Forum Standaardisatie

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

notitie

Aanpassing functioneel toepassingsgebieden internet- en beveiligingsstandaarden

FORUM STANDAARDISATIE 25 april 2018

Agendapunt:	3H		
Bijlagen:	Expertadvies functioneel toepassingsgebieden internet- en beveiligingsstandaarden		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Standaardisatie		
Datum:	3 april 2018	**Versie**	1.0

Aanleiding en achtergrond
Van iedere verplichte standaard op de lijst met open standaarden is het functioneel toepassingsgebied omschreven. Dit functioneel toepassingsgebied bepaalt voor welke ICT-producten en -diensten een standaard relevant is en wanneer de standaard dus moet worden toegepast.

Niet alle functioneel toepassingsgebieden zijn even duidelijk omschreven. Dit kan adoptie van standaarden in de weg staan. Om deze reden zijn de huidige omschrijvingen van IPv6 en IPv4, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, SAML, STARTTLS en DANE en WPA2 Enterprise geanalyseerd en zijn voorstellen gedaan voor duidelijker omschrijvingen die het oorspronkelijke functionele toepassingsgebied niet wijzigen.

IPv6 en IPv4, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, SAML, STARTTLS en DANE en WPA2 Enterprise zijn standaarden op het gebied van internet en beveiliging. Deze standaarden zijn al opgenomen op de lijst met open standaarden waarvoor een ‘pas toe of leg uit’-verplichting geldt.

Betrokkenen en proces
In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates voorstellen gedaan voor nieuwe, duidelijkere omschrijvingen van de functioneel toepassingsgebieden van de internet- en beveiligingsstandaarden. Parallel hieraan is een expertgroep samengesteld en een voorzitter aangesteld.

De expertgroep is op 30 november 2017 bijeengekomen om de voorgestelde omschrijvingen van de functioneel toepassingsgebieden te bespreken en verder te verduidelijken. Op basis hiervan is een concept expertadvies opgesteld en aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van de reacties uit de expertgroep, is het rapport nogmaals toegestuurd aan de experts en afgerond.

Het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) heeft het expertadvies openbaar gemaakt ten behoeve van een publieke consultatie. Deze publieke consultatie heeft plaatsgevonden van 23 februari 2018 tot en met 23 maart 2018. Gedurende de consultatieperiode zijn geen reacties op het expertadvies ontvangen.

Op basis van het expertadvies is dit Forumadvies opgesteld.

Consequenties en vervolgstappen
Indien het Forum Standaardisatie dit advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid voorlegt, kan het OBDO al dan niet besluiten om de omschrijvingen van de functioneel toepassingsgebieden van de internet- en beveiligingsstandaarden IPv6 en IPv4, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, SAML, STARTTLS en DANE en WPA2 Enterprise overeenkomstig aan te passen op de lijst met open standaarden.

Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies:

Het Forum Standaardisatie adviseert het Overheidsbrede Beleidsoverleg Digitale Overheid om:
1. de omschrijving van het functioneel toepassingsgebied van IPv6 en IPv4 aan te passen op de lijst met open standaarden;
2. de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27001 aan te passen op de lijst met open standaarden;
3. de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27002 aan te passen op de lijst met open standaarden;
4. de omschrijving van het functioneel toepassingsgebied van SAML aan te passen op de lijst met open standaarden;
5. de omschrijving van het functioneel toepassingsgebied van STARTTLS en DANE aan te passen op de lijst met open standaarden;
6. de omschrijving van het functioneel toepassingsgebied van WPA2 ENTERPRISE aan te passen op de lijst met open standaarden.

Ad 1) Aanpassen van de omschrijving van het functioneel toepassingsgebied van IPv6 en IPv4 op de lijst met open standaarden
Als functioneel toepassingsgebied voor IPv6 en IPv4 wordt geadviseerd:
IPv6 en IPv4 moeten in combinatie ('dual stack') worden toegepast op communicatie tussen toepassingen in (een) netwerk(en).

Ad 2) Aanpassen van de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27001 op de lijst met open standaarden
Als functioneel toepassingsgebied voor NEN-ISO/IEC 27001 wordt geadviseerd:
NEN-ISO/IEC 27001 moet worden toegepast op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en het vaststellen van het toepassingsgebied (de scope) van dit managementsysteem.

Ad 3) Aanpassen van de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27002 op de lijst met open standaarden
Als functioneel toepassingsgebied voor NEN-ISO/IEC 27002 wordt geadviseerd:
NEN-ISO/IEC 27002 moet worden toegepast op het formuleren van beheersmaatregelen inzake informatiebeveiliging, hierbij rekening houdend met de omgeving(en) waarin de informatiebeveiligingsrisico's gelden.

Ad 4) Aanpassen van de omschrijving van het functioneel toepassingsgebied van SAML op de lijst met open standaarden
Als functioneel toepassingsgebied voor SAML wordt geadviseerd:
SAML moet worden toegepast op de uitwisseling van authenticatie- en autorisatiegegevens om gebruikers na eenmalig inloggen toegang te geven tot meerdere diensten.

Ad 5) Aanpassen van de omschrijving van het functioneel toepassingsgebied van STARTTLS en DANE op de lijst met open standaarden
Als functioneel toepassingsgebied voor STARTTLS en DANE wordt geadviseerd:
STARTTLS en DANE moeten in combinatie worden toegepast op ontvangende e-mailservers.

Ad 6) Aanpassen van de omschrijving van het functioneel toepassingsgebied van WPA2 ENTERPRISE op de lijst met open standaarden
Als functioneel toepassingsgebied voor WPA2 ENTERPRISE wordt geadviseerd:
WPA2 Enterprise moet worden toegepast op het tot stand brengen van toegang tot WiFi-netwerken, met uitzondering van openbare netwerken voor gastgebruik.

Toelichting

1. Waar gaat het inhoudelijk over?
IPv6 en IPv4, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, SAML, STARTTLS en DANE en WPA2 Enterprise zijn standaarden op het gebied van internet en beveiliging.

2. Hoe is het proces verlopen?
In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates voorstellen gedaan voor nieuwe omschrijvingen van de functioneel toepassingsgebieden van de internet- en beveiligingsstandaarden IPv6 en IPv4, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, SAML, STARTTLS en DANE en WPA2 Enterprise. Parallel hieraan is een expertgroep samengesteld en een voorzitter aangesteld.

De leden van de expertgroep hebben voorafgaand aan de expertbijeenkomst een notitie met de voorgestelde omschrijvingen ontvangen en zijn in de gelegenheid gesteld om deze notitie door te nemen en aandachtspunten te identificeren.

De expertgroep is op 30 november 2017 bijeengekomen om de voorgestelde omschrijvingen van de functioneel toepassingsgebieden te bespreken en verder te verduidelijken. Op basis hiervan is een concept expertadvies opgesteld en aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van de reacties uit de expertgroep, is het rapport nogmaals toegestuurd aan de experts en afgerond.

Het Bureau Forum Standaardisatie heeft het expertadvies openbaar gemaakt ten behoeve van een publieke consultatie. Deze publieke consultatie heeft plaatsgevonden van 23 februari 2018 tot en met 23 maart 2018. Gedurende de consultatieperiode zijn geen reacties gegeven op het expertadvies.

Op basis van het expertadvies is dit advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid opgesteld.

3. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De expertgroep adviseert het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid om:
1. de omschrijving van het functioneel toepassingsgebied van IPv6 en IPv4 aan te passen op de lijst met open standaarden;
2. de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27001 aan te passen op de lijst met open standaarden;
3. de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27002 aan te passen op de lijst met open standaarden;
4. de omschrijving van het functioneel toepassingsgebied van SAML aan te passen op de lijst met open standaarden;
5. de omschrijving van het functioneel toepassingsgebied van STARTTLS en DANE aan te passen op de lijst met open standaarden;
6. de omschrijving van het functioneel toepassingsgebied van WPA2 ENTERPRISE aan te passen op de lijst met open standaarden.

Ad 1) Aanpassen van de omschrijving van het functioneel toepassingsgebied van IPv6 en IPv4 op de lijst met open standaarden
De expertgroep adviseert als functioneel toepassingsgebied voor IPv6 en IPv4:
IPv6 en IPv4 moeten in combinatie ('dual stack') worden toegepast op communicatie tussen toepassingen in (een) netwerk(en).

De expertgroep maakt de algemene kanttekening dat duidelijker naar voren moet worden gebracht dat de lijst met open standaarden geldt voor de elektronische uitwisseling van gegevens tussen overheidsorganisaties en bedrijven, tussen overheidsorganisaties en burgers en tussen overheidsorganisaties onderling (en dus niet voor elektronische uitwisseling van gegevens binnen overheidsorganisaties).

De expertgroep maakt de kanttekening dat de adoptie van IPv4 niet meer hoeft te worden gestimuleerd en dat deze standaard dus van de lijst met verplichte open standaarden kan worden gehaald. Hiervoor zal een andere procedure moeten worden gestart. De onderhavige procedure is bedoeld om de functioneel toepassingsgebieden te verduidelijken, niet om de inhoud van de verplichtingen te veranderen.

Ad 2) Aanpassen van de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27001 op de lijst met open standaarden
De expertgroep adviseert als functioneel toepassingsgebied voor NEN-ISO/IEC 27001:
NEN-ISO/IEC 27001 moet worden toegepast op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en het vaststellen van het toepassingsgebied (de scope) van dit managementsysteem.

De expertgroep maakt geen (aanvullende) kanttekeningen bij het functioneel toepassingsgebied van NEN-ISO/IEC 27001.

Ad 3) Aanpassen van de omschrijving van het functioneel toepassingsgebied van NEN-ISO/IEC 27002 op de lijst met open standaarden
De expertgroep adviseert als functioneel toepassingsgebied voor NEN-ISO/IEC 27002:
NEN-ISO/IEC 27002 moet worden toegepast op het formuleren van beheersmaatregelen inzake informatiebeveiliging, hierbij rekening houdend met de omgeving(en) waarin de informatiebeveiligingsrisico's gelden.

De expertgroep maakt geen (aanvullende) kanttekeningen bij het functioneel toepassingsgebied van NEN-ISO/IEC 27002.

Ad 4) Aanpassen van de omschrijving van het functioneel toepassingsgebied van SAML op de lijst met open standaarden
De expertgroep adviseert als functioneel toepassingsgebied voor SAML:
SAML moet worden toegepast op de uitwisseling van authenticatie- en autorisatiegegevens om gebruikers na eenmalig inloggen toegang te geven tot meerdere diensten.

De expertgroep maakt de kanttekening dat SAML veel verschillende implementatieprofielen kent. Zonder nadere afspraken, kunnen er verschillende implementaties ontstaan die niet interoperabel zijn. De lijst met open standaarden verwijst in dit verband naar het eGovernment SAML 2.0 Implementation Profile van het Kantara Initiative (bij 'Community en Organisaties' onder 'Implementatie').

De expertgroep maakt de kanttekening dat er standaarden bestaan met gedeeltelijk overlappende functionaliteit. Als voorbeelden worden genoemd OAuth 2.0 en Kerberos. De relatie met deze en andere standaarden kan worden verduidelijkt op de lijst met open standaarden (bij 'Relatie met andere standaarden' onder 'Implementatie').

De expertgroep maakt de kanttekening dat SAML ruimer kan en moet worden toegepast volgens de eIDAS verordening. Om het functioneel toepassingsgebied te veranderen, zal een andere procedure moeten worden gestart.

Ad 5) Aanpassen van de omschrijving van het functioneel toepassingsgebied van STARTTLS en DANE op de lijst met open standaarden
De expertgroep adviseert als functioneel toepassingsgebied voor STARTTLS en DANE:
STARTTLS en DANE moeten in combinatie worden toegepast op ontvangende e-mailservers.

De expertgroep maakt de kanttekening dat bij opname van STARTTLS en DANE op de lijst met open standaarden is geadviseerd om een jaar na opname te toetsen of het functioneel toepassingsgebied kan worden uitgebreid met verzendende e-mailservers. Hiervoor dient te zijner tijd opnieuw een expertgroep bijeen te worden gebracht.

Ad 6) Aanpassen van de omschrijving van het functioneel toepassingsgebied van WPA2 ENTERPRISE op de lijst met open standaarden
De expertgroep adviseert als functioneel toepassingsgebied voor WPA2 ENTERPRISE:
WPA2 Enterprise moet worden toegepast op het tot stand brengen van toegang tot WiFi-netwerken, met uitzondering van openbare netwerken voor gastgebruik.

De expertgroep maakt geen (aanvullende) kanttekeningen bij het functioneel toepassingsgebied van WPA2 Enterprise.

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies zijn geen reacties ontvangen.

Bijlage

- Expertadvies functioneel toepassingsgebieden internet- en beveiligingsstandaarden: https://www.forumstandaardisatie.nl/sites/default/files/FS/2018/0425/171_207-Expertadvies-toepassingsgebieden-IV-standaarden.pdf