FS-20131029.03D

Forum Standaardisatie

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

notitie

Toetsing 13 standaarden voor de lijst met gangbare standaarden

FORUM STANDAARDISATIE
Concept

Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	16 oktober 2013	**Versie**	0.9
Betreft:	Toetsing 13 standaarden voor de lijst met gangbare standaarden		

Achtergrond
In oktober 2012 besloot Forum Standaardisatie een onderzoek te laten uitvoeren naar de lijst met gangbare standaarden. Hierbij werd enerzijds gekeken of de lijst met gangbare standaarden geactualiseerd diende te worden en werd anderzijds geïnventariseerd welke standaarden mogelijk in aanmerking kwamen voor opname op de lijst. Uit dit onderzoek kwamen 14 kandidaat standaarden naar voren. Forum Standaardisatie heeft in februari 2013 besloten deze standaarden gelijktijdig te laten toetsen voor opname op de lijst met gangbare standaarden.

Hoe zijn de adviezen tot stand gekomen?
In mei & juni 2013 zijn de 14 kandidaat standaarden getoetst tegen de toetsingscriteria voor de lijsten met standaarden en is geverifieerd ,bij verschillende gebruikers van de standaarden, of deze daadwerkelijk als gangbaar te beschouwen zijn. Van 8 augustus tot 16 september zijn de resultaten van deze toetsing aangeboden ter openbare consultatie. De resultaten van de toetsing en de ontvangen consultatiereacties hebben geleid tot een positief opnameadvies voor negen standaarden. Eén advies om een kandidaat-standaard niet op te nemen en drie adviezen waarbij wordt geadviseerd de standaard wel op ten nemen, maar aanvullend een klein onderzoek te starten. Tot slot bleek bij één kandidaat standaard (txt) onvoldoende informatie beschikbaar om deze effectief te kunnen toetsen.

Zijn er risico's verbonden aan de keuze?
Nee. Met de opname van deze nieuwe standaarden wordt de lijst met gangbare standaarden geactualiseerd waardoor deze lijst meer waarde krijgt als informatiebron m.b.t. gangbare standaarden. Voor de lijst met gangbare standaarden geldt geen verplichtend karakter.

Gevraagd besluit

Datum
17 oktober 2013

1) College standaardisatie wordt gevraagd in te stemmen met de opname van de volgende standaarden op de lijst met gangbare standaarden:

- **ASN.1** (Uitwisseling van gegevens in computernetwerken)
- **ISO4217** (Codes voor het weergeven van valuta's)
- **JSON** (Javascript object notatie)
- **MTOM** (versturen van grote hoeveelheden data van en naar webservices)
- **RDF** (Gestructureerde beschrijving (bron)gegevens voor linken van data)
- **XMI2.x** (Standaard voor uitwisseling van metadata via XML)
- **SSH-2** (Cryptografisch netwerkprotocol)
- **X509** (Authenticatie middels certificaten op het internet)
- **ETSI TS 102 176-1** (Creëren van hashes op berichten voor een elektronische handtekening)

Toelichting

Voor bovenstaande standaarden geldt dat zij voldoen aan de criteria die gelden voor opname op de lijst met gangbare standaarden. Aanvullend de gangbaarheid van deze standaarden bevestig door verschillende organisaties en ondersteunen de ontvangen consultatiereactie de opname van de standaarden.

2) College standaardisatie wordt gevraagd in te stemmen met de opname van de volgende standaarden op de lijst met gangbare standaarden en het gegeven aanvullende advies.

- **AES** (Encryptie standaard)

  Met het aanvullende advies aan het Forum om in de toekomt te onderzoeken wanneer het opportuun is om de verouderde voorloper van deze standaard DES van de lijst te verwijderen.

- **Genericode** (Eenduidig definiëren van codelijsten)

  Met het aanvullende advies aan het Forum om te bekijken of bekende gangbare alternatieven voor deze standaard: VDEX en SKOS, ook moet worden opgenomen en hoe de toepassingsgebieden van deze standaarden zich tot elkaar verhouden.

  Vooralsnog zal bij de opname van Genericode op de lijst melding worden gemaakt van het bestaan de alternatieve standaarden.

- **ISO3166-1** (Codes voor het weergeven van landen)

  Met het aanvullende advies aan het Forum om bij de opname van deze standaard te vermelden dat in verschillende domeinen lijsten met alternatieve landcodetabellen worden gebruikt. Dit zodat potentiële gebruikers weten welke alternatieve gangbaar zijn in welke specifieke domeinen.

Toelichting

Voor bovenstaande standaarden geldt dat zij voldoen aan de criteria die gelden voor opname op de lijst met gangbare standaarden. Aanvullend de gangbaarheid van deze standaarden bevestig door verschillende organisaties en ondersteunen de ontvangen consultatiereactie de opname van de standaarden.

Uit de consultatie is evenwel naar voren gekomen dat een klein aanvullend onderzoek meer duidelijkheid kan verschaffen op de vraag hoe de standaard zich verhoudt tot gangbare alternatieven en in welke situatie deze standaard of het alternatief het best kan worden toegepast.

3) College standaardisatie wordt gevraagd in te stemmen met het niet opnemen van de volgende standaard.

- **ISO Schematron** (Standaard voor XML validatie)

Toelichting

Schematron wordt in samenhang met overige reeds opgenomen standaarden in specifieke gevallen gehanteerd. Zelfstandige opname van de standaard heeft weinig toegevoegde waarde voor interoperabiliteit. Beter wordt bij de overige relevante gangbare standaarden (XML) verwezen naar de optie om via Schematron te valideren.

Niet te toetsen

Voor één van de 14 kandidaat standaarden bleek niet mogelijk om details m.b.t. de specificaties en het beheer daarvan te achterhalen, waardoor deze standaard niet getoetst kon worden. Het gaat om de txt standaard (plain tekst).

Over de standaarden

Datum
17 oktober 2013

De AES standaard

De AES-standaard is een versleutelingstechniek voor de bescherming van de vertrouwelijkheid van de opgeslagen en verzonden data. Het is de winnaar van een wereldwijde wedstrijd van het NIST om tot een nieuwe AES (Advanced Encryption Standard) te komen die de verouderde standaard DES zou vervangen.

AES wordt zowel binnen Nederland als wereldwijd zeer veel en op, op zeer veel verschillende wijzen gebruikt. Voorbeelden van het gebruik zijn:

1. In programma's zoals WinRAR, WinZip, PowerArchiver, e.d. wordt AES als encryptie aangeboden.
2. AES wordt toegepast voor beveiliging (WPA2) in draadloze netwerken (Wifi), zie IEEE 802.11i.
3. AES wordt toegepast voor het versleutelen van gegevens voor verzending over het internet, https verkeer etc.
4. In hardware voor netwerken wordt veelvuldig gebruikt gemaakt van AES.

De ASN.1 standaard

Abstract syntax notation one (ASN.1). ASN.1 wordt veel gebruikt voor het beschrijven van X.509 certificaten en de toepassing ervan. Voorbeeld van een toepassing is RSA public key voor beveiliging van het transactieverkeer in de elektronische handel. Hiernaast beschrijft deze standaard rollen en structuren om data in telecommunicatie en computer netwerken te representeren, te coderen, over te brengen en te decoderen. Hierdoor is het mogelijk grote hoeveelheden gegevens geautomatiseerd te valideren aan de hand van specificaties met behulp van software tools

De Genericode standaard

Genericode is een standaard formaat voor het definiëren van codelijsten. De standaard biedt een model en XML representatie voor ten eerste de inhoud van een codelijst, ten tweede data die gerelateerd zijn aan de items op de codelijst en ten derde voor hoe nieuwe codelijsten worden afgeleid van bestaande codelijsten. Het model bestaat uit o.a. een tabelstructuur voor de codelijst informatie, document typen, sleutels en metadata.
Binnen de Nederlandse overheid wordt Genericode gebruikt binnen DigiInkoop.

De ISO 3166-1 standaard

ISO 3166-1:2006 is een overzicht van codes voor de weergave van landnamen en hun onderverdelingen. De norm legt alle landen van de wereld vast met unieke tweeletterige (alpha-2) landcodes, drieletterige (alpha-3) landcodes en driecijferige (numeric-3) landcodes.
Voorbeeld: Nederland – NL – NLD – 528.

De Schematron standaard

De ISO/IEC 19757-3 Rule-based validation (Schemtron) standaard is een taal die gebruikt kan worden om inhoud en structuur van XML documenten te valideren in interfaces. Als het om afhankelijkheden van gegevens onderling gaat, om aanvullende beperkingen van het gebruik van vocabulaire of proces-georiënteerde regels is de W3C schemataal niet meer voldoende. Om deze redenen worden ter ondersteuning van leveranciers (doel- of bronsystemen) schematron's ter beschikking gesteld.

De ETSI TS 102 176-1 standaard
De ETSI TS 102 176-1 standaard definieert algoritmes en sleutellengtes. De algoritmes worden gebruikt voor het plaatsen van een hash over een document of transactie en is de eerste stap naar de elektronische ondertekening van een bericht.Hiernaast geeft deze standaard een beschrijving van andere aspecten zoals algoritmen en methoden voor "Signature schemes" , "Key pair generation" en "Random number generation".

Binnen Nederland is deze standaard een onderdeel van PKI Overheid, internationaal ondersteund door o.a. Deutsche Telekom AG, SNG, Telenor, Uninfo.

De ISO 4217 standaard
De ISO 4217 standaard is een internationale standaard die drielettercodes definieert voor valuta. De eerste twee letters zijn doorgaans de letters van de ISO 3166-1 landcode (meestal gelijk aan de 2-letter topleveldomein-internetcode), gevolgd door de eerste letter van de betreffende munt. De code is ontworpen voor gelijkwaardige geschiktheid voor handmatige gebruikers en voor het gebruik van geautomatiseerde systemen. Voorbeelden zijn de euro, ISO code EUR, en Brits Pond Sterling GBP.

De JSON standaard
JSON (JavaScript Object Notation) is een deelverzameling van de programmeertaal JavaScript. Het wordt gebruikt voor het uitwisselen van datastructuren, met name in webapplicaties die asynchroon gegevens ophalen van de webserver. De eenvoud van JSON heeft geleid tot een grote populariteit ervan, met name als een 'light' alternatief voor XML.

De MTOM standaard
Message Transmission Optimization Mechanism of kortweg MTOM (een W3C-standaard) is een methode om op efficiënte wijze binaire data naar en van webservices te versturen.

MTOM wordt gebruikt voor het efficiënt verzenden van grote hoeveelheden data (bijvoorbeeld attachments) in SOAP-berichten. MTOM wordt bijvoorbeeld gebruikt in Digikoppeling in combinatie met WUS, in de online registratie bij KvK, en het Aktenverkeer met Notarissen.

De RDF standaard
De RDF-standaard (Resource Description Format) is een formaat om gegevens voor te stellen en uit te wisselen. Met het RDF-model worden uitspraken gedaan over de kenmerken van bronnen op het web (resources) in de vorm van een drieledige subject-predicaat-object-structuur (in RDF-termen een triple). Het subject is in essentie de resource die beschreven wordt. Het predicaat is welk kenmerk of aspect van die bron beschreven wordt. Het object tenslotte is wat de waarde van dat kenmerk is. Overheden die gegevens gestructureerd ter beschikking willen stellen kunnen RDF hiervoor gebruiken zodat zijzelf of overige partijen (geautomatiseerd) deze gegevens kunnen koppelen.
De standaard wordt door meerdere overheden gebruikt, waaronder RCE, Informatiehuiswater en Kennisnet. Wereldwijd wordt de standaard door een zeer groot aantal partijen gebruikt.

Datum
17 oktober 2013

De SSH-2 standaard
SSH-2 is een cryptografisch netwerk protocol dat het mogelijk maakt om op een versleutelde manier in te loggen op een andere computer, op afstand commando's op de andere computer uit te voeren via een shell en andere veilige network services tussen 2 netwerk computers te laten werken die via een secure channel over een onbeveiligd netwerk communiceren. Omdat SSH met encryptie werkt, is het voor eventuele afluisteraars, die de (internet)verbinding aftappen, zo goed als onmogelijk om wachtwoorden of commando's te achterhalen.

De X.509- standaard
De X.509-standaard (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) beschrijft een systeem van certificaten met een beperkte levensduur en de wijze waarop de intrekking van deze certificaten in een zogenaamde Blacklist (de CRL) geregeld wordt. Elke gebruiker kan op deze manier via bijvoorbeeld zijn browser verifiëren of het certificaat dat gebruikt wordt voor de beveiligde koppeling nog valide is of ingetrokken is. De standaard wordt zowel binnen Nederland als wereldwijd zeer veel gebruikt. De standaard is belangrijk onderdeel in de communicatie tussen de overheid met burgers en bedrijven, en is een integraal component voor PKIoverheid.

Bijlagen:

Expertadviezen: https://lijsten.forumstandaardisatie.nl/lijsten/open-standaarden?terms=&lijst=All&status%5B%5D=In+behandeling+%26gt%3B+In+afwachting+van+Forum