

**Forum Standaardisatie**Wilhelmina van Pruisenweg 52
2595 AN Den HaagPostbus 96810
2509 JE Den Haagwww.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE

Agendapunt:			
Betreft:	Intake-advies Framework Secure Software (FSS)		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	16 december 2015	Versie	1.0

Bijlagen: -

Advies

Het Forum Standaardisatie wordt geadviseerd om het Framework Secure Software (hierna: FSS) niet in behandeling te nemen voor opname op de lijst. Het FSS is een kader voor het veilig ontwikkelen van software en niet specifiek voor elektronische gegevensuitwisseling. Daardoor voldoet de standaard niet aan de criteria voor inbehandelname.

Over de standaard

Software wordt veelal pas na oplevering getest op eventuele lekken en zwakheden door middel van code-reviews en penetratietesten. Het FSS is een framework om dit te voorkomen en geeft maatregelen en normen voor veilige softwareontwikkeling. Hierdoor kunnen veiligheidsincidenten zoals het hacken van websites en software bij voorbaat worden verminderd.

Advies en Aandachtspunten

Het FSS is een kader voor het veilig ontwikkelen van software. Hoewel software ontwikkeling indirect een relatie kent met gegevensuitwisseling is FSS niet specifiek toepasbaar voor elektronische gegevensuitwisseling. Bovendien is de kansrijkheid van een eventuele procedure onvoldoende doordat de beheerorganisatie nog in ontwikkeling is. Verder zijn de meerkosten voor softwareontwikkeling door het gebruik van het FSS nog niet duidelijk. Het is aannemelijk om te verwachten dat de kosten substantieel zullen zijn gezien de omvang van softwareontwikkeling binnen het organisatorisch werkingsgebied. Het advies is daarom ook om de standaard niet in behandeling te nemen voor opname op de lijst.

Datum
3 december 2015

Toelichting

1. Aanmelding, intakegesprek en toetsingsprocedure

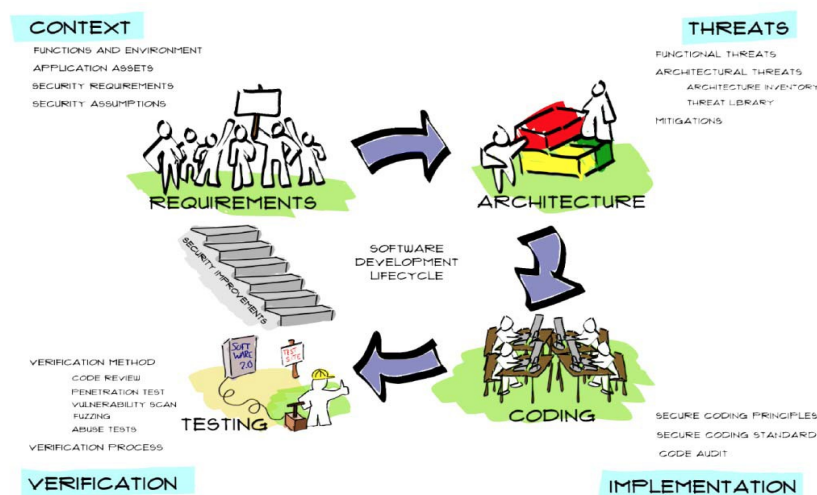
Op 23 oktober 2015 is door de heer Rick Strijbos, Ambassadeur van de Secure Software Foundation, het FSS als standaard aangemeld voor de lijst met open standaarden. De aanmelder heeft als doel de standaard verplicht ('pas-toe-of-leg-uit') te stellen.

Op 12 november 2015 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 de standaard over?

Het FSS is een framework met maatregelen en normen voor veilige softwareontwikkeling. FSS richt zich op alle belanghebbenden in de softwareketen die baat hebben bij duidelijke en objectief meetbare veiligheidskenmerken van software. Opdrachtgevers kunnen deze veiligheidskenmerken gebruiken als vereisten in de formulering van hun opdracht. Ontwerpers en ontwikkelaars kunnen er gebruik van maken bij het bouwen van applicaties, terwijl auditors aan de hand van diezelfde kenmerken de veiligheid van de geproduceerde software kunnen beoordelen. Het framework geeft richtlijnen en criteria voor veilige softwareontwikkeling gedurende alle fasen van het ontwikkeltraject (requirements-, architectuur-, codeer-, - en testfase) en de consolidatie.



Afbeelding 1 Fasen ontwikkeltraject waar FSS betrekking op heeft

Welk probleem lost de standaard op?

Software wordt veelal pas na oplevering getest op eventuele lekken en zwakheden door middel van code-reviews en penetratietesten. Het Framework Secure Software biedt daarentegen een alomvattend en

applicatie-onafhankelijk framework waarmee softwareontwikkelaars handvatten hebben om veilige software te ontwikkelen. Hierdoor kan in de toekomst het aantal veiligheidsincidenten zoals het hacken van websites en software aanzienlijk worden verminderd.

Datum
3 december 2015

Wie beheert de standaard?

Het beheer en de ontwikkeling zijn belegd bij de Secure Software Foundation. De Secure Software Foundation is een stichting in oprichting. De initiatiefnemers van de Secure Software Foundation zijn de Information Security Academy en iComply. Zij deden dit in nauwe samenwerking met ECP.

Waarom is de standaard aangemeld voor pas toe of leg uit?

Het beoogde doel van de aanmelding is het verplicht stellen van het gebruik van FSS door overheden. Dit zal daardoor leiden tot een brede adoptie van de standaard bij toeleveranciers.

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie 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 richt zich primair op softwareontwikkeling en heeft tot doel het veiliger maken van software. De ontwikkeling van veilige software is van belang voor gegevensuitwisseling, maar de standaard ziet niet direct op gegevensuitwisseling.

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 beoogd 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. Het organisatorisch werkingsgebied betreft overheden en instellingen uit de (semi-) publieke sector).

Het gebied waarop de standaard betrekking heeft is daarmee zeer omvangrijk. Echter, 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.

Conclusie

De standaard voldoet niet aan de criteria voor inbehandelname.

Datum

3 december 2015

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 de Secure Software Foundation (SSF), een stichting in oprichting. De initiatiefnemers van de Secure Software Foundation zijn de Information Security Academy en iComply. Zij deden dit in nauwe samenwerking met ECP. Er is nog geen formeel bestuur geïnstalleerd.

Omdat de stichting nog in oprichting is, is niet alle documentatie over het ontwikkel- en beheerproces beschikbaar. Het specificatiedocument FSS is gratis beschikbaar onder een creative commons opensource licentie.¹

Partijen kunnen via een *silver*, *gold* of *platinum* partnership van SSF toetreden tot een bestuursfunctie of werkgroepen. De contributiekosten hiervan bedragen respectievelijk € 1.000, € 5.000 en € 10.000. Een ieder kan ideeën inbrengen welke al of niet in de "roadmap" van de standaard worden opgenomen. De beslissing hierover ligt bij de normcommissie. Besluitvorming vindt plaats bij meerderheid. Op dit moment is nog niet voorzien in een bezwaarprocedure voor belanghebbenden of derden.

De financiering van de stichting, en daarmee de ontwikkeling en beheer van de standaard, is op dit moment afhankelijk van een bijdrage van het Ministerie van EZ en contributie van partners. Hoewel het vooruitzicht is dat de stichting binnen afzienbare tijd financieel onafhankelijk is, is dat op dit moment nog niet het geval.

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.

Het gebruik van FSS leidt tot veiliger software en de potentiële baten daarvan zijn onder andere het voorkomen van *hacks* en de daarmee gepaard gaande schade. Daarbij kan gedacht worden aan imagoschade maar ook financiële schade door herstelwerkzaamheden. De meerkosten

¹ <https://www.securesoftwarefoundation.org/FrameworkSecureSoftware-Downloads.html>

voor softwareontwikkeling door het gebruik van het FSS zijn nog niet duidelijk. Het is echter aannemelijk om te verwachten dat de kosten substantieel zullen zijn gezien de omvang van softwareontwikkeling binnen het organisatorisch werkingsgebied.

Datum
3 december 2015

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.

De publieke annoncering van de standaard was in mei 2014. Sinds die tijd is het specificatiedocument (internationaal) circa 2500 keer gedownload. Van een aantal organisatie is bekend dat zij inmiddels zijn gestart met de adoptie van dit framework, waaronder de Belastingdienst en het CBP.

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 FSS door overheden. Dit zal daardoor leiden tot een brede adoptie van de standaard bij toeleveranciers.

Conclusie

Er zijn op voorhand meerdere struikelblokken te verwachten. De beheerorganisatie is nog in oprichting, waardoor het open standaardisatieproces nog niet volledig is ingericht. De businesscase van het gebruik van FSS is daarnaast onduidelijk. Er zijn zeker baten te verwachten maar de implementatiekosten zijn onbekend en vormen mogelijk een drempel. De signalen van overheidspartijen die de standaard aan het implementeren zijn, zijn positief. Echter, gezien het relatief korte bestaan van de standaard is er nog niet veel ervaring bij deze partijen.

5. Samenhang

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?*

FSS kent een relatie met de ISO standaarden 27001 en 27002 (met name paragraaf 14.2.1 *Beleid voor beveiligd ontwikkelen*). FSS biedt een inhoudelijke verdieping van de standaarden met betrekking tot de ontwikkeling van veilige software. Daarnaast kent FSS een relatie met andere standaarden en best practices binnen het domein van veilige

software ontwikkeling, zoals Grip op SSD (CIP) ,SDL (Microsoft), OWASP en BSIMM. Deze relaties zijn niet van invloed op de toetsing.

Datum
3 december 2015

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?*

FSS 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)?*

FSS richt zich primair op softwareontwikkeling. Er is daarom geen directe samenhang tussen FSS 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?*

De aanmelding van FSS als open standaard heeft geen formele sponsor, hoewel de verwachting is uitgesproken door de indiener dat ten minste één overheidsinstantie als sponsor zou willen optreden. De ontwikkeling van FSS is gesubsidieerd door het Ministerie van Economische zaken (via ECP).

2. *Hebben deze organisaties de standaard geïmplementeerd?*

FSS is op dit moment in gebruik bij de Belastingdienst en het CBP. Het CBP laat de nieuwe "applicatie datalekken" (waarmee de rapportage van datalekken wordt geadministreerd) bouwen door een partij die ontwikkelt volgens het Framework Secure Software.

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.

Er is op dit moment geen use case beschreven van de standaard. FSS richt zich primair op softwareontwikkeling en dus niet op een specifiek interoperabiliteitsprobleem.