Aanmelding van een nieuwe standaard

Voor dit type aanmelding geldt dat alle criteria van toepassing zijn en alle vragen beantwoord dienen te worden. U wordt als eerst gevraagd uw persoonsgegevens en de basisinformatie van de standaard te geven. Vervolgens dienen de criteriavragen beantwoord te worden. De criteria vallen uiteen in *criteria voor inbehandelname* en *inhoudelijke criteria*.

0. Persoonsgegevens indiener & relatie tot standaard

Deze gegevens worden door het Forum gebruikt om met u in contact te kunnen treden. De gegevens worden vertrouwelijk behandeld.

0.	**Persoonsgegevens en relatie tot de standaard**
0.1	Naam:
	Marcel Koers Ad Kint
0.2	Organisatie:
	CIP (Centrum voor Informatiebeveiliging en Privacy Bescherming) CIP-UWV
0.3	Functie:
	Senior Enterprise architect Project manager
0.4	Telefoonnummer:
	0651406805 06-52464200
0.5	E-mailadres
	Marcel.Koers@uwv.nl Ad.Kint@uwv.nl
0.6	Welke relatie bestaat er tussen uw organisatie en de standaard?
	Het CIP is eigenaar van Grip op SSD, die bestaat uit de methode, de beveiligingsnormen voor server en mobiele applicaties en het SSD testkader. UWV is gebruiker van SSD.
0.7	Zijn er (andere) overheidsorganisaties die de aanmelding van deze standaard ondersteunen?
	DUO, SVB, (UWV), ICTU, CBIG. Min VWS ondersteunen (naast marktpartijen) Grip op SSD en hebben hiervoor het Grip op SSD manifest ondertekend.

I. Basisinformatie aanmelding standaard

De basisinformatie van de standaard vormt de basis voor de toetsing tegen de criteria. Probeer hier zo volledig mogelijk in te zijn.

1.	**Basisinformatie standaard(en)** (In geval van een set van standaarden, meerdere malen invullen)
1.1	Volledige naam van de standaard
	Grip op Secure Software Development; de beveiligingseisen voor server en de beveiligingseisen mobiele applicaties.
1.2	Verkorte naam van de standaard
	Grip op SSD
1.3	Versie van de standaard, vaststellingsdatum en status
	Beveiligingseisen voor server applicaties 2.0, CIP categorie 'Becommentarieerde Practice' oktober 2014.

	Beveiligingseisen voor mobile applicaties 1.0, CIP categorie "Becommentarieerde Practice" februari 2016.
1.4	Oudere en aanstaande versies van de standaard inclusief (verwachte) publicatiedata en ondersteuningsstatus
	Medio 2018 worden nieuwe versies uitgebracht van • Beveiligingseisen voor serverapplicaties • Beveiligingseisen voor mobiele applicaties • SSD het proces
1.5	Naam en vindplaats specificatiedocument (bij voorkeur URL of bijvoegen bij aanmelding)
	www.cip-overheid.nl----> producten--→SSD Vrij te downloaden.
1.6	Naam van de standaardisatieorganisatie
1.7	Kosten van deelname aan het standaardisatieproces (bijv. voor lidmaatschap)
1.8	Kosten voor het verkrijgen van het specificatiedocument
	0
1.9	Andere standaarden die genoemd worden in het specificatiedocument van de standaard
	NCSC, NIST, ISO 27002, OWASP
1.10	Hoe werkt de standaard? (graag op een bondige en voor een buitenstaander duidelijke manier beschrijven hoe de standaard werkt en wat deze mogelijk maakt)
	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 oa 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 informatieuitwisselingen 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.

2.	**Toepassings- en werkingsgebied van opname**
2.1	Wat is het beoogde functioneel toepassingsgebied voor de standaard?
	(Bedrijfs)Software nieuwbouw en onderhoud. Toetsing van standaard pakketten
2.2	Wat is het beoogde organisatorisch werkingsgebied voor de standaard? (*hoeft alleen ingevuld te worden als de standaard op voor de status 'pas toe of leg uit' wordt ingediend)*
	De leveranciersrelatie (intern en/of extern) tussen opdrachtgever en softwareleverancier. Waarbij de keten start bij de initiatie en eindigt (dan wel start met een nieuwe cyclus) bij de hostingpartij. Alle partijen zijn actief betrokken, waarbij hun bijdrage duidelijk is.

II. Criteria voor inbehandelname

De criteria voor inbehandelname worden gebruikt tijdens de intake om te bepalen of een aanmelding correct is en binnen de scope van de lijsten valt. U kunt voor het beantwoorden van deze vraag de tekstvlakken bij de betreffende criteriavragen gebruiken.

Criteria: De aanmelding is correct en valt binnen scope van de lijsten, d.w.z. de standaard:

- Is toepasbaar voor elektronische gegevensuitwisseling tussen en met (semi-)overheidsorganisaties;
- Draagt binnen het beoogde opnamegebied substantieel bij aan de interoperabiliteit van de (semi-)overheid;
- Is niet reeds wettelijke verplicht.

1.	**Valt de aangemelde standaard binnen de scope van de lijsten?**
1.1	Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-) overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?
	Ja, Grip op SSD draagt direct bij aan veilige digitale uitwisseling, zowel technisch als relationeel. Dit laatste omdat de onderlinge duidelijkheid over de inbraakveiligheid het vertrouwen in de samenwerking in de keten verbeterd.
1.2	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?
	Het Grip op SSD-dashboard is prima binnen overheidsketens toe te passen. Het hanteren van een zelfde beveiligingsniveau wordt daardoor eenvoudiger te waarborgen en waardoor de keten aantoonbaar aan veiliger is en voor de interoperabiliteit vereiste voorwaarden van veiligheid worden geborgd.
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, omdat SSD direct bijdraagt aan veilige software voor server en mobiele applicaties, een level playing field creëert wordt de uitwisseling binnen de overheid en de samenwerking tussen partijen, inclusief die tussen opdrachtgever en softwareleverancier verbeterd.

III. Inhoudelijke criteria

De inhoudelijke criteria worden gebruikt voor het expertonderzoek om te adviseren over het al dan niet opnemen van de standaard op één van de lijsten. U kunt voor het beantwoorden van deze vragen de tekstvlakken bij de betreffende criteriavragen gebruiken. De vragen dienen beantwoord te worden met Ja, Nee of Onbekend en altijd te worden voorzien van een toelichting op het antwoord.

1. Inhoudelijk criterium: Toegevoegde waarde

Criterium: De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

Vragen:

1.1	**Verhoudt de standaard zich goed tot andere standaarden?**
1.1.1	Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?

	De standaard maakt gebruik van bestaande standaarden. Daar waar andere standaarden referentiestandaarden zijn, die nog niet de duidelijkheid geven van hoe toepassing moet plaatsvinden, is SSD juist een standaard die kan worden aangeduid worden als toepassingsnorm.
1.1.2	Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? *(Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)*
	Ja, omdat zonder technologiespecifiek te worden, de beveiligingsstandaarden in de vorm van volgens een specifieke beschrijvingswijze vastgelegde criteria begrijpbaar zijn gemaakt voor de opdrachtgever, duidelijkheid geeft naar de softwarebouwer en de testers en zonder op de stoel te gaat zitten van de ontwikkelaar. Daar waar bestaande referentiekaders de onderlinge verwachtingen niet duidelijk maken, zijn die bij SSD expliciet gemaakt, waardoor de samenwerking in de keten verbeterd.
1.1.3	Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?
	Ja, het lukte opdrachtgevende organisaties niet om softwareleveranciers eisen mee te geven die wel zouden leiden tot veilige software. Het lukte omgekeerd softwareleveranciers in ene level playing field veilige software te leveren. Het resultaat was dat partijen zich op basis van prijs konden inkopen of dat er eisen werden gesteld die enerzijds niet toetsbaar waren en anderzijds te rigide werden geëist. In tegenstelling tot bestaande standaarden betreft dit een toepassingsnorm die ingaat op onderlinge verwachtingen, daar waar dat bij anderen ontbreekt.
1.1.4	Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?
	NIST, OWASP, ISO 20002

1.2	**Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?**
1.2.1	Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?
	Ja, het toepassen van Grip op SSD draagt bij aan het algehele veiligheidsgevoel, de kans dat de organisatie een vertrouwde organisatie blijft voor de burger en/of ander organisatie en het maakt op een eenvoudige manier duidelijk wat het beveiligingsniveau is in vergelijking met andere partijen.
1.2.2	Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?
	Ja, elke (intern/extern) leverancier kan SSD toepassen. Doordat geen dure audits nodig zijn op de organisatie van de leveranciers draagt SSD bij aan de mogelijkheid te kiezen voor meerdere partijen en bevordert het de strategie van de modulaire inkoop.
1.2.3	Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?
	Ja, de methode is laagdrempelig, er zijn geen dure audits nodig en mogelijkheid te kiezen voor meerdere partijen en de mogelijkheid te kiezen voor de strategie van de modulaire inkoop maakt een betere prijsstelling en een bedrijfsvoering op tegen lagere kosten mogelijk.
1.2.4	Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

	De beveiligingsrisico's nemen af, omdat het die risico's minimaliseert vergroot het de informatie- en de gegevensuitwisseling veiligheid
1.2.5	Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
	De beveiligingsrisico's nemen af, omdat het die risico's minimaliseert vergroot het de informatie- en de gegevensuitwisseling veiligheid

2. Inhoudelijk criterium: Open standaardisatieproces

Criterium: De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

Let op: ook de grijs gemarkeerde vragen dienen positief beantwoord te worden wil een organisatie in aanmerking komen voor de status uitstekend beheerproces.

Vragen:

2.1	**Is de documentatie voor eenieder drempelvrij beschikbaar?**
2.1.1	Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?
	Ja, is zonder kosten te downloaden en is voor iedere organisatie beschikbaar en toepasbaar.
2.1.2	Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?
	De documentatie sluit aan op wat nodig is op strategisch, tactisch en operationeel niveau

2.2	**Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is**
2.2.1	Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?
	Voor de CIP producten geldt de Creative Commons Naamsvermelding GelijkDelen 4.0
2.2.2	Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?
	Ja.

2.3	**Is de inspraak van eenieder in voldoende mate geborgd?**
2.3.1	Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?

	Ja door de inzet van een practitioner community, waarin de markt, maar ook de gebruikende organisaties vertegenwoordigd zijn.
2.3.2	Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
	Ja, besluitvorming in de SSD practitioner community. Hierin zijn overheid organisaties en marktpartijen vertegenwoordigd.
2.3.3	Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?
	Niet van toepassing. De community is een open community. De meerderheid beslist.
2.3.4	Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?
	Ja, www.cip.pleio.nl en de SSD practitioner community (3xper jaar).
2.3.5	Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld? Zie ook bijlage 3 uit de toetsingsprocedure en criteria.
	Ja, www.cip.pleio.nl Consultatie in SSD practitionar community.

2.4	**Is de standaardisatieorganisatie onafhankelijk en duurzaam?**
2.4.1	Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?
	Ja, www.cip-overheid.nl
2.4.2	Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?
	Ja, CIP is één van de speerpunten van de compacte overheid en is sinds 6 jaar operationeel.

2.5	**Is het (versie) beheer van de standaard goed geregeld?**
2.5.1	Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers). Bij voorkeur is dit beleid ook beschreven in een beheerplan.
	Ja, www.cip.pleio.nl
2.5.2	Is de beheerdocumentatie goed vindbaar en verkrijgbaar?
	Ja, www.cip.pleio.nl.
2.5.2	Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

	Ja
2.5.3	Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?
	Ja volledig, via CIP als speerpunt van de compacte overheid
2.5.4	Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?
	Ja, beiden zijn tientallen jaren werkzaam in het functioneel toepassingsgebied.

3. Inhoudelijk criterium: Draagvlak

Criterium: Aanbieders en gebruikers hebben voldoende positieve ervaring met de standaard.

Vragen:

3.1	**Bestaat er voldoende marktondersteuning voor de standaard?**
3.1.1	Bieden meerdere leveranciers ondersteuning voor de standaard?
	Ja, www.cip-overheid.nl manifestpartijen.
3.1.2	Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
	Ja, SSD kan volledig getoetst worden door audits en/of testen
3.1.3	Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn?
	Ja, SSD is voor elk software object toepasbaar.
3.1.4	Zijn er referentieprofielen van de standaard aanwezig en zijn deze referentieprofielen vrij te gebruiken?
	nvt

3.2	**Kan de standaard rekenen op voldoende draagvlak?**
3.2.1	Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
	Ja, www.cip-overheid.nl manifestpartijen
3.2.2	Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
	Ja, UWV, CBIG, Cap Gemini, CGI, ICTU, Centric, min VWS.

3.2.3	Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
	Ja
3.2.4	Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
	Ja, SSD is geaccepteerd door het BOCU en de markt. Voor het laatste zie de persvermeldingen en uitingen. 21 manifestpartijen die SSD ondersteunen. Practitioner bijeenkomsten 3 x per jaar sinds 4 jaar en nog steeds er g aktief.

4. Inhoudelijk criterium: Opname bevordert adoptie

Criterium: De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Toelichting lijsten:

a. Met de lijst wil het Nationaal Beraad de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (open standaardisatieproces, toegevoegde waarde, draagvlak);
b. Met 'pas toe of leg uit' beoogt het Nationaal Beraad dit soort standaarden verplichten als:
    1. hun huidige adoptie binnen de (semi-)overheid beperkt is;
    2. opname op de lijst bijdraagt aan de adoptie door te stimuleren o.b.v. het 'PToLU; - regime. (functie=stimuleren).
c. Met aanbevolen beoogt het Nationaal Beraad dit soort standaarden aan te bevelen als:
    1. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
    2. Standaarden interoperabiliteit bevorderen maar waarvoor verplichting een te zwaar middel is.
    3. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen. (functie=informeren)

Vragen:

4.1	**Opname op de lijst bevordert de adoptie van de standaard.**
4.1.1	Is "pas toe of leg uit" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?
	Nader te bepalen!
4.1.2	Is de status aanbevolen open standaard het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?
	Ja, het geeft direct een versnelling in het realiseren van een veilige overheid voor het object (bedrijfs) software.

Verzending

Als u het aanmeldingsformulier zo volledig mogelijk heeft ingevuld, dan kunt u deze als bijlage versturen naar forumstandaardisatie@logius.nl

Gebruikt u dan als onderwerp: "Aanmelding standaard".
Na ontvangst van het formulier ontvangt u binnen 5 dagen een ontvangstbevestiging per e-mail.

Bedankt voor uw aanmelding.