**Forum Standaardisatie**

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

# HAMERSTUK

## Nationaal Beraad Digitale Overheid

| | | | |
|---|---|---|---|
| **Aan:** | Nationaal Beraad Digitale Overheid | | |
| **Van:** | Forum Standaardisatie | | |
| **Datum:** | 29 april 2015 | **Versie** | 1.0 |
| **Betreft:** | opname standaarden op de 'pas-toe-of-leg-uit'-lijst. | | |

2015-0000255138

**Het Nationaal Beraad wordt gevraagd in te stemmen met:**

1. Het opnemen van standaarden voor e-mailbeveiliging (anti-phishing en anti-spam: *DMARC* en *SPF*) op de 'pas-toe-of-leg-uit'-lijst;
2. Het opnemen van een standaard voor het uitwisselen en koppelen van woordenlijsten (*SKOS*) in de vorm van open data op de 'pas toe of leg uit'-lijst;
3. Het opnemen van nieuwe versies van standaarden voor informatiebeveiliging (*NEN-ISO/IEC 27001 en 27002*) op de 'pas-toe-of-leg-uit'-lijst.

**Toelichting op het 'pas toe of leg uit'-beleid**

Het is kabinetsbeleid dat open standaarden overheidsbreed worden gebruikt op basis van een 'pas-toe-of-leg-uit'-regime voor concrete standaarden van de 'pas-toe-of-leg-uit'-lijst van het Forum Standaardisatie. De bekrachtiging van de standaarden die op deze lijst worden geplaatst, op advies van het Forum Standaardisatie, ligt bij Nationaal Beraad.

Overheden en semi-overheden zijn verplicht om de standaarden met de status 'pas toe of leg uit' te vragen bij aanschaf of (ver)bouw van ICT-systemen/-diensten ('pas toe'). Afwijken mag alleen met zwaarwegende redenen en verantwoording hierover moet worden afgelegd in het jaarverslag ('leg uit'). 'Pas-toe-of-leg-uit'-standaarden zijn open standaarden met overheidsbrede werking en met reeds bewezen meerwaarde, maar die nog niet voldoende breed toegepast worden. Gebruik van deze standaarden verbetert de digitale communicatie (interoperabiliteit) en daarmee de samenwerking tussen overheden onderling en tussen overheden en bedrijven en overheden en burgers. Daarnaast kunnen open standaarden door iedere leverancier worden ingebouwd, wat de leveranciersafhankelijkheid (vendor lock-in) voor overheden vermindert. Het proces voor het toetsen van standaarden is transparant en robuust op basis van expertsessies en openbare consultaties.

**Hierna worden de beslispunten toegelicht.**

## Ad.1 Het opnemen van standaarden voor e-mailbeveiliging (DMARC en SPF)



DMARC en SPF zijn standaarden voor het veiliger maken van email verkeer door het tegengaan van spam en phisingmail door misbruik van domeinnamen bij e-mail te voorkomen. De open standaard DMARC maakt het mogelijk om te bepalen hoe een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. De open standaard SPF controleert of de mailserver die een e-mail wil versturen namens het e-maildomein deze e-mail mag verzenden. Op de lijst staat al de e-mailbeveiliging standaard DKIM. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. Opname van DMARC en SPF op de lijst zou betekenen dat er een complete set van e-mail beveiligingstandaarden op de lijst staat.

Na toetsing van de criteria en de doorlopen procedure[1] adviseert het Forum aan het Nationaal Beraad om in te stemmen met:

1. *Opname van DMARC op de 'pas-toe-of-leg-uit'-lijst onder de voorwaarde dat het beheer van DMARC is geformaliseerd bij de beheerorganisatie IETF.*

Zodra het Forum Standaardisatie vaststelt dat hieraan is voldaan kan de standaard op de lijst worden geplaatst.

2. *Opname van SPF op de 'pas-toe-of-leg-uit'-lijst.*
3. *Het door de expertgroep gedefinieerde functionele toepassingsgebied en organisatorische werkingsgebied.*

    - Toepassingsgebied DMARC: voor alle domeinnamen, waarvan de overheid de houder is, om betrouwbare e-mailcommunicatie met burgers, bedrijven en (semi)overheidsorganisaties te bevorderen en de overheid zelf te beschermen tegen e-mail van ongeauthenticeerde afzenders.
    - Toepassingsgebied SPF: het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.
    - Het organisatorisch werkingsgebied voor beide standaarden: overheden (rijk, provincies, gemeenten en waterschappen) en overige instellingen uit de publieke sector.

## Ad.2 Het opnemen van een standaard voor het uitwisselen en koppelen van woordenlijsten (SKOS)

Het publiceren van gegevensbestanden in de vorm van begrippenlijsten, digitale woordenboeken en taxonomieën door overheidsorganisaties gebeurt vaak in de vorm van documenten die niet bruikbaar zijn voor computerprogramma's. De open standaard Simple Knowledge Organization System (SKOS) zorgt ervoor dat deze kennisrepresentaties via het internet aan elkaar kunnen worden gelinked en maakt het mogelijk dat gegevensbestanden makkelijker als open data kunnen worden hergebruikt.

Door het toepassen van de standaard worden de (familie)relaties tussen de verschillende definities van begrippen beter inzichtelijk en is data uit verschillende systemen beter te vergelijken en te interpreteren. Zo is bijvoorbeeld het begrip 'adres' in het Handelsregister een breder begrip dan het begrip 'adres' in de Basisregistratie Adressen en Gebouwen (BAG). Met SKOS kunnen deze begrippen (ondanks dat ze niet exact hetzelfde zijn) toch met elkaar in verband worden gebracht. Hierdoor hoeven definitiekwesties niet eerst te worden beslecht voordat er gegevensuitwisseling kan plaatsvinden. Dit zorgt voor tijdswinst omdat relevante

[1] *Documentatie over de procedure, het expertadvies en het forumadvies met adoptiemaatregelen zijn te vinden op: https://lijsten.forumstandaardisatie.nl/open-standaard/dmarc*

informatie sneller gevonden kan worden en geeft inzicht in de samenhang en (in)consistentie van begrippen (en bijbehorende definities). Een ander voorbeeld van gebruik is in de culturele erfgoedsector. Verschillende instituten maak daar gebruik van verschillende beheersapplicaties voor hun collecties. Deze applicaties hanteren ieder hun eigen trefwoordenlijsten. Het is echter belangrijk dat erfgoed toegankelijk is en dat collecties digitaal zijn te ontsluiten. Daarom heeft het NWO in samenwerking met universiteiten, Rijksdienst voor Cultureel Erfgoed, het Nationaal Archief en het Nederlands Instituut voor Beeld en Geluid een platform opgezet waardoor mede dankzij SKOS collecties van erfgoedinstellingen aan elkaar kunnen worden gekoppeld.

Gebruik van de standaard wordt aanbevolen door het platform Linked Data. Hierin zijn organisaties als het Ministerie van OCW, Belastingdienst, Kadaster, Rijkswaterstaat, Geonovum en Ministerie van BZK betrokken. Na toetsing van de criteria en de doorlopen procedure[2] adviseert het Forum aan het Nationaal Beraad om in te stemmen met:

1. *Opname van SKOS op de 'pas toe of leg uit'-lijst;*
2. *Het door de expertgroep gedefinieerde functionele toepassingsgebied en organisatorische werkingsgebied.*

    - Toepassingsgebied: het in een gestructureerde vorm op het Web publiek beschikbaar stellen van een 'niet geformaliseerd' Knowledge Organization System (KOS), met als doel kennis over de betekenissen en samenhang van de onderliggende begrippen te ordenen en toegankelijk te maken als open data.
    - Organisatorisch werkingsgebied: Overheden (Rijk, provincies, gemeenten en waterschappen) en overige instellingen uit de publieke sector.

### Ad.3 Nieuwe versies van standaarden voor informatiebeveiliging (*NEN-ISO/IEC 27001 en 27002*)

Op de lijst staan de normen voor informatiebeveiliging NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. 27001 beschrijft de eisen om de risico's op het gebied van informatiebeveiliging te kunnen beheersen (organisatorisch, technisch). De bijbehorende 27002 standaard is een "best practice" van beveiligingsmaatregelen om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De versies op de lijst dateren uit 2005 (NEN-ISO/IEC 27001) en 2007 (NEN-ISO/IEC 27002). Beide normen zijn in 2013 vernieuwd.

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 kaders zijn gebaseerd op de 27001 en 27002 normen. In samenwerking met de beheerders van de Baselines Informatiebeveiliging (Ministerie van BZK, IPO, KING en Unie van Waterschappen) heeft het Forum een onderzoek uitgevoerd om de relatie tussen Baselines en de nieuwe versie van de normen te duiden. Aansluitend hierop heeft een expertonderzoek en openbare consultatie plaatsgevonden.

[2] *Documentatie over de procedure, het expertadvies en het forumadvies met adoptiemaatregelen zijn te vinden op: https://lijsten.forumstandaardisatie.nl/open-standaard/skos*

Het advies is om de versie van deze standaarden op de 'pas toe of leg uit'-lijst aan te passen. Dit is belangrijk omdat auditcertificaten op basis van de oude 27001 norm per 1 oktober 2015 verlopen. Het toepassingsgebied en het organisatorische werkingsgebied blijft gelijk. Daarnaast zal op de lijst goed de verhouding tot de Baselines Informatiebeveiliging moeten worden weergegeven.

**Datum**
29 april 2015

Na toetsing van de criteria en de doorlopen procedure[3] adviseert het Forum aan het Nationaal Beraad om in te stemmen met:

1. *Het op de 'pas-toe-of-leg-uit'-lijst aanpassen van de NEN-ISO/IEC 27001 standaard naar versie 2013;*
2. *Het op de 'pas-toe-of-leg-uit'-lijst aanpassen van de NEN-ISO/IEC 27002 standaard naar versie 2013.*

**TER KENNISNAME**

**Eerste standaard verwijderd van de 'pas toe of leg uit'-lijst vanwege succesvolle adoptie**

Forum Standaardisatie is verheugd om aan te kondigen dat de SEPA standaard voor (digitaal) betalingsverkeer van de 'pas toe of leg uit'-lijst kan worden verwijderd vanwege succesvolle adoptie. Het is niet meer nodig om adoptie van deze standaard aan te jagen middels plaatsing op de standaardenlijst omdat de standaard nagenoeg 100% wordt toegepast en bij Europese wet is verplicht voor alle Europese lidstaten.

[3] *Documentatie over de procedure, het expertadvies en het forumadvies met adoptiemaatregelen zijn te vinden op: https://lijsten.forumstandaardisatie.nl/open-standaard/nen-isoiec-27001-0 & https://lijsten.forumstandaardisatie.nl/open-standaard/nen-isoiec-27002-0*