

ebMS3/AS4 als opvolger van ebMS2 binnen Digikoppeling



17 oktober 2018

Auteurs:
Frans van Basten
Fred van Blommestein

ebMS3/AS4 als opvolger van ebMS2 binnen Digikoppeling

Ondersteuning, functionele dekking, draagvlak en
roadmap

Inhoud	Pagina
1. Management samenvatting	4
2. Inleiding	5
2.1 Aanleiding	5
2.2 Vraagstelling	5
3. Functionaliteit	6
4. IST Situatie grote partijen	9
4.1 Belastingdienst	9
4.2 BKWI	9
4.3 RINIS	10
4.4 Justitiële Informatiedienst (JustID)	11
4.5 Conclusie	11
5. IST Situatie gemeenten	13
5.1 VNG Realisatie	13
5.2 Gemeenten Purmerend, Oostzaan en Amsterdam	13
5.3 Conclusie	14
6. IST Situatie samenwerkingsverbanden en Europa	15
6.1 Entsog	15
6.2 EDSN	15
6.3 Peppol	15
6.4 eDelivery	16
6.5 Conclusie	16
7. Ontwikkeling en ondersteuning	17
7.1 Standaardisatie ontwikkelingen	17

7.2 Leveranciers	17
7.3 Vragenlijst	17
7.4 Conclusie	19
8. Proeftuin en kennisborging	20
8.1 Proeftuin	20
8.2 Bevindingen uit de proeftuin	21
8.3 Kennisborging	21
8.4 Conclusie	22
9. Beheer van een ebMS configuratie	23
9.1 Problematiek rondom de configuratie ebMS3/AS4	23
9.2 Standaarden voor certificaat uitwisseling	24
9.3 ebCore Agreement Update Protocol	24
9.4 SMP/SML	24
9.5 ebXML Collaboration Protocol Profile and Agreement (CPPA) versie 3	25
9.6 Alternatieve oplossing	25
9.7 Conclusie	25
10. Alternatieven voor ebMS3/AS4	26
11. Migratie	27
12. Conclusie en aanbevelingen	29
12.1 Conclusies	29
12.2 Beantwoording van de onderzoeksvragen	30
12.3 Aanbevelingen	31

1. Management samenvatting

Digikoppeling maakt voor transactieberichten, waarbij aflevering van berichten gegarandeerd moet kunnen worden, gebruik van het ebMS2 protocol. De nieuwe Europese initiatieven voor B2G (business to government) en G2G (government to government) berichtenverkeer gebruiken ebMS3/AS4. Logius heeft VKA/Berenschot gevraagd onderzoek te doen of het voor Digikoppeling noodzakelijk is ook over te stappen op ebMS3/AS4.

VKA/Berenschot concludeert na onderzoek dat er niet een acute reden is om over te stappen, maar dat het wel verstandig is op termijn te migreren. Functioneel voldoet ebMS2 en ebMS3/AS4 biedt nauwelijks additionele functies die voor Digikoppeling van belang zijn. Leveranciers die ebMS2 ondersteunen zullen dat blijven doen. Migratie is een complexe en kostbare operatie, vooral omdat Digikoppeling gebruikt wordt door een groot aantal kleinere partijen (m.n. gemeenten) die daarvoor kennis moeten inhuren.

De Europese Commissie propageert ebMS3/AS4 in te zetten voor internationaal B2G en G2G berichtenverkeer. Al dit verkeer zal van het ebMS3/AS4 protocol gebruik gaan maken. Ook gemeenten zullen op termijn in toenemende mate internationaal moeten communiceren.

Een knelpunt voor aangeslotenen op Digikoppeling is het vervangen van certificaten en het toevoegen, verwijderen en wijzigen van communicatiepartners. Noch in ebMS2 noch in ebMS3/AS4 zijn hier panklare oplossingen voor. Het oplossen van dit knelpunt in combinatie met migratie naar ebMS3/AS4 zal het draagvlak voor migratie verstevigen.

Een roadmap of migratieplan dat enkele jaren beslaat en de oprichting van een “center of expertise” biedt de partijen de gelegenheid de migratie in alle rust voor te bereiden, te financieren en uit te voeren. Het is verstandig zo'n plan op korte termijn op te stellen en voldoende budget te alloceren alvorens deze transitie in gang te zetten (minimaal voor een periode van 5 jaar).

2. Inleiding

2.1 Aanleiding

Digikoppeling is een oplossing voor het uitwisselen van transactieberichten, waarbij gegarandeerd kan worden dat een bericht exact één keer wordt afgeleverd, het bericht onderweg niet is gewijzigd, dat de afzender van het bericht onomstotelijk kan worden vastgesteld en dat de afzender het bericht niet kan ontkennen. Digikoppeling maakt hiervoor momenteel gebruik van het OASIS ebMS2 protocol. Logius heeft geconstateerd dat dit protocol niet verder wordt ontwikkeld door OASIS. Logius vreest ook dat de ondersteuning door leveranciers van softwareproducten die dit protocol ondersteunen zal afnemen, met name omdat ebMS2 vooral in Nederland wordt gebruikt en in het buitenland voorzover bekend geen grootschalige toepassingen kent.

De opvolger van ebMS2 is ebMS3. Het configureren van ebMS3 biedt veel keuzevrijheid. OASIS heeft zelf een profiel opgesteld, het AS4 profiel. Dit profiel perkt de keuzevrijheid in, maar biedt mogelijk nog steeds ruimte voor verschillende implementaties. ebMS3/AS4 is niet “backwards compatible” met ebMS2. Voor het invoeren van ebMS3/AS4 is dus een migratie-inspanning nodig. ebMS3 heeft meer functionaliteit, maar het is niet duidelijk of die in de praktijk toegevoegde waarde biedt.

Logius heeft daarom VKA/Berenschot gevraagd te onderzoeken in hoeverre het ebMS2 protocol voor Digikoppeling voldoet, of ebMS2 voldoende blijvend wordt ondersteund door leveranciers en of en hoe gemigreerd zou moeten worden naar ebMS3/AS4. Het vaststellen van het draagvlak voor zo'n migratie onder de gebruikers van Digikoppeling behoorde eveneens tot deze opdracht.

2.2 Vraagstelling

De hoofdvraag die wij zullen beantwoorden is:

Is ebMS3/AS4 een geschikte opvolger voor de huidige ebMS2-versie binnen de Digikoppeling standaard?

Hierbij komen de volgende aspecten aan de orde:

- Ondersteuning (door leveranciers, standaard-organisaties en compliance testers)
- Functionele dekking
- Draagvlak (binnen de overheid)
- Consequenties van migratie (kosten, doorlooptijd)
- De roadmap van leveranciers m.b.t. het AS4 profiel
- Risico's (disruptie)
- Uitrol van ebMS3/AS4 en afbouw van ebMS2
- Lifecycle management

3. Functionaliteit

ebMS3/AS4 is de opvolger van ebMS2. Beide protocollen zijn bedoeld om betrouwbaar en veilig berichtenverkeer ("reliable messaging") tot stand te brengen (waarbij alle berichten precies één keer – eventueel versleuteld – worden afgeleverd). Beide zijn agnostisch met betrekking tot de payload. Het belangrijkste verschil tussen ebMS3/AS4 en ebMS2 is dat ebMS3/AS4 beter geïntegreerd is met ondersteunende W3C protocollen en OASIS standaarden, bijvoorbeeld om encryptie tot stand te brengen. In de tijd dat ebMS2 werd ontwikkeld, waren die protocollen nog niet beschikbaar en moest die functionaliteit ingebouwd worden op specifieke wijze. In ebMS3/AS4 wordt gebruik gemaakt van generieke ondersteunende protocollen.

ebMS3 bevat enkele functionele uitbreidingen. Zo bevat het functionaliteiten om zeer grote berichten (groter dan enkele gigabytes) op te knippen en functionaliteit om grote hoeveelheden kleine berichten te bundelen, om te besparen op protocol overhead. Deze functionaliteiten zijn niet opgenomen in het AS4 profiel. Beide functies zijn ook mogelijk wanneer ebMS2 wordt gebruikt, maar de wijze waarop moet dan bilateraal worden afgesproken.

ebMS3/AS4 bevat, in tegenstelling tot ebMS2, een "pull" functie. Kleinere organisaties en organisaties die geen inkomend netwerkverkeer toestaan hoeven dan niet constant in staat te zijn berichten te ontvangen, maar kunnen regelmatig opvragen of er berichten klaar staan.

Het belangrijkste functionele verschil tussen ebMS2 en ebMS3/AS4 zit in de functies voor partnermanagement. ebMS2 ondersteunt Collaboration Partner Agreements (CPA). Organisaties wisselen CPA's uit. Deze functie is nuttig wanneer het aantal partners beperkt is en de dynamiek laag.

ebMS3/AS4 maakt gebruik van een (gedistribueerd) adresboek, waarin potentiële partners hun "capabilities" opslaan. De gegevens in het adresboek kunnen worden gedistribueerd over verschillende servers die elkaar raadplegen, zodat de gebruiker één logisch adresboek ziet. Deze methode is vooral geschikt wanneer het aantal potentiële partners zeer groot is en de dynamiek hoog. Bij Digikoppeling is het aantal partners echter beperkt en de dynamiek laag.

Voor Digikoppeling lijkt ebMS3/AS4 functioneel niet veel toegevoegde waarde te hebben ten opzichte van ebMS2, behalve wat betreft security. Als securityrichtlijnen in de toekomst worden aangescherpt en in de uitwisseling de berichten versleuteld moeten worden, is dat in een omgeving waarbij verschillende softwareproducten worden gebruikt met ebMS3/AS4 makkelijker te realiseren, omdat binnen ebMS3/AS4 de W3C en OASIS beveiligingsprotocollen worden gebruikt. Deze zijn strak gedefinieerd en idealiter interoperabel geïmplementeerd in de meeste B2B softwareproducten.

Het partnermanagement van ebMS2 lijkt geschikter voor de Digikoppeling omgeving dan dat van ebMS3/AS4, aangezien binnen Digikoppeling het aantal partners beperkt is en de

dynamiek laag. Het in ontwikkeling zijnde CPPA3 maakt ook CPA's voor ebMS3 mogelijk. De "pull" functie lijkt aantrekkelijk voor kleine deelnemers (bijvoorbeeld gemeenten), maar het ontbreken daarvan geeft in de praktijk weinig problemen, omdat deze deelnemers meestal gebruik maken van "software as a service", waarbij de software in het rekencentrum van de leverancier draait en altijd online is.

Er bestaan diensten om producten te testen op functionaliteit en compliance met de standaarden. De belangrijkste is de Drummond Group. Drummond certificeert producten op conformance en interoperabiliteit. Drummond test compliance door het te testen product te vergelijken met een referentie-implementatie. Drummond test interoperabiliteit door alle producten in een community (volgens een bepaald profiel) met elkaar te laten communiceren.

Momenteel test Drummond (volgens hun website) alleen ebMS2, niet ebMS3/AS4. Drummond is een Amerikaanse commerciële onderneming die een behoorlijke prijs vraagt voor zijn diensten. Die prijs is soms te hoog voor softwareproducten van kleine leveranciers en voor open source ontwikkelingen. De Europese Commissie heeft daarom een test bed opgezet om producten te testen die claimen eDelivery te ondersteunen. eDelivery is een ebMS3/AS4 profiel dat is ontwikkeld door de Europese Commissie voor het berichtenverkeer met en tussen overheidsorganisaties in Europa. Het is nog onduidelijk welke functionaliteit door dat test bed zal worden getest, maar dat zal minimaal interoperabiliteit met andere producten zijn.

In de volgende tabel wordt de functionaliteit van ebMS2 en ebMS3/AS4 vergeleken.

Functie	EBMS 2.0	ebMS3/AS 4
WS-Addressing	Nee	Nee
WS-Security	Ja	Ja
Service Beschrijving	CPA	P-mode, SML/SMP (discovery)
Multi hop (intermed.)	Nee	Ja
SOAP versie	1.1	1.2
Push	Ja	Ja
Pull (asynchr)	Nee	Ja

Conclusie

De functionaliteit van ebMS2 voldoet voor de toepassingen van Digikoppeling. ebMS3 kent enkele features die voor sommige partijen van belang kunnen zijn (grote berichten, bundeling van berichten) maar die features zijn geen onderdeel van het AS4 profiel en rechtvaardigen geen migratie. Wanneer security eisen worden verhoogd kan dit veranderen (Digikoppeling ebMS2 gebruikt nog SHA1, dat inmiddels bewezen onveilig is).

Het ebMS3/AS4 adresboek is vooral geschikt voor grote communities waarin met veel partners gecommuniceerd moet worden, partners die vaak wisselen. Dat is niet het geval in de Digikoppeling omgeving. Voor ebMS3/AS4 zijn test- en certificeringsdiensten voorhanden, maar deze zijn in ontwikkeling.

4. IST Situatie grote partijen

In dit hoofdstuk wordt de situatie met betrekking tot Digikoppeling binnen een aantal grote overheidsorganisaties weergegeven. Deze informatie is verzameld middels een aantal interviews.

4.1 Belastingdienst

De Belastingdienst maakt voor Digikoppeling gebruik van een B2B Gateway van Axway. Aanvankelijk voor de implementatie van ebMS2 voor het digitaliseren van het toeslagen proces (uitwisseling met RDW/Berichtenbox). Inmiddels wordt de B2B gateway ingezet voor een aanzienlijk aantal koppelingen met een navenant aantal partijen. ebMS2 wordt ervaren als een vrij zwaar protocol, maar voor het doel (reliable messaging) goed en stabiel.

De Belastingdienst heeft een Proof of Concept uitgevoerd met het ebMS3/AS4 protocol. Dit bood voldoende vertrouwen om een bestaande koppeling om te zetten van WebDAV naar ebMS3/AS4.

De Belastingdienst zou graag een andere oplossing hebben voor uitwisseling van grote berichten in Digikoppeling. ebMS3 leek hiervoor beloftevol, want biedt ondersteuning voor de verwerking van grote berichten. De Belastingdienst geeft aan dat in de praktijk ebMS3/AS4 implementaties toch een 2Gb grens kennen, waarbij als oorzaak: de "Java security library" wordt genoemd.

Interoperabiliteit verdient speciale aandacht. Binnen ebMS2 kun je CPA gebruiken, maar de certificaten zitten hierin besloten, hetgeen leidt tot een verversingsprobleem. ebMS3/AS4 werkt met p-modes en kan een service metadata publishing (SMP) netwerk gebruiken om onderlinge afspraken hoe te communiceren uit te wisselen. Dit concept wordt door de Belastingdienst als plezierig ervaren.

In geval van een migratie is een goed uitgewerkt migratieplan en verwachtingsmanagement over de transitie/co-existentie essentieel, voor de Logius-Digikoppeling standaard zelf, maar ook voor de verschillende bestaande ebMS2 implementaties.

4.2 BKWI

Van origine is binnen Digikoppeling (Overheidsservicebus) voor ebMS2 gekozen als technologie voor meldingen. Voor de uitwisselingen in het SUWI-domein paste deze slecht en is dus nooit geïmplementeerd. De komst van WSRM - waar BKWI zelf aan heeft bijgedragen - was een zeer wenselijke ontwikkeling. BKWI is voorstander van een model waarin partijen binnen grenzen wat te kiezen hebben. Het verwijderen van WSRM heeft BKWI dan ook voor een probleem gesteld aangezien de ketenbrede standaard inmiddels op basis van WSRM was opgesteld en klaar stond voor implementatie.

Het ebMS2 protocol ziet BKWI als een te zwaar protocol met een te hoge implementatie- en beheerlast. Bovendien ziet BKWI dat er geen ontwikkelingen meer plaatsvinden op ebMS2.

BKWI ziet de ebMS2 standaard als “mogelijk verouderd” en “end-of-life”. Om die redenen kijken ze liever naar ebMS3/AS4, mede ook door de strategische keuzen die Europa maakt.

De Suwi-keten is voornamelijk gebaseerd op bevestigingen verkeer (>95%). Gezien het beperkte meldingen berichtenverkeer is een “zware” implementatie niet te rechtvaardigen. Het gaat om enkele tienduizenden berichten per jaar, er is momenteel geen Europees verkeer via de BKWI-systemen (wel elders in de Suwi-keten overigens).

BKWI volgt dan ook graag wat er met Digikoppeling gaat gebeuren, de BKWI-standaarden zijn daarop gebaseerd, omdat ze hergebruik belangrijk vinden. BKWI hoopt dat de keuze voor een standaard wordt gebaseerd op de meerwaarde en kwaliteiten die de standaard heeft en niet enkel op financiële consequenties van een eventuele migratie.

4.3 RINIS

RINIS wisselt per jaar zo'n 600 miljoen berichten via Digikoppeling uit voor haar deelnemers. Zij doet dit namens het UWV, de SVB, Stichting Inlichtingenbureau, Zorgverzekeraars Nederland, de Belastingdienst, het CAK, het CBS en het CIZ. Het gaat hier om uitwisselingen met het Register Niet-Ingezetenen (RNI) van de Rijksdienst voor Identiteitsgegevens (RvIG), de Stichting Netwerk Gerechtsdeurwaarders (SNG), MijnOverheid BerichtenBox, MijnOverheid Lopende Zaken, DigiPoort, het Landelijk Register van Zorgaanbieders (LRZa), de Koninklijke Notariële Beroepsorganisatie (KNB) en LV-WOZ van het Kadaster. En het gaat hierbij om alle standaarden binnen Digikoppeling, dus naast ebMS2 ook WUS en de Grote Berichten standaard.

Voor de huidige Digikoppeling/ebMS implementatie gebruikt RINIS de open source oplossing Jentrata, een afsplitsing van Hermes, dat door de Universiteit van Hong Kong is ontwikkeld.

In het algemeen is een ebMS2 implementatie vrij zwaar. Dat is niet uniek voor de Jentrata implementatie, maar heeft te maken met de opbouw van de ebMS2 standaard. Jentrata ondersteunt wel het digitaal ondertekenen van berichten maar ondersteunt niet het digitaal versleutelen van berichten. Ook dat is redelijk standaard voor ebMS2 implementaties. De reden hiervoor is dat de ebMS2 standaard niet specifiek genoeg is m.b.t. het digitaal versleutelen van berichten. Hierdoor zijn er weinig of geen ebMS2 implementaties die in staat zijn om onderling digitaal versleutelde berichten uit te wisselen.

RINIS heeft ervaring met ebMS3/AS4 door participatie in een aantal Europese projecten: eDelivery en European Exchange of Social Security Information (EESSI). RINIS heeft voor deze projecten gebruik gemaakt van de open source oplossing van Holodeck. In tegenstelling tot ebMS2 is ebMS3/AS4 over het algemeen een lichte implementatie. ebMS3/AS4 maakt namelijk gebruik van de WS-Security standaarden; een implementatie bouwt dus voort op frameworks die gebaseerd zijn op deze standaarden. Hierdoor is de eigenlijke implementatie lichter, zeker t.o.v. ebMS2.

De p-modes van ebMS3/AS4 zijn wel gestandaardiseerd wat betreft inhoud (wat staat er in een p-mode file) maar er zijn binnen ebMS3/AS4 geen afspraken gemaakt over het formaat

van de p-mode file (wat bijvoorbeeld zou kunnen d.m.v. een XSD). Hierdoor heeft iedere implementatie haar eigen p-mode file formaat en moet je bij een uitwisseling tussen twee verschillende implementaties van ebMS3/AS4 altijd de p-mode vertalen tussen beide implementaties.

Daarnaast is er wel de optie voor 'discovery' hiermee kan je vanuit je ebMS3/AS4 implementatie aan 'het netwerk' de specifieke p-mode gegevens van een instelling opvragen. Dit is als SMP/SML geïntroduceerd met het PEPPOL project en is inmiddels door OASIS gestandaardiseerd als BDXL (Business Document Metadata Service Location, <http://docs.oasis-open.org/bdxml/BDX-Location/v1.0/BDX-Location-v1.0.html>).

4.4 Justitiële Informatiedienst (JustID)

JustID heeft 10 jaar ervaring met elektronisch berichtenverkeer en Digikoppeling en met JuBes (=Justitiële Berichten Service) en eCodex (Europese Justitiële berichten, voornamelijk met Duitsland). Er is ook intersectoraal berichtenverkeer, onder andere met DUO, KVK, BRP, Nationaal Archief en RDW.

RINIS heeft een Proof of Concept gedaan inzake het gebruik van ebMS3/AS4, waarbij JustID als ketenpartner betrokken was. JustID is zijdelings betrokken bij eDelivery in een toehoorders/review rol. Er zijn op dit moment ongeveer 100 ketenpartners waarmee met ebMS2 wordt gecommuniceerd.

ebMS3/AS4 wordt door JustID gebruikt binnen eCodex (internationale justitiële berichten). De ebMS3/AS4 koppelingen gaan via software van Axway. Hierbij is gebruik gemaakt van de connector van Europa, Domibus (een branch van Holodeck), voor de integratie tussen Axway en de achterliggende systemen. Deze is echter behoorlijk aangepast om aan de voorwaarden van JustID te voldoen. Buiten Digikoppeling om zijn er uitwisselingen met banken en telecom.

Ten opzichte van ebMS2 wordt binnen ebMS3/AS4 het ontbreken van CPA/CPD (machine leesbare configuratie) als een gemis ervaren. Er is voor JustID op dit moment geen acute noodzaak om binnen Digikoppeling over te stappen op ebMS3/AS4. ebMS2 voor Digikoppeling en ebMS3/AS4 voor communicatie binnen eCodex draaien prima naast elkaar.

Er worden ongeveer 1,5 miljoen berichten per dag verstuurd. Berichten met een groot volume komen voor bij uitwisseling met het nationaal archief (ongeveer 350 Gb). Er worden twee (wat tegenstrijdige) trends gesignaleerd: a) Steeds grotere berichten, gedreven vanuit de behoefte om onder andere multimedia met elkaar uit te kunnen wisselen, en b) Een grotere nadruk op de kleinere realtime berichten, deels vanuit apps en deels vanuit een steeds meer realtime werkende overheidsorganisatie, waarbij just-in-time informatie steeds belangrijker wordt.

4.5 Conclusie

De meeste geïnterviewde grote partijen hebben al ervaring met ebMS3/AS4, in een pilot omgeving of in productie. Er is voor hen geen noodzaak te migreren naar ebMS3/AS4,

omdat ebMS2 ook prima naast ebMS3/AS4 kan draaien en ebMS2 prima voldoet waarvoor het is bedoeld: “reliable messaging”. Voor hen heeft een eventuele migratie natuurlijk impact, maar is technisch niet onoverkomelijk. BKWI heeft nog geen keuze gemaakt, maar heeft in verband met externe ontwikkelingen de voorkeur om ebMS3/AS4 te gaan gebruiken binnen Digikoppeling.

5. IST Situatie gemeenten

5.1 VNG Realisatie

Er zijn 46 buitengemeentelijke voorzieningen, een onbekend deel daarvan maakt gebruik van ebMS2. Met ebMS2 zijn er koppelingen met:

- Collectieve Opdracht Routeervoorziening (CORV), justitie
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Handelsregister (NHR)
- Omgevingsloket Online (OLO), omgevingsvergunningen
- MijnOverheid berichtenbox, lopende zaken en WOZ inzage
- ebMS2 koppelingen met Landelijke Voorziening WOZ (LV WOZ)
- Gemeentelijk Gegevensknooppunt (GGK)
- Basisregistratie Voertuigen (BRV)

In de Softwarecatalogus staan 42 pakketten van 27 leveranciers die ebMS2 ondersteunen.

Met betrekking tot een mogelijke migratie zijn voornamelijk kosten, continuïteit en functionele meerwaarde van belang: de vraag of de ebMS2 koppeling vanuit gemeenteperspectief beter wordt.

Daarnaast dienen tijdens de migratieperiode de spelregels uit 'Architectuurschets gegevensuitwisseling' te worden gevolgd: een aanbieder is verplicht meerdere transportvarianten aan te bieden, de afnemer heeft dan keuze. Bij voorkeur géén vertaalservice voor protocolconversie omdat bij WSRM het niet gelukt is de vertaalservice vanuit het perspectief van de afnemer transparant te houden.

Aangezien gemeenten geen ebMS2 services aanbieden aan ketenpartners, zijn ze volgend in een mogelijk migratietraject. De ontwikkeling binnen gemeenten gaan momenteel richting een API strategie (DSO), API kennisplatform (Geonovum, I&W, VNG Realisatie, BKWI, ...) en de Gemeentelijke beweging 'Samen organiseren' en de daarin te ontwikkelen Common ground.

Common Ground richt zich op de hervorming van de informatievoorziening van gemeenten op zowel technisch, organisatorisch als juridisch vlak. Een van de uitgangspunten van deze beweging is het ontwikkelen van kleine bouwstenen in doorlopende trajecten via een agile methodiek. Onderdeel van de Common ground is de NLX: door applicaties en databronnen (services) van elkaar te scheiden, kunnen applicaties data voortaan direct bij de bron raadplegen via een gemeenschappelijke servicelaag. Niet alleen gemeenten, maar ook andere overheden en particuliere organisaties kunnen de servicelaag van NLX gebruiken.

5.2 Gemeenten Purmerend, Oostzaan en Amsterdam

Purmerend en Oostzaan hebben ongeveer 15 communicatiepartners waarmee via Digikoppeling informatie wordt uitgewisseld, zoals de Landelijke voorziening WOZ. Dit

betekent dat er 15 configuraties moeten worden beheerd. Voor het initieel instellen of wijzigen van één configuratie wordt meestal een externe expert ingehuurd, die daar ongeveer 0,5 - 1 dag mee bezig is (externe kosten). Er is geen internationale gegevensuitwisseling. Voor een grote gemeente als Amsterdam is het aantal configuraties groter (minimaal 60), omdat deze koppelingen oorspronkelijk per stadsdeel zijn ontwikkeld.

Bij veel gemeenten wordt de implementatie van Centric hiervoor gebruikt. Centric koopt de ebMS2 oplossing in van Enable-U. Enable-U levert op basis van op de markt beschikbare pakketten een WUS / ebMS2 adapter. Enige tijd geleden zijn ze gebruik gaan maken van CA Layer 7, dat certificaatbeheer gemakkelijker zou moeten maken, omdat certificaten dan nog maar op één plaats staan. JNet, Yenlo en Enable-U hebben samen ongeveer 75% van de gemeentelijke ebMS2 markt in handen.

De aansluiting op Digimelding / Digilevering is momenteel in testfase in de gemeente Purmerend. Belangrijke communicatiepartner is het Gemeentelijk Gegevens Knooppunt (GGK). Via dit knooppunt communiceren gemeenten met andere gemeenten en zorgaanbieders.

Voor een mogelijke migratie van ebMS2 naar ebMS3/AS4 binnen Digikoppeling is een centrale regie en planning nodig, omdat anders alle gemeenten op het laatste moment over gaan. Er zijn dan geen externe experts genoeg om dat te begeleiden.

Als knelpunt en hoofdpijndossier wordt genoemd het certificaatonderhoud en CPA. Het kost al snel 2 uur tijd om een certificaat te vervangen, maar het testen kan meer tijd kosten. Daarnaast moet dit nu synchroon worden uitgevoerd tussen communicatiepartners. Doordat de geldigheid van certificaten van 3 naar 2 jaar gaat, neemt het aantal certificaatupdates ook nog eens toe.

5.3 Conclusie

Voor de gemeenten zal migratie naar ebMS3/AS4 een grote impact hebben. De meeste gemeenten moeten daar externe expertise voor inhuren. Momenteel is de grootste behoefte bij gemeenten een oplossing voor geautomatiseerd certificaat- en partnerbeheer.

6. IST Situatie samenwerkingsverbanden en Europa

6.1 Entso-g

ENTSO-g (European Network of Transmission System Operators for Gas) is de organisatie die coördineert hoe de Europese distributeurs, handelaars en netwerkbeheerders samenwerken om de gashandel en –distributie in goede banen te leiden. ENTSOG beheert de procedures die de verschillende partijen moeten volgen, alsmede de berichten die daarin worden uitgewisseld en de protocollen die daarvoor worden gebruikt.

ENTSO-g is de afgelopen jaren overgegaan tot het gebruik van het ebMS3/AS4 protocol. Daartoe is in werkgroepen het AS4 profiel opgesteld en verder gespecificeerd.

De partijen in het ENTSOG netwerk gebruiken nu ongeveer een jaar ebMS3/AS4 om berichten uit te wisselen. Zij gebruiken meer dan 12 verschillende software producten, waaronder open source producten. Dit is gebeurd zonder veel problemen. Leden van de AS4 OASIS werkgroep zijn betrokken geweest bij de ENTSOG ontwikkelingen. ENTSOG laat het uitwisselen van certificaten over aan de communicatiepartners. Die wisselen nieuwe certificaten uit middels het ebMS3/AS4 protocol. Het certificaat wordt simpelweg als payload in de ebMS3/AS4 envelop geplaatst en handmatig verwerkt.

6.2 EDSN

EDSN is een Nederlandse organisatie die het berichtenverkeer ondersteunt tussen Nederlandse gas- en elektriciteitsbedrijven. EDSN ontwikkelt en standaardiseert berichten en processen, maar exploiteert ook een netwerk waarin de berichten worden uitgewisseld.

EDSN is onlangs gestart met een project om het berichtenverkeer via het ebMS3/AS4 protocol af te wikkelen. Hierbij wordt gemikt op de elektriciteitsmarkt, maar ENTSOG dient als leidend voorbeeld. De eerste gesprekken hebben aangetoond dat het precies definiëren van de betekenis en inhoud van protocolelementen veel overleg vergt, zelfs als uitgegaan wordt van bestaande profielen (AS4, ENTSOG). Inmiddels heeft EDSN het te gebruiken profiel gedefinieerd.

EDSN beheert momenteel een hub/spoke netwerk voor berichtenverkeer in de Nederlandse energiesector. Partijen wisselen berichten uit met centrale EDSN applicaties; niet met elkaar. Voor encryptie wordt hierin gebruik gemaakt van door KPN uitgegeven certificaten.

6.3 Peppol

Peppol is een afsprakenstelsel voor de uitwisseling van berichten ten behoeve van elektronische inkoop. Peppol is ook de naam van de organisatie die het stelsel beheert. Het stelsel bevat protocollenspecificaties, een adresboek, certificaatbeheer en richtlijnen voor deelnemende organisaties. De ontwikkeling van Peppol is in een stroomversnelling geraakt na publicatie van een Europese richtlijn, die Europese aanbestedende diensten verplicht facturen elektronisch te kunnen ontvangen.

Peppol gebruikt momenteel het AS2 protocol. Onder druk van de Europese commissie, die eDelivery over zoveel mogelijk domeinen wil uitrollen, wordt nu in een paar jaar migratie naar ebMS3/AS4 voorbereid. De Peppol gemeenschap heeft wel een document opgesteld met voorwaarden waaraan voldaan moet worden wil men migreren.

In veel landen (waaronder Nederland) wordt het door Peppol voorgeschreven protocol gehanteerd voor het ontvangen van elektronische facturen. Peppol beheert een berichtenbibliotheek met voornamelijk UBL berichten (Peppol Business Interoperability Specifications), maar ook UN/CEFACT facturen worden ondersteund alsmede branche-specifieke berichten voor sub-communities. Overheidsorganisaties dienen het protocol zelf te ondersteunen of zij dienen een dienstverlener te contracteren die dat voor hen doet, via het zogenoemde '4-corner model'. Dit betekent in de praktijk dat alle (Nederlandse) overheidsorganisaties in ieder geval voor elektronisch factureren direct of indirect ebMS3/AS4 zullen moeten ondersteunen.

6.4 eDelivery

De Europese Commissie heeft in het kader van de Connecting Europe Facility (CEF) een eDelivery bouwblok gedefinieerd. Dit bouwblok is een profiel op ebMS3/AS4. Met het profiel is een grootschalige infrastructuur ontwikkeld voor eFactureren (Peppol) en zijn in het kader van e-Sens inmiddels een aantal pilots afgerond in eProcurement (in het bijzonder eTendering), eJustice en eHealth. e-Sens was een omvangrijk project om in pilots internationale communicatie tussen overheidsorganisaties te testen en te implementeren. In deze pilots heeft Nederland een actieve rol gespeeld. De pilots worden nu voortgezet als permanente infrastructuur.

Het BRIS (Business Registers Interconnection System) is sinds juni 2017 in gebruik en sindsdien wisselt de KvK gegevens uit met andere beheerders van Handelsregisters. Alle communicatie verloopt o.b.v. eDelivery via het Europees Centraal Platform beheerd door Digit. Alle aangesloten lidstaten maken hiervoor gebruik van Domibus, de voorbeeldimplementatie van de Europese Commissie van een ebMS3/AS4 access point.

Het wordt voor overheidsorganisaties steeds belangrijker om ook met buitenlandse diensten (vooral binnen de EU) gegevens uit te wisselen. Het is te verwachten dat de wijze waarop dit dient te gebeuren door de Europese Commissie wordt voorgeschreven. Daarbij zal in veel gevallen gebruik worden gemaakt van eDelivery.

6.5 Conclusie

Nieuwe toepassingen in Europa, en vooral tussen overheden in Europa, maken gebruik van ebMS3/AS4 en daarbinnen van het eDelivery profiel. Overheden in Nederland (ook gemeenten) zullen in toenemende mate ook met het buitenland moeten communiceren. ebMS3/AS4 wordt dan een protocol dat ze moeten ondersteunen.

7. Ontwikkeling en ondersteuning

7.1 Standaardisatie ontwikkelingen

AS1, AS2 en AS3 waren standaarden (RFC's) van het IETF. ebMS en AS4 zijn uitgebracht door OASIS. Hierbij zijn de principes van AS1/2/3 verwerkt in een profiel voor webservices om gestructureerde documenten uit te wisselen. AS4 is een profiel op ebMS3: een keuze hoe protocolelementen worden gebruikt voor “reliable messaging”.

Stabiliteit en toekomstvastheid van standaarden zijn van groot belang, maar ook het bestaan van een actieve gemeenschap die ondersteuning kan bieden, problemen kan oplossen en indien nodig de functionaliteit kan uitbreiden. Wij hebben bij OASIS getoetst in hoeverre dit geldt voor ebMS3/AS4.

ebMS2 is in feite uitontwikkeld. Er worden geen nieuwe functies meer aan toegevoegd. Fouten en bugs worden nog gecorrigeerd, maar die zijn momenteel niet gerapporteerd.

ebMS3/AS4 is een betrekkelijk jonge standaard (2007). De standaard is stabiel, maar kan nog op kleine punten worden aangepast, naar aanleiding van implementatie ervaringen.

7.2 Leveranciers

Leveranciers van producten die de standaarden (zowel ebMS2 als ebMS3/AS4) ondersteunen zijn middleware leveranciers met generieke B2B oplossingen (zoals Tibco, Software AG, Axway en Fujitsu). Deze producten zijn generiek en ondersteunen meerdere technische protocollen.

Daarnaast zijn er ook applicaties waarin deze standaarden zijn ingebouwd en stand-alone ebMS producten (soms open source, zoals Holodeck, Domibus en Jentrata) die aan applicaties kunnen worden gekoppeld.

Middleware is geïntegreerd in het applicatielandschap van organisaties en zorgt bij een juiste configuratie ook tussen de B2B gateway en de “back-end” applicatie voor “reliable messaging” (waarbij alle berichten precies één keer en in de juiste volgorde worden afgeleverd). Migratie kan daarom een grote impact hebben. Niet alleen moet het protocolprofiel opnieuw ingeregeld worden, vooral de integratie met de “back-end” systemen moet vaak opnieuw worden geconfigureerd. Het applicatielandschap stelt ook allerlei eisen aan de architectuur en technologie van de middleware.

7.3 Vragenlijst

In het kader van dit onderzoek is een vragenlijst opgesteld, die is gestuurd naar 46 leveranciers waarvan bekend is dat ze ebMS2 dan wel ebMS3 ondersteunende software leveren. Aan hen zijn de volgende vragen gesteld:

ebMS 2.0:

1. Levert u één of meer software producten of diensten die communicatie volgens ebMS 2.0 mogelijk maken (ebMS2 nu)?
2. Verwacht u de komende jaren een ebMS 2.0 gerelateerd product of dienst op de markt te brengen (ebMS2 later)?
3. Blijft u uw ebMS 2.0 product of dienst de komende vijf jaar ondersteunen (ebMS2 blijvend)?

ebMS3.0 / AS4:

4. Levert u één of meer software producten of diensten die communicatie volgens ebMS 3.0 / AS4 mogelijk maken (ebMS3 nu)?
5. Verwacht u de komende jaren een ebMS 3.0 / AS4 gerelateerd product of dienst op de markt te brengen (ebMS3 later)?
6. Blijft u uw ebMS 3.0 / AS4 product of dienst de komende vijf jaar ondersteunen (ebMS3 blijvend)?

Van de 46 leveranciers hebben 16 leveranciers de vragen beantwoord.

	Vraag 1. ebMS2 nu	Vraag 2. ebMS2 later	Vraag 3. ebMS2 blijvend	Vraag 4. ebMS3 nu	Vraag 5. ebMS3 later	Vraag 6. ebMS3 blijvend
Jnet	ja		ja	nee	ja	ja
Centric	ja		ja	nee	ja	ja
ECS International	ja		ja	ja		ja
Itrajectum	ja		ja	ja		ja
Ponton	ja		ja	ja (AS4)		ja (AS4)
Genetics	ja (via derden)		ja	ja (via derden)		ja
Mendelson	nee	nee	nee	ja		ja
Seeburger	ja		ja	ja		ja
Axway	ja		ja	ja		ja
Chasquis	nee	ja	ja	ja		ja
Enable-U	ja		ja	nee	ja	ja
Arpha	ja		ja	nee	ja	ja
eGem	ja		ja	nee	ja	ja
Yenlo	ja		ja	nee	ja	ja
RSSBUS	nee	nee	nee	ja		ja
Tibco	ja		ja	ja		ja

Geconcludeerd kan worden dat de leveranciers die ebMS2 ondersteunen dat zullen blijven doen. Zij bieden ook allen ebMS3/AS4 producten aan zodra de markt daarom vraagt.

7.4 Conclusie

ebMS2 zal blijvend worden ondersteund door leveranciers. Al deze leveranciers zullen ook ebMS3 ondersteunen wanneer daar vraag naar komt. De markt voor ebMS3/AS4 software is groter dan die voor ebMS2. Nieuwe standaardisatieontwikkelingen vinden plaats in ebMS3/AS4. Het aanbod van software die ebMS3/AS4 ondersteunt is groter dan de ondersteuning van ebMS2.

8. Proeftuin en kennisborging

8.1 Proeftuin

Tijdens het project is een proeftuin opgezet om de mogelijkheid te hebben bepaalde zaken die naar voren komen tijdens de interviews nader te kunnen analyseren. Er is gekozen om in de proeftuin gebruik te maken van een commercieel B2B product, Tibco Business Connect (BC), en een open source product, Holodeck. De keuze op deze producten is gevallen, omdat dit twee verschillende producten zijn die ook bij verschillende partijen worden gebruikt.

Tibco BC is een generieke B2B gateway, die naast ebMS ook allerlei andere uitwisselingsprotocollen ondersteunt. Tibco BC ondersteunt een volledige B2B functionaliteit, gemanaged middels meegeleverde portal waarbij volledig B2B management wordt geleverd (logging, partner management business agreements managent, audit reports etcetera). Door middel van een ebMS plugin wordt op de generieke B2B implementatie de specifieke functionaliteit voor ebMS2 en ebMS3/AS4 toegevoegd. Tibco BC ondersteunt ook een aparte TIBCO BC-Gateway voor een secure DMZ oplossing direct vanuit het product.

De berichten kunnen vanuit de Tibco BC via Tibco middleware met achterliggende (backoffice) applicaties worden uitgewisseld. Tibco middleware levert – mits goed geconfigureerd – een gegarandeerde doorgifte van berichten tussen de B2B gateway en de “back-end” applicatie, waarbij het interne proces (“private proces”) er voor zorg draagt dat de berichten gegarandeerd tot in de applicatie worden afgeleverd.

Van Tibco BC is een instantie geïnstalleerd en geconfigureerd. Daar Tibco BC “multitenancy” is (een instantie kan meerdere gebruikers bedienen), kunnen er met een enkele installatie ook berichten tussen twee geconfigureerde partijen worden uitgewisseld. De configuratieschermen van Tibco BC zijn bestudeerd, om te analyseren hoe de partnerprofielen zijn gestructureerd. Bijvoorbeeld, op welk niveau wordt een certificaat geconfigureerd.

De open source versie van Holodeck is een ebMS3/AS4 product, waarbij input en output berichten in een folder (directory) van het besturingssysteem worden geplaatst. De uitwisseling van de berichten met de achterliggende (backoffice) applicaties moet dan zelf geprogrammeerd worden. Bestand (file) gebaseerde oplossingen en oplossingen die afleveren middels de aanroep van een webservice van de “back-end” applicatie kennen geen “end-to-end” gegarandeerde aflevering. Bij Holodeck is de configuratie van de installatie een configuratiebestand, dat met de hand aangepast moet worden.

Van Holodeck zijn twee instanties geïnstalleerd en geconfigureerd in een test netwerk. Tussen de twee instanties zijn testberichten uitgewisseld. Configuratie gebeurt middels XML bestanden; er wordt dus geen applicatie met gebruikersinterface meegeleverd. Input en output geschiedt door middel van bestanden.

8.2 Bevindingen uit de proeftuin

Een volledige end-to-end opbouw van een keten waarin vanuit een applicatie via middleware en een ebMS exchange informatie wordt uitgewisseld kost redelijk wat tijd. Mede door onduidelijkheden in de configuratie (bijv. "waar zit een p-mode parameter in de configuratie van een generieke B2B gateway") is het zeer lastig om tussen verschillende producten die toch beide ebMS3/AS4 ondersteunen op relatief eenvoudige wijze een volledige implementatie in te richten.

De proeftuin geeft wel inzicht in het verschil tussen theorie en praktijk. Zo blijkt een product als Tibco BC in de laatste versie mogelijkheden te hebben om alvast certificaten klaar te zetten als vervanger voor de huidige certificaten. Hierdoor wordt het mogelijk om in te regelen dat vanaf een bepaalde datum nieuw certificaat wordt gebruikt.

Transversale principes in een B2B product die te maken hebben met protocol onafhankelijke inrichting staan soms tegenover een product dat enkel en alleen voor ebMS3/AS4 is ontworpen. Zo lijkt het moeilijk om nieuwe OASIS voorstellen één op één in een commercieel product als Tibco BC te implementeren.

De opensource variant van Holodeck die is bekeken, is geen kant en klaar eindproduct voor "reliable messaging" in de hele keten, want het implementeert alleen de ebMS3/AS4 communicatie met de externe partij en niet de communicatie van het "back-end" systeem met Holodeck. Je kunt het als een bruikbaar framework zien, dat als basis van een maatwerk implementatie voor ebMS3/AS4 kan dienen. Diverse "forks" van Holodeck hebben het daglicht gezien maar wel met versplintering van source code tot gevolg.

8.3 Kennisborging

De ebMS3 standaard en het AS4 profiel zijn veel omvattend. Mede omdat ebMS3 ook gebruik maakt van een aantal W3C standaarden, bijvoorbeeld voor security. Het gebruik van ebMS3/AS4 binnen Digikoppeling (het Digikoppeling profiel) zal toegelicht en uitgelegd moeten worden. Tijdens het technisch overleg Digikoppeling is gebleken dat naast papieren standaarden er behoefte is aan praktijkkennis en testfaciliteiten. Voor een goede borging van kennis en ervaring is het nodig de kennis op een gestructureerde manier vast te leggen die onafhankelijk is van een afdeling of een persoon.

Er zijn anno 2018 een paar populaire mechanismen voor kennisborging: Wiki's, E-learning en een online omgeving om te kunnen experimenteren. Een wiki op een centrale plek waar geregistreerde gebruikers kennis, kunde en informatie kunnen achterlaten over een bepaald onderwerp (in dit geval dan ebMS3/AS4). Eventueel aanvullend op en verwijzend naar de Wiki die door de EU is opgezet voor eDelivery:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery>.

Een andere manier zou zijn om een interactieve cursus over ebMS aan te bieden en hiervoor bijvoorbeeld e-learning modules te ontwikkelen. Daarbinnen zou je een practicum

kunnen opzetten, zodat een geïnteresseerde ook praktijkervaring kan opdoen. Zo ontstaat een e-learning omgeving, waarin de theorie en het gebruik van ebMS3/AS4 en de toepassing ervan binnen Digikoppeling wordt uitgelegd en kan worden getoetst met online opdrachten.

Aanbieden van kennis kan worden gescheiden tussen enerzijds theorie en standaarden en anderzijds praktijkvoorbeelden voor veelvoorkomende situaties. Het eerste deel zal meer zijn voor studenten en softwareleveranciers, terwijl het tweede deel meer gericht zal zijn op gebruikers binnen Digikoppeling. Dit zou kunnen bijdragen aan de adoptie van een standaard als ebMS3/AS4.

Tijdens de sessies met de Werkgroep Digikoppeling bleek dat er ook behoefte is aan een testomgeving om te experimenteren, waarbij het mogelijk is om vanaf buiten een bepaald berichtenprotocol met de testomgeving uit te wisselen. Dit zou eventueel als uitbreiding van de e-Learning omgeving kunnen worden geïmplementeerd. Uiteraard kost een “Live Test” omgeving resources, licenties en onderhoud. Bij voldoende schaalgrote zou dat een waardevolle toevoeging kunnen zijn en een manier om adoptie te versnellen.

Om bovenstaande faciliteiten te creëren en te beheren, alsmede te helpen bij de migratieprojecten zou een centraal “center of expertise” kunnen worden opgezet, dat als centraal kennispunt van ebMS3/AS4 fungeert. Hiervoor dient voldoende budget gealloceerd te worden, zodat deze organisatie minimaal vijf jaar kan functioneren.

8.4 Conclusie

Open source producten zijn veelal halffabricaten die in een zelfbouw oplossing voor “end-to-end guaranteed delivery” geprogrammeerd dienen te worden. De open source producten hebben meestal geen grafische user interface (GUI) voor configuratiemanagement. Het maken van een complete oplossing op basis van open source brengt derhalve extra complexiteit, risico's en indirecte kosten met zich mee. Voor open source software is vaak wel support beschikbaar via commerciële partijen.

Commerciële oplossingen bieden daarentegen een totaaloplossing zonder programmeerwerk en met support, maar kunnen hoge licentiekosten met zich meebrengen. Daarnaast heeft men dan expertise nodig van deze producten.

Binnen de proeftuin is gebleken dat de inrichting van een ebMS3/AS4 implementatie tussen twee verschillende producten complex is. Vooral kleine partijen (gemeenten) zullen daarbij geholpen moeten worden. Een online omgeving waarin naast papieren standaarden praktijkkennis kan worden uitgewisseld en waarin getest kan worden kan daarbij van groot belang zijn. Om dit serieus aan te pakken zou een “center of expertise” moeten worden opgezet, die de centrale faciliteiten beheert en participeert in migratieprojecten. Hiervoor dient voldoende budget gealloceerd te worden, zodat deze organisatie minimaal vijf jaar kan functioneren.

9. Beheer van een ebMS configuratie

9.1 Problematiek rondom de configuratie ebMS3/AS4

Vanuit de praktijk gezien is een B2B systeem een systeem dat voor meerdere protocollen en berichtbibliotheken geschikt is. Bijvoorbeeld voor UBL, Rosettanet, ebMS 2.0, ebMS3/AS4, SOAP, en vele andere protocollen. Het begrip protocol is hierbij ook diffuus, omdat het de ene keer om een zuiver transport protocol gaat (bijvoorbeeld SOAP) en de andere keer om een interactiepatroon van XML over HTTP. Vanuit gangbare B2B pakketten - zoals Tibco BusinessConnect of Software AG Integration Server Trading Networks - wordt de registratie van een participant (trading partner of host) en het vastleggen van een Business Agreement (een bepaald berichtuitwisselingscontract tussen twee trading partners) ontkoppeld van het gekozen protocol.

Kijken we vervolgens naar de p-mode parameters voor een ebMS3/AS4 uitwisseling, dan worden bij een B2B implementatie sommige parameters op het niveau van ebMS3 (het protocol) opgeslagen, terwijl andere parameters op een hoger en daarmee een meer generiek (protocol onafhankelijk) niveau worden vastgelegd.

Producten als Holodeck zijn louter en alleen gericht op op een beperkt aantal protocollen (waaronder ebMS3/AS4) en zijn daarmee minder generiek van opzet. Qua configuratie volgen ze de OASIS gedefinieerde P-Mode parameters waar mogelijk. Zo heeft Holodeck een XML Schema gedefinieerd voor het standaardiseren van de p-mode parameters in een XML bestand (pmode.xsd). Dat lijkt enerzijds de configuratie te vereenvoudigen, maar maakt het tegelijk complex als 2 partijen een verbinding dienen op te zetten. Neem Tibco BC en Holodeck als voorbeeld, dan is het een waar puzzelwerk om te zien hoe een configuratie aan de ene kant zich verhoudt met een configuratie aan de andere kant. Een meer logische opgebouwde configuratie enerzijds (Tibco) zonder een referentie naar een p-mode parameter, en anderzijds een meer technisch opgebouwde configuratie, met het letterlijk volgen van de p-mode parameters (Holodeck) zorgt ervoor dat er zelfs binnen de proeftuin niet genoeg tijd was om een soort configuratie mapping, op een eenvoudige manier uit te voeren.

Er zijn immers veel scenario's mogelijk met ebMS3/AS4 die allemaal geconfigureerd moeten kunnen worden. Als de ene zijde een one-way-push configureert (de verzendende partij), wat moet dan de andere partij (de ontvangende MSH) exact configureren? De vrijheidsgraden in de scenario's en de vele instelmogelijkheden aan beide kanten, maakt het zeer moeilijk een werkende configuratie met twee verschillende producten te realiseren. Het zou enorm helpen om goed uitgewerkte voorbeelden van de in Digikoppeling gebruikte scenario's beschikbaar te hebben, waarbij die voorbeelden voor veel gebruikte producten (commercieel en open source) ter beschikking gesteld kunnen worden (vanuit Logius of een ander gremium).

9.2 Standaarden voor certificaat uitwisseling

Gedurende het onderzoek is er met name de pijn van deelnemers blootgelegd met betrekking tot het probleem dat certificaten verlopen en derhalve vernieuwd moeten worden. Het inregelen van deze certificaten doet deelnemende partijen die werken met ebMS3/AS4 (en ook ebMS2) pijn, er is externe expertise nodig en door het random over de tijd verdeeld verlopen van de certificaten, ook moeilijk planbaar. Mede om dit certificaten probleem op te lossen zijn er vanuit de community enkele suggesties gedaan om het certificaten probleem te op te lossen. Drie standaarden zijn genoemd en worden hieronder kort besproken en gewogen. Het is van belang te realiseren dat certificaat- en configuratie-updates niet specifiek zijn voor ebMS3/AS4, maar bij elke transportprotocol een issue zijn.

9.3 ebCore Agreement Update Protocol

Deze standaard is bekeken en getoetst op toepasbaarheid. Uitgangspunt van deze standaard is dat deelnemende partijen hun certificaten en ook hun meta data (namen, contactpersonen e.d.) tussen participanten (handelspartijen) onderling automatisch zouden kunnen updaten. Ook een “agreement termination” kan verstuurd worden.

Er is getoetst hoe bruikbaar een dergelijke standaard is. Is er de verwachting dat commerciële partijen zoals Software AG, Tibco en Axway deze standaard default gaan implementeren? Wij verwachten van niet. Geen van de geïnterviewde software leveranciers heeft de standaard op dit moment geïmplementeerd. De oorzaak hiervoor is mogelijk dat de voorgestelde standaard nog veel te veel vrijheidsgraden kent (alleen “certificate update” en “agreement termination” zijn beschreven. De standaard bevat geen metagegevens voor het wijzigen van een complete “agreement”, eventueel aangevuld met een protocolspecifieke metagegevens. Voor het wijzigen van bijvoorbeeld contactgegevens zou je zelf de betreffende gegevens moeten modelleren in een XML Schema en als maatwerk laten implementeren door de softwareleverancier.

9.4 SMP/SML

Service Metadata Locator (SML) en Service Metadata Publisher (SMP) is een protocol onafhankelijke standaard. Het is door Peppol ingezet in combinatie met het AS2 protocol. SMP beschrijft welke documenten partijen kunnen ontvangen op endpoints, en bij een endpoint kun je met een identifier aangeven, welk transport protocol dat endpoint ondersteunt. Daarbij kunnen ook opties worden aangegeven.

SMP/SML worden reeds toegepast in specifieke toepassingen zoals Peppol (op AS2) en eDelivery (op AS4). Commerciële partijen leveren B2B oplossingen die veel meer protocollen ondersteunen. De vraag is of deze oplossing generiek genoeg is om deze commerciële partijen te verleiden om deze standaard in hun softwareproducten te implementeren.

9.5 ebXML Collaboration Protocol Profile and Agreement (CPPA) versie 3

Versie 2.0 van CPPA ondersteunt ebMS 2.0 sinds 2004. OASIS ontwikkelt momenteel versie 3 van deze standaard, die ook ebMS3 ondersteunt. Deze standaard definieert een Collaboration Protocol Profile (CPP) en een Collaboration Protocol Agreement (CPA). Het CPP definieert de functionele (business) en technische mogelijkheden van een communicatiepartner in de vorm van een XML-document. Het CPA definieert een uitwisselingsovereenkomst in de vorm van een XML-document. Dit XML-document kan worden gebruikt om B2B messaging systemen te configureren en daarbij de afgesproken instellingen te gebruiken. Het ebCore Technical Committee (ebXML Core) onderhoudt de CPPA-specificatie, die momenteel de status "Draft" heeft.

9.6 Alternatieve oplossing

Kijken we naar het certificaten update probleem en de voorstellen om die middels een nieuwe uitwisselingsstandaard op te lossen, dan zijn er ook andere oplossingen denkbaar, die organisatorisch van aard zijn en die goed kunnen werken.

In sommige sectoren worden de certificaten jaarlijks op een vast tijdstip voor de hele markt en alle marktpartijen ge-update. Dat levert een overzichtelijk probleem op, dat is in te plannen. Vaak zijn tools aangeschaft dan wel ontwikkeld om ineens alle certificaten voor alle handelspartners te updaten. Nu werken veel partijen met PKI-overheid certificaten, die standaard 2 of 3 jaar geldig zijn vanaf moment van aanvraag. Als het mogelijk zou zijn om bijvoorbeeld e-Herkenning certificaten met een vaste einddatum aan te vragen (stel 31 jan) dan zou bijvoorbeeld elke 2 jaar 1 zipfile met alle publieke certificaten gedistribueerd kunnen worden en is er jaarlijks of tweejaarlijks een gepland onderhoudsmoment mogelijk.

9.7 Conclusie

Er zijn verschillende opties voor het geautomatiseerd beheren van certificaten en partners. Geen van deze opties kan echter panklaar ingezet worden voor Digikoppeling. Dit onderwerp moet verder worden uitgediept voor een migratie naar ebMS3 binnen Digikoppeling wordt overwogen.

10. Alternatieven voor ebMS3/AS4

Veel organisaties hebben vaak nog maar 3 typen van interactie met de buitenwereld:

- 1) Via een generiek B2B portal, die ook ebMS2 en ebMS3 kan ondersteunen
- 2) Via een Webservice/API Gateway
- 3) Via een Managed File Transport (MFT) framework.

Optie 1 betreft een oplossing waarbij ebMS2 en/of ebMS3 als communicatieprotocol kan worden gebruikt. De vraag is nu of optie 2 en/of 3 wellicht alternatieven zijn voor ebMS3 als opvolger van ebMS2 binnen Digikoppeling.

API's zijn op dit moment zeer populair en veel organisaties ontwikkelen momenteel een API-strategie. API's worden gekenmerkt door een service contract en http(s) als transport. Dit kan met SOAP over https worden gerealiseerd met WSDL als service contract. Maar het kan ook op REST en JSON gebaseerd worden met WADL, Swagger/OpenAPI of RAML als service contract.

Echter, de vraag of API's een volwaardige vervanger van ebMS3/AS4 (of ebMS2) zouden kunnen zijn, moet met nee worden beantwoord. API's bieden geen goede mogelijkheden voor "attachments", geen goede identificatie van de tegenpartij, etc. Het is een synchroon, "non-transactional request-response" patroon dat geen "guaranteed delivery" levert en dat niet primair ontworpen is voor transport van "attachments".

MFT is veelal een transactie monitor en gateway voor het verplaatsen van files, waarbij ook sprake is van "guaranteed delivery". Vaak ligt daar FTPS of SFTP aan ten grondslag, soms gecombineerd met job control management. Diverse leveranciers van MFT-producten zouden een volwaardig alternatief kunnen bieden voor ebMS3/AS4. Veel functies zijn niet gestandaardiseerd en moeten bilateraal worden afgesproken, of binnen Digikoppeling worden gestandaardiseerd.

Conclusie

Van alle alternatieven lijkt ebMS3/AS4 het meest geschikt voor berichtuitwisseling binnen Digikoppeling. API's zijn geen alternatief voor ebMS3/AS4. Mocht men toch een alternatief willen overwegen, dan kan men Managed File Transfer (MFT) nader onderzoeken. Dit laatste kost extra standaardisatie inspanning.

11.Migratie

Het migreren naar een nieuwe standaard voor berichtuitwisseling heeft een enorme impact. Alle ketenpartners moeten zo goed als gelijk overschakelen of twee protocollen ondersteunen, tenzij conversiediensten kunnen worden aangeboden. Conversiediensten brengen verlies aan functionaliteit, risico's, kosten en vertraging in de uitwisseling. Het is belangrijk om voorafgaand aan de invoering van een nieuw protocol binnen Digikoppeling conversie- en migratieproblematiek in kaart te brengen en een migratieplan op te stellen. Het maken van een volledig migratieplan valt buiten de scope van deze opdracht.

Er zijn verschillende migratie strategieën mogelijk:

- "Big-bang": alle partijen stappen tegelijkertijd over
- Vrijwillig: partijen krijgen gedurende lange tijd de vrije keuze welk(e) protocol(len) ze ondersteunen
- Geregisseerd: Centraal wordt bepaald welke partijen wanneer migreren.

Peppol hanteert bijvoorbeeld een strategie waarin het nieuwe protocol een periode optioneel is voor deelnemers, gevolgd door een periode waarin het oude protocol optioneel is (en het nieuwe verplicht) waarna het oude protocol wordt uitgefaseerd.

De Digikoppeling gemeenschap bestaat uit enkele grote partijen (Kadaster, I&W-OLO, RDW, Dictu, Belastingdienst, Justid) en een groot aantal kleinere partijen (met name gemeenten). Bij migratie van ebMS2 naar ebMS3/AS4 is het verstandig de grote partijen het voortouw te laten nemen en enige tijd (bijvoorbeeld een jaar) beide protocollen te laten ondersteunen. Tegelijkertijd zal dan de migratie van de kleinere partijen geregisseerd moeten worden. Hun migratie dient gespreid te worden over de periode. De voornaamste reden is dat voor migratie per partij schaarse kennis moet worden ingehuurd. Spreiding stelt zeker dat deze beschikbaar is.

Aangezien er geen sterke urgentie is om binnen Digikoppeling over te stappen op ebMS3/AS4, kan de migratie goed worden voorbereid en kan er voldoende tijd voor uitgetrokken worden (3 tot 5 jaar). Migratie zal (hoge) kosten met zich meebrengen: software moet worden aangepast en geconfigureerd en alle partnerprofielen moeten worden gewijzigd. Echter, over een periode van enkele jaren houdt iedere organisatie er rekening mee dat software moet worden vernieuwd. Een lange migratieperiode maakt dat de vernieuwing in de budgetten kan worden verwerkt.

Vooraf kleine partijen (met name de gemeenten) moeten begeleid worden, om te voorkomen dat er disrupties ontstaan in de diensten die van uitwisseling gebruik maken. Een gedetailleerd draaiboek is daarbij onmisbaar. Het is verstandig dit draaiboek af te stemmen met de belangrijkste softwareleveranciers en dienstverleners.

Conclusie

Een migratie naar ebMS3/AS4 moet (en kan) zorgvuldig worden voorbereid en zal strak moeten worden geregisseerd. Grote partijen zullen eerst ebMS3/AS4 moeten implementeren. Zij zullen een periode beide protocollen moeten ondersteunen, zodat de kleinere partijen geleidelijk in groepen kunnen migreren.

De migratie van de kleinere partijen moet worden gecoördineerd om de benodigde ondersteuning te spreiden. Pas wanneer alle kleine partijen zijn overgeschakeld kunnen de grote partijen hun ebMS2 verbinding uitschakelen. De hele migratie zal moeten worden begeleid en goed worden voorbereid, vooral wat betreft documentatie. Lessons learned bij de vroege migranten moeten worden gedocumenteerd zodat ze kunnen worden gebruikt bij latere migraties.

12. Conclusie en aanbevelingen

12.1 Conclusies

- 1) Er zijn nauwelijks functionele verschillen tussen ebMS2 en ebMS3/AS4. In ieder geval is er functioneel geen aanleiding op korte termijn te migreren.
- 2) Als securityrichtlijnen verder worden aangescherpt en in de uitwisseling de berichten versleuteld moeten worden, is dat in een omgeving waarbij verschillende producten worden gebruikt met ebMS3 makkelijker te realiseren.
- 3) Voor grotere overheidsorganisaties (Justid, RINIS, BD) brengt migratie kosten met zich mee, maar technisch is er voldoende kennis (de meeste gebruiken al ebMS3 buiten Digikoppeling).
- 4) BKWI staat voor de keuze wat te implementeren en is gebaat bij duidelijkheid op korte termijn.
- 5) Voor de gemeenten is migratie een groot project met hoge kosten, dat goed moet worden voorbereid en ondersteund. Hierbij is centrale sturing nodig.
- 6) ebMS2 is stabiel, het blijft een OASIS standaard. Bugs worden opgelost.
- 7) De definitie van een Digikoppeling profiel op het AS4 profiel kan veel overleg vergen.
- 8) ebMS3 wordt nog verder ontwikkeld (bijv. CPP/A); nieuwe functionaliteit wordt ondergebracht in ebMS3
- 9) Europa zet in op ebMS3/AS4 en overheidscommunicatie over de grens neemt toe.
- 10) Peppol migreert 'onwillig' van AS2 naar ebMS3, en daarmee zullen alle overheidsorganisaties ebMS3/AS4 moeten ondersteunen (e-Invoicing), al dan niet via een dienstverlener.
- 11) Leveranciers blijven ebMS2 ondersteunen.
- 12) De meeste ebMS2 leveranciers zullen ook ebMS3 gaan ondersteunen.
- 13) Belangrijkste aandachtspunt is het beheer van partners en certificaten, dit geldt zowel bij ebMS2 als bij ebMS3/AS4. Het updaten van certificaten is het belangrijkste knelpunt bij huidige gebruikers van ebMS2 binnen Digikoppeling.
- 14) Er worden verschillende opties genoemd om het beheer te automatiseren (bijv. 2016: ebCore Agreement Update). Deze oplossingen zijn nog niet geïmplementeerd in zowel standalone oplossingen als in generieke B2B gateways van middleware leveranciers. Bij commerciële COTS B2B producten is beheer van een ebMS configuratie een onderdeel van de B2B portal configuratie. Voorgestelde oplossingen om het beheer van ebMS te automatiseren, zoals ebCore Agreement Update en SMP/SML zijn te veel gericht op ebMS en gaan daarmee voorbij aan het generieke karakter van B2B oplossingen.
- 15) API's zijn geen alternatief voor transactieberichten via ebMS in Digikoppeling. Als men een alternatief voor ebMS wil overwegen voor opname in Digikoppeling als opvolger van ebMS2 zou men Managed File Transport (MFT) moeten overwegen.
- 16) Er zijn verschillende opties voor het geautomatiseerd beheren van certificaten en partners. Geen van deze opties kan echter panklaar ingezet worden voor Digikoppeling.

Dit onderwerp moet verder worden uitgediept voor een migratie naar ebMS3 binnen Digikoppeling wordt overwogen.

- 17) Open source producten zijn veelal halffabricaten die in een zelfbouw oplossing voor “end-to-end guaranteed delivery” geprogrammeerd dienen te worden. De open source producten hebben meestal geen grafische user interface (GUI) voor configuratiemanagement. Het maken van een complete oplossing op basis van open source brengt derhalve extra complexiteit, risico's en indirecte kosten met zich mee.
- 18) Commerciële oplossingen (COTS) bieden daarentegen een totaaloplossing zonder programmeerwerk en met support, maar kunnen hoge licentiekosten met zich meebrengen. Daarnaast heeft men dan expertise nodig van deze producten.

12.2 Beantwoording van de onderzoeksvragen

Is ebMS3/AS4 een geschikte opvolger voor de huidige ebMS2-versie binnen de Digikoppeling standaard?

Ja. Vooral vanwege de brede adoptie in grensoverschrijdend berichtenverkeer is ebMS3/AS4 de logische en geschikte opvolger van ebMS2.

Heeft ebMS3/AS4 voldoende ondersteuning van de softwareleveranciers, met name de huidige Digikoppeling leveranciers?

Ja. Het aanbod van software die ebMS3/AS4 ondersteunt is groter dan de ondersteuning van ebMS2. Verreweg de meeste aanbieders van ebMS2 gaan ook ebMS3/AS4 ondersteunen zodra daar vraag naar is.

Heeft ebMS3/AS4 voldoende functionele dekking?

Ja. De functionele dekking van ebMS3/AS4 is hetzelfde als van ebMS2. Er zijn wel enkele verschillen in de wijze waarop de functionaliteit is geïmplementeerd.

Heeft ebMS3/AS4 Minimaal zelfde functionele dekking als ebMS2, zoals reliable messaging?

Ja.

Wat is de impact van het gebruik van p-modes (p-modes vervangen het CPA van ebMS2)?

De wijze van werken van p-modes is verschillend dan die van CPP/CPA. In het algemeen zal partnermanagement bij migratie naar ebMS3/AS4 anders moeten worden gedefinieerd. Partnermanagement en certificaatbeheer vormt nu het grootste knelpunt voor de toepassing van Digikoppeling.

Biedt ebMS3/AS4 aansluiting op de Europese standaard, eDelivery?

Het feit dat eDelivery gebruik maakt van ebMS3/AS4 is mogelijk de voornaamste motivator voor migratie. Omdat communicatie over de grens steeds belangrijker wordt zullen alle overheidsorganisaties op termijn alleen daarvoor al ebMS3/AS4 moeten implementeren.

Is ebMS3/AS4 volwassen?

Ja. ebMS3/AS4 wordt al op grote schaal toegepast. Het protocol wordt nog wel verder ontwikkeld.

Hoe staat het met interoperabiliteit?

De bestaande implementaties bewijzen dat ebMS3/AS4 interoperabel is. De Europese Commissie biedt test- en certificatiediensten voor ebMS3/AS4 interoperabiliteit. Juist bij encryptie van berichten zullen implementaties beter interoperabel zijn dan bij ebMS2.

Is er voldoende draagvlak binnen de Nederlandse overheid voor het invoeren van ebMS3/AS4?

De meeste grotere organisaties hebben al ervaring met ebMS3/AS4 en zijn bereid op termijn te migreren. De kleine organisaties (gemeenten) zijn nog niet overtuigd van de noodzaak.

Is er voldoende draagvlak voor het uitschakelen van ebMS2?

Kleine overheidsorganisaties willen slechts één protocol ondersteunen. Zodra ebMS3/AS4 wordt ingevoerd zullen zij ebMS2 willen uitschakelen.

Wat is de roadmap van leveranciers m.b.t. het AS4 profiel?

Vooraf vanwege uitrol in Europa is het AS4 profiel de de-facto standaard. Alle leveranciers ondersteunen dit profiel of zeggen dit te gaan doen.

Hoe kan ebMS3/AS4 worden uitgerold en hoe kan het gebruik van ebMS2 worden afgebouwd?

Zie het hoofdstuk Migratie

Hoe moet het lifecycle management worden aangepakt?

Voorafgaand aan de ingebruikname van ebMS3/AS4 binnen Digikoppeling dient een oplossing voor geautomatiseerde certificaat- en overige configuratie updates te worden ontwikkeld. Vervolgens kan de standaard stabiel binnen Digikoppeling minimaal 5 jaar worden gebruikt.

12.3 Aanbevelingen

- Neem op korte termijn de beslissing om ebMS3/AS4 als opvolger van ebMS2 binnen Digikoppeling op te nemen. Invoering zelf heeft geen haast, maar deelnemende partijen weten graag waar ze aan toe zijn. Vooral BKWI wil graag voorsorteren op de juiste route.
- Maak een migratieplan (roadmap), waarin in ieder geval voldoende tijd is ingeruimd om een Digikoppeling conformance profiel voor ebMS3 en een oplossing voor configuratie updates te ontwikkelen. Bij voorkeur is dit profiel een subset van het eDelivery profiel, dat binnen Europa al is ontwikkeld. Idealiter kan een implementatie voor Digikoppeling dan ook gebruikt worden voor communicatie over de grens.

- Overweeg of er subprofielen van AS4 binnen Digikoppeling moeten worden uitgesloten van implementatie (bijvoorbeeld het Light Client profiel en/of het Minimal Client profiel).
- Doe onderzoek naar het uitwisselen van protocol onafhankelijke B2B configuraties met als doel ook ebMS configuraties uit te kunnen wisselen en softwareleveranciers mee te krijgen deze generieke oplossing in hun B2B producten te implementeren. Vind zo een (geautomatiseerde) oplossing voor certificaatvernieuwing en partnermanagement (ook binnen ebMS2). Neem leveranciers van B2B softwareproducten hierin mee, zodat deze oplossing ook gegarandeerd daarin geïmplementeerd wordt.
- Zet een center of expertise op, die als centraal kennispunt van ebMS3 fungeert, inclusief de migraties. Zorg dat er voldoende budget is om dit center minimaal 5 jaar in de lucht te houden. Dit is een investering in de digitale infrastructuur van Nederland.
- Als het Digikoppeling profiel gereed is, moet er geruime tijd (3 tot 5 jaar) zijn om het stap voor stap te gaan implementeren. Stel daartoe een gedetailleerd migratiedraaiboek samen voor kleine partijen (gemeenten). Centrale planning van de migratie (grote partijen eerst, kleine partijen in fasen) is van groot belang, vooral om de ondersteuning door leveranciers te spreiden.