Forum Standaardisatie
www.forumstandaardisatie.nl
info@forumstandaardisatie.nl
Bureau Forum Standaardisatie
gehuisvest bij Logius
Postadres
Postbus 96810
2509 JE Den Haag
Bezoekadres
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Bij bezoek aan Logius is legitimatie verplicht

notitie

FORUM STANDAARDISATIE 13 december 2017

Agendapunt:	3E		
Betreft:	Intake-advies voor Grip op SSD		
Aan:	Stuurgroep open standaarden		
Van:	Bureau Forum Standaardisatie		
Datum:	20 november 2017	**Versie**	0.2

Advies

Het Forum Standaardisatie wordt geadviseerd om de standaard Grip op Secure Software Development (hierna: SSD) niet in behandeling te nemen voor opname op de 'pas toe of leg uit' lijst.

Korte toelichting:
De standaard "Grip op secure software development (SSD)" beschrijft hoe een opdrachtgever grip krijgt op het ontwikkelen van goed beveiligde software. SSD 2.0 richt zich op het proces van software ontwikkeling binnen een organisatie en is geen standaard voor gegevensuitwisseling. Derhalve voldoet SSD niet aan het eerste criterium om in procedure genomen te worden ("*Is de standaard toepasbaar voor elektronische gegevensuitwisseling..*").

Hoewel veilige software kan bijdragen aan veilige gegevensuitwisseling draagt SSD niet direct bij aan de interoperabiliteit van de (semi-)overheid. SSD 2.0 voldoet derhalve ook niet aan het tweede criterium voor inbehandelname ("*Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de overheid?*").

Het beheer van de standaard is nog onvoldoende beschreven. Er is geen eenduidige beschrijving hoe het versiebeheer is ingericht, hoe besluiten over de standaard worden genomen, wie deze besluiten nemen, hoe bezwaar kan worden ingediend, enz. Daardoor is er geen zicht op de openheid van het standaardisatieproces. SSD zou daarom ook het risico lopen om niet door het eerste toetsingscriterium ("*Open standaardisatieproces*") voor de procedure te komen.

Toelichting

1. Aanmelding, intakegesprek en toetsingsprocedure

Op 23 oktober 2017 is door Ad Kint en Marcel Koers van het Centrum voor Informatiebeveiliging en Privacy Bescherming (het CIP) een standaard aangemeld, betreffende de aanmelding van SSD voor de lijst met open standaarden. De aanmelder heeft als doel de standaard verplicht ('pas-toe-of-leg-uit') te stellen.

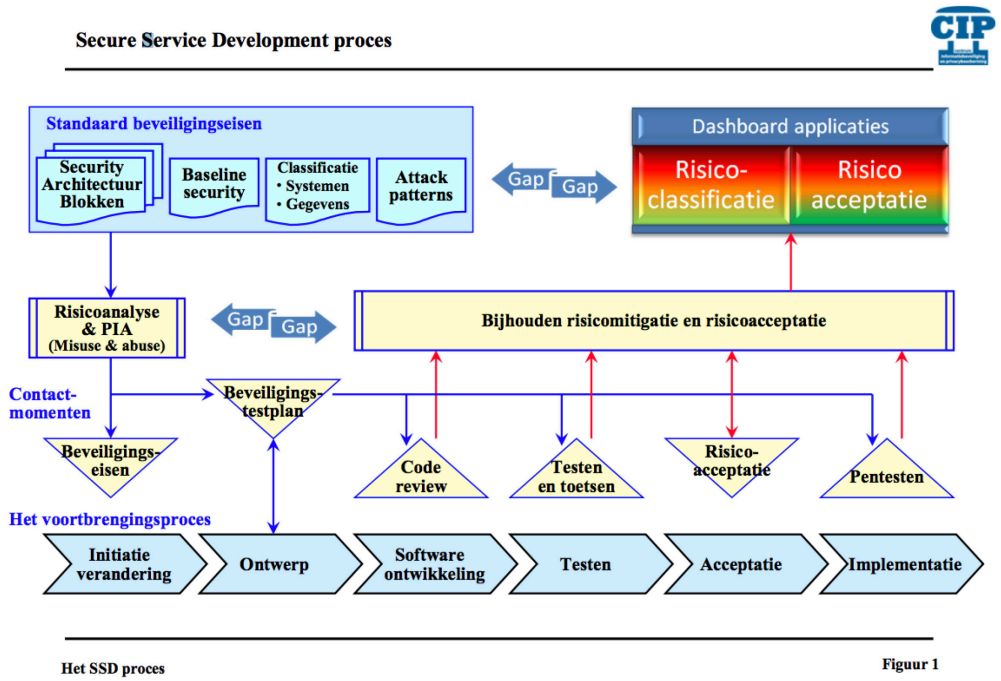
Op 7 november 2017 heeft een intakegesprek plaatsgevonden met de aanmelder. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

2. Korte beschrijving standaard

Waar gaat SSD over?

De methode "Grip op secure sofware development (SSD)" beschrijft hoe een opdrachtgever grip krijgt op het ontwikkelen van goed beveiligde software. De drie pijlers daarbij zijn 1) standaard beveiligingseisen, 2) contactmomenten en 3) inrichten van SSD processen.

Hun relatie met het voortbrengingsproces is als volgt:



De SSD beveiligingseisen voor server en mobiele applicaties bevat een hanteerbaar aantal normen met maatregelen. De maatregelen worden ingebouwd in de software. Bij de beschrijving van de maatregelen wordt aangegeven wie in de keten van opdrachtgever-softwareontwikkelaar- hostingpartij wat moet doen. Toetsing en auditing kan plaats vinden o.a. bij het testen. Door toepassing van de SSD

beveiligingseisen/maatregelen is er een standaard niveau van beveiliging aanwezig in de software. Daardoor hebben ook de informatie uitwisselingen tussen SSD beveiligde objecten een standaard niveau van beveiliging. De normen zijn zo op gesteld dat zij het gesprek tussen de opdrachtgever en de opdrachtnemer ondersteunen.

Welk probleem lost de standaard op?
Organisaties hebben nog onvoldoende vat op security, getuige de explosieve groei van incidenten. In de praktijk blijkt dat 75% van die incidenten hun oorzaak vinden in softwarefouten.[1] SSD bevat normen en maatregelen om te komen tot veilige software.

Wie beheert de standaard?
Het CIP beheert de standaard. Het CIP is opgezet door de Belastingdienst, DUO, SVB en UWV en komt voort uit het programma Compacte Rijksdienst.

Waarom is de standaard aangemeld voor pas toe of leg uit?
Het opnemen van SSD verplicht volgens het voorgestelde toepassingsgebied overheden om SSD toe te passen bij nieuwbouw en onderhoud van software voor zover deze betrekking heeft de uitwisseling van persoonsgegevens.

(zie ook: *7. Functionele use case*)

3. Criteria voor inbehandelname
Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden vier criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?
Nee, de standaard heeft veilige softwareontwikkeling tot doel. Hoewel veilige software indirect bijdraagt aan veilige gegevensuitwisseling is de standaard niet toepasbaar voor gegevensuitwisseling zelf.

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?
Nee. Het beoogde functioneel toepassingsgebied betreft maatregelen en criteria op het gebied van softwareontwikkeling. De standaard is zowel toepasbaar bij de ontwikkeling van nieuwe software, als de doorontwikkeling van bestaande software. De standaard draagt niet substantieel bij aan de interoperabiliteit van de (semi-) overheid. (zie antwoord op vraag 1)

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?
Ja. Er is nog geen wettelijk kader met betrekking tot de ontwikkeling van veilige software. De standaard is niet wettelijk verplicht.

[1] *https://www.cip-overheid.nl/downloads/grip-op-ssd/*

4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?
Ja, de standaard draagt bij aan de ontwikkeling van veilige software. Elke leverancier kan bovendien SSD toepassen.

Conclusie
De standaard voldoet niet aan de criteria voor inbehandelname.

4. Toetsing kansrijkheid procedure
Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

1. Open standaardisatieproces
De ontwikkeling en het beheer van de standaard moeten op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.
De ontwikkeling en het beheer van de standaard zijn belegd bij het CIP, een publiek-private netwerkorganisatie die bestaat uit Participanten en Kennispartners. De documentatie is zonder kosten te downloaden en gelicenseerd onder de Creative Commons Naamsvermelding GelijkDelen 4.0. De wijze waarop ontwikkeling en beheer is ingericht is op dit moment nog onvoldoende beschreven.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.
Toepassing van SSD leidt tot veiliger software en de potentiële baten daarvan zijn onder andere het voorkomen van datalekken en de daarmee gepaard gaande schade. Daarbij kan gedacht worden aan imagoschade maar ook financiële schade door herstelwerkzaamheden. Verwacht mag worden van leveranciers dat zij veilige software leveren. Eventuele meerkosten als gevolg van het toepassen van SSD zou dan ook beperkt moeten zijn.
Er zijn geen beveiligings- en/of privacyrisico's verbonden aan het gebruik van de standaard. De standaard richt zich juist op het terugdringen en voorkomen van dergelijke risico's.

3. Draagvlak
Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.
Er zijn meerdere aanbieders en gebruikers die (een vorige versie) van de standaard toepassen waaronder: UWV, CBIG, Cap Gemini, CGI, ICTU, Centric, min VWS.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

De standaard is aangemeld voor de lijst met open standaarden met de status pas toe of leg uit. Het beoogde doel van de aanmelding is het verplicht stellen van het gebruik van SSD door overheden. Dit zal daardoor leiden tot een brede adoptie van de standaard bij toeleveranciers.

Conclusie
De wijze waarop ontwikkeling en beheer is ingericht is op dit moment nog onvoldoende beschreven. Hierdoor kan onvoldoende getoetst worden of en in welke mate sprake is van een open standaardisatieproces.

5. Samenhang
Het Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. *Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   SSD kent een relatie met de standaard kent een relatie met de ISO standaarden 27001 en 27002 (met name paragraaf 14.2.1 *Beleid voor beveiligd ontwikkelen*).

2. *Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   SSD kent geen directe relatie met aanbevolen standaarden die reeds op de lijst met open standaarden zijn opgenomen.

3. *Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden).*
   SSD kent een relatie met NCSC, NIST, OWASP maar richt zich primair op softwareontwikkeling. Er is daarom geen directe samenhang tussen SSD en standaarden die in aanmerking komen voor opname op de lijst met open standaarden.

6. Sponsorschap
De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. *Welke overheden en/of (semi)publieke organisaties ondersteunen de aanmelding van de standaard?*
   SSD is aangemeld door het CIP. Het CIP bestaat uit meerdere overheden waaronder het UWV, DUO, SVB en de Belastingdienst.

2. Hebben deze organisaties de standaard geïmplementeerd?
   (zie ook punt 7 voor een uitwerking)
   Ja, dit geldt in ieder geval voor het UWV.

7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.
Geef een aantal bestaande functionele usecases van de standaard en geef aan welk 'interoperabiliteitsprobleem' de standaard helpt oplossen.
(tenminste één publieke usecase, en indien relevant een usecase uit de private sector)

Geef hierbij ook aan wat de oorspronkelijke situatie was en wat de nieuwe situatie is. M.a.w.: welk interoperabiliteitsprobleem de standaard dus heeft opgelost.
Er is op dit moment geen use case beschreven van de standaard. SSD richt zich primair op softwareontwikkeling en dus niet op een specifiek interoperabiliteitsprobleem.