notitie

# FORUM STANDAARDISATIE 16 december 2014
# Agendapunt 5. Open standaarden, lijsten
# Stuknummer 5. Oplegnotitie lijsten

| | |
|---|---|
| **Bijlagen:** | A. Intakeadvies DMARC<br>B. Intakeadvies SKOS<br>C. Intakeadvies Digikoppeling<br>D. Intakeadvies OSI-licenties<br>E. Vooronderzoek nieuwe versie ISO27001/2 en baselines |
| **Aan:** | Forum Standaardisatie |
| **Van:** | Stuurgroep open standaarden |

*U wordt gevraagd **in de stemmen** met de volgende intakeadviezen:*

1. Uitvoeren van een experttoets op **DMARC**, een standaard voor e-mailbeveiliging.
2. Uitvoeren van een experttoets op **SKOS**, standaard voor het delen en linken van thesauri en begrippenwoordenboeken.
3. Uitvoeren van een experttoets op de nieuwe versie van **Digikoppeling** (een standaard voor berichtenuitwisseling) en de aanvraag voor uitstekend beheerproces.
4. Het niet in behandeling nemen van de **OSI-licenties** (licenties voor open source software), maar wel in te stemmen met de aanbeveling om referentie-implementaties in de toetsingsprocedure mee te nemen.
5. Het opnemen van referentie-implementaties, in de criteria voor toekomstige toetsingsprocedure
6. Het in procedure nemen van de nieuwe versie van **NEN-ISO/IEC 27001 en 27002** (standaard voor informatiebeveiliging) en het advies over de relatie tussen deze standaarden en de Baselines informatiebeveiliging op de 'pas toe of leg uit'-lijst.

*U wordt gevraagd **kennis te nemen** van:*

7. **Samenhangonderzoeken** in relatie tot dossier lijsten en adoptie
8. Toetsen **SEPA, ePortfolio, Semantisch model e-factureren** en **SETU**.

Datum
03-04-2014

**Intakeadviezen algemeen**
Na de aanmelding van een standaard houdt BFS een intakegesprek met de aanmelder. Tijdens dit gesprek wordt als eerst bepaald of de standaard binnen de scope van de lijsten valt. Aanvullend wordt besproken hoe kansrijk de toetsing van de standaard is. Hiervoor wordt bekeken hoe de standaard, volgens de aanmelder, scoort op de inhoudelijke toetsingscriteria. Op basis van de intake wordt een intakeadvies opgesteld, dat eerst met de stuurgroep Open Standaarden wordt besproken en vervolgens aan het Forum wordt voorgelegd[1].

# Ter besluitvorming

### Ad 1. Uitvoeren van een experttoets op DMARC, een standaard voor e-mailbeveiliging

Het Forum Standaardisatie wordt geadviseerd om DMARC, een standaard voor de verificatie van de authenticiteit van e-mailberichten, in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst.

**Over de standaard**
DMARC is een open standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het eigen domein. Hierdoor wordt het inzichtelijk als anderen e-mails versturen namens het e-maildomein van de organisatie. Hierbij kan gedacht worden aan phishing e-mail en spam. Het gebruik van DMARC kan ingezet worden voor het verminderen en/of voorkomen van misbruik van een domeinnaam middels e-mail. Ook kan door het gebruik van de standaard worden voorkomen dat e-mailmailingen door e-mailproviders onterecht voor spam worden aangezien. Doormiddel van DMARC kunnen organisaties aangeven wat er met een ongeauthenticeerd e-mailbericht moet gebeuren (blokkeren of toch verzenden naar een ontvanger). Verder kan een organisatie aangeven op welke manier de organisatie hierover gerapporteerd wil worden.

DMARC kan gezien worden als een aanvulling op de al opgenomen DKIM-standaard. DMARC maakt gebruik van DKIM. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. DMARC gebruikt het DKIM-mechanisme om de authenticiteit van een e-mail te verifiëren. Zodra deze verificatie niet mogelijk is wordt het DMARC-beleid in werking gezet.

**Proces**
Er heeft een intakegesprek plaatsgevonden en de standaard voldoet aan de criteria voor inbehandelname. Mede door de toepasbaarheid van de standaard en de relatie tot de al op de lijst opgenomen standaard DKIM (DomainKeys Identified Mail) is de kansrijkheid van de procedure voldoende. De standaard is ingediend door Measuremail en wordt naar verwachting ondersteund door de Dienst Publiek en Communicatie (onderdeel van het ministerie van Algemene Zaken), de gemeente Den Bosch en de gemeente Heerlen. Deze organisaties maken gebruik van de standaard en hebben hier beleid op ontwikkeld.

**Aandachtspunten**
Geadviseerd wordt om tijdens de expertsessie stil te staan bij een goede definiëring van het functioneel toepassingsgebied. De standaard zou in ieder geval verplicht

[1] *Zie voor meer informatie m.b.t. de procedure:*
*https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0903/toetsingsprocedure-en-criteria.pdf*

gesteld moeten worden voor alle domeinnamen (van partijen in het organisatorisch werkingsgebied) die burgers en bedrijven vertrouwen als zij daar e-mail van zouden ontvangen (uitgaande mail). Het is de vraag of het functioneel toepassingsgebied ook gericht moet zijn op het toepassen van DMARC op alle inkomende e-mail.

**Ad 2. Uitvoeren van een experttoets op SKOS, standaard voor het delen en linken van thesauri en begrippenwoordenboeken**

Het Forum Standaardisatie wordt geadviseerd om SKOS, een standaard voor het online delen en linken van systemen voor kennisrepresentaties via het internet (zoals thesauri, begrippenwoordenboeken en classificatielijsten), in procedure te nemen voor op de 'pas toe of leg uit'-lijst.

**Over de standaard**
Het publiceren van thesauri en taxonomieën door overheidsorganisaties gebeurt vaak in een vorm van documenten die niet bruikbaar zijn voor computerprogramma's. Daarnaast worden aan de begrippen die in thesauri en taxonomieën zijn opgenomen verschillende classificaties toegekend. Een goed voorbeeld hiervan is de SBI-lijst, een classificatielijst van economische activiteiten, die door de Kamer van Koophandel in de vorm van een downloadbaar document met een 'platte tabel' wordt gepubliceerd. Wanneer een andere organisatie met de SBI-codes wil werken moeten er eerst handmatig relaties worden gelegd met de in de eigen organisatie gehanteerde begrippen. Dit is onnodig en kan leiden tot interpretatieverschillen. Als daarbij ook gegevens worden gekoppeld uit een ander systeem is de kans op interpretatiefouten nog groter.

Simple Knowledge Organization System (SKOS) zorgt er voor dat gegevensmodellen van kennisrepresentaties (zoals, begrippenwoordenboeken thesauri en classificatielijsten) bruikbaar zijn voor computerprogramma's (machine readable) en uitgewisseld kunnen worden tussen computerprogramma's onderling. Gebruik van de standaard maakt de (familie)relaties tussen de verschillende definities van begrippen inzichtelijk. Hierdoor kunnen 'begrippenapparaten' geanalyseerd, vergeleken en vertaald worden naar de eigen organisatie. Dit zorgt voor tijdswinst omdat relevante informatie sneller gevonden kan worden en geen tijd hoeft te worden verspild aan het creëren van eigen begrippenlijsten. Het geeft inzicht in de samenhang en (in)consistentie van begrippen (en bijbehorende definities) en zorgt daarmee voor toename in het gebruik van overheidsinformatie.

**Proces**
Er heeft een intakegesprek plaatsgevonden en de standaard voldoet aan de criteria voor inbehandelname. De standaard is aangemeld door het Platform Linked Data Nederland. In Nederland wordt de standaard momenteel door een aantal (semi-) overheidsorganisaties gebruikt zoals de Rijksdienst voor Cultureel Erfgoed, Brandweer Nederland, Stichting Bibliotheek.nl en het Nederlands Instituut voor Beeld en Geluid. Verwacht wordt dat deze organisaties en de organisaties achter het Platform Linked Data Nederland (zoals de Belastingdienst, Kamer van Koophandel en de provincie Overijssel) de aanmelding van de standaard ondersteunen.

**Aandachtspunten**
Gezien de complexiteit en het vernieuwende karakter van de standaard is het belangrijk om tijdens de procedure continu in oog te houden hoe de standaard onder het voetlicht te brengen. Hierbij is het belangrijk om inzichtelijk te maken wat de meerwaarde is, hoe de standaard werkt en wat de kosten zijn. Geadviseerd wordt om

bij de expertsessie ook stil te staan bij een goede definiëring van het functioneel toepassingsgebied van de standaard.



**Ad 3. Uitvoeren van een experttoets op een nieuwe versie van Digikoppeling (een standaard voor berichtenuitwisseling en uitstekend beheerproces**

Het Forum Standaardisatie wordt geadviseerd om Digikoppeling 3.0 in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst. Digikoppeling 2.0 staat al op deze lijst. Aanvullend op het toetsen van de nieuwe versie zal getoetst moeten worden of de status 'uitstekend beheerproces' van toepassing is.

**Over de standaard**
Digikoppeling maakt het mogelijk om met en tussen overheden gestructureerd en gecontroleerd berichten uit te wisselen. Het bestaat uit een set van standaarden voor elektronisch berichtenverkeer. Deze standaarden bevatten afspraken om berichten juist te adresseren, leesbaar en uitwisselbaar te maken en veilig en betrouwbaar te verzenden. Digikoppeling bestaat uit drie domeinen: ten eerste de WUS-standaard voor de bevraging van informatiesystemen, waarop direct een reactie wordt verwacht. Snelheid van afleveren is belangrijk. Ten tweede de ebMS-standaard voor meldingen tussen informatiesystemen, waarbij snelheid van minder belang is. Als derde is er de GB-standaard voor het uitwisselen van grote berichten en het toevoegen van bijlagen.

Digikoppeling 2.0 staat momenteel op de 'pas toe of leg uit'-lijst. De standaard Digikoppeling 3.0 is aangemeld omdat Digikoppeling 3.0 ten opzichte van Digikoppeling 2.0 een aantal belangrijke wijzigingen kent. Het gaat dan om:

- de mogelijkheid om ook met de WUS-standaard (een onderdeel van Digikoppeling) meldingen te kunnen doen,
- de specificatie voor vertaling tussen ebMS en WUS van meldingen, en
- een verhelderde architectuur.

Daarnaast is er een aanvraag gedaan voor 'uitstekend beheerproces', Logius is de beheerorganisatie. Getoetst zal moeten worden of 'uitstekend beheerproces' voor Digikoppeling van toepassing is.

**Proces**
Er heeft een intakegesprek plaatsgevonden en de standaard voldoet aan de criteria voor inbehandelname. De organisaties betrokken in het Technisch Overleg Digikoppeling en de organisaties betrokken in de Programmaraad Stelsel van Basisregistraties (PSB) ondersteunen de aanmelding van Digikoppeling 3.0. In de stuurgroep Digikoppeling van de PSB is besloten tot deze aanmelding.

**Aandachtspunten**
Op voorhand heeft de procedure twee specifieke aandachtspunten. Ten eerste zal getoetst worden of 'uitstekend beheerproces' van toepassing is. Ten tweede zal het toepassingsgebied bijgesteld worden ten opzichte van het toepassingsgebied van Digikoppeling 2.0. Voor beide onderwerpen zal voor aanvang van het opstellen van het expertadvies voorbereidend onderzoek plaatsvinden door de procedurebegeleider en de indiener. De nadere afbakening van het toepassingsgebied is enerzijds nodig om de relatie met NEN3610 (basismodel geo-informatie) te verduidelijken en anderzijds om de toepassing van Digikoppeling binnen sectoren (zoals onderwijs, zorg en het justitiedomein) te bevorderen.

**Ad 4. Het niet in behandeling nemen van OSI open source software licenties**

**Datum**
**03-04-2014**

Het Forum Standaardisatie wordt geadviseerd om de OSI open source licenties niet in procedure te nemen voor opname op een van de lijsten met open standaarden. De OSI open source licenties zijn namelijk geen standaarden voor gegevensuitwisseling.

**Over de Licenties**
De OSI open source licenties zorgen ervoor dat de rechten en plichten van maker en gebruiker van een stuk software zijn vastgelegd. De gebruiker die er voor kiest de software te gebruiken, kiest ervoor zich te committeren aan de in de licentie vastgelegde regels. Het bijzondere van de OSI open source licenties is dat zij bepalen dat de broncode openbaar en herbruikbaar moet zijn. Ook wordt de gebruiker verregaande rechten verleend om de broncode zelf aan te passen, te hergebruiken en anders toe te passen. De standaard heeft echter betrekking op de licentievorm van open source software en is geen standaard voor informatie-uitwisseling.

Door gebruik van de licenties wordt beter inzichtelijk hoe standaarden geïmplementeerd zijn in software. Als er bijvoorbeeld voor de implementatie van standaarden op basis van OSI open source licenties vrij beschikbare referentie-implementaties geraadpleegd kunnen worden, dan kan daarmee de adoptie en implementatie van standaarden worden gestimuleerd.

**Proces**
De licenties zijn aangedragen door de gemeente Vught. Er heeft een intakegesprek plaatsgevonden, daaruit is naar voren gekomen dat de OSI open source licenties niet voldoen aan de criteria voor inbehandelname.

**Ad 5. Aanvulling op de criteria van toekomstig toetsingsprocedure**

Het Forum wordt gevraagd om in te stemmen om in toekomstige toetsingprocedures niet alleen te vragen naar het aantal leveranciers dat een standaard ondersteunen. Maar ook te vragen naar beschikbaarheid van een of meer open source referentie-implementaties. Dit kan als zachte voorwaarde worden opgenomen in de toetsingsprocedure en bevordert de adoptie.

**Advies**
Als uitkomst van de intake van de OSI open source licenties is het advies is om in de toetsingsprocedure van standaarden nadrukkelijker de openheid en aanwezigheid van referentieprofielen te betrekken en inzichtelijk te maken. Vooralsnog beperken toetsingsprocedures zich tot de vraag of er meerdere leveranciers zijn die de standaard implementeren. Om ook te kijken naar de kwaliteit, conformiteit en eenduidigheid van deze implementaties dient dit te worden geverifieerd. Dit is belang van de interoperabiliteit en adoptie van een standaard. Zo kan de beschikbaarheid van een of meer open source referentie-implementaties van een standaard een zacht criterium zijn in de toetsingsprocedure. Als leidraad kan er voor worden gekozen dat deze referentie-implementaties beschikbaar zijn onder een OSI open source licentie.

Datum
03-04-2014

**Ad 6. Het in procedure nemen van de nieuwe versies van NEN-ISO/IEC 27001 en 27002 en het advies over de relatie tussen deze standaarden en de Baselines informatiebeveiliging op de 'pas toe of leg uit'-lijst.**

**Aanleiding en achtergrond**
Op de 'pas toe of leg uit'-lijst staan de normen voor informatiebeveiliging ISO/IEC 27001 en ISO/IEC 27002. ISO 27001 beschrijft de eisen aan het managementsysteem voor informatiebeveiliging. De bijbehorende ISO-norm 27002 bevat de maatregelen voor informatiebeveiliging. De versies die op de lijst staan dateren uit 2005 (NEN-ISO/IEC 27001) en 2007 (NEN-ISO/IEC 27002). Beide normen zijn in 2013 vernieuwd. Omdat bedrijven (leveranciers van de overheid) en auditoren volgens deze nieuwe versie gaan werken en toetsen, zal deze versie op de lijst moeten worden aangepast.

De 27001 en 27002-normen zijn geschikt voor bedrijfsleven als overheid. De Nederlandse overheid heeft ook haar eigen kaders voor informatiebeveiliging. Dit zijn de sectorale baselines informatiebeveiliging, oftewel de Baseline Informatiebeveiliging Rijksdienst (BIR), de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de Baseline Informatiebeveiliging Waterschappen (BIWA) en de Interprovinciale Baseline Informatiebeveiliging (IBI). Deze baselines informatiebeveiliging zijn gebaseerd op de (oude) NEN-ISO/IEC 27002:2007 standaard en bevatten verder uitgewerkte beveiligingsmaatregelen.

Om de adoptie van de baselines niet te belemmeren is dit vooronderzoek gestart om te besluit of, wanneer en hoe NEN-ISO/IEC 27001:2013 en 27002:2013 in procedure genomen moeten worden voor opname op de 'pas toe of leg uit'-lijst. Het onderzoek helpt daarnaast ook om de relatie tussen de 'pas toe of leg uit'-lijst en de baselines informatiebeveiliging beter te duiden.

**Betrokkenen en proces**
In totaal zijn achttien betrokkenen samengebracht in de onderzoeksgroep, die de vragen uit het onderzoek hebben beantwoord. Voor de onderzoeksgroep zijn personen uitgenodigd die vanuit hun persoonlijke betrokkenheid of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaarden en / of sectorale baselines. Zowel technisch deskundigen als betrokkenen die inzicht hebben in de functionele en organisatorische impact zijn uitgenodigd.

Parallel hieraan zijn de concept resultaten en een gedeelte van de vraagstelling gepresenteerd en besproken in de Werkgroep Normatiek van de Taskforce BID. De input vanuit deze werkgroep is meegenomen in dit eindrapport en afgestemd met de onderzoeksgroep.

**Consequenties en vervolgstappen**
Op basis van de resultaten en het advies van dit verkennende onderzoek kan het Forum Standaardisatie besluiten hoe met de nieuwe versies van de Nederlandse normen NEN-ISO/IEC 27001 en 27002 om te gaan. Het vervolg is dat de toetsingsprocedure voor opname van de nieuwe versie wordt gestart. Daarnaast dient de informatie op de 'pas toe of leg uit'-lijst te worden aangepast zodat het (voor inkopers) duidelijker wordt hoe om te gaan bij het vragen naar de normen en/of de sectorale baselines in aanbestedingen.

**Datum**
**03-04-2014**

## 1. De nieuwe versie en de toetsingsprocedure

In ogenschouw nemende dat:

- De geldigheid van ge-audite certificaten van de oude 27001 norm uiterlijk per 1 oktober 2015 verlopen;
- De doorlooptijd van de toetsingsprocedure minimaal 6 maanden is;
- De nieuwe 2013 versies een verbetering zijn, onder andere met betrekking tot de context van een organisatie;
- De nieuwe 2013 versies voortbouwen op de oude versies en de nieuwe versies niet strijdig zijn met de baselines.

Wordt het Forum geadviseerd om de nieuwe versies van de standaarden direct in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst.

Om te voorkomen dat de toetsingsprocedure van de nieuwe 27001 en 27002 standaarden, de adoptie van de sectorale baselines informatiebeveiliging belemmert is het belangrijk om een onderscheid te maken tussen de baselines, de nieuwe normen en de implementatie van dezen. Het is dus van belang om de communicatie rondom de procedure af te stemmen met belanghebbenden, zoals de Werkgroep Normatiek. Wel worden de baselines geadviseerd om bij het updaten van de baselines deze in ieder geval in lijn te brengen met de nieuwe 27001/2 normen.

## 2. De normen, de Baselines en de 'pas toe of leg uit'-lijst

Het Forum Standaardisatie wordt geadviseerd om de conclusie uit het onderzoek in de 'pas toe of leg uit'-lijst uit te werken. Daarbij is het van belang om de exacte teksten af te stemmen met de diverse vertegenwoordigers van de sectorale baselines en de Werkgroep Normatiek.

Door het implementeren van de baselines hoeven overheidsorganisatie niet alsnog te voldoen aan de ISO27002 standaard. De baselines informatiebeveiliging zijn namelijk een nadere uitwerking van ISO27002/2005. Dit gaat niet op voor ISO27001, organisaties zouden deze standaard wel moeten implementeren en zich zo nodig laten certificeren.

Het is belangrijk dat er voor overheidsinstellingen en leveranciers een aanvullende toelichting komt op de 'pas toe of leg uit'-lijst over hoe met de verschillende baselines en standaarden dient te worden omgegaan. Uitgangspunt is dat aan leveranciers wordt gevraagd te voldoen aan de ISO27001 norm voor informatiebeveiligingsmanagement en zich afhankelijk van de gewenste zekerheid ook laten certificeren. Voor concrete beveiligingsmaatregelen dient naar de ISO27002 norm of gelijkwaardig te worden gevraagd. Additioneel kan door een overheid aanvullend geformuleerde beveiligingseisen worden geëist gebaseerd op de desbetreffende baseline.

*Voor overheidsorganisatie:*

- 1. Schenk meer nadrukkelijk aandacht aan de implementatie van de beveiligingsprincipes omtrent het managementsysteem zoals is vastgelegd in NEN-ISO/IEC 27001 norm en het Voorschrift Informatiebeveiliging Rijksdienst. Laat je hierop *eventueel* certificeren.
- 2. Implementeer de beveiligingsmaatregelen zoals vastgelegd in je informatiebeveiligingsbeleid.

- 3. Deze beveiligingsmaatregelen dienen gebaseerd te zijn op de eigen sectorale baseline. Deze baselines zijn een invulling van de NEN-ISO/IEC 27002 norm. Door implementatie van de baselines wordt ook voldaan aan de adoptie van deze norm.

*Voor leveranciers:*
- 1. Voldoe aan de NEN-ISO/IEC 27001 norm en laat je hierop certificeren.
- 2. Implementeer beveiligingsmaatregelen, hierbij dient de 27002 norm als referentie.
- 3. Aanvullend kunnen er door overheidsorganisaties beveiligingsmaatregelen worden geëist. Deze aanvullende maatregelen zijn beschreven in hun informatiebeveiligingsbeleid die zijn gebaseerd op de baselines.

# Ter Kennisname

**Ad 7. Samenhangonderzoeken in relatie tot dossier lijsten en adoptie**

In september heeft het Bureau Forum Standaardisatie een inventarisatie gemaakt van mogelijke thema's voor de samenhang van standaarden. Dit naast het thema beveiligingsstandaarden, dit thema staat ook in 2015 centraal. Bij samenhang is de vraag: welke set van standaarden zijn relevant op een bepaald thema en hoe verhouden deze zich tot elkaar? In oktober heeft de stuurgroep samenhang een shortlist samengesteld en deze is uitgezet naar stakeholders en besproken met de NORA. De uitkomst is dat er ook vraag is naar meer inzicht op de volgende thema's:

- Welke specifieke Cloud standaarden zijn er en hoe verhouden deze zicht tot elkaar (met aandacht voor de aspecten zaakgericht werken en linked data). Op dit moment loopt er een inventarisatie welke standaarden er zijn;
- Welke documentatie/ publicatie standaarden zijn er en hoe verhouden deze zich tot elkaar

De drie decentralisaties kwam ook als thema naar voren. Met KING is echter afgesproken dat we ons in 2015 hier niet specifiek op focussen, behalve als er vragen zijn vanuit KING en/of VWS. In januari zal de stuurgroep samenhang nader naar de thema's kijken en bespreken of we deze thema's nader oppakken of niet. Als randvoorwaarde geldt daarbij dat we aanhaken bij internationale ontwikkelingen en de al lopende ontwikkelingen vanuit andere overheidspartijen.

Voor lijsten en adoptie is dit belangrijk omdat hierdoor beter inzichtelijk wordt welke standaarden we op de lijst missen, zo nodig kunnen standaarden in procedure worden gebracht. Ook is het belangrijk voor de actualiteit van de informatie op de lijst. Verder is het voor adoptie belangrijk omdat inzichtelijk wordt hoe het staat met adoptie, welke bottlenecks er zijn en wat het speelveld is.

**Ad. 8 Toetsen SEPA, ePortfolio, Semantisch model e-factureren (SMEF) en SETU.**

Op de 'pas toe of leg uit'-lijst staan enkele standaarden met een oude versie, voor de actualiteit en kwaliteit van de lijst is het belangrijk dat deze up to date zijn. Daarnaast staat de SEPA standaard op de lijst, deze standaard is echter wettelijk verplicht. Vandaar dat we nu de volgende standaarden nader onderzoeken:

- *ePortfolio standaard*: van deze onderwijsstandaard staat een 2009 versie op de

lijst. Ondertussen is er een versie uit 2013. Op dit moment zijn we aan het controleren wat de verschillen zijn tussen deze versies en kijken we of dit van invloed is op het toepassingsgebied en de 'pas toe of leg uit'-lijst.

- *SMEF en SETU*: update van de standaarden SMEF en SETU. Voor SMEF is er een nieuwe versie (1.3 ipv 1.2.7) en voor een van de SETU standaarden is er ook een nieuwe versie (1.2 ipv 1.1) De beheerders geven aan dat de wijzigingen miniem zijn en niet van invloed op het toepassingsgebied. Toch zullen we hiervoor nog een onafhankelijk toets moeten uitvoeren.
- *SEPA*: SEPA is per september 2014 wettelijk verplicht en de standaard is breed geadopteerd. Op dit moment wordt met betrokkenen afgestemd of de standaard per direct van de lijst kan of dat hier nog bezwaren tegen zijn.

De uitkomsten uit deze onderzoeken komen in de volgende Forumvergadering terug.