VERDONCK KLOOSTER & ASSOCIATES

UPDATE AANBEVOLEN STANDAARDEN

Advies voor actualisatie van de lijst open standaarden

UPDATE AANBEVOLEN STANDAARDEN

Advies voor actualisatie van de lijst open standaarden

Martijn Hunsche

DATUM	03 augustus 2016
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20152306
INTERNE TOETS	Paul Dam

MANAGEMENTSAMENVATTING

Voorliggende rapportage is het resultaat van een onderzoek naar de aanbevolen standaarden op de lijst. Het resultaat is een advies aan het Forum Standaardisatie om oude versies te vervangen door nieuwe versies van standaarden en het laten vervallen van een aantal standaarden. De scope van het onderzoek betrof alle aanbevolen standaarden op de lijst. De resultaten van het separate onderzoek naar beveiligingsstandaarden zijn in dit document meegenomen. Onderstaande tabel is een samenvatting van de geadviseerde wijzigingen. Voorgestelde wijzigingen zijn in **vet** aangeduid.

Standaard	Huidige versie	Nieuwe versie	Advies
Internet- en beveiligingsstandaarden			
ASN.1	**ISO/IEC 8824-1:2008**	**ISO/IEC 8824-1:2015**	**Update**
ETSI TS 102 176-1	**v2.0.0 (nov 2007)**	**v2.1.1 (jul 2011)**	**Update**
HTML	**v4.01**	**v5 (okt 2014)**	**Update**
HTTP	**v1.1 (RFC 7230)**	**v1.1 (RFC 7230) en v2 (RFC 7540)**	**Update**
HTTPS en HSTS	**v1.1 (RFC 2818, 1 mei 2000)**	**v1.1 (RFC 2818, 1 mei 2000) RFC 6797**	**Update**
IPsec	**RFC 4301 (1 dec 2005)**	**RFC 4301 (1 dec 2005)**	**Update tekst**
NTP	**v3 (RFC 1305)**	**v4 (RFC 5905)**	**Update**
POP3	**v3 (RFC 1939)**	**~~v3 (RFC 1939)~~**	**Verwijderen**
SHA-2	**FIPS PUB 180-3 (okt 2008)**	**FIPS PUB 180-3 (aug 2015)**	**Update**
SIP	**v2 (RFC 3261, 1 jun 2002)**	**v2 (RFC 3261, 1 jun 2002)**	**Update tekst**
URI en IRI	**RFC 2396 (1 aug 1998)**	**RFC 3986 STD 66 (Jan 2005)**	**Update**
URL	**RFC 2717 (1 nov 1999)**	**~~RFC 2717 (1 nov 1999)~~**	**Verwijderen**
URN	**RFC 2141 (mei 1997)**	**~~RFC 2141 (mei 1997)~~**	**Verwijderen**
VCF	**RFC 2425 (1 sep 1998)**	**RFC 6350 (aug 2011)**	**Update**
WSDL	**v1.1**	**v2.0 (jun 2007)**	**Update**
X509	**v3 (RFC 5280, mei 2008)**	**v3 (RFC 5280, mei 2008)**	**Update tekst**
XSLT	**v1.0 (16 nov 1999)**	**~~v1.0 (16 nov 1999)~~**	**Verwijderen**
AES	FIPS PUB 197 (21 nov 2001)	FIPS PUB 197 (21 nov 2001)	
LDAP	v3 (RFC 4511, jun 2006)	v3 (RFC 4511, jun 2006)	
UDDI	v3.0.2	v3.0.2	
MTOM	MTOM jan 2005 (SOAP v1.2)	MTOM jan 2005 (SOAP v1.2)	
NNTP	RFC 3977 (1 okt 2006)	RFC 3977 (1 okt 2006)	
RTP	RFC 3550 (1 juli 2003)	RFC 3550 (1 juli 2003)	
SMTP	RFC 5321 (1 okt 2008)	RFC 5321 (1 okt 2008)	
SNMP	v3 (STD0062, 01 dec 2002)	v3 (STD0062, 01 dec 2002)	

SOAP	v1.2	v1.2	
SSH-2	RFC 4251: 2006.	RFC 4251: 2006.	
TCP/IP	Dec 1974 / sep 1981	Dec 1974 / sep 1981	
UDP	RFC 768 (1 aug 1980)	RFC 768 (1 aug 1980)	
UTF-8	RFC 3629 STD63 (1 nov 2003)	RFC 3629 STD63 (1 nov 2003)	
XML	v1.0 (26 nov 2008)	v1.0 (26 nov 2008)	
CSS	v2.1	v2.1	
DHCP	RFC 2131 (1 mrt 1997)	RFC 2131 (1 mrt 1997)	
DNS	RFC 1035 (1 nov 1987)	RFC 1035 (1 nov 1987)	
FTP	RFC 959 (1 okt 1985)	RFC 959 (1 okt 1985)	
IMAP	v4, rev 1 (RFC 3501 mrt 2003)	v4, rev 1 (RFC 3501 mrt 2003)	
IPP	v1.1 (RFC 2911)	v1.1 (RFC 2911)	
E-facturatie- en administratiestandaarden			
EI standaarden	**Div berichten**	**Update/extra berichten**	**Update**
NEN-ISO 4217	**NEN-ISO 4217:2008**	**NEN-ISO 4217:2015**	**Update**
SQL	**ISO/IEC 9075:2008**	**ISO/IEC 9075:2011**	**Update**
XMI 2.x	**v2.4.1 (aug 2011)**	**v2.5.1 (juni 2015)**	**Update**
Documenten- en (web)contentstandaarden			
IPM	**v4.0**	**~~v4.0~~**	**Verwijderen**
JSON	**RFC 4627 (Jul 2006)**	**RFC7159 (mrt 2014)**	**Update**
RDF	**v1 (10 feb 2004)**	**v1.1 (feb 2014)**	**Update**
SLD	**v1.0**	**v1.1.0 (jul 2012)**	**Verwijderen**
SVG	v1.1 SE (aug 2011)	v1.1 SE (aug 2011)	
CSV	RFC 4180 (1 okt 2005)	RFC 4180 (1 okt 2005)	
MIME	RFC 2045	RFC 2045	
Genericode	v1.0	v1.0	
iCalendar	RFC 5545 (1 nov 1998)	RFC 5545 (1 nov 1998)	
Overige standaarden			
ISO 3166-1	**ISO 3166-1:2006 Landcodes**	**ISO 3166:2013**	**Update**
Datum en tijd	ISO 8601:2004	ISO 8601:2004	

INHOUDSOPGAVE

1 INLEIDING

1.1 Aanleiding

Het Forum Standaardisatie beheert de lijst met ICT-standaarden ter bevorderingen van interoperabiliteit tussen informatiesystemen en uitwisselbaarheid van ICT-leveranciers. De lijst ondersteunt (semi-) overheidsinstellingen in de keuze bij aanschaf, beheer en/of realisatie van ICT-voorzieningen. De lijst bestaat uit verplicht toe te passen standaarden, de zogenaamde 'pas toe of leg uit'-verplichting, en aanbevolen standaarden die worden aangeraden maar niet verplicht zijn.

Gezien de snelle ontwikkelingen in de ICT vergt de lijst regelmatig onderhoud, 'updaten', in de zin van aanvulling, aanpassing dan wel opschoning van standaarden.

1.2 Doel

Voorliggende rapportage is het resultaat van een onderzoek naar de aanbevolen standaarden op de lijst en bevat een advies voor aanpassing. Aanpassingen zijn nieuwere versies van standaarden of standaarden die van de lijst af kunnen.

Aanvullingen op de lijst met standaarden die nu nog niet op de lijst staan, worden separaat onderzocht en in een separaat document opgenomen.

1.3 Scope

Voor update van de lijst werd tot nu toe vooral gekeken naar meer volwassen standaarden, die al langere tijd zijn vastgesteld en die regulier worden gebruikt in de praktijk, en standaarden die achteraan in de levenscyclus zitten (vergelijk 'Hype cycle' van Gartner) waarvoor mogelijk al kandidaten zijn die in toekomst de standaard opvolgen/vervangen.

Het Forum Standaardisatie heeft geconcludeerd dat het in de update van de aanbevolen standaarden op de lijst ook verstandig is om standaarden mee te nemen die nog eerder in de levensfase zitten: denk aan standaarden die wel zijn vastgesteld maar nog niet regulier/breed gebruikt worden en veelbelovend zijn in toepassing in de nabije toekomst.

Scope van het onderzoek is een update van de aanbevolen standaarden op de lijst met duiding van kandidaat standaarden, zowel volwassen als meer prematuur in de levenscyclus, en overbodige/verouderde standaarden.

Parallel aan dit onderzoek loopt een uitgebreid onderzoek specifiek op het gebied van beveiligingsstandaarden. De resultaten daarvan zijn in dit document meegenomen.

1.4 Aanpak

Voor dit onderzoek is gebruik gemaakt van openbare bronnen op het internet. Per standaard is gezocht naar wijzigingen op basis van beschrijving en verwijzing van de huidige standaard en

versie. Bronnen zijn vluchtig beoordeeld op toegankelijkheid van de informatie zoals beschreven in de 'Toetsingsprocedure en criteria'[1] van het Forum Standaardisatie. Bronnen die op het eerste gezicht niet voldoen aan criteria als 'drempelvrij' of 'royalty free' dan wel een beperkt geografische spreidingsgebied kennen, zijn niet meegenomen.

Voor standaarden die worden beheerd door de IETF is gecontroleerd of de huidige standaard de status 'obsoleted' (overbodig) heeft, en zo ja, door welke nieuwere versie deze is vervangen. Aanvullende standaarden of updates van delen van de standaard zijn niet meegenomen, zolang de oorspronkelijke standaard niet 'obsoleted' is. Een standaard is als overbodig betiteld als deze is vervangen door een andere standaard.

1.5 Leeswijzer

Na deze inleiding worden wijzigingen op de aanbevolen standaarden in hoofstukken 2 tot en met 5 toegelicht voor de categorieën 1) Internet- en beveiligingsstandaarden, 2) E-facturatie- en administratiestandaarden, 3) documenten en (web)content en 4) overige.

[1] https://www.forumstandaardisatie.nl/content/toetsen-van-standaarden

2 INTERNET- EN BEVEILIGINGSSTANDAARDEN

De (sub)categorie *Beveiliging* is buiten scope van dit onderzoek.

2.1 ASN 1

Over de standaard
Abstract syntax notation one (ASN.1) beschrijft de rollen en structuren om data in telecommunicatie en computernetwerken te representeren, te coderen, over te brengen en te decoderen. Dit ongeacht de taal en de data representatie en ongeacht de applicatie waarin het gebruikt wordt. Hierdoor is het mogelijk grote hoeveelheden gegevens geautomatiseerd te valideren aan de hand van specificaties met behulp van software tools. De standaard wordt met name gebruikt in relatie tot X.509 (PKI) standaarden. ASN 1 is verkrijgbaar als ISO standaard onder de naam: ISO/IEC 8824:1 of NEN-ISO/IEC 8224:1.

Aanbeveling
Op de lijst met standaarden staat een oude versie uit 2008. Ondertussen is er een nieuwe versie uit 2015. Het wordt aanbevolen om de versie te updaten.

Toelichting
Deze vijfde editie van de standaard is technisch geheel geüpdate en vervangt de 2008 versie en de correcties op deze versie uit 2012 en 2014.

Relatie met andere standaarden
Er is met name een relatie met de X509 standaard. ASN.1 wordt veel gebruikt voor het beschrijven van X.509 certificaten en de toepassing ervan. X.509 is de standaard voor een public key infrastructure (PKI). Voorbeeld van een toepassing is RSA public key voor beveiliging van het transactieverkeer in de elektronische handel.

Referenties
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=68350 of bij het NEN via: https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-882412015-en.htm

2.2 ETSI TS 102 176-1

Over de standaard
ETSI TS 102 176-1 (Electronic Signatures and Infrastructures) 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 en internationaal wordt deze standaard ondersteund door onder andere Deutsche Telekom AG, SNG, Telenor en Uninfo.

Aanbeveling
Update van standaard*:* **v2.0.0 (nov 2007)→ v2.1.1 (jul 2011)**.

Toelichting
Aanpassingen naar aanleiding van de laatste stand van zaken van cryptografie. SHA-1 is niet meer aanbevolen. RIPEMD-160 is niet meer aanbevolen en RSA1024 is ook niet meer aanbevolen. Deze worden als onveilig beschouwd.

Relatie met andere standaarden
Relatie met veel cryptostandaarden vanuit de aanbevelende achtergrond van de standaard.

Referenties
https://archive.org/details/etsi_ts_102_176-1_v02.01.01

2.3 HTML

Over de standaard
HTML (HyperText Markup Language) is een taal waarmee vastgelegd kan worden hoe webpagina's opgemaakt moeten worden. HTML maakt het mogelijk om de structuur van een tekst gebaseerd document te beschrijven door links, hoofdstukken, paragrafen, lijsten enz. aan te geven.

Aanbeveling
Update van standaard: **versie 4.01 → versie 5**.

Toelichting
De nieuwe versie van standaard HTML 5 bevat functionaliteit van zowel HTML als XHTML, verbetert kleine foutjes van de eerdere versie en levert betere ondersteuning voor webapplicaties.

Relatie met andere standaarden
- JSON: standaard voor het uitwisselen en opslaan van HTML-data.
- SVG: standaard voor presentatie van schaalbare graphics in HTML-webpagina's.
- JavaScript: standaard voor extra/aanvullende functionaliteit op HTML-webpagina's.
- XML: specifieke syntax voor HTML-webpagina's, gebuikt in XHTML.
- CSS: standaard voor definitie van opmaak (presentatie) van HTML-webpagina's.
- Webrichtlijnen: set van richtlijnen voor het maken van HTML-webpagina's.

Referenties
http://www.w3.org/TR/html5/

2.4 HTTP

Over de standaard
Hypertext Transfer Protocol (HTTP) is hét protocol voor communicatie tussen een webclient (zoals een browser) en een webserver. HTTP ondersteunt gegevensuitwisseling over datacommunicatienetwerken gebruikmakend van TCP. Het is een protocol voor gedistribueerde, samenwerkende, hypermedia informatiesystemen. De standaard kan worden gebruikt voor vele doeleinden naast het uitwisselen van hypertext. Versie 1.1 staat op de lijst. De nieuwe versie HTTP/2 is een alternatief voor HTTP/1.1, maar vervangt deze niet. HTTP/2 biedt met name verbeteringen ten behoeve van de snelheid waarmee (interactieve) webpagina's geladen en gebruikt kunnen worden.

Doordat een aantal makers van webbrowsers hebben aangegeven dat zij HTTP/2 alleen ondersteunen in combinatie met TLS, is de facto sprake van gebruik van HTTPS. Dit is ook gelijk het grote voordeel van http/2 ten opzichte van http/1.1

Aanbeveling
Naast versie HTTP/1.1 op de lijst ook versie HTTP/2 opnemen.

Toelichting
Versie HTTP/1.1 is nog zeer gangbaar en eenvoudiger, maar versie HTTP/2 biedt voor gevallen waar de snelheid van het laden en gebruiken van (interactieve) webpagina's van belang is, ten behoeve van de gebruikerservaring, meer en betere functionaliteit. HTTP/2 is backwards compatibel aan versie 1.1. en worden ondersteund door de meeste webbrowsers.

Relatie met andere standaarden
TLS: de standaard ondersteunt tevens gegevensuitwisseling over TLS (voor HTTPS URI's), gangbare webbrowsers ondersteunen zelfs HTTP/2 alleen in combinatie met TLS.
TCP: de standaard maakt gebruik van TCP als onderliggend transportprotocol.

Referenties
HTTP/1.1: https://tools.ietf.org/html/rfc7230
HTTP/2: https://tools.ietf.org/html/rfc7540

2.5 HTTPS en HSTS

Over de standaard
De HTTPS-standaard (HTTP Strict Transport Security) legt vast hoe het HTTP-protocol beveiligd kan worden door gebruikmaking van TLS. Hierdoor is een beveiligde verbinding over het internet mogelijk. Dit is de meest gangbare praktijk om communicatie met websites te beveiligen.

Het advies is HTTPS altijd te gebruiken met HTTP Strict Transport Security (HSTS), om deze reden is ervoor gekozen om deze standaarden gezamenlijk in aanmerking te laten komen voor opname op de lijst met open standaarden. HSTS zorgt ervoor dat de browser voor elke terugkerende bezoeker vereist dat de website opnieuw via HTTPS wordt aangeboden. Dit helpt man-in-the-middle-aanvallen te voorkomen.

Aanbeveling
Toevoegen aan HTTPS de aanbeveling altijd HSTS te gebruiken (RFC 6797). Op de hoogte stellen van de updates: RFC 5785 en RFC 7230.

Toelichting
De update RFC 5785 gaat over het definiëren van Well-Known Uniform Resource Identifiers. RFC 7230 is een aanpassing van het HTTP-protocol. Met name URI schema requirements, de HTTP message syntax, passing requirements en related security concerns.

Het is van belang dat altijd gebruik gemaakt wordt van HTTPS in combinatie met HSTS. Het Nationaal Cyber Security Centrum (NCSC) heeft dit opgenomen in de ICT-beveiligingsrichtlijnen. Om de inzet van TLS binnen HTTPS nog meer te kunnen ondersteunen is de extra aanbeveling om de volgende veilige varianten van mail toegangsprotocollen op te nemen als toelichting bij TLS op de lijst met open standaarden (ieder versleuteld protocol zou opgenomen moeten worden als toelichting):

- Simple Mail Transfer Protocol Secure (SMTPS): zorgt voor authenticatie van de communicatiepartners en daarnaast voor data integriteit en vertrouwelijkheid.
- Internet Message Access Protocol over TLS (IMAPS): veilig synchroniseren van e-mail.
- Post Office Protocol 3 (SSL-POP3): veilig e-mailverkeer via de server.

Relatie met andere standaarden
SAML, TLS, SOAP, HTTP.

Referenties
HTTPS: https://tools.ietf.org/html/rfc2818
HSTS: https://tools.ietf.org/html/rfc6797

2.6 IPsec

Over de standaard
IPsec definieert een basisarchitectuur voor het toevoegen van services op het gebied van security voor de IP-laag. Het kan zowel in IPv4-omgevingen als in IPv6-omgevingen gebruikt worden.

Aanbeveling
Toelichting opnemen op de lijst over de aanvullingen op de al opgenomen RFC 4301. De aanvullingen betreffen RFC 6040 en RFC 7619.

Toelichting
RFC 6040 omvat de behandeling van signalen in het geval als er verstopping optreedt. RFC 7619 is een 0-authenticatie methode in IKE versie 2 die gebruikt kan worden om opportunistische encryptie mogelijk te maken.

Vooral relevant voor VPN's. In andere gevallen is beveiliging op transport niveau meer toepasselijk. Het voordeel van vercijfering op IP niveau is dat er geen applicaties hoeven te worden gewijzigd.

Relatie met andere standaarden
AES, SHA-2, IPv6 en IPv4.

Referenties
https://tools.ietf.org/html/rfc4301
https://tools.ietf.org/html/rfc6040
https://tools.ietf.org/html/rfc7619

2.7 NTP

Over de standaard
Network Time Protocol (NTP) specificeert een protocol dat het mogelijk maakt om de tijd te synchroniseren en om de distributie van de tijd te coördineren in grote, diverse internetverbindingen met verschillende snelheden.

Aanbeveling
Update van standaard: **versie 3 → versie 4** (RFC5905).

Toelichting
De nieuwe versie van standaard NTP 4 bevat aanpassingen op de vorige versie met o.a. hogere nauwkeurigheid, ondersteuning van IPv6, dynamische server discovery, herstel van foutjes in de vorige versie en is backward compatible versie 3 en versie 2 van NTP.

Relatie met andere standaarden

-

Referenties

http://datatracker.ietf.org/wg/ntp/documents/
http://www.ntp.org/index.html
http://tools.ietf.org/html/rfc5905

2.8 POP3

Over de standaard

Post Office Protocol 3 (POP3) is een internetstandaard voor het overbrengen van e-mail van een server naar een cliënt over een TCP/IP-verbinding.

Aanbeveling

Verwijderen van de standaard: **versie 3**.

Toelichting

POP3 is een veelgebruikte standaard, maar kent een beter alternatief in standaard IMAP. Functioneel verschilt IMAP van POP3 er in dat IMAP de e-mailberichten op de server laat staan. De e-mailberichten blijven met IMAP beschikbaar voor meerdere clients (devices). POP3 haalt het e-mailbericht over naar de client en verwijdert het bericht op de e-mailserver. Daarmee is het e-mail bericht niet meer beschikbaar voor andere devices. Met de hoge penetratiegraad van smartphones en tablets, naast laptops en PC's, beschikken mensen vaak over meerdere verschillende devices die ook naast elkaar worden gebruikt voor activiteiten als e-mail en surfen. POP3 ondersteunt dit karakteristieke gebruik van meerdere verschillende devices voor dezelfde e-mailbox niet.

Relatie met andere standaarden

- IMAP: standaard voor bekijken van e-mail op de server over een TCP/IP-verbinding
- MIME: standaard voor uitbreiden van karakterset in e-mailberichten
- SMTP: standaard voor het uitwisselen van e-mailberichten
- TLS: standard het versleutelen van een TCP/IP verbinding voor het veilig versturen van e-mailberichten.

Referenties

https://tools.ietf.org/html/rfc1939

2.9 SHA-2

Over de standaard

SHA-2 (Secure Hash Algorithm 2) behoort tot de zogenaamde cryptografische hash algoritmen die uit een willekeurige hoeveelheid gegevens (bijvoorbeeld een stuk tekst) een unieke vingerafdruk

(van een vaste vooraf vastgestelde lengte) kunnen genereren. Een wijziging in de gegevens zal leiden tot een wijziging in de vingerafdruk. Bovenstaande eigenschappen maken dat deze algoritmen bij uitstek geschikt zijn voor het gebruik in bepaalde beveiligingstoepassingen, zoals een elektronische handtekening.

Aanbeveling
Update van standaard: **FIPS PUB 180-3 (okt 2008) → FIPS PUB 180-4 (aug 2015)**.

Toelichting
SHA-0 is volstrekt onveilig, SHA-1 wordt inmiddels ook breed als onveilig beschouwd en dient niet meer te worden gebruikt. SHA-2 is momenteel de gangbare standaard, in diverse varianten met verschillende lengtes van de hash, bijvoorbeeld SHA-256 en SHA-512. SHA-3 heeft een heel nieuw algoritme en is recent als FIPS 202 gepubliceerd.

Relatie met andere standaarden
DKIM, IPsec, DNSSEC, SAML.

Referenties
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

2.10 SIP

Over de standaard
Session Initiation Protocol (SIP) is een protocol om multimediacommunicatie (audio-, video- en andere datacommunicatie) mogelijk te maken en wordt onder meer gebruikt voor Voice over IP (VoIP). Het protocol is qua ambities vergelijkbaar met H.323 waarbij SIP meer uit de Internet/IETF-hoek komt terwijl H.323 meer uit de telefonie/ITU-T-hoek komt. SIP kent overeenkomsten met andere internetprotocollen zoals HTTP en SMTP.

Aanbeveling
Het updaten van tekst bij huidige standaard, zie toelichting.

Toelichting
[Huidige tekst website] De SIP standaard specificeert een protocol op de applicatielaag die gebruikt kan worden voor het opzetten, aanpassen en afsluiten van sessies met één of meerdere deelnemers. Sessie kunnen onder andere telefoongesprekken over het internet, multimedia distributie en multimedia uitzendingen zijn. In de praktijk wordt dit protocol veel gebruik voor VOIP (Voice over IP) applicaties, in veel gevallen bellen over het internet.

[Aanvullende tekst] SIP wordt als opvolger van H.323 breed ondersteund door leveranciers, niet in de laatste plaats door de minder complexe implementatie (in vergelijking met H.323). SIP is een

standaard die in de implementatie van producten van leveranciers nog veel vrijheid laat. Dit heeft geleid tot een grote variëteit in implementaties van de SIP-standaard. In de praktijk blijkt dat SIP-compliant producten van verschillende leveranciers niet altijd out-of-the-box met elkaar samenwerken.

Relatie met andere standaarden

- H.323: een langer bestaande standaard, voorganger van SIP, gelijkend protocol vanuit de telefonie/ITU-T-hoek
- WEBRTC: nieuw opkomende standaard uit de HTML5 hoek, ter ondersteuning van browser-to-browser voice calling, video chat, en P2P file sharing (RTP verkeer).

Referenties

https://tools.ietf.org/html/rfc3261

2.11 URI en IRI

Over de standaard

Uniform Resource Identifier (URI) is een gestandaardiseerde manier om bronnen (resources, denk aan webpages, tekst, afbeeldingen, etc.) op het internet te identificeren. Internationalized Resource Identifier (IRI) is een standaard om bronnen (zoals webpagina's, tekst en afbeeldingen) op het internet te identificeren, maar waarbij gebruik kan worden gemaakt van de internationale karakterset ISO 10646, waaronder Arabische, Hebreeuwse en Chinese karakters. IRI en URI zijn complementair, waarbij URI de minder brede ASCII-karakterset ondersteunt.

Aanbeveling

Update van URI-standaard: **RFC 2396 (aug 1998) → RFC 3986 (jan 2005)**.
Aanvullen met IRI-standaard: **RFC 3987 (jan 2005)**.

Toelichting

Een URI is specifieke vorm van een IRI – Internationalized Resource Identifier (RFC 3987 - 2005). Een URI maakt gebruik van alleen de ASCII-karakterset. Een IRI maakt gebruik van de universele karakter set conform Unicode/ISO 10646.

De nieuwe versie van standaard URI RFC3986 is een uitbreiding op de vorige versie met o.a. IPv6, de grammaticaregels zijn versimpeld en meer geformaliseerd.

Relatie met andere standaarden

- URL (Uniform Resource Locator): specifieke vorm van een URI.
- URN (Uniform Resource Name): specifieke vorm van een URI.
- Standaarden zoals XML, XPath en HTML ondersteunen IRI's.

Referenties
URI: https://tools.ietf.org/html/rfc3986 en http://www.w3.org/TR/uri-clarification/
IRI: https://tools.ietf.org/html/rfc3987

2.12 URL

Over de standaard
Een Uniform Resource Locator (URL) (als het begint met een http vaak ook wel webadres genoemd), is een URI met een bepaalde semantiek die beschrijft hoe en waar men aan de bron (resource) kan komen op het Internet.

Aanbeveling
Het verwijderen van de standaard van de lijst, **RFC 2717 (nov 1999)**.

Toelichting
De URL-standaard kan worden verwijderd omdat deze is opgenomen in de URI-standaard, alle URL's zijn een specifieke vorm van URI's. IETF-standaard RFC2717 met status 'Best current practice' is vervangen ('obsoleted') door standaard RFC4395 (status 'Best current practice') met richtlijnen en registratie procedures voor URI's.

Relatie met andere standaarden
- URI (Uniform Resource Identifier): superset van URL en bevat ook URN's.

Referenties
http://www.w3.org/TR/uri-clarification/

2.13 URN

Over de standaard
Uniform Resource Names (URN) een standaard heeft als doel om als persistente, locatie-onafhankelijke identifier te dienen. Het is een URI die slechts gebruikt wordt voor het beschrijven van een (unieke) naam, maar niets zegt over waar en hoe deze bron gevonden kan worden. Dit zorgt ervoor dat links persistent blijven.

Aanbeveling
Het verwijderen van de standaard van de lijst, **RFC 2141.**

Toelichting
De URN-standaard kan worden verwijderd als losse standaard omdat deze is opgenomen in de URI-standaard, net zoals URL, zijn alle URN's een specifieke vorm van URI's. Wel is de URN (IETF-standaard RFC2141) niet komen te vervallen zoals bij URL. Maar aangezien de URN een onderdeel

is in de URI standaard is het niet nodig om deze standaard als aparte standaarden op de lijst te laten staan.

Relatie met andere standaarden

- URI (Uniform Resource Identifier): net zoals bij URL is URI een superset van URN's.
- URL

Referenties

- http://www.den.nl/standaard/266/
- https://tools.ietf.org/html/rfc2141

2.14 VCF

Over de standaard

vCard File (VCF) beschrijft een set van velden die gebruikt kunnen worden om gegevens over personen uit te wisselen. Het kan gezien worden als een soort van digitaal visitekaartje waarmee individuen onderling hun gegevens digitaal uit kunnen wisselen.

Aanbeveling

Update van standaard : **RFC 2425 (sep 1998) → RFC 6350 (aug 2011)**.

Toelichting

De nieuwe versie van standaard VCF RFC6350 is niet alleen een MIME type maar een zelfstandig formaat, gebruikt alleen UTF-8 en is onder andere uitgebreid met standaard voor het vindbaar maken van personen op basis van vCard (de voormalige standaard RFC 2426).

Relatie met andere standaarden

-

Referenties

http://tools.ietf.org/html/rfc6350

2.15 WSDL

Over de standaard

Web Services Description Language (WSDL) is een XML-taal waarmee de interfaces van webservices kunnen worden beschreven. Over het algemeen zullen deze WSDL-documenten voornamelijk door applicaties gelezen worden en beschikbaar zijn voor aanroepende applicaties.

Aanbeveling

Update van standaard: **versie 1.1 → versie 2.0**.

Toelichting
De nieuwe versie van standaard WSDL 2.0 wordt aanbevolen door W3C en omvat betere ondersteuning voor RESTfull webservices en is eenvoudiger te implementeren.

Relatie met andere standaarden
- UDDI (Universal Description and Discovery Protocol) = standaard voor een (verwijs)index van webservices met te gebruiken interface in WSDL

Referenties
http://www.w3.org/TR/2007/REC-wsdl20-primer-20070626/

2.16 X.509

Over de standaard
De X.509-standaard[2] 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 verbinding nog valide is of ingetrokken is. De standaard wordt zowel binnen Nederland als wereldwijd zeer veel gebruikt. De standaard is een belangrijk onderdeel in de communicatie tussen de overheid met burgers en bedrijven, en is een integraal component voor PKIoverheid.

Het is niet mogelijk de X.509 standaard te gebruiken zonder gebruik te maken van een aanvullende set bindende afspraken die zijn vastgelegd in een zogenaamd Certificate Profile. Dit is bijvoorbeeld voor PKIoverheid gebeurd. X.509 beschrijft een PKI systeem en is oorspronkelijk in de context van X.500 strikt hiërarchisch opgezet door de ITU. Meestal wordt X.509 gebruikt voor de beschrijving van een certificaat formaat (X.509 v3) en is hiervoor een profiel ontwikkeld in IETF verband (PKIX-werkgroep).

X.509 v3-certificaten zijn het meest gebruikte formaat voor PKI-certificaten.

Aanbeveling
Op de hoogte stellen van de updates: RFC 6818 en aanvullende profielen zijn aangepast. De set van acceptabele encodeermethoden geeft meer inzicht in de regels voor het converteren van internationale domeinen naar ASCII. Het geeft met name een update van beveiligingsoverwegingen.

Toelichting

[2] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile.

Een deel van de standaard is geüpdatet. X.509 v3-certificaten zijn het meest gebruikte formaat voor PKI-certificaten.

Relatie met andere standaarden
IPsec, SSL en TLS.

Referenties
http://tools.ietf.org/html/rfc5280

2.17 XSLT

Over de standaard
Extensible Stylesheet Language (XSL) is een formele taal waarin beschreven kan worden hoe XML-documenten geformatteerd moeten worden. XSL is daarmee een aanvulling op XML, welke reeds op de lijst is opgenomen als aanbevolen standaard. Ook omvat XSL een notatiewijze voor stylesheets ten behoeve van de opmaak van XML-documenten. XSLT, XPath en XSL-FO zijn onderdeel van de XSL-standaard:

1. XSLT (XSL Transformation): taal voor het transformeren van XML-documenten,
2. XSL-FO (XSL Formatting Objects): taal voor het specificeren van de visuele weergave van een XML-document, en
3. XPath: onderdeel van XSLT voor het adresseren van onderdelen van een XML-document.

Aanbeveling
Vervangen van de standaard **XSLT versie 1.0** door de **XSL** standaard.

Toelichting
Advies is om de XSL als nieuwe standaard op te voeren als vervanging voor de (verouderde versie) XSLT v1.0. De standaard XSL wordt sinds 2001 door W3C geadviseerd om te gebruiken. De opsplitsing naar substandaarden heeft ervoor gezorgd dat XSL een moeizame ontwikkeling heeft doorgemaakt maar inmiddels wel meer gebruikt wordt.

Relatie met andere standaarden
- XML: syntax voor beschrijven berichteninhoud die getransformeerd kunnen worden met XSLT.

Referenties
http://www.w3.org/Style/XSL/

3 E-FACTURATIE- EN ADMINISTRATIESTANDAARDEN

3.1 EI-standaarden

Over de standaard

Externe Integratiestandaarden (EI) is een set declaratieberichten en bijbehorende retourberichten ten behoeve van het declaratieverkeer tussen zorgverzekeraars en zorgverleners in het kader van de zorgverzekeringswet. Het gaat om semantische standaarden.

Aanbeveling

Wijzigingen in de set van berichten zijn gearceerd weergegeven in onderstaande tabel:

Berichttype	Huidige versie	Nieuwste versie	Wijziging
AP304/AP305	V7.0	**V8.0**	Update
AW319/AW320	-	**V1.4**	Nieuw
DG301/DG302		**V1.0**	Nieuw
EF301/EF302	-	**V1.1**	Nieuw
EP301/EP302	V1.2	V1.2	
FZ301/FZ302	-	**V2.0**	Nieuw
FZ303/FZ304	-	**V1.0**	Nieuw
GZ311/GZ312	V1.1	**V2.1**	Update
GZ321/GZ322	-	**V1.0**	Nieuw
GZ340		**V1.0**	Nieuw
HA304/HA305	V4.2	V4.2	
JW303/JW304	-	**V2.1**	Nieuw
JW321/JW322	-	**V2.0**	Nieuw
KZ301/KZ302	V3.2	V3.2	
LH307/LH308	V5.2	V5.2	
MA801	-	**V4.3**	Nieuw
MZ301/MZ302	V1.3	V1.3	
OS301/OS302	-	**V1.0**	Nieuw
PM304/PM305	V3.2	V3.2	
QA301/QA302	-	**V2.0**	Nieuw
QD301	-	**V1.0**	Nieuw
QDG301/302		**V1.0**	Nieuw
QE301	-	**V1.0**	Nieuw
QF301/QF302	-	**V2.0**	Nieuw
QG301/QG302	-	**V2.0**	Nieuw
QG321/QG322	-	**V1.0**	Nieuw
QH301	-	**V1.1**	Nieuw
QK301/302		**V1.0**	Nieuw
QM301	-	**V1.1**	Nieuw
QP301	-	**V1.0**	Nieuw
QV301/302		**V1.0**	Nieuw
QX301/QX302	-	**V2.1**	Nieuw
QZ301/QZ302	-	**V2.0**	Nieuw
SB311/SB312	-	**V2.0**	Nieuw
VE303/VE304	V4.2	V4.2	
VK301/VK302	V2.2	V2.2	
VZ301	-	**V1.0**	Nieuw
VZ37/VZ38	v.4	**~~v.4~~**	Vervallen
VZ801/VZ802	-	**V1.0**	Nieuw
WMO303/WMO304	-	**V2.1**	Nieuw
ZH308/ZH309	V7.2	**V9.0**	Update
ZH310/ZH311	-	**V1.0**	Nieuw

Toelichting
Oorspronkelijke zijn er 11 standaarden die vielen onder de ei-standaarden opgenomen. In de loop der jaren is deze set uitgebreid. De Ei-standaarden zijn met name sterk uitgebreid als gevolg van de decentralisatie van Jeugd, Werk en Zorg naar de gemeenten (3 D's). Het voorstel is dan ook om de gehele set op te nemen en niet specifiek te beperken tot oorspronkelijk getoetste set van berichten

Relatie met andere standaarden
-

Referenties
http://ei.vektis.nl/WespStandaardenOverzicht.aspx

3.2 NEN-ISO 4217

Over de standaard
De ISO 4217 standaard is een internationale standaard die drielettercodes definieert voor valuta. Voorbeelden zijn de euro, ISO code EUR, en Brits Pond Sterling GBP. Daarnaast bevat de standaard ook codes en eenheden voor fondsen en edelmetalen. De standaard wordt met name gebruikt voor internationale handelsstromen en voor gebruik in het bankwezen (de plekken waar veel verschillende valuta's bij elkaar komen). De code is ontworpen voor gelijkwaardige geschiktheid voor handmatige gebruikers en voor het gebruik van geautomatiseerde systemen.

Aanbeveling
Het updaten van de standaard: NEN-ISO 4217 2008 → NEN-ISO 4217-2015

Toelichting
Het betreft een update van de 2008 versie van de norm met toevoegingen, verwijderingen en wijzigingen van o.a. valutacodes.

Relatie met andere standaarden
- ISO 3166-1 (landcodes): Bij het vaststellen van de drielettercodes zijn de eerste twee letters 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.

Referenties
https://www.nen.nl/NEN-Shop/Norm/NENISO-42172015-en.htm

3.3 SQL

Over de standaard
Structured Query Language (SQL) is een ANSI/ISO-standaardtaal voor een relationeel 'database management systeem' (DBMS). Het is een gestandaardiseerde taal die gebruikt kan worden voor taken zoals het bevragen en het aanpassen van informatie in een relationele databank.

Aanbeveling
Update van standaard: **ISO/IEC 9075:2008 → ISO/IEC 9075:2011**.

Toelichting
De nieuwe versie van standaard SQL ISO/IEC 9075:2011 is uitgebreid met onder andere support voor temporal databases (timelining van opgeslagen data).

Relatie met andere standaarden
-

Referenties
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53681

3.4 XMI 2.x

Over de standaard
XML Metadata Interchange (XMI) 2x is een standaard voor het uitwisselen van metadata-informatie via XML. XMI wordt het meest gebruikt als een uitwisselingsformaat voor UML-modellen via XML. Het kan worden gebruikt voor metadata waarvan het metamodel kan worden uitgedrukt in Meta-Object Facility (MOF).

Aanbeveling
Update van standaard: **versie 2.4.1 → versie 2.5.1**.

Toelichting
De nieuwe versie van standaard XMI 2.5.1 bevat een aantal minor uitbreidingen en updates.

Relatie met andere standaarden
- XML: Syntax voor beschrijven van berichteninhoud, bv UML modellen.
- UML (Unified Modelling Language):standaard voor beschrijven/specificeren van business-, informatie- en IT technologie modellen.
- MOF (Meta Object Facility): standaard voor beschrijven van modellen, bv UML modellen.

Referenties
http://www.omg.org/spec/XMI/2.5.1/

4 DOCUMENTEN EN (WEB)CONTENTSTANDAARDEN

4.1 IPM

Over de standaard
Het Informatie Publicatie Model ‘xyz’ (IPM) beschrijft de randvoorwaarden voor het publiceren van informatie over ‘xyz’ op internet en bevordert daarmee de vindbaarheid van dienst of product ‘xyz’. Voorbeelden zijn Samenwerkende Catalogi en Vergunningen (beheer is in handen van KOOP). Het IPM beschrijft de metadata standaard waarmee gegevens worden uitgewisseld, beschrijft de mogelijkheden die de centrale zoekdienst de deelnemende overheden biedt en geeft een toelichting op de aansluitvormen.

Aanbeveling
Verwijderen van standaard: **versie 4.0**.

Toelichting
IPM is een onderdeel van een Contentmodel en beschrijft de component 'Structuurmodel'. Het is daarmee te weinig een generieke standaarden. Verder wordt IPM als zodanig niet als open standaard beheerd (dit betreft niet de afzonderlijk contentmodellen). De standaard hoort daarmee niet echt thuis op de lijst.

Relatie met andere standaarden
- OWMS (Overheid.nl Web Metadata Standaard): standaard voor het beschrijven van metadata van informatie van de Nederlandse Overheid op internet. In IPM zijn een aantal metadatavelden gegroepeerd in een toepassingsprofiel.

Referenties
http://standaarden.overheid.nl/contentmodellen

4.2 JSON

Over de standaard
JavaScript Object Notation (JSON) een formaat om net zoals XML gegevens op te slaan en te versturen. Het wordt gebruikt voor het uitwisselen van datastructuren, met name in webapplicaties die asynchroon gegevens ophalen van de webserver. De standaard is met name gericht op efficiënt programmeren en kent een compacte notatie bijvoorbeeld:
{
“naam”: Jan,
“geboren”: 1983
}

Aanbeveling
Update van standaard : **RFC 4627 (juli 2006) → RFC 7159 (mrt 2014)**.

Toelichting
De nieuwe versie van standaard JSON RFC 7159 is een kleine uitbreiding van de vorige versie onder andere op het vlak van inconsistenties en bugfixes.

Relatie met andere standaarden
- JavaScript: programmeertaal waarvan de basis syntax beschrijving is afgeleid voor gebruik in JSON.

Referenties
https://tools.ietf.org/html/rfc7159
http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf

4.3 RDF

Over de standaard
Resource Description Format (RDF) 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). Doordat alle partijen de data als ˜RDF-Triplets" uitwisselen, wordt het voor de ontvangende partij makkelijker om de data geautomatiseerd te interpreteren en te linken aan andere data(sets).

Een RDF "triple" is een drieledige subject-predicaat-object-structuur. 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.

Aanbeveling
Update van standaard : **versie 1 → versie 1.1**.

Toelichting
De nieuwe versie van standaard RDF 1.1 is een uitbreiding van de vorige versie met onder andere RDF-datasets (graphs) en IRI's.

Relatie met andere standaarden
- RDFa (RDF in Attributes): syntax voor het opnemen van RDF-informatie in HTML webpagina's

- SKOS (Simpel Knowledge Organization System): standaard voor het beschrijven van KOS's (bijvoorbeeld classificaties schema's, ontologieën, woordenboeken) middels RDF.
- IRI: standaard om bronnen (zoals webpagina's, tekst en afbeeldingen) op het internet te identificeren, waarbij gebruik kan worden gemaakt van de internationale karakterset ISO 10646, waaronder Arabische, Hebreeuwse en Chinese karakters.

Referenties
http://www.w3.org/standards/techs/rdf#w3c_all

4.4 SLD

Over de standaard
Styled Layer Description (SLD) is een standaard voor visualisatie die wordt toegepast in combinatie met WMS. Het definieert een encoding die de WMS-standaard daarmee uitbreidt en het mogelijk maakt om gebruiker gedefinieerde symbolen en kleuren te gebruiken in geografische gegevens.

Aanbeveling
Verwijderen van de standaard: **versie 1.0 → versie 1.1.0**

Toelichting
SLD is een optionele standaard die alleen werkt tezamen met WMS en WFS en het werkt niet voor andere geo-standaarden. Het is daarmee een te kleine en specifieke standaard. Verder is de huidige versie deprecated (op dit moment is er versie 1.1.0). Ook dekt SLD niet alle visualisatie, de standaard SE hoort hier ook bij. Net zoals de standaarden WMS en WFS staat SE niet op de lijst. Alleen SLD op de lijst hebben staan is niet consistent en geeft verwarring.

Relatie met andere standaarden
- WMS v1.3.0 is complementair aan SLD v1.1.0 en Symbology Encoding Standard (SE).

Referenties
http://www.opengeospatial.org/standards/sld

5 OVERIGE STANDAARDEN

5.1 ISO 3166-1

Over de 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 2-letterige (alpha-2) landcodes, 3-letterige (alpha-3) landcodes en 3-cijferige (numeric-3) landcodes.

Aanbeveling

Update van standaard: **ISO 3166-1:2006 → ISO 3166-1:2013**.

Toelichting

De nieuwe versie van standaard ISO3166 is een uitbreiding op de vorige versie met nieuwe landen.

Relatie met andere standaarden

-

Referenties

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63545
https://www.nen.nl/NEN-Shop/Norm/NENENISO-316612014-en.htm