

#	Vraag	Antwoord
1	Kunt u iets duiden qua aanleiding, doelstelling en scope van uw behoefte? Kunt u bijvoorbeeld qua scope inzicht geven in aantallen server certificaten, end-user-device certificaten, SSH-keys, zijn er binnen software development specifieke certificate usecases (zoals Kubernetes CI/CD en Codesigning)?	De aanleiding is eenvoudig dat de geldigheidsduur van externe certificaten de komende jaren sterk wordt verkort. We willen daarom voor alle certificaten het proces van vervangen zoveel mogelijk automatiseren. Wij willen voor zoveel mogelijk, zowel interne als externe, certificaten menselijke handelen overbodig maken. Wij hebben op dit moment zo'n 160 externe en 360 interne certificaten. Op dit moment richten wij ons op SSL/TLS en PKI certificaten voor servers en applicaties, maar er moet rekening gehouden worden met de mogelijkheid dat wij dit ook op andere fronten zullen gaan inzetten.
2	Daarnaast vernemen wij graag hoe het proces voor aanvraag en uitgifte van interne certificaten momenteel is ingericht?	Het proces voor de aanvraag en uitgifte van interne certificaten is momenteel beperkt geautomatiseerd en grotendeels handmatig ingericht. Aanvragen worden ingediend via handmatige kanalen, waarna beoordeling en validatie door beheerders plaatsvinden. De uitgifte van certificaten gebeurt met behulp van afzonderlijke tooling, waarbij integratie tussen systemen beperkt is. Hierdoor ontbreekt een end-to-end geautomatiseerde workflow en is het proces relatief arbeidsintensief en minder schaalbaar.

3	Welke requirements zijn er vanuit compliance ten aanzien van beheer van type certificaten (bijvoorbeeld in relatie tot reporting en enterprise policies)?	De compliance-requirements richten zich op centrale regie, volledige traceerbaarheid en naleving van standaarden over de gehele certificaat-lifecycle. Certificaten en sleutels moeten centraal worden beheerd via een Key Management System met functiescheiding en strikte toegangscontrole, waarbij eigenaarschap expliciet is belegd. Voor reporting en auditing geldt dat alle handelingen rondom certificaten en sleutels (zoals uitgifte, gebruik en intrekking) volledig worden gelogd en gemonitord, inclusief wie, wat en wanneer, en dat relevante kenmerken van certificaten worden geregistreerd. Daarnaast is het verplicht om erkende (inter)nationale standaarden en richtlijnen te volgen, certificaten periodiek te evalueren en proactief te vernieuwen, en een formeel aanvraag- en uitgifteproces via de interne Registration Authority te hanteren. Samengevat ligt de nadruk vanuit compliance op controleerbaarheid, standaardisatie en duidelijke verantwoordelijkheden binnen het beheerproces.
4	Kunt u aangeven welke interne Certificate Authority (leverancier en versie) momenteel in gebruik is binnen uw organisatie?	Dat is voor deze fase van dit traject geen relevante informatie.
5	Bevat de scope van deze RFI en te verwachten RFP het leveren van een (interne) CA, of blijft de bestaande CA behouden?	Initieel zullen wij hoogstwaarschijnlijk de bestaande CA's behouden, dus het leveren van een CA zal dan geen onderdeel zijn van de RFP. Wij verwachten van de voorgestelde oplossing wel de flexibiliteit om gemakkelijk over te stappen naar een andere CA en/of meerdere CA's te kunnen gebruiken.
6	Welke publieke PKI gebruikt u momenteel?	Dat is voor deze fase van dit traject geen relevante informatie.

7	Vallen TLS-certificaten binnen de scope van de uitvraag? Zo ja, waar worden deze ingezet? Omvat dit web servers, WAF, load balancers, appliances, applicaties en hoeveel TLS-certificaten worden er beheerd?	Ja, TLS-certificaten vallen binnen de scope van de uitvraag. TLS-certificaten worden binnen de organisatie breed ingezet voor het beveiligen van communicatie en identiteiten van systemen. Dit omvat onder andere toepassingen op web servers, web application firewalls (WAF), load balancers, appliances en applicaties. Tegelijkertijd is de inzet niet beperkt tot deze categorieën; TLS-certificaten worden ook toegepast op overige en toekomstige platformen, componenten en diensten waar versleutelde communicatie of authenticatie vereist is. De gevraagde oplossing dient daarom rekening te houden met een breed en dynamisch toepassingsgebied, waarbij ondersteuning nodig is voor zowel bekende inzetgebieden als voor nog niet gespecificeerde of toekomstige toepassingen en technologieën. Het aantal TLS-certificaten dat wordt beheerd varieert en is afhankelijk van ontwikkelingen in het landschap, waardoor schaalbaarheid en flexibiliteit belangrijke uitgangspunten zijn voor de gevraagde oplossing.
8	Maken certificaten ten behoeve van Domain Control Validation (DCV) ook onderdeel uit van de uitvraag en maakt de DCV-automatisering ook deel uit van uw automatiseringsbehoeften voor de CLM?	Op dit moment valt dit nog niet binnen de scope van de uitvraag. Wel is het goed mogelijk dat dit in de nabije toekomst alsnog aan de orde komt. De gekozen oplossing zou daarom hierop voorbereid moeten zijn, zodat uitbreiding naar DCV en DCV-automatisering later zonder ingrijpende aanpassingen kan worden gerealiseerd.
9	Vallen apparaat certificaten binnen de scope van deze marktverkenning? Zo ja, aan hoeveel apparaten wilt u certificaten uitreiken? Hoeveel certificaten per apparaat?	Vooralsnog gaat het alleen om servercertificaten. Er zijn vooralsnog geen concrete plannen voor overige apparaat certificaten, deze optie willen we echter wel openhouden.
10	Welke private PKI gebruikt u momenteel?	Dat is voor deze fase van dit traject geen relevante informatie.
11	Zijn uw apparaten gekoppeld aan een Mobile Device Management tool? Zo ja, welke technologie gebruikt u?	Dat is voor deze fase van dit traject geen relevante informatie.
12	Wat is uw voorkeur: on-premises of een SaaS-model?	In principe denkt de SVB aan een SaaS-model. Maar wij zijn nadrukkelijk op zoek naar een gefundeerd advies over de beste keuze, mede maar niet uitsluitend vanwege de discussies over digitale soevereiniteit. Wij achten het niet onmogelijk dat een (deels) on-premise oplossing uiteindelijk de beste keuze blijkt te zijn.
13	Welke Hardware Security Module (HSM) en/of Key Management System (KMS) gebruikt u momenteel?	Het gebruik van HSM en de keuze voor een specifieke HSM-oplossing vallen op dit moment buiten de scope van deze aanbesteding. Wel is van belang dat de aangeboden CLM-oplossing geschikt is voor samenwerking met bestaande en toekomstige KMS-oplossingen, HSM-omgevingen en BYOK-functionaliteit, zodat eventuele uitbreiding in een later stadium zonder ingrijpende aanpassingen mogelijk is.

14	Op welk platform wilt u de oplossing implementeren (Kubernetes, OpenShift, VM)?	Hier heeft de SVB nog geen duidelijke voorkeur en zijn wij vooral benieuwd naar uw gefundeerde advies.
15	Kunt u uw DevOps-omgeving beschrijven?	Dat is voor deze fase van dit traject geen relevante informatie.
16	In nr.10 van uw vragenlijst stelt u dat u de kosten van het hogere SEAL-niveau wilt weten voor de CLM-oplossing. De bepaling van het SEAL-niveau is echter afhankelijk van de toegepaste PKI-architectuur waarbij de digitale sleutels bijvoorbeeld worden opgeslagen in een HSM van Europees fabricaat. Wenst u uw PKI-architectuur te beveiligen met behulp van HSM's en vallen deze binnen de scope van de uitvraag?	Wij voorzien inderdaad dat wij binnen afzienbare termijn gebruik gaan maken van een HSM. U zou in de beantwoording van onze vraag uit kunnen gaan van de beschikbaarheid daarvan. De HSM zelf is buiten scope van deze aanbesteding.
17	Kunt u meer informatie geven over het type certificaten voor deze use cases? Is er een menselijke identiteitscertificaat nodig? Stelt het contract van SVB met PKIOverheid uw team in staat hun API te gebruiken?	De huidige scope betreft uitsluitend SSL/TLS en PKI. Menselijke identiteitscertificaten zijn momenteel niet benodigd, maar kunnen in de toekomst mogelijk wel van toepassing zijn. Het contract van SVB met PKIOverheid maakt het gebruik van de PKIOverheid-API mogelijk, maar daarvan wordt op dit moment nog geen operationeel gebruik gemaakt.
18	We hebben in 2025 een uitgebreide POC gedaan voor een On-premise CLM-oplossing. Heeft een on-premise oplossing de voorkeur boven de cloudoplossing? Of zoekt u een softwareoplossing die kan worden geïmplementeerd in de EU-cloud of de soevereine cloud, of een echt cloud native SaaS-oplossing? Kunt u dit beargumenteren.	Zie het antwoord op vraag 12. Wij hebben op dit moment nog geen duidelijke voorkeur. We zijn zeer benieuwd naar uw advies en/of de voor- en nadelen van de verschillende opties.
19	Welk niveau van SEAL is vereist om het operationele proces van SVB te waarborgen met betrekking tot certificaatbeheer?	Dat is een goede vraag die wij helaas nog niet goed kunnen beantwoorden. Het uitgangspunt is in principe het hoogst haalbare niveau. Wij willen door deze marktverkenning een beter beeld krijgen van wat leveranciers tegen acceptabele kosten kunnen bieden, zodat we bij de aanbesteding deze vraag wel concreet kunnen beantwoorden.
20	Bent u van plan de bestaande Microsoft AD CS te vervangen door een interne PKI of private CA te hosten? Is dit onderdeel van het huidige initiatief, samen met de CLM-vereiste? Kunt u dit in context zetten en beargumenteren.	Wij hebben hiervoor op dit moment geen concrete plannen, maar sluiten het op voorhand ook niet uit. Wij hopen met de reacties op deze marktverkenning dit soort beslissingen te kunnen maken.