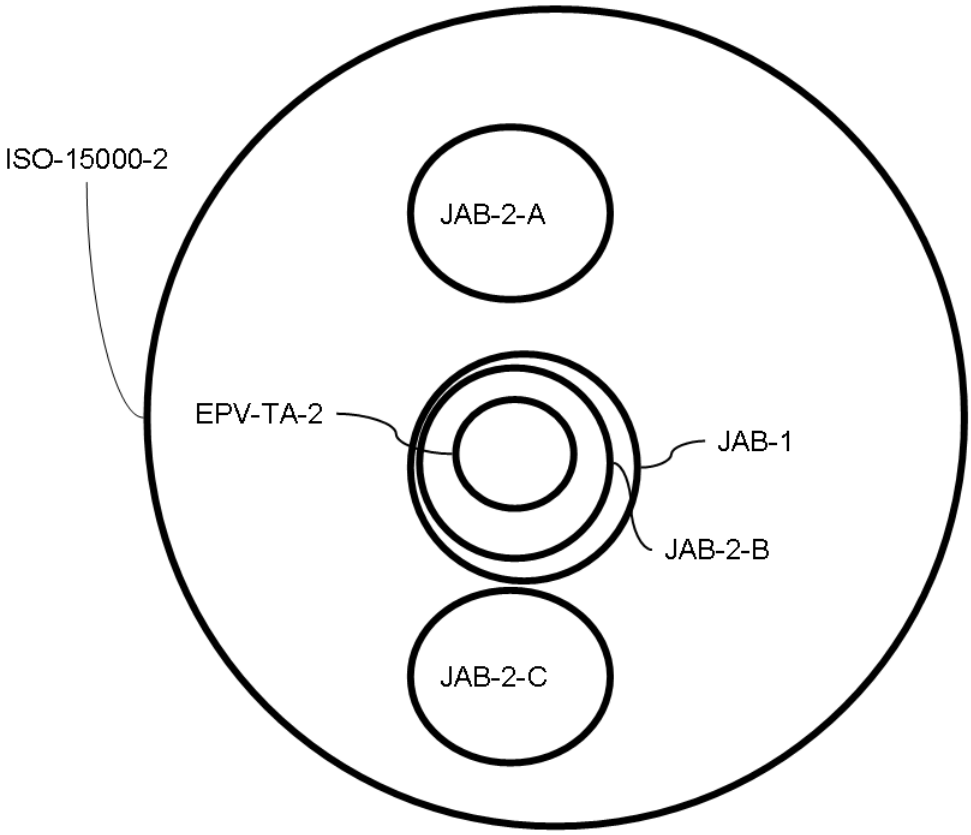
Bevragingen: dit zijn asynchrone uitwisselingen die beperkt zijn tot beveiliging op transportniveau, en die geen faciliteiten voor betrouwbaarheid (ontvangstbevestigingen, ontdubbeling van berichten etc.) nodig hebben.

Bedrijfstransacties met beveiligingsniveau Basis: asynchrone uitwisseling met ontvangst-bevestigingen en bericht-ontdubbeling door de ontvangende message handler. Beveiliging is beperkt tot authenticatie en vertrouwelijkheid op transportniveau.

Bedrijfstransacties met beveiligingsniveau Hoog: dit is gelijk aan Bedrijfstransacties met beveiligingsniveau Basis, maar voegt daaraan toe dat de aspecten authenticatie, vertrouwelijkheid, onweerlegbaarheid van oorsprong en ontvangst worden gerealiseerd door gebruik van XML digitale handtekening **[XMLDSIG]** en XML versleuteling **[XML Encryption]**.

1.3 Verschillen met JAB 1.0

Dit document is de opvolger van versie 1.0 van de Justitiestandaard Asynchroon Berichtenverkeer **[JAB 1.0]**. Deze was een generalisatie van **[EPV-TA-1]**, een specificatie voor uitwisseling rond routinezaken tussen Politie en OM.



Figuur 1 Relaties tussen specificaties

JAB-2 verschilt in de volgende opzichten van deze eerdere versie:

De profielen “Bevragingen” (label *JAB-2-A* in het figuur) en “Bedrijfstransacties met beveiligingsniveau Hoog” (label *JAB-2-C*) zijn toegevoegd. In versie 1.0 is alleen een profiel dat correspondeert met “Bedrijfstransacties met beveiligingsniveau basis” (*JAB-2-B*). De nieuwe profielen zijn geschikter voor bepaalde interacties die in de afgelopen periode onder de aandacht zijn gekomen. **[EPV-TA-2]** is een toepassing van het “JAB bedrijfstransacties basis” profiel voor uitwisseling tussen Politie en OM inzake Routinezaken. Het is een voorbeeld dat aangeeft dat voor een specifiek interactieproces tussen twee ketenpartners soms maar een van de profielen relevant is, en dat daarnaast specifieke extra beperkingen gelden.

De optionele ondersteuning van Message Order in versie 1.0 is vervallen in deze versie. De reden is dat deze functionaliteit in de praktijk in weinig producten weinig is geïmplementeerd en interoperabiliteit daarom niet gegarandeerd is. Veel wensen rond volgordelijke verwerking die in de praktijk bestaan, hebben eerder betrekking op het niveau van de bedrijfsapplicatie dan van berichtenverkeer. De waarde van volgordelijkheid op het niveau van berichtenverwerking is dan ook beperkt.

Het document is afgestemd op een soortgelijke specificatie voor intersectoraal berichtenverkeer **[SBG-IBS]**.

Er is gebruik gemaakt van de 1.1 versie van de ebXML Messaging deployment gids **[Deployment Guide 1.1]**. In versie 1.0 is uitgegaan van de 1.0 voorloper hiervan **[Deployment Guide 1.0]**.

In het profiel “Bedrijfstransacties met beveiligingsniveau Hoog” wordt gebruik gemaakt van geavanceerdere vormen van beveiliging (**[XMLDSIG]**,**[XML Encryption]**), en heeft dus meer te profileren opties.

De **[EPV-TA-2]** specificatie kan gebruik worden met deze specificatie of haar voorloper.

1.4 Verschillen tussen JAB 2.0 en JAB 2.0.1

Versie 2.0.1 van deze standaard bevat aanscherpingen en verhelderingen die naar boven zijn gekomen in twee jaar praktijkervaring met JAB 2.0. Het ondersteunt ook een alternatieve codering van organisaties dan de SYSDA instantiecodering **[SYSDA]**, onder meer in verband met communicatie met andere overheidsorganisaties via de Overheids Servicebus (OSB). Voor invulling van elementen die gebruikt (kunnen) worden voor routering wordt verwezen naar aanvullende conventies die hiervoor in het kader van EBV inmiddels zijn ontwikkeld. Geen van de wijzigingen hebben enige impact op bestaande toepassingen van JAB 2.0.

1.5 Functionele specificatie

Naast dit document is een meer algemeen document **[JAB 2.0 Func]** opgesteld over berichtenuitwisseling in de strafrechtsketen dat een achtergrond geeft van de problematiek en functionaliteit die met deze specificatie wordt behandeld en in algemene zin de functionaliteit van berichtenuitwisseling beschrijft. Dat document is een geactualiseerde versie van de JAB 1.0 *Functionele Standaard* **[JAB 1.0 Func]**. De relatie tussen dit document en **[JAB 2.0 Func]** is anders dan die van de twee JAB 1.0 documenten. **[JAB 1.0 Func]** maakte formeel gesproken volwaardig deel uit van de JAB 1.0 standaard, die uit twee documenten bestat.

[JAB 2.0 Func] is geen normatief document, en in gevallen waar het functionaliteit beschrijft die afwijkt van dit document, geldt dat dit document normatief is. Hiermee is de vraag welk document uitsluitsel moet geven als een vergelijking van de twee documenten onduidelijkheden of mogelijk zelfs tegenstrijdigheden oplevert beantwoord.

1.6 Beveiligingsaspecten

Deze specificatie maakt gebruik een aantal standaarden op het gebied van beveiliging en voldoet op het moment van schrijven aan geldend Justitie-beleid. Doordat in de loop der tijd kwetsbaarheden kunnen worden ontdekt in deze standaarden, is het van belang dat deze specificatie regelmatig op geldigheid hiervan wordt bezien. De specifieke toegepaste referenties zijn:

- Advanced Encryption Standard 256-cbc **[FIPS 197]**
- NIST richtlijnen voor sleutelbeheer **[NIST-Keys]**
- RSA-SHA1 **[RFC 2437]**
- Transport Level Security 1.0 **[RFC 2246]** of 1.1 **[RFC 4346]**
- XML Canonicalization **[Canonical XML]**.
- XML Encryption **[XML Encryption]**
- XML Digital Signatures **[XMLDSIG]**

Het gebruik van de volgende algorithmes verdient de voorkeur boven RSA-SHA1 zodra deze ondersteund zijn in nieuwere versies van de W3C aanbevelingen (**[XML Encryption]** en **[XMLDSIG]**) en in de gangbare beschikbare ebXML Messaging software:

- RSA-SHA-224 **[FIPS 180-2]**

- RSA-SHA-256 **[FIPS 180-2]**

1.7 Conventies voor stringwaarden

In het XML schema voor de ebXML Message header hebben de waarden van veel ebMS header elementen, waaronder CPAId, ConversationId, Service, Action, PartyId en Role als type de waarde non-empty-string. In de praktijk worden sommige van deze waarden (her)gebruikt om bestandsnamen te genereren, worden ze gebruikt voor routering en daarbij gematcht met andere tabellen, of anderszins hergebruikt in situaties die aanvullende beperkingen op de waarde van deze strings opleveren. Dit betekent dat het zinvol is om:

- De lengte van deze strings zoveel mogelijk beperkt te houden.
- Geen waarden te gebruiken die bij hergebruik als onderdelen van bestandsnamen zouden leiden tot ongeldige bestandsnamen in sommige besturingssystemen.

2 Profiling the Modules of ebMS 2.0

In this section, users will only specify which modules of the source specification are used in this profile (i.e. modules that business partners need to use or support in order to comply with the profile and communicate with others who do comply). For each used module, users also specify whether the module has been profiled or not. If yes, some profiling details should be given for this module in section 3 or 4.

2.1 Core Modules

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
Module Name and Reference	Core Extension Elements (section 3)	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Ondersteuning van Core Extension Elements van ebXML Messaging 2.0 is van toepassing op elk van deze drie profielen.		
Notes				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	Security Module (section 4.1)			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Niet van toepassing		Wel van toepassing
Notes		Security profile 3: "*Sending MSH* authenticates and both MSHs negotiate a secure channel to transmit data" wordt toegepast. De HTTPS connectie verzorgt *in transit* versleuteling van het volledige ebXML bericht. Security profile 0: "No security services are applied to data" is toegestaan indien gebruik wordt gemaakt van een beveiligde VPN of in besloten netwerksegmenten waar het beveiligingsbeleid vereist of toestaat om geen versleuteling toe te passen. In multihop scenario's dient elke hop apart te worden geconfigureerd voor toepassing van ofwel profile 0 of 3. Het is mogelijk dat de ene hop in een multihop pad met HTTP wordt uitgevoerd en een andere hop met HTTPS.		Security Profile 0 of 3 zijn van toepassing in dezelfde omstandigheden als dat het geval is voor het profiel Bevragingen en Bedrijfstransacties met beveiligingsniveau Basis. Daarnaast wordt toegepast security profile 14: "*Sending MSH* applies XML/DSIG structures to message and applies confidentiality structures (XML-Encryption) and *Receiving MSH* returns a signed receipt". XML encryptie garandeert end-to-end vertrouwelijkheid van de in het bericht opgenomen bedrijfsdocumenten en bijlagen, ook bij *store-and-forward* intermediairs. De ebXML message headers zijn ook in dit profiel altijd onversleuteld bij eventuele intermediairs om routering op basis van *To/PartyId* mogelijk te maken. Wanneer Security Profile 3 wordt toegepast, kan de inhoud van bedrijfsdocumenten onderweg tussen zender en ontvanger echter op geen enkel moment gelezen worden.

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	SyncReply Module (section 4.3)			
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Niet van toepassing. SyncReply wordt niet ondersteund in deze profielen.		
Notes		Asynchrone berichtuitwisseling sluit snelle responstijd en daarmee pseudo-synchrone (“functioneel synchrone”), interactieve applicaties niet uit.		

2.2 Additional Modules

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	Reliable Messaging Module (section 6)			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Niet van toepassing. Reliable messaging profile 8, *Best Effort*.	Wel van toepassing. Reliable messaging profile 2, Once-And-Only-Once Reliable Messaging at the End-To-End level only based upon end-to-end retransmission.	
Notes		In dit geval wordt geen gebruik gemaakt van het ebXML reliable messaging protocol.	In deze variant wordt alleen van de *ToParty MSH* (de uiteindelijke ontvanger) een ontvangstbevestiging gevraagd, niet van een eventuele *NextMSH* (waaronder eventuele tussenliggende stations, zoals de Justitie-voorziening *JUBES* en daarmee vergelijkbare voorzieningen bij andere organisaties en ketens). Dit geldt ongeacht het beveiligingsniveau.	

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	Message Status Service (section 7)			
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Niet van toepassing. Message Status Service wordt niet ondersteund in deze profielen.		
Notes				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	Ping Service (section 8)			
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Ping Service is optioneel in deze profielen.		
Notes				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	Message Order (section 9)			
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	Niet toegestaan. Message Order wordt niet ondersteund in deze profielen.		
Notes		Message Order was optioneel in JAB 1.0. Deze mogelijkheid is vervallen vanwege beperkte interoperabiliteit tussen ebXML messaging implementaties. Indien in een bepaalde interactie de volgordelijkheid van berichten relevant is dienen hiervoor voorzieningen op applicatie-integratie niveau gerealiseerd te worden.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Module Name and Reference	Multi-Hop (section 10)			
Profiling Status	Usage: <required / optional / never used in this profile> Profiled: <yes / no>	De profielen maken gebruik van intermediairs voor routering.		
Notes		De intermediairs hebben een beperkte functionaliteit en zijn volledig transparant.		

2.3 Communication Protocol Bindings

2.3.1 Profile Requirement Item: Transport Protocol

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements:			
Specification Reference	ebMS 2, Appendix B			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	Is HTTP a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	HTTP is toegestaan indien gebruik wordt gemaakt van een beveiligde VPN of in besloten netwerksegmenten waar het beveiligingsbeleid vereist of toestaat om geen versleuteling toe te passen.		
Profiling (b)	Is HTTPS a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	HTTPS is toegestaan.		
Profiling (c)	Is (E)SMTP a required or allowed transfer protocol? (See section B.3 for specifics of this protocol.)	(E)SMTP is niet toegestaan. De profielen zijn beperkt tot HTTP en HTTPS.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (d)	If SMTP, What is needed in addition to the ebMS minimum requirements for SMTP?	Niet van toepassing.		
Profiling (e)	Are any transfer protocols other than HTTP and SMTP allowed or required? If so, describe the protocol binding to be used.	Geen andere transfer protocollen zijn vereist.		
Alignment				
Test References				
Notes				

3 Profile Requirements Details

3.1 Module: Core Extension Elements

3.1.1 Profile Requirement Item: PartyId

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	In message Header: /SOAP:Header/eb:MessageHeader/eb:From/eb:PartyId /SOAP:Header/eb:MessageHeader/eb:To/eb:PartyId Is a specific standard used for party identification? Provide details.			
Specification Reference	ebMS 2, section 3.1.1.1 PartyId Element			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	Is a specific standard used for party identification? Provide details. Example - EAN•UCC Global Location Number. Ref.: ISO6523 - ICD0088.	Ketenpartners moeten gebruik kunnen maken van codes uit de **[SYSDA]** instantietabel als waarde van PartyId om specifieke partijen in Justitie- of Politieketens te identificeren en berichten naar deze partijen te routeren. Sommige toepassingen van deze specificatie zullen niet alleen met partijen die geïdentificeerd zijn in **[SYSDA]** gegevens uitwisselen maar ook met andere partijen. Deze toepassingen zullen in die gevallen naast de **[SYSDA]** adressering andere registratiesystemen moeten ondersteunen die in die projectcontext relevant zijn. Een voorbeeld hiervan is de adressering voor communicatie met organisaties via de Overheids Service Bus (OSB). Meer algemeen geldt dat de in sectie 1.7 genoemde conventies voor stringwaarden zoveel mogelijk gevolgd moeten worden.		
Profiling (b)	Should multiple PartyId elements be present in From and To elements?	Message handlers moeten PartyId elementen gebaseerd op SYSDA instantie identificatie kunnen identificeren. Daarnaast kunnen toepassingen andere classificatiesystemen gebruiken voor organisaties die niet in SYSDA geclassificeerd zijn. Elk JAB bericht mag in een From en To element ten hoogste één PartyId element bevatten.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (c)	Is the type attribute needed for each PartyId, and if so, what must it contain? Example – within the EAN•UCC system, the PartyId element and type are represented using Global Location Number. <eb:PartyId eb:type="http:/www.iso.int/schemas/eanucc/gln">1234567890128</eb:PartyId>	Voor identificatie van een partij volgens de SYSDA instantie codelijst moet het attribuut *type* van het SYSDA PartyId element de vaste waarde *urn:epv:sysda* hebben. Voorbeeld: <eb:PartyId eb:type="urn:epv:sysda">PL1300</eb:PartyId> Toepassingen die andere classificatiesystemen hanteren, moeten aanvullende conventies afspreken om deze aan te duiden. In deze versie van JAB moeten berichten gerouteerd kunnen worden op alleen de waarde van PartyId. Onder SYSDA wordt in deze context bedoeld de SYSDA instantie tabelwaarden (zoals: *PL1300*) en waarden die daaruit worden afgeleid voor testdoeleinden door het toevoegen van het *_OTA* suffix (bijvoorbeeld: *PL1300_OTA*).		
Alignment	appears as PartyId element in CPA. (c) appears as PartyId/@type in CPA			
Test References				
Notes		Als ook andere partij-identificatiesystemen ondersteund moeten worden (zoals GS1 Global Location Numbers, of de OSB codering), dan wordt het type attribuut gebruikt om dat partij-identificatiesysteem te identificeren. De tekst-inhoud van het PartyId element geeft dan de identificatie van de partij binnen het partij-identificatiesysteem. Zo kunnen naast elkaar verschillende symbolische identificatiesystemen gebruikt worden. Aandachtspunt is wel dat ook intermediairs die alternatieve systematiek en adressen moeten kunnen hanteren. De *JUBES* intermediair eist dat er geen overlap mag zijn in waarden van *PartyId* in verschillende coderingssystemen (ongeacht het mogelijke verschil in de waarde van PartyId/@type).		

3.1.2 Profile Requirement Item: Role

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:From/eb:Role /SOAP:Header/eb:MessageHeader/eb:To/eb:Role			
Specification Reference	ebMS 2, section 3.1.1.2 “Role Element”			
Profiling	Are Roles defined for each party of each business process? List them, or provide a reference to the source of these values. Example – within the EAN•UCC system, approved values are specified by the EAN•UCC Message Service Implementation Guide. <eb:Role>http:/www.ean-ucc.org/roles/seller</eb:Role>	Nader in te vullen In het algemeen geldt dat de in sectie 1.7 genoemde conventies voor stringwaarden zoveel mogelijk gevolgd moeten worden.		
Alignment	[Per-process; may reference Role values in BPSS [BPSS] definitions. Appears as Role/@name in CPA.]	Als deze specificatie wordt gebruikt voor berichtenverkeer dat is geanalyseerd en gemodelleerd conform de EBV methode **[EBV Methode]**, dan moeten de aanvullende EBV routeringsconventies voor het gebruik van dit element **[EBV Routering]** toegepast worden.		
Test References				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Notes				

3.1.3 Profile Requirement Item: CPAId

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:CPAId			
Specification Reference	ebMS 2, section 3.1.2			
Profiling	What identification scheme is used for the CPAId, and what form should it take? If a URI, how is it constructed? Does it reference a real CPA, or is it just a symbolic identifier? Example – within the EAN•UCC system, the value of the CPAId is the concatenation of the Sender and Receiver GLNs followed by a four digit serial number. 1234567890128 - GLN Party A 3456789012340 - GLN Party B 0001 - CPA Number between parties A and B	Een consistente naamgeving voor CPAId is wenselijk om monitoring van berichtstromen goed te kunnen verrichten. Het wordt aanbevolen om de CPAId samen te stellen als de concatenatie van de aanduiding van het interactieproces, de code-waarden gebruikt voor PartyId en een viercijfering versienummer, oplopend van “0001”, gescheiden door underscores. Een voorbeeld hiervan is: JCO-1-0a_PL7500_OTA-JD0021_OTA_0001 Meer algemeen geldt dat de in sectie 1.7 genoemde conventies voor stringwaarden zoveel mogelijk gevolgd moeten worden.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Alignment	Appears as CollaborationProtocolAgreement/@cpaid in CPA.			
Test References				
Notes		Het Competence Center Integratie (CCI) houdt een overzicht bij van alle in gebruik zijnde CPA's.		

3.1.4 Profile Requirement Item: ConversationId

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:ConversationId			
Specification Reference	ebMS 2, section 3.1.3			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	What is the user definition of a Conversation? What is the business criterion used to correlate messages considered parts of the same conversation?	Het element kan worden gebruikt voor het monitoren van meerdere samenhangende berichten over de voortgang van de behandeling van zaak (als zaaknummer gebruikt wordt als waarde van dit element) door een keten. Het kan ook gebruikt worden om berichten over een bepaalde persoon (als het VIP nummer gebruikt wordt als identificatie van het “gespreksthema”) te correleren. *ConversationId* hoeft in de ebXML Messaging standaard alleen uniek te zijn binnen de context van een *CPAId.* Hergebruik van waarden wordt ook bij berichten met andere *CPAId* of tussen andere ketenpartners aanbevolen indien deze berichten deel uitmaken van dezelfde conversatie. Meer algemeen geldt dat de in sectie 1.7 genoemde conventies voor stringwaarden zoveel mogelijk gevolgd moeten worden.		
Profiling (b)	In case the MSH implementation gives exposure of the ConversationId as it appears in the header, what identification scheme should be used for its value, and what format should it have? If a URI, how is it constructed? In case the ConversationId is not directly exposed, but only a handle that allows applications to associate messages to conversations, if the value of this handle is under control of the application, what format should it have?	Nader in te vullen.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Alignment	If BPSS is used, ConversationId typically maps to a business transaction. Is that the case? Does it map instead to a business collaboration?	Bij het gebruik van BPSS (ebXML Business Process **[ebBP]**) moet *ConversationId* corresponderen met een ebXML business collaboration. Als deze specificatie wordt gebruikt voor berichtenverkeer dat is geanalyseerd en gemodelleerd conform de EBV methode **[EBV Methode]**, dan moeten de aanvullende EBV routeringsconventies voor het gebruik van dit element **[EBV Routering]** toegepast worden.		
Test References				
Notes		De *ConversationId* is (in tegenstelling tot informatie in bedrijfsdocumenten) een ebXML header element. Voor het monitoren van de voortgang van een zaak door een keten, kunnen waarden worden hergebruikt per conversatie binnen een interactieproces met eventueel meerdere ketenpartners. Een knooppunt als *JUBES* ziet berichten tussen alle aangesloten ketenpartners langskomen en kan de *ConversationId* gebruiken om berichten, ook tussen meer dan twee partijen, over langere tijd te correleren. Het kan hiermee *Business Activity Monitoring* functionaliteit over de keten en onafhankelijk van aangesloten applicaties gaan bieden, naast de routeringsfunctie die het nu primair biedt.		

3.1.5 Profile Requirement Item: MessageId

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:MessageId			
Specification Reference	ebMS 2, section 3.1.6.1			
Profiling (a)	Although there is no requirement for an MSH to give control about MessageID to an application, some implementations may allow this. In this case, is there any requirement on the source of this ID? Any length and format restrictions if the ID is generated?	Niet van toepassing. De waarde van MessageId hoeft niet aan aanvullende vormeisen te voldoen, anders dan de waarde gespecificeerd in **[ISO 15000-2]**.		
Alignment				
Test References				
Notes				

3.1.6 Profile Requirement Item: Service

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Service /SOAP:Header/eb:MessageHeader/eb:Service/@type			
Specification Reference	ebMS 2, section 3.1.4			
Profiling (a)	Are Services (related groups of Actions) defined for each party of each business process? List them, or provide a reference to the source of these values. [Per-process; absent from BPSS definitions.] Is there a URI format scheme for this element?	Nader in te vullen Algemeen geldt dat de in sectie 1.7 genoemde conventies voor stringwaarden zoveel mogelijk gevolgd moeten worden.		
Profiling (b)	Is there a defined "type" for Service elements? If so, what value must the type attribute contain?	Nader in te vullen		
Alignment	Appears as Service element in CPA Appears as Service/@type in CPA	Als deze specificatie wordt gebruikt voor berichtenverkeer dat is geanalyseerd en gemodelleerd conform de EBV methode **[EBV Methode]**, dan moeten de aanvullende EBV routeringsconventies voor het gebruik van dit element **[EBV Routering]** toegepast worden.		
Test References				
Notes				

3.1.7 Profile Requirement Item: Action

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Action	In het algemeen geldt dat de in sectie 1.7 genoemde conventies voor stringwaarden zoveel mogelijk gevolgd moeten worden. Meer specifiek geldt dat in verband met beperkingen van de in Justitie gebruikte software voor business activity monitoring mogen de waarden van dit elementen geen spaties bevatten maar uitsluitend uit alfanumerieke tekens bestaan.		
Specification Reference	ebMS 2, section 3.1.5			
Profiling	Are Actions defined for each party to each business process? List them, or provide a reference to the source of these values. [Per-process; may reference BusinessAction values in BPSS definitions. Example – within the EAN•UCC system, approved values are specified by the EAN•UCC Message Service Implementation Guide. <eb:Action>Confirmation</eb:Action>	Nader in te vullen		
Alignment	Appears as ThisPartyActionBinding/@action in CPA.]	Als deze specificatie wordt gebruikt voor berichtenverkeer dat is geanalyseerd en gemodelleerd conform de EBV methode **[EBV Methode]**, dan moeten de aanvullende EBV routeringsconventies voor het gebruik van dit element **[EBV Routering]** toegepast worden.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.1.8 Profile Requirement Item: Timestamp

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:Timestamp /SOAP:Header/eb:MessageHeader/eb:Acknowledgment/eb:Timestamp			
Specification Reference	ebMS 2, section 3.1.6.2, 6.3.2.2, 6.4.5, 7.3.2			
Profiling	Must Timestamp include the 'Z' (UTC) identifier?	Timestamps moeten de ‘Z’ (UTC) identifier bevatten.		
Alignment				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.1.9 Profile Requirement Item: Description

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Description			
Specification Reference	ebMS 2, section 3.1.8			
Profiling	Are one or more Message Header Description elements required? In what language(s)? Is there a convention for its contents?	Niet van toepassing. *Description* elementen zijn niet vereist. Message handlers mogen *Description* elementen negeren.		
Alignment				
Test References				
Notes				

3.1.10 Profile Requirement Item: Manifest

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Body/eb:Manifest			
Specification Reference	ebMS 2, section 3.2.2			
Profiling (a)	How many Manifest elements must be present, and what must they reference? Does the order of Manifest elements have to match the order of the referenced MIME attachments? Any restriction on the range of value for xlink:reference (e.g. nothing other than content id references)?	*Manifest* elementen mogen uitsluitend verwijzen naar bedrijfsdocumenten en/of andere bijlagen die als MIME delen opgenomen zijn in de ebXML envelop. In **[ISO 15000-2]** wordt ook de mogelijkheid geboden om bedrijfsdocumenten door middel van verwijzingen naar externe documenten (zoals door middel van HTTP URIs) “logisch” onderdeel van het bericht te maken. Deze mogelijkheid is in deze profielen niet toegestaan.		
Profiling (b)	Must a URI that cannot be resolved be reported as an error?	Het is een fout als MIME delen waarnaar wordt verwezen niet in de MIME envelop zitten.		
Alignment				
Test References				
Notes		Dit sluit niet uit dat in een XML bedrijfsdocument in de payload verwijzingen opgenomen kunnen worden naar bijlagen die niet als MIME delen opgenomen zijn in de ebXML envelop.		

3.1.11 Profile Requirement Item: Reference

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference	Onderdelen worden uitsluitend geïdentificeerd door middel van *Content Id* verwijzingen **[RFC 2392]**. Sommige ebMS software producten ondersteunen de MIME functionaliteit om namen van bijgevoegde bestanden op te nemen in de MIME envelop structuurvelden. *Content-Disposition: attachment; filename=VerifyRequest.xml* Deze functionaliteit is niet vereist in de ebXML Messaging standaard en wordt niet ondersteund door andere gebruikte messaging producten. Om deze reden is het niet toegestaan om ervan uit te gaan dat de bestandsnaam (als deze wordt meegegeven in de MIME structuur) beschikbaar is bij de ontvangende ketenpartner. Wanneer twee partijen die berichten uitwisselen beide software gebruiken die deze functionaliteit ondersteunt, dan is er nog een mogelijk interoperabiliteits-probleem rond bestandsnamen. Verschillende besturingssystemen hebben verschillende eisen aan welgevormheid van bestandsnamen. Het wordt aanbevolen om conventies van ISO 9660, level 2 te hanteren voor bestandsnaam interoperabiliteit **[ISO 9660]**.		
Specification Reference	ebMS 2, section 3.2.1			
Profiling (a)	Is the xlink:role attribute required? What is its value?	Niet van toepassing. Het xlink:rol attribuut is niet vereist.		
Profiling (b)	Are any other namespace-qualified attributes required?	Niet van toepassing. Geen andere namespace-gekwalificeerde attributen zijn vereist.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Alignment				
Test References				
Notes				

3.1.12 Profile Requirement Item: Reference/Schema

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Schema			
Specification Reference	ebMS 2, section 3.2.1.1			
Profiling	Are there any Schema elements required? If so, what are their location and version attributes?	Nader in te vullen		
Alignment				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.1.13 Profile Requirement Item: Reference/Description

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Description			
Specification Reference	ebMS 2, section 3.2.1.2			
Profiling	Are any Description elements required? If so, what are their contents?	Niet van toepassing. *Description* elementen zijn niet vereist.		
Alignment				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.2 Module: Security

3.2.1 Profile Requirement Item: Signature generation

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/Signature			
Specification Reference	ebMS 2, section 4.1.4.1			
Profiling (a)	Must messages be digitally signed? [Yes, for Security Services Profiles 1, 6-21.	Niet van toepassing. In deze profielen wordt geen gebruik gemaakt van digitale handtekeningen.		Ja
Profiling (b)	Are additional Signature elements required, by whom, and what should they reference?	Niet van toepassing		Nee

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (c)	What canonicalization method(s) must be applied to the data to be signed? [Recommended method is "http://www.w3.org/TR/2001/REC-xml-c14n-20010315".]	Niet van toepassing		Toepassing van XML canonicalization **[Canonical XML]**.
Profiling (d)	What canonicalization method(s) must be applied to each payload object, if different from above?	Niet van toepassing		
Profiling (e)	What signature method(s) must be applied?	Niet van toepassing		RSA-SHA-1. **[XMLDSIG]**, **[RFC 2437]**. Zie de opmerkingen in sectie 1.6 Beveiligingsaspecten.
Profiling (f)	What Certificate Authorities (issuers) are allowed or required for signing certificates?	Niet van toepassing		Een CA die in de "chain of trust" voor de keten is opgenomen: voor overheidsorganisaties geldt als minimum PKI Overheid. Voor uitwisseling met partijen buiten de overheid zijn alternatieve afspraken noodzakelijk.
Profiling (g)	Are direct-trusted (or self-signed) signing certificates allowed?	Niet van toepassing		Nee

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (h)	What certificate verification policies and procedures must be followed?	Niet van toepassing		Message handlers moeten de revocatielijsten van de trusted CA's volgen.
Alignment	(a) Appears as BusinessTransactionCharacteristics/@isAuthenticated=persistent and BusinessTransactionCharacteristics/@isTamperProof=persistent in CPA			
Test References				
Notes				Het SHA1 algoritme is op dit moment voldoende veilig. Het verdient echter aanbeveling om het gebruik uit te faseren ten gunste van minder kwestbare algoritmen uit de SHA2 familie, zodra ondersteuning daarvan door softwareproducten gebruikelijk is.

3.2.2 Profile Requirement Item: Persistent Signed Receipt

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			
Specification Reference	ebMS 2, section 4.1.4.2			
Profiling (a)	Is a digitally signed Acknowledgment message required? [Yes, for Security Services Profiles 7, 8, 10, 12, 14, 15, 17, 19-21. See the items beginning with Section 4.1.4.1 for specific Signature requirements.]	Niet van toepassing		Ja
Profiling (b)	If so, what is the Acknowledgment or Receipt schema?	Niet van toepassing		Dit wordt gerealiseerd door een digitale ondertekening van het bericht van ontvangstbevestiging door middel van XML Digital Signatures **[XMLDSIG]**.
Alignment	Appears as BusinessTransactionCharacteristics/@isNonRepudiationReceiptRequired=persistent in CPA.			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.2.3 Profile Requirement Item: Non Persistent Authentication

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			
Specification Reference	ebMS 2, section 4.1.4.3			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling	Are communication channel authentication methods required? [Yes, for Security Services Profiles 2-5.] Which methods are allowed or required?	Het gebruik van HTTPS op basis van TLS versie 1.0 **[RFC 2246]** of 1.1 **[RFC 4346]** met 2-zijdige authenticatie is verplicht bij berichtuitwisseling in een niet besloten netwerk (segment). Bij uitzondering is, wanneer de gebruikte ebXML Messaging software geen TLS client authenticatie biedt en alleen voor zover niet uitgesloten door de andere Justitie- en/of Politie-beveiligingsrichtlijnen, client authenticatie niet vereist als client IP nummer toegangscontrole is geïmplementeerd en het aantal client IP adressen beperkt is tot een zeer gering aantal. TLS implementaties moeten kunnen opereren in backwards compatiblity modus met SSLv3.		
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthenticated=transient in CPA.]			
Test References				
Notes				

3.2.4 Profile Requirement Item: Non Persistent Integrity

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			
Specification Reference	ebMS 2, section 4.1.4.4.			
Profiling	Are communication channel integrity methods required? [Yes, for Security Services Profile 4.] Which methods are allowed or required?	Niet van toepassing		
Alignment	[Appears as BusinessTransactionCharacteristics/@isTamperproof=transient in CPA.]			
Test References				
Notes				

3.2.5 Profile Requirement Item: Persistent Confidentiality

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			
Specification Reference	ebMS 2, section 4.1.4.5			
Profiling (a)	Is selective confidentiality of elements within an ebXML Message SOAP Header required? If so, how is this to be accomplished? [Not addressed by Messaging Specification 2.0.]	Niet van toepassing		
Profiling (b)	Is payload confidentiality (encryption) required? [Yes, for Security Services Profiles 13, 14, 16, 17, 21, 22.] Which methods are allowed or required?	Niet van toepassing. Eventuele versleutelde payloads kunnen niet door de message handler ontcijferd worden (mogelijk wel door een achterliggende applicatie).		Ja. Hiervoor wordt gebruikt gemaakt van het algoritme AES 256-cbc **[FIPS 197]** in XML versleuteling **[XML Encryption]**.
Alignment	(b) [Appears as BusinessTransactionCharacteristics/@isConfidential=persistent in CPA.]			
Test References				
Notes				

3.2.6 Profile Requirement Item: Non Persistent Confidentiality

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			
Specification Reference	ebMS 2, section 4.1.4.6			
Profiling	Are communication channel confidentiality methods required? [Yes, for Security Services Profiles 3, 6, 8, 11, 12.] Which methods are allowed or required?	Versleuteling middels eenmalige symmetrische versleuteling op basis van TLS 1.0. Het gebruik van HTTPS op basis van TLS 1.0 **[RFC 2246]** of 1.1 **[RFC 4346]** met 2-zijdige authenticatie is verplicht bij berichtuitwisseling in een niet besloten netwerk (segment). TLS implementaties moeten kunnen opereren in backwards compatiblity modus met SSLv3.		
Alignment	[Appears as BusinessTransactionCharacteristics/@isConfidential=transient in CPA.]			
Test References				
Notes				

3.2.7 Profile Requirement Item: Persistent Authorization

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0

		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			
Specification Reference	ebMS 2, section 4.1.4.7			
Profiling	Are persistent authorization methods required? [Yes, for Security Services Profiles 18-21.] Which methods are allowed or required?	Niet van toepassing		
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired=persistent in CPA.]			
Test References				
Notes				

3.2.8 Profile Requirement Item: Non Persistent Authorization

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Reference	ebMS 2, section 4.1.4.8			
Profiling	Are communication channel authorization methods required? [Yes, for Security Services Profile 2.] Which methods are allowed or required?	De tweezijdige authenticatie functionaliteit van TLS 1.0 **[RFC 2246]** of 1.1 **[RFC 4346]** moet gebruikt worden in de context als beschreven in 3.2.3.		
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired=transient in CPA.]			
Test References				
Notes				

3.2.9 Profile Requirement Item: Trusted Timestamp

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:Signature			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Reference	ebMS 2, section 4.1.4.9			
Profiling	Is a trusted timestamp required? [Yes, for Security Services Profiles 9-12, 15-17, 20, 21.] If so, provide details regarding its usage.	Niet van toepassing		
Alignment				
Test References				
Notes				

3.3 Module : Error Handling

3.3.1 Profile Requirement Item:

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:ErrorList/eb:Error /SOAP:Header/eb:ErrorList/ eb:Error/@codeContext /SOAP:Header/eb:ErrorList/ eb:Error/@errorCode			
Specification Reference	ebMS 2, section 4.2.3.2.			
Profiling (a)	Is an alternative codeContext used? If so, specify	Niet van toepassing		
Profiling (b)	If an alternative codeContext is used, what is its errorCode list?			
Profiling (c)	When errors should be reported to the sending application, how should this notification be performed (e.g. using a logging mechanism or a proactive callback)?	Nader in te vullen		
Alignment				
Test References				
Notes				

3.4 Module : SyncReply

3.4.1 Profile Requirement Item: SyncReply

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:SyncReply/			
Specification Reference	ebMS 2, section 4.3			
Profiling (a)	Is SyncReply mode allowed, disallowed, or required, and under what circumstances? [May be process-specific.]	Niet van toepassing. Alle communicatie conform JAB is (technisch) asynchroon.		
Profiling (b)	If SyncReply mode is used, are MSH signals, business messages or both expected synchronously?			
Alignment	[Affects setting of 6.4.7 syncReplyMode element. Appears as MessagingCharacteristics/@syncReplyMode in CPA.]			
Test References				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Notes		De functionele kernvereiste voor interactieve applicaties waar een gebruiker binnen een aantal seconden een resultaat op een scherm wil zien is een snelle response tijd. Deze functionele vereiste is een vorm van “functioneel synchrone” communicatie. Deze kan echter evengoed opgevangen worden met “near real-time” asynchrone communicatie als met synchrone communicatie. Synchrone aanroepen zijn voor programmeurs eenvoudiger te implementeren. Een voordeel van asynchrone communicatie is echter dat deze veel meer schaalbaar en robuuster is, vooral in combinatie met communicatie via een knooppunt als *JUBES*.		

3.5 Module : Reliable Messaging

3.5.1 Profile Requirement Item: SOAP Actor attribute

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/			
Specification Reference	ebMS 2, section 6.3.1.1			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	SOAP Actor attribute: Are point-to-point (nextMSH) MSH Acknowledgments to be requested? [Yes, for RM Combinations 1, 3, 5, 7; refer to ebMS section 6.6. Appears as MessagingCharacteristics/@ackRequested with @actor=nextMSH in CPA.]	Niet van toepassing in deze profielen .		
Profiling (b)	Are end-to-end (toParty) MSH Acknowledgments to be requested? [Yes, for RM Combinations 1, 2, 5, 6. Appears as MessagingCharacteristics/@ackRequested with @actor=toPartyMSH in CPA.]	Niet van toepassing	Ja, deze profielen vereisen ebXML ontvangstbevestigingen van de uiteindelijke ontvangende message handler.	
Test References				
Notes				

3.5.2 Profile Requirement Item: Signed attribute

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Reference	ebMS 2, section 6.3.1.2			
Profiling	Must MSH Acknowledgments be (requested to be) signed ?	Niet van toepassing	Nee	Ja
Alignment	[Appears as MessagingCharacteristics/@ackSignatureRequested in CPA.]			
Test References				
Notes				

3.5.3 Profile Requirement Item: DuplicateElimination

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/			
Specification Reference	ebMS 2, section 6.4.1			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	Is elimination of duplicate messages required? [Yes, for RM Combinations 1-4. .]	Niet van toepassing	Duplicate Elimination is verplicht	
Profiling (b)	What is the expected scope in time of duplicate elimination? In other words, how long should messages or message Ids be kept in persistent storage for this purpose?		Nader in te vullen	
Alignment	Appears as MessagingCharacteristics/@duplicateElimination in CPA			
Test References				
Notes				

3.5.4 Profile Requirement Item: Retries and RetryInterval

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Reference	ebMS 2, section 6.4.3, 6.4.4			
Profiling (a)	If reliable messaging is used, how many times must an MSH attempt to redeliver an unacknowledged message?	Niet van toepassing	Nader in te vullen In toepassingen van berichtenverkeer als vervanger van het uitwisselen van papieren dossiers moeten de waarden van *Retries* en *RetryInterval* voldoende zijn om downtime van de berichtensoftware van de ketenpartner te kunnen opvangen. In sommige situaties kan dit oplopen tot meerdere werkdagen en/of moet reliable messaging uitval van een weekeinde kunnen overbruggen.	
Profiling (b)	What is the minimum time a Sending MSH should wait between retries of an unacknowledged message?		Nader in te vullen	
Alignment	(a) [Appears as ReliableMessaging/Retries in CPA.] (b) [Appears as ReliableMessaging/RetryInterval in CPA.]			
Test References				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Notes			Sommige ebXML producten onderkennen naast herzenden van ebXML berichten een mechanisme voor herzenden op transportniveau. Het ebXML interval moet dan ingesteld zijn dat de eerste ebXML retry pas plaatsvindt nadat alle retries op transportniveau (zonder succes) hebben plaatsgevonden.	

3.5.5 Profile Requirement Item: PersistDuration

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements:			
Specification Reference	ebMS 2, section 6.4.6			
Profiling	How long must data from a reliably sent message be kept in persistent storage by a receiving MSH, for the purpose of retransmission?	Niet van toepassing	Nader in te vullen	
Alignment	[Appears as ReliableMessaging/PersistDuration in CPA.]			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes			*JUBES* bewaart berichten minimaal 24 uur.	

3.5.6 Profile Requirement Item: Reliability Protocol

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements:			
Specification Reference	ebMS 2, section 6.5.3, 6.5.7		Voor betrouwbare aflevering wordt gebruik gemaakt van het Reliable Messaging Protocol van **[ISO 15000-2]**.	
Profiling (a)	Must a response to a received message be included with the acknowledgment of the received message, are they to be separate, or are both forms allowed?	Niet van toepassing	Ontvangstbevestigingen dienen als losstaande berichten verstuurd te worden en nooit gebundeld te worden met business response of andere ebXML berichten.	
Profiling (b)	If a DeliveryFailure error message cannot be delivered successfully, how must the error message's destination party be informed of the problem?	Dit is onderdeel van de operationele beheersafspraken van de ebXML diensten (intermediairs, eindpunten); intermediairs hoeven hiertoe geen aanvullende functionaliteit (zoals genereren van foutberichten) te bieden.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Alignment				
Test References				
Notes		Het is mogelijk dat er bij intermediairsvoorzieningen als *JUBES* berichten worden afgeleverd die ofwel tijdelijk (door onbeschikbaarheid van de ontvangende message handler) of permanent (doordat de ebXML *PartyId* niet opgevoerd is in de routeringstabellen van de intermediair) niet doorgerouteerd kunnen worden.		

3.6 Module : Message Status

3.6.1 Profile Requirement Item: Status Request message

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: Eb:MessageHeader/eb:StatusRequest			
Specification Reference	ebMS 2, section 7.1.1			
Profiling (a)	If used, must Message Status Request Messages be digitally signed?	Niet van toepassing. Message Status wordt niet ondersteund.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (b)	Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns?	Niet van toepassing. Message Status wordt niet ondersteund.		
Alignment				
Test References				
Notes				

3.6.2 Profile Requirement Item: Status Response message

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: Eb:MessageHeader/eb:StatusResponse			
Specification Reference	ebMS 2, section 7.1.2			
Profiling	If used, must Message Status Response Messages be digitally signed?	Niet van toepassing. Message Status wordt niet ondersteund.		
Alignment				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.7 Module : Ping Service

3.7.1 Profile Requirement Item: Ping-Pong Security

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: Eb:MessageHeader/eb:Service Eb:MessageHeader/eb:Action			
Specification Reference	ebMS 2, section 8.1, 8.2			
Profiling (a)	If used, must Ping Messages be digitally signed?	Ping Service berichten hoeven niet te worden ondertekend.		
Profiling (b)	If used, must Pong Messages be digitally signed?	Pong Service berichten hoeven niet te worden ondertekend.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (c)	Under what circumstances must a Pong Message not be sent?	Organisaties moeten geen Pong berichten sturen aan organisaties met wie ze geen CPA overeengekomen zijn.		
Profiling (d)	If not supported or unauthorized, must the MSH receiving a Ping respond with an error message, or ignore it due to security concerns?	In onderzoek.		
Alignment				
Test References				
Notes				

3.8 Module : Multi-Hop

3.8.1 Profile Requirement Item: Use of intermediaries

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements:			
Specification Reference	ebMS 2, section 10			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (a)	Are any store-and-forward intermediary MSH nodes present in the message path?	Deze profielen maken in alle gevallen gebruik van intermediairs voor routering van ebXML berichten, voor het verbinden van partijen die niet op hetzelfde (virtuele besloten) netwerk zijn aangesloten en voor het monitoren van berichtenstromen. Deze intermediairs hebben een beperkte functionaliteit en zijn volledig transparant. Routering vindt plaats op basis van een routeringstabel die To/PartyId waarden relateert aan een nextMSH URL en eventuele transport beveiligingsparameters (zoals certificaten voor versleuteling en authenticatie op basis van TLS.).		
Profiling (b)	What are the values of Retry and RetryInterval between intermediate MSH nodes?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging, dus geven zelf geen ontvangstbevestigingen en filteren geen duplicaten.		
Alignment				
Test References				
Notes		De intermediair heeft store-and-forward functionaliteit, en ook optioneel enige transport retry functionaliteit zodat tijdelijke storingen op transportniveau (zoals HTTP connecties die niet kunnen worden opgezet) kunnen worden afgevangen. Omdat de intermediair geen verantwoordelijkheid heeft voor de betrouwbaarheid van eindpunten, maken deze profielen gebruik van end-to-end reliability op ebXML niveau. Eindpunten moeten zelf ebXML reliable messaging functionaliteit (retries, duplicate elimination) toepassen als dat nodig is. De beperking op routering bij knooppunten op de waarde van To/PartyId betekent dat routering op basis van aanvullende header-elementen (zoals Service) niet wordt ondersteund. Alle berichten gericht aan een specifieke PartyId worden op een en hetzelfde endpoint afgeleverd, dan wel aan een en dezelfde volgende intermediair doorgestuurd.		

3.8.2 Profile Requirement Item: Acknowledgements

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements: Eb:MessageHeader/			
Specification Reference	ebMS 2, section 10.1.1, 10.1.3			
Profiling (a)	Must each intermediary request acknowledgment from the next MSH?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging.		
Profiling (b)	Must each intermediary return an Intermediate Acknowledgment Message synchronously?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging.		
Profiling (c)	If both intermediary (multi-hop) and endpoint acknowledgments are requested of the To Party, must they both be sent in the same message?	Niet van toepassing. Intermediairs spelen geen actieve rol in reliable messaging. Endpoint message handlers dienen geen intermediaire ontvangstbevestigingen te vragen.		
Alignment				
Test References				
Notes				

3.9 SOAP Extensions

3.9.1 Profile Requirement Item: #wildCard, Id

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements:			
Specification Reference	ebMS 2, section 2.3.6, 2.3.7, 2.3.8			
Profiling (a)	**(Section 2.3.6)** #wildcard Element Content: Are additional namespace-qualified extension elements required? If so, specify.	Er zijn geen aanvullende namespace-gekwalificeerde extensie-elementen. Ontvangende message handlers moeten onbekende extensie elementen negeren.		
Profiling (b)	**(Section 2.3.7)** Is a unique “id” attribute required for each (or any) ebXML SOAP extension elements, for the purpose of referencing it alone in a digital signature?	Niet van toepassing. ID attributen zijn niet verplicht.		
Profiling (c)	**(Section 2.3.8)** Is a version other than "2.0" allowed or required for any extension elements?	Deze specificatie is beperkt tot versie 2 van de ebXML Messaging specificatie.		
Alignment				
Test References				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Notes		Er is een versie 3.0 van ebXML Messaging. Deze is in onderzoek. Op korte termijn is er geen noodzaak en intentie om deze te gaan ondersteunen.		

3.10 MIME Header Container

3.10.1 Profile Requirement Item: charset

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	MIME Header elements: Content-Type			
Specification Reference	ebMS 2, section 2.1.3.2			
Profiling	Is the "charset" parameter of Content-Type header necessary? If so, what is the (sub)set of allowed values? Example: Content-Type: text/xml; charset="UTF-8"	UTF-8		
Alignment				

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.11 HTTP Binding

3.11.1 Profile Requirement Item: HTTP Headers

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements, MIME parts			
Specification Reference	ebMS 2, Appendix B.2.2.			
Profiling (a)	Is a (non-identity) content-transfer-encoding required for any of the MIME multipart entities?	Nader in te vullen		
Profiling (b)	If other than "ebXML" what must the SOAPAction HTTP header field contain?	De waarde van het SOAPAction http header veld dient altijd “ebXML” te zijn		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (c)	What additional MIME-like headers must be included among the HTTP headers?	Geen andere dan de minimaal verplichte HTTP headers zijn vereist. Ontvangende message handlers mogen alle headers die niet vereist zijn maar toegestaan zijn in de MIME en HTTP specificaties negeren.		
Alignment				
Test References				
Notes				

3.11.2 Profile Requirement Item: HTTP Response Codes

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements, MIME parts			
Specification Reference	ebMS 2, Appendix B.2.3.			
Profiling	What client behaviors should result when 3xx, 4xx or 5xx HTTP error codes are received?	Het gedrag van de message handler in het geval van een HTTP 5xx foutcode moet de aanbevelingen van **[SOAP1.1]** volgen. Codes in het 3xx en 4xx bereik moeten geïnterpreteerd worden als foutmeldingen.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Alignment				
Test References				
Notes				

3.11.3 Profile Requirement Item: HTTP Access Control

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements, MIME parts			
Specification Reference	ebMS 2, Appendix B.2.6.			
Profiling	Which HTTP access control mechanism(s) are required or allowed? [Basic, Digest, or client certificate (the latter only if transport-layer security is used), for example. Refer to item 4.1.4.8 in Security section.	Niet van toepassing. HTTP access control wordt niet toegepast.		
Alignment	Appears as AccessAuthentication elements in CPA.]			

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Test References				
Notes				

3.11.4 Profile Requirement Item: HTTP Confidentiality and Security

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements, MIME parts			
Specification Reference	ebMS 2, Appendix B.2.7.			
Profiling (a)	Is HTTP transport-layer encryption required? What protocol version(s)? [SSLv3, TLSv1, for example. Refer to item 4.1.4.6 in Security section.]	Het gebruik van HTTPS op basis van TLS 1.0 **[RFC 2246]** of 1.1 **[RFC 4346]** met 2-zijdige authenticatie is verplicht bij berichtuitwisseling in een niet besloten netwerk (segment). TLS implementaties moeten kunnen opereren in backwards compatiblity modus met SSLv3.		
Profiling (b)	What encryption algorithm(s) and minimum key lengths are required?	Nader te bepalen.		

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Profiling (c)	What Certificate Authorities are acceptable for server certificate authentication?	PKI overheid Certificaat Autoriteiten. PKI Overheid houdt een lijst toegetreden certificatiedienstverleners bij. Zie URL http://www.pkioverheid.nl/voor-certificaatverleners/toegetreden-certificaatverleners/.		
Profiling (d)	Are direct-trust (self-signed) server certificates allowed?	Self-signed server certificaten zijn toegestaan in test-situaties.		
Profiling (e)	Is client-side certificate-based authentication allowed or required?	Client-side authenticatie is vereist bij het gebruik van HTTPS, behalve in de eerder onder 3.2.3 Non Persistent Authentication genoemde uitzonderingen.		
Profiling (f)	What client Certificate Authorities are acceptable?	Een CA die in de "chain of trust" voor de keten is opgenomen: PKI overheid.		
Profiling (g)	What certificate verification policies and procedures must be followed?	De gangbare richtlijnen voor PKI moeten gehanteerd worden.		
Alignment				
Test References				
Notes		Een gangbare aanbeveling is om een minimale sleutellengte van 1024 bits te hanteren **[NIST-Keys]** en waar mogelijk 2048.		

3.12 SMTP Binding

3.12.1 Profile Requirement Item: MIME Headers

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0

		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements, MIME parts			
Specification Reference	ebMS 2, Appendix B.3.2.	Niet van toepassing. Deze versie van de Justitiestandaard Asynchrone Berichtenuitwisseling ondersteunt uitsluitend HTTP en HTTPS transport protocollen.		
Profiling (a)	Is any specific content-transfer-encoding required, for MIME body parts that must conform to a 7-bit data path? [Base64 or quoted-printable, for example.]	Niet van toepassing.		
Profiling (b)	If other than "ebXML" what must the SOAPAction SMTP header field contain?	Niet van toepassing		
Profiling (c)	What additional MIME headers must be included among the SMTP headers?	Niet van toepassing.		
Alignment				
Test References				
Notes				

3.12.2 Profile Requirement Item: SMTP Confidentiality and Security

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

		Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
		Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Specification Feature	Header elements, MIME parts			
Specification Reference	ebMS 2, Appendix B.3.4, B.3.5			
Profiling (a)	What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.]	Niet van toepassing.		
Profiling (b)	Is transport-layer security required for SMTP, and what are the specifics of its use? [Refer to item 4.1.4.6 in Security section.]	Niet van toepassing.		
Alignment				
Test References				
Notes				

4 Operational Profile

This section defines the operational aspect of the profile: type of deployment that the above profile is supposed to be operated with, expected or required conditions of operations, usage context, etc.

4.1 Deployment and Processing requirements for CPAs

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Is a specific registry for storing CPAs required? If so, provide details.	De Justitiële Informatiedienst ontwikkelt, beheert en publiceert CPAs voor uitwisseling met Justitieorganisaties via het EBV samenwerkingsportaal.		
Is there a set of predefined CPA templates that can be used to create given Parties' CPAs?	CPA templates zijn beschikbaar voor alle drie de sjablonen die in dit document zijn gedefinieerd.		
Is there a particular format for file names of CPAs, in case that file name is different from CPAId value?	De aanbeveling is om bestandsnamen van CPA's af te leiden van de CPAId, met toevoeging van de extensie ".XML"		
Others	Dit is geen registry in de zin van ebXML Registry of UDDI.		

4.2 Security Profile

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Which security profile(s) are used, and under what circumstances (for which Business Processes)? [Refer to Appendix C of Message Service Specification. May be partially captured by BPSS isConfidential, isTamperproof, isAuthenticated definitions.]	Security profile 3: “Sending MSH authenticates and both MSHs negotiate a secure channel to transmit data” wordt toegepast. Security profile 0: “No security services are applied to data" is toegestaan indien gebruik wordt gemaakt van een beveiligde VPN of in besloten netwerksegmenten waar het beveiligingsbeleid vereist of toestaat om geen versleuteling toe te passen.		Security Profile 0 of 3 zijn van toepassing in dezelfde omstandigheden als dat het geval is voor het profiel Bevragingen en Bedrijfstransacties met beveiligingsniveau Basis. Daarnaast wordt toegepast security profile 14:: “*Sending MSH* applies XML/DSIG structures to message and applies confidentiality structures (XML-Encryption) and *Receiving MSH* returns a signed receipt” toegepast
(section 4.1.5) Are any recommendations given, with respect to protection or proper handling of MIME headers within an ebXML Message?	Niet van toepassing. Er zijn geen aanvullende beveiligingsmaatregelen aan MIME headers.		
Are any specific third-party security packages approved or required?	Nader in te vullen		
What security and management policies and practices are recommended?	Nader in te vullen		

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Any particular procedure for doing HTTP authentication, e.g. if exchanging name and password, how?	Niet van toepassing		
Others			

4.3 Reliability Profile

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
If reliable messaging is required, by which method(s) may it be implemented? [The ebXML Reliable Messaging protocol, or an alternative reliable messaging or transfer protocol.]	Niet van toepassing	Door middel van het ebXML reliable messaging protocol.	
Which Reliable Messaging feature combinations are required? [Refer to Section 6.6 of Message Service Specification.]		Betrouwbaar berichtenverkeer profiel 2: Duplicate elimination Y AckRequested ToPartyMSH Y AckRequested NextMSH N	
Others			

4.4 Error Handling Profile

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0

	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
(Section 4.2.4.2) Should errors be reported to a URI that is different from that identified within the From element? What are the requirements for the error reporting URI and the policy for defining it?	Nader in te vullen		
What is the policy for error reporting? In case an error message cannot be delivered, what other means are used to notify the party, if any?	Tactisch beheer is verantwoordelijk voor het doorlopend actief monitoren van de message logs van eindpunten en intermediairs.		
(Appendix B.4) What communication protocol-level error recovery is required, before deferring to Reliable Messaging recovery? [For example, how many retries should occur in the case of failures in DNS, TCP connection, server errors, timeouts; and at what interval?]	In onderzoek.		
Others			

4.5 Message Payload and Flow Profile

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
What are typical and maximum message payload sizes that must be handled? (maximum, average)	Toepassingen waarin berichten die ontvangen worden door een message handler verder gerouteerd moeten worden via een andere berichteninfrastructuur die een maximum omvang van berichten heeft, zullen dat maximum ook aan ebXML berichten op willen leggen. Dit beperkt (bij protocollen als JMS, MQSeries) berichtomvang tot enkele megabytes. HTTP Proxy servers en firewalls hebben soms ook beperkingen op omvang van berichten. Deze verschillen van organisatie tot organisatie. De Justitie Berichtenservice (*JUBES*) maakt ook gebruik van een HTTP Proxy en is beschermd door firewalls. *JUBES* heeft geen bekend maximum berichtomvang, en vervoert in de praktijk berichten tot 150 MB.		
What are typical communication bandwidth and processing capabilities of an MSH for these Services?	De bandbreedte van de connecties van de Justitie Berichtenservice (*JUBES*) naar andere message handlers is begrensd door *packet shaping*. De grenswaarden variëren per organisatie.		
Expected Volume of Message flow (throughput): maximum (peak), average?			
(Section 2.1.4) How many Payload Containers must be present?	Berichten anders dan op zichzelf staande foutmeldingen en ontvangstbevestigingen hebben minimaal één payload bedrijfsdocument. Sommige toepassingen zullen een aantal al dan niet samenhangende bedrijfsdocumenten in een enkel bericht willen versturen. Deze specificatie stelt geen minimum of maximum.		
What is the structure and content of each container? [List MIME Content-Types and other process-specific requirements.] Are there restrictions on the MIME types allowed for attachments?	Aantal, aard en (betekenis van een) volgorde van Payload Containers die zijn toegestaan in berichten zijn nader te bepalen op het niveau van systemen ter ondersteuning van specifieke interactieprocessen.		

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
How is each container distinguished from the others? [By a fixed ordering of containers, a fixed Manifest ordering, or specific Content-ID values.]. Any expected relative order of attachments of various types?	Er is geen aanbevolen semantiek voor de volgorde van containers in relatie tot het ebMS Manifest element of waarden van Content-Id. De te ondersteunen Content-Typen zijn afhankelijk van de specifieke toepassing.		

4.6 Additional Messaging Features beyond ebMS Specification

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Are there additional features out of specification scope, that are part of this messaging profile, as an extension to the ebMS profiling?	Niet van toepassing		

4.7 Additional Deployment or Operational Requirements

	Justitiestandaard Asynchrone Berichtenuitwisseling 2.0		
	Bevragingen	Bedrijfstransacties met beveiligingsniveau Basis	Bedrijfstransacties met beveiligingsniveau Hoog
Operational or deployment aspects that are object to further requirements or recommendations.	Niet van toepassing		

5 References

5.1 Normative

[FIPS 197] NIST FIPS 197. Advanced Encryption Standard (AES). URL http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[Canonical XML] Canonical XML. URI http://www.w3.org/TR/xml-c14n

[EBV Methode] EBV methode voor het modelleren van interactieprocessen.

[EBV Routering] Standaard gebruik ebXML-envelop t.b.v. routering EBV-berichten v1.0

[EPV-TA-1] Uitwerking technische architectuur van de berichtenuitwisseling – korte termijn. Versie 1.0 beta. URL http://www.e-pv.nl/groepen/Architectuur_Infrastructuur/Technische_Architectuur/EPV_TA_1_0_beta

[ETSI TS 102 176-1] Electronic Signatures and Infrastructures (ESI). Algorithms and Parameters for Securie Electronic Signatures. Part 1: hash functions and asymmetric algoritms. URL http://www.etsi.org/

[ISO 9660] ISO 9660. Information processing -- Volume and file structure of CD-ROM for information interchange URL http://www.iso.ch/

[ISO 14662] ISO 14662. Open-edi reference model. URL http://www.iso.ch/

[ISO 15000-2] ISO 15000-2 *ebXML Message Service Specification*. URL http://www.oasis-open.org/specs/index.php#ebxmlmsgv2 .

[RFC 2246] T. Dierks, C. Allen. The TLS Protocol. URL http://www.ietf.org/rfc/rfc2246.txt?number=2246

[RFC 2392] Content-ID and Message-ID Uniform Resource Locators URL URL URL http://www.ietf.org/rfc/rfc2392.txt

[RFC 2437] PKCS #1: RSA Cryptography Specifications. IETF RFC 2437. URL http://www.ietf.org/rfc/rfc2437.txt.

[RFC 4346] T Dierks, C. Allen., *The Transport Layer Security (TLS) Protocol Version 1.1.* http://www.ietf.org/rfc/rfc4346.txt. IETF RFC 4346, April 2006.

[SOAP1.1] Simple Object Access Protocol (SOAP) v1.1. W3C Note 08 May 2000. URL http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[SYSDA] SYSDA instantatietabel van organisaties in de strafrechtsketen.

[XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification. URL http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.

[XML Encryption] XML Encryption Syntax and Processing. W3C Recommendation. URI http://www.w3.org/TR/xmlenc-core/

5.2 Non-normative

[Deployment Guide 1.1] Pete Wenzel, Jacques Durand. *Deployment Profile Template For OASIS ebXML Message Service 2.0.* OASIS Committee Draft 1.1, 20 June 2005.
URL http://www.oasis-open.org/apps/org/workgroup/ebxml-iic/download.php/13750/ebxml-iic-ebms2_deploy_template-spec-cd-11-final.doc

[Deployment Guide 1.0] P. Wenzel. *ebXML Deployment Guide Template.* OASIS Committee Draft 1.0 28 March 2003.
URL http://www.oasis-open.org/committees/download.php/1713/ebMS_Deployment_Guide_Template_10.doc

[ebBP] ebXML Business Process Specification Schema Technical Specification
URL http://docs.oasis-open.org/ebxml-bp/2.0.4/OS/.

[EPV-TA-2] EPV Technische Architectuur Berichtenuitwisseling Politie OM Routinezaken.

[FIPS 180-2] NIST FIPS 180-2 Secure Hash Standard
URL http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[ISO 15000-1] ISO 15000-1 ebXML Collaboration Protocol Profile and Agreement Specification. OASIS ebXML Collaboration Protocol Profile and Agreement Specification (2.0).
URL http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf

[JAB 1.0] Justitiestandaard Asynchroon Berichtenverkeer 1.0. Technische Standaarden ebXML Configuratiegids.
URL
http://justitieweb.minjus.nl/040_bedrijfsvoering/ict/Beleid_en_standaarden/Standaarden/Infrastructuur.asp

[JAB 1.0 Func] Justitiestandaard Asynchroon Berichtenverkeer 1.0. Functionele Standaard.
URL
http://justitieweb.minjus.nl/040_bedrijfsvoering/ict/Beleid_en_standaarden/Standaarden/Infrastructuur.asp

[JAB 2.0 Func] Justitiestandaard Asynchroon Berichtenverkeer 1.0. Onderbouwing en toelichting.

[NIST-Keys] NIST Key Management Guideline. .
URL http://csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-(workshop).pdf.

[SBG-IBS] Expertteam Framework Draft Intersectorale Berichtenstandaard. Deel B. Technische Specificatie. Programma Stroomlijnen Basisgegevens.

Appendix A. Versiegeschiedenis

Rev	Datum	Door wie	Omschrijving
0.1	5 Januari 2005	P. van der Eijk	Concept versie.
0.2	21 januari 2005	P. van der Eijk	Feedback eerste workshop verwerkt in secties: 2.3.7 2.3.8 3.1.1.1 3.1.1.2 2.1.4 3.1.6.2 4.3
0.3	11 februari 2005	P. van der Eijk	Gebruik van SSL/TLS beter beschreven. Release als **[JAB 1.0]**
0.4	24 januari 2006	A. Kappe	Toevoeging profielen “Bevragingen” en “Bedrijfstransacties met beveiligingsniveau Hoog”. Structuur aangepast aan nieuwe versie Deployment Profile Template.
0.5	3 maart 2006	A. Kappe	Uitwerking profiel “Bedrijfstransacties met beveiligingsniveau Hoog”.
0.6	9 maart 2006	P. van der Eijk	Literatuurverwijzingen, relatie tot eerdere versies, nieuwe koppelvlakspecifieke profielen als TA-2. Veel detailwijzigingen.
0.7	20 mei 2006	A. Kappe P. van der Eijk	Hashing, signing en encryption algoritmen ingevuld; referenties compleet gemaakt; CPA uitgewerkt en voorbeeldberichten
0.8	18 september 2006	A. Kappe P. van der Eijk	Client-side authentication Aanvullend commentaar

Rev	Datum	Door wie	Omschrijving
			Tjerk Zwanenburg verwerkt Geen spaties in Actions i.v.m. Transaction Director (sectie 3.1.7) Versie voor Review DJI
0.9	27 september 2006	P. van der Eijk	Herziene versie met TLS client en server authenticatie; tekstuele verbeteringen.
0.10	1 december 2006	P. van der Eijk	Commentaar Tjerk Zwanenburg verwerkt. PKI Overheid referenties. SHA2 toevoegingen.
2.0	29 juni 2006	P. van der Eijk	Definitieve versie gemaakt naar aanleiding van besluit Standaardisatiecommissie
2.0.1.1	1 juli 2008	P. van der Eijk	Versie .1 van JAB 2.0.1, een minor release, verwerkt cumulatief een aantal kleine verhelderingen en verduidelijkingen.
2.0.1.2	4 augustus 2008	P. van der Eijk	Versie .2; feedback Tjerk Zwanenburg verwerkt.