

**Forum Standaardisatie**

Wilhelmina v Pruisenweg 52
 2595 AN Den Haag
 Postbus 96810
 2509 EJ Den Haag
www.forumstandaardisatie.nl

notitie

COLLEGE STANDAARDISATIE

Bijlagen:	A. Conceptrapport "Monitor adoptie Open Standaarden over 2012" B. Advies adoptie normen voor informatiebeveiliging NEN-ISO 27001/27002 C. Nota aan dagelijks bestuur BRG D. Notitie voortgang adoptie SEPA-standaarden		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	12 november 2013	Versie	1.0
Betreft:	Adoptie van open standaarden		

Doel

U wordt gevraagd **in te stemmen** met:

1. Monitor open standaardenbeleid en aanscherping lopende adoptieaanpak;
2. Advies ter bevordering van adoptie van normen voor informatiebeveiliging NEN-ISO 27001/27002;
3. Nota voor Bestuurlijke Regiegroep (BRG) betreffende samenwerking adoptie van open standaarden.

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

4. Voortgang adoptie van SEPA standaarden (Europese betaalstandaarden) deadline implementatie- 1-2-2014.

Toelichting

Datum
12 november 2013

Ter besluitvorming**Ad 1. Monitor open standaardenbeleid en aanscherping lopende adoptieaanpak [bijlage A]**

Het College Standaardisatie wordt gevraagd om:

- 1) In te stemmen met het voortzetten van de in begin 2013 ingezette koers voor de bevordering van de adoptie van open standaarden en met de acties tot nadere aanscherping van deze ingezette koers.
- 2) Kennis te nemen van:
 - a) Het nieuwe monitorrapport open standaardenbeleid;
 - b) De resultaten van de sessie "*pas toe of leg uit' in de praktijk*" die op initiatief van het College Standaardisatie naar aanleiding van het vorige monitorrapport is georganiseerd.

Toelichting***Ad 1. Ingezette koers en aanscherping***

Op basis van de monitor van vorig jaar hebben het College en Forum Standaardisatie een nieuwe koers voor adoptie uitgezet met de onderstaande belangrijkste uitgangspunten:

- Stimulering aan de voorkant van een aanschaftraject (proactief);
- Adoptieaanpak per standaard en ondersteuning op maat;
- Samenwerking met stakeholders (o.a. KING, IPO, UvW, Manifestgroep, ICCIO, BRG, leveranciers);
- Stimulering via centrale voorzieningen en shared services;
- Gericht op feitelijke adoptie, naast stimulering via aanbestedingen.

De monitor geeft niet direct aanleiding om deze koers te wijzigen. Wel wil het Forum Standaardisatie de ingezette koers nader aanscherpen. Daartoe zal het Bureau Forum Standaardisatie een nadere analyse maken van bottlenecks (drempels) en best practices (succesverhalen) op basis van interviews met stakeholders en op basis van eerdere studies en ervaringen. Het doel is om op basis van deze analyse de adoptieaanpak voor 2014 verder aan te scherpen en eventueel aanvullende afspraken te maken.

Ad 2a. Monitor open standaardenbeleid

Ook dit jaar heeft ICTU in opdracht van Forum Standaardisatie en het Ministerie van Economische Zaken de monitor open standaardenbeleid uitgevoerd. Het rapport bevat vijf onderzoeksonderdelen. Hieronder volgt per onderdeel kort het beeld dat naar voren komt:

1. **Shared services:** Alhoewel er verbeteringen mogelijk zijn, voldoen deze redelijk goed aan open standaarden. Met name Rijksoverheid.nl biedt ondersteuning voor veel open standaarden. Een paar voorzieningen scoren minder goed dan de rest. De meeste shared services worden ook al door veel partijen gebruikt wat het effect van de open standaarden vergroot. De ondersteuning van een standaard door een voorziening betekent niet altijd dat de standaard ook automatisch gebruikt wordt; soms is er een afhankelijkheid van andere

voorzieningen of van de gebruiker. Het verzamelen van de informatie blijkt in veel gevallen niet eenvoudig.

Datum
12 november 2013

2. NUP-bouwstenen: Het gebruik van verschillende NUP-bouwstenen (o.a. Antwoord voor Bedrijven en eHerkenning) is gestegen. Dit heeft een positief effect op het gebruik van verschillende open standaarden. De monitor van vorig jaar liet namelijk zien dat de NUP-voorzieningen redelijk goed voldoen aan open standaarden. Ook hier blijkt het niet altijd eenvoudig om informatie over de koppelvlakken en standaarden te achterhalen. Logius vormt daarop een positieve uitzondering; zij publiceert jaarlijks een overzicht van de al dan niet gebruikte standaarden per voorziening.
3. Gebruiksgegevens: Het beeld wisselt hier per standaard. Digikoppeling (berichtenverkeer), SAML (identiteitsgegevens) en DNSSEC (veilige domeinnamen) zitten bijvoorbeeld duidelijk in de lift. Bij andere standaarden, zoals bij IPv6 (internetnummers), is de groei minder duidelijk. Niet voor iedere standaard zijn automatische tools of onderzoeksbronnen beschikbaar om een beeld van de mate van gebruik te krijgen. Hier ligt ook een rol voor de beheerders van de standaarden.
4. Zelfrapportage: Het percentage overheidsorganisaties dat het 'pas toe of leg uit'-principe ingevoerd heeft is gestegen van 54% naar 59%. Deze cijfers worden mogelijk beïnvloed door de veranderende samenstelling van de responsgroep. Kijken we alleen naar de 87 overheden die zowel in 2012 als in 2011 als in 2010 de vragenlijst hebben beantwoord, dan is het beeld positiever: het totaalpercentage dat het 'pas toe of leg uit'-principe ingevoerd heeft is gestaag toegenomen van 56% in 2010, via 60% in 2011 tot 64% in 2012.
5. Aanbestedingen: De meting had betrekking op aanbestedingen van 2012. Het beeld is nauwelijks veranderd ten opzichte van het jaar ervoor. In een belangrijk deel van de aanbestedingen (63%) wordt in het geheel niet gevraagd om de relevante open standaarden en daarover ook geen uitleg gegeven in het jaarverslag. In 37% van de onderzochte gevallen is wel om een deel of om alle relevante standaarden gevraagd. Verschillende organisaties (o.a. Ministerie van Algemene Zaken, Ministerie van Veiligheid en Justitie, Gemeente Steenwijkerland en Provincie Gelderland) doen het wel goed en laten zien dat het goed mogelijk is om bij een aanbesteding om alle relevante standaarden te vragen.

Ad 2b. Sessie "pas toe of leg' uit in de praktijk"

Naar aanleiding van het vorige monitorrapport, dat in de vergadering van het College Standaardisatie in november 2012 aan de orde was, hebben Forum Standaardisatie en de Standaardisatiecommissie Rijk op 28 mei 2013 de sessie 'pas-toe-of-leg-uit in de praktijk' georganiseerd. In de sessie is met ICT-inkopers en ICT-architecten het gesprek gevoerd. Het doel van de bijeenkomst was om van elkaar leren, zodat de overheid de voordelen van open standaarden nog meer benut.

Samengevat werden de volgende belangrijke punten naar voren gebracht:

- Dat het inrichten van ICT-governance (waaronder portfoliomanagement) ook ten goede komt aan de implementatie van open standaarden.
- Dat er goede ervaringen zijn opgedaan met het opnemen van open standaarden in procedures, zoals inkoopprocedures, in formulieren, in formats voor Plannen van Aanpak (met als strekking: check of er naar

open standaarden is gevraagd, zijn ze toegepast, zo niet: meteen 'explain' opvragen). Het is belangrijk dat de inkoopafdeling van meet af aan bij projecten betrokken wordt.

Datum
12 november 2013

- Dat open standaarden niet alleen SMART dienen te worden opgenomen in het bestek, maar dat het ook belangrijk is om te controleren of er conform bestelling geleverd wordt (neem dat in aanbesteding op).
- Zorg dat het Forum Standaardisatie de inkopers daadwerkelijk bereikt. Er is soms sprake van onbekendheid met de 'pas-toe-of-leg-uit'-lijst, en de toepassing ervan (wanneer is een open standaard relevant en wanneer niet?). Relevante informatie is niet altijd even makkelijk te vinden, bijvoorbeeld ver weggestopt op een site (bijv. PIANO-website).

Ad 2. Advies ter bevordering van adoptie van normen voor informatiebeveiliging NEN-ISO 27001/27002 [bijlage B]

Het College Standaardisatie wordt gevraagd om in te stemmen met het bijgevoegde advies om de adoptie van de normen voor informatiebeveiliging NEN-ISO27001/27002 verder te bevorderen.

Toelichting

Waar gaat dit over?

NEN-ISO 27001/27001 bevatten eisen en richtlijnen voor het inrichten van informatiebeveiliging in een organisatie. De normen vormen een hulpmiddel voor een (overheids)organisatie waarmee deze de informatiebeveiliging op een hoger niveau kan brengen. Daardoor kan ook de betrouwbaarheid van de gegevensuitwisseling met andere partijen toenemen. De beide normen zijn sinds medio 2008 opgenomen op de lijst met open standaarden voor 'pas toe of leg uit'.¹ De beschrijving in de normen is op een relatief hoog abstractieniveau. De diverse sectorale Baselines Informatiebeveiliging, zoals de Baseline Informatiebeveiliging Rijk (BIR) en de Baseline Informatiebeveiliging Gemeenten (BIG), zijn gebaseerd op deze normen en geven deze nadere invulling.

Welk proces is doorlopen?

Op 12 september jl. heeft een expertgroep in opdracht van het Forum Standaardisatie de adoptie van de standaarden geëvalueerd. De expertgroep heeft de status van de adoptie van de standaarden geanalyseerd en heeft geadviseerd over maatregelen die mogelijke adoptiedrempels kunnen wegnemen. In de expertgroep zaten vertegenwoordigers vanuit o.a. Ministerie van BZK, Ministerie van Financiën/Belastingdienst, Ministerie van SZW, Ministerie van V&J, Provincie Zeeland, KING, Erasmus Universiteit, Auditdienst Rijk, NEN en Logius. Daarnaast is afstemming gezocht met de Taskforce Bestuur en Informatieveiligheid Dienstverlening (TF BID).

De resultaten zijn vastgelegd in een expertadvies. De bijgevoegde 10 adviespunten waarover een besluit wordt gevraagd, zijn opgesteld op basis van het genoemde expertadvies.²

¹ Zie: <https://lijsten.forumstandaardisatie.nl/open-standaard/nen-isoiec-27001>

² Zie: <https://www.forumstandaardisatie.nl/sites/default/files/FS/2009/0211/NEN-ISO-Expertadvies-19005-1-2005-PDFA-1.pdf>

Datum
12 november 2013

Wat is het doel?

Het besluit heeft tot doel om de adoptie van de standaarden NEN-ISO 27001/27002 verder te bevorderen en daarmee de informatiebeveiliging binnen de publieke sector op een hoger niveau te brengen. Een aantal partijen wordt opgeroepen om concrete maatregelen te nemen zodat geïdentificeerde adoptie-drempels worden weggenomen. De hoofdpunten van het advies betreffen:

- Het belang van de Baselines Informatiebeveiliging en de daadwerkelijke implementatie ervan;
- De noodzaak voor het ontwikkelen en het delen van implementatie-hulpmiddelen;
- De vrije, publieke beschikbaarheid van de normen en van de Baselines Informatiebeveiliging;
- Open beheer van de Baselines Informatiebeveiliging (o.a. grotere betrokkenheid marktpartijen);
- Doorontwikkeling en harmonisatie van de Baselines.

Ad 3. Nota voor Bestuurlijke Regiegroep (BRG) betreffende samenwerking adoptie van open standaarden [bijlage C]

Het College Standaardisatie wordt gevraagd om in te stemmen met het versturen van de nota aan de Bestuurlijke Regiegroep (BRG).

Toelichting

Zoals eerder afgesproken in het College wordt - met het oog op het stimuleren van de adoptie van open standaarden - ingezet op samenwerking met o.a. ICCIO en BRG. Daartoe stuurde het College eerder dit jaar een brief aan ICCIO. Bijgevoegd treft u een concept-nota voor het Dagelijks Bestuur BRG aan (dat 4 december bij elkaar komt), op weg naar de BRG zelf (begin januari). Deze nota is eerder afgestemd in het overleg Informatie Strategie Overheden (ISO) van de vier overheidssectoren (Rijk/ZBO's, provincies, gemeenten en waterschappen).

In de totstandkoming van de nota is meermaals de behoefte naar voren gekomen om de gevraagde actie van de BRG (partijen) te concretiseren. Het concrete voorstel aan de BRG is om een aantal keer per jaar - via de koepelorganisaties (Rijk/ICCIO, IPO, UvW, VNG) - over het openstandaardenbeleid met hun achterban te communiceren. In die communicatieboodschap zal worden aangehaakt op de samenwerkingsverbanden van de gezamenlijke sector inkoop (indien aanwezig; bijvoorbeeld PIANOo), en de sector modelarchitecturen (GEMMA, NORA, PETRA, WILMA).

Ter kennisname

Ad 4. Voortgang adoptie van SEPA-standaarden (Europese betaalstandaarden, deadline implementatie 1-2-2014) [bijlage D]

Het College Standaardisatie wordt gevraagd om:

1. Kennis te nemen van de voortgang m.b.t. de adoptie van SEPA-standaarden gezien de naderende deadline van 1 februari 2014;
2. Kennis te nemen van de urgentie en de achterban hierover te blijven informeren.

Datum
12 november 2013

Toelichting

Adoptiestatus op hoofdlijnen

Veel overheden zijn in beweging gekomen en zijn of klaar of ver gevorderd met de invoering van SEPA. Toch lijken er ook verschillende overheden te zijn voor wie er nog veel werk aan de winkel is, zeker als het gaat om de Europese incasso (SDD's). Soms komt dat ook omdat hun leveranciers (nog) niet volledig klaar zijn. Als een overheidsorganisatie niet op tijd klaar is, dan kan deze vanaf 1 februari 2014 betalingen niet meer uitvoeren.

Gezien de naderende deadline, waarvoor geen uitstel komt, is het van groot belang om de urgentie te blijven communiceren. Daarnaast kan het zinvol zijn voor overheden om ervaringen te delen en van elkaar te leren o.a. via online groepen op LinkedIn en Pleio.³

Het voorgaande beeld is gebaseerd op een recente uitvraag die door Forum Standaardisatie is uitgevoerd via de sectorale koepels. Het resultaat daarvan is opgenomen in de bijlage. Daarnaast is het beeld gebaseerd op de laatste SEPA migratiemonitor (voorjaar 2013) van het Nationaal Forum SEPA-migratie en de Second Migration Monitor Report (oktober 2013) van de Europese Centrale Bank.⁴

Achtergrond

De SEPA-standaarden zijn door het College Standaardisatie medio 2011 op de 'pas stoe of leg uit'-lijst geplaatst. De Europese Commissie heeft vervolgens in 2012 bepaald dat SEPA (Single European Payment Area) op 1 februari 2014 gerealiseerd moet zijn. Dat betekent dat vanaf dat moment alle elektronische betalingen (zowel overmakingen als incasso's) moeten voldoen aan het SEPA-formaat dat o.a. het nieuwe rekeningnummer IBAN omvat. Overheden en bedrijven moeten de koppelvlakken van hun betaalsystemen, die betalingsopdrachten communiceren naar banken, dus voor die datum hebben aangepast.

Als een organisatie zijn systeem niet tijdig heeft aangepast, dan kan niet meer via dat systeem worden betaald. Vanuit de Taskforce SEPA Nederland is er onlangs nogmaals gewaarschuwd dat er geen plan B is; er komt vanuit Europa geen uitstel.

³ Zie: <https://www.pleio.nl/groups/profile/20215092/sepa> en <https://www.linkedin.com/groups?gid=5043707>.

⁴ Zie: http://www.dnb.nl/binaries/SEPA%207e%20Migratiemonitor%2C%20voorjaar%202013_tcm46-291131.pdf en <http://www.ecb.europa.eu/pub/pdf/other/secondsepmigrationreport201310en.pdf>