Forum Standaardisatie

Expertadvies functioneel toepassingsgebieden internet- en beveiligingsstandaarden

Datum 7 december 2017

Colofon

Projectnaam	Expertadvies functioneel toepassingsgebieden internet- en beveiligingsstandaarden
Versienummer	0.2
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteur(s)	Rick van Rooijen (Verdonck Klooster & Associates)
Onafhankelijk voorzitter	Wilbert Enserink (Verdonck Klooster & Associates)

Inhoud

Samenvatting en Forumadvies

Advies aan het Forum

Dit expertadvies geeft de uitkomsten weer van de expertbijeenkomst over 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.

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).

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.
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.

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.

Als functioneel toepassingsgebied voor STARTTLS en DANE wordt geadviseerd:

STARTTLS en DANE moeten in combinatie worden toegepast op ontvangende e-mailservers.

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.

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.

Hoe is het proces verlopen?
De internet- en beveiligingsstandaarden zijn al opgenomen op de lijst met open standaarden waarvoor een 'pas toe of leg uit'-verplichting geldt. In opdracht van het Forum Standaardisatie heeft Verdonck, Klooster & Associates voorstellen gedaan voor nieuwe, duidelijkere omschrijvingen van de functioneel toepassingsgebieden van deze standaarden. Parallel hieraan is een expertgroep samengesteld en een voorzitter aangesteld. De experts zijn bijeengekomen om de voorgestelde omschrijvingen te bespreken en verder te verduidelijken. Dit expertadvies geeft de uitkomsten van de expertbijeenkomst weer.

Vervolg
Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 23 februari 2018 tot en met 23 maart 2018. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad op. Het Nationaal Beraad besluit met dit advies om de omschrijvingen van de functioneel toepassingsgebieden wel of niet aan te passen op de lijst met open standaarden.

1 Doelstelling expertadvies

1.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een 'pas toe of leg uit'-verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Nationaal Beraad Digitale Overheid (hierna Nationaal Beraad) besluit welke standaarden op deze lijst worden opgenomen. Het Nationaal Beraad baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

1.2 Doelstelling expertadvies

Dit document is een expertadvies voor 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 gericht aan het Nationaal Beraad en Forum Standaardisatie. De omschrijvingen van de functioneel toepassingsgebieden van deze standaarden zijn verduidelijkt in opdracht van het Forum Standaardisatie.

Doel van dit document is om het Nationaal Beraad te adviseren over 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. Deze standaarden zijn al opgenomen op de lijst met open standaarden waarvoor een 'pas toe of leg uit'-verplichting geldt.

1.3 Doorlopen proces

Voor het opstellen van dit document is de volgende procedure doorlopen:

1. 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.
2. 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.
3. De expertgroep is op 30 november 2017 bijeengekomen om de voorgestelde omschrijvingen van de functioneel toepassingsgebieden te bespreken en verder te verduidelijken.

Dit expertadvies geeft de uitkomst van de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde.

1.4 Vervolg

Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 23 februari 2018 tot en met 23 maart 2018. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad op. Het Nationaal Beraad besluit met dit advies om de omschrijvingen van de functioneel toepassingsgebieden wel of niet aan te passen op de lijst met open standaarden.

1.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft in dit geval naar een representatieve expertgroep met een vertegenwoordiging van hoofdzakelijk (publieke) gebruikers. De expertgroep heeft een onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Wilbert Enserink. Rick van Rooijen heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:
- Paddy Verberne, Gemeente 's-Hertogenbosch
- Harry Biersteker, Justitiële Informatiedienst
- Peter Smeenk, Justitiële Informatiedienst
- Haaino Beljaars, KING
- Joris Joosten, Logius
- Theo van Diepen, Logius
- John Stienen, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Willem Vegten, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- René van Rijn, Ministerie van Infrastructuur en Waterstaat
- Maarten Aertsen, NCSC
- Arjan de Jong, NCSC
- Martin Mulder, Provincie Groningen
- Ferdinand Nobibux, UWV
- Zarco Zwier, UWV

Han Zuidweg van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Toelichting standaarden

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.

1.7 Leeswijzer

Hoofdstuk 2 beschrijft de functioneel toepassingsgebieden (situaties waarin de standaarden functioneel gebruikt moet worden).

2 Functioneel toepassingsgebieden

De *instructie rijksdienst inzake de aanschaf van ICT-producten en ICT-diensten* verplicht overheidsorganisaties om relevante standaarden op de 'pas toe of leg uit'-lijst te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de 'pas toe of leg uit'-lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke organisaties moeten de standaard gebruiken) beschreven.

De hiernavolgende paragrafen geven het advies van de expertgroep voor de functioneel toepassingsgebieden van IPv6 en IPv4, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, SAML, STARTTLS en DANE en WPA2 Enterprise.

2.1 IPv6 en IPv4

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.

2.2 NEN-ISO/IEC 27001

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.

2.3 NEN-ISO/IEC 27002

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.

2.4 SAML

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.

2.5 STARTTLS en DANE

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.

2.6 WPA2 Enterprise

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.

2.7 Aanvullende adviezen

De expertgroep adviseert om de nummering van de elementen waaruit de omschrijving van een functioneel toepassingsgebied volgens de ideaaltypische syntactische structuur kan zijn opgebouwd, te gebruiken om aan te geven welke elementen uit de ideaaltypische syntactische structuur in de omschrijving van een functioneel toepassingsgebied zijn gebruikt.