PKI

Drie belangrijke aandachtspunten voor een Public Key Infrastructure (PKI)

Digitale sleutels (certificaten) worden gebruikt om bij de uitwisseling van gegevens de vertrouwelijkheid en authenticiteit van zowel de zender als de ontvanger vast te stellen en de onderlinge communicatie te versleutelen. Om die redenen is een solide PKI van onschatbare waarde voor de organisatie.

Een PKI zorgt voor het uitdelen, controleerbaar maken en bewaren van certificaten via een waterdicht proces en met hoogwaardige technologie. Voor highend/hightech oplossingen op het gebied van informatietechnologie en informatiebeveiliging, is het belangrijk dat de oplossing:

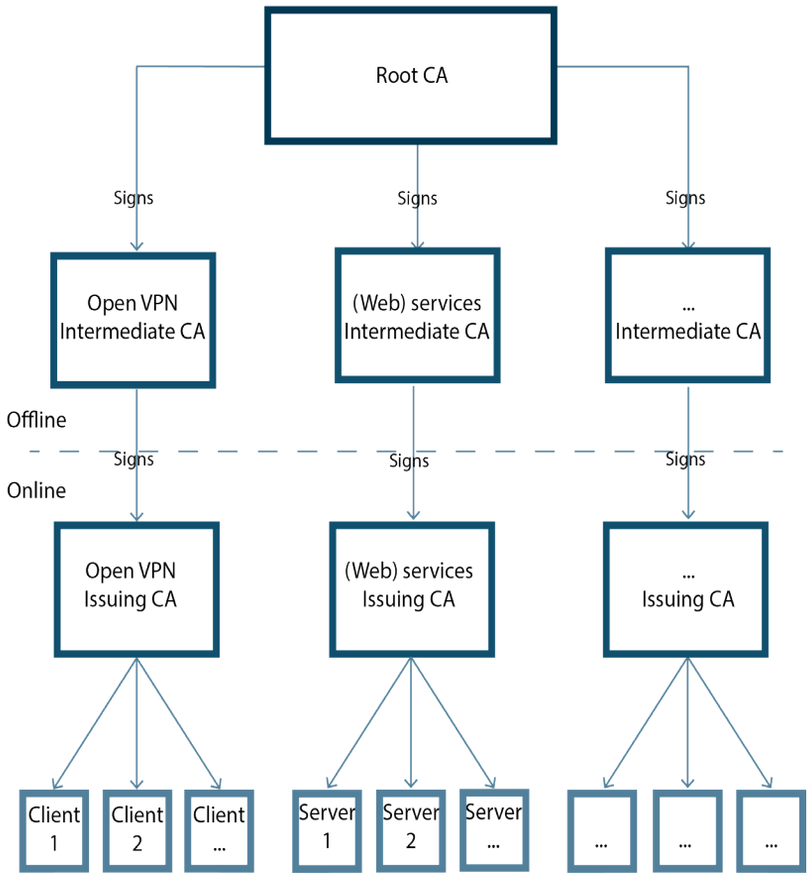
1. is ontworpen vanuit de praktijk;
2. nu al rekening houdt met de techniek van de toekomst;
3. het governance proces rond uitgifte, verspreiding en intrekking van certificatenondersteunt.

De praktijk

De verschillende certificaten in een PKI worden bij meerdere soorten digitale processen gebruikt. Bijvoorbeeld voor het controleren van iemands identiteit, voor het versleutelen van gegevens 'in transit' (denk aan SSL/TLS en VPN verbindingen en IoT device communicatie) en voor het zetten van een elektronische handtekening. Omdat een certificaat bestaat uit een publieke en private sleutel en het essentieel is dat de private sleutel niet wordt gedeeld is het noodzakelijk om voor elk persoon, apparaat en/of dienst een eigen certificaat beschikbaar te stellen.

TEDAS
SENSE FOR SAFETY

Een situatie, waarbij het mogelijk is om onrechtmatig een certificaat te bemachtigen, leidt tot een verlies aan vertrouwen in de uitgevende PKI. Het onrechtmatig verkregen certificaat zorgt ervoor dat er geen garantie meer kan worden afgegeven ten aanzien van de authenticiteit en vertrouwelijkheid van gegevens. Mocht er zich, om welke reden dan ook, toch een compromittatie voordoen dan zorgt een goed ontworpen PKI hiërarchie ervoor dat de effecten worden beperkt en de overige certificaten kunnen blijven functioneren.



Afb. 1
Hiërarchie

Dit laat onverlet dat alle certificaten in de hiërarchie fysiek goed moeten worden beveiligd, en dat toegang tot de certificaten moet worden gecontroleerd via een proces dat een onomstotelijke relatie vastlegt tussen een persoon en/of systeem, en de betreffende handeling. De crisis bij DigiNotar in 2011[3], laat goed zien dat misbruik van certificaten grote gevolgen heeft voor het vertrouwen in de betrokken gegevensketens.

Iedereen begrijpt dat bij grote organisaties het beheer van certificaten complex is. Veel mensen, veel data, systemen en devices, veel communicatiekanalen.

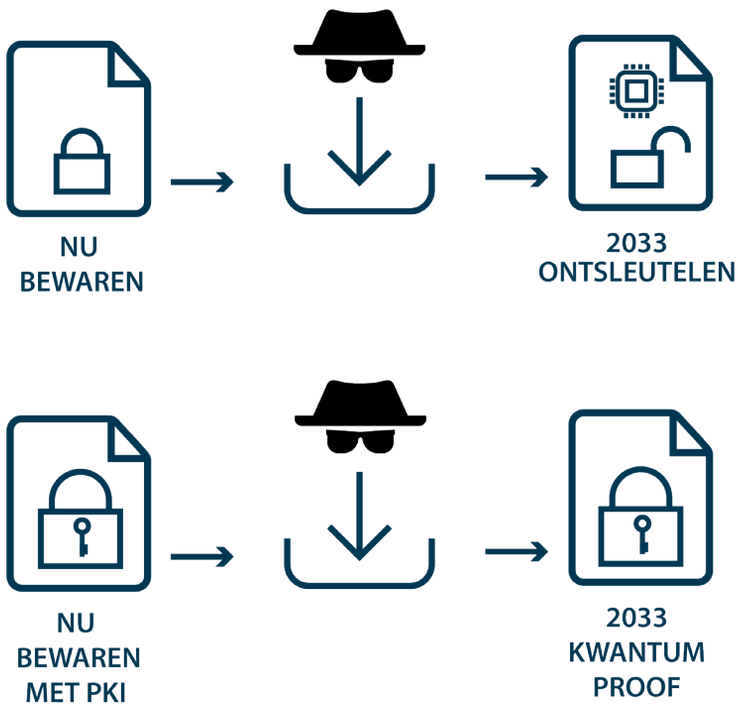
Afb. 2
Het beheer van certificaten is complex

Toch kunnen ook kleine organisaties of zelfs projecten baat hebben bij een PKI. Denk hierbij aan situaties waar een hoog beveiligingsniveau vereist is. Certificaten hebben hier een relatief korte levensduur en de uitgifte en inname ervan moet waterdicht worden geregeld.

Nu en de toekomst

Toekomstbestendig zijn betekent in het geval van PKI: 'nu handelen'. De verwachting is, dat er rond 2033 kwantumcomputers te koop zijn[7], waarmee de vandaag versleutelde gegevens eenvoudig kunnen worden ontcijferd. Om die reden zijn er nu al criminelen die onder het mom van 'Nu bewaren, later ontsleutelen'[6] op grote schaal versleutelde gegevens verzamelen om ze, zodra kwantumcomputers genoeg mogelijkheden hebben, te ontcijferen!

Nieuwe, betere versleutelingsalgoritmes zijn nodig. Hoe groot dit probleem is hangt af van het moment waarop de versleutelde gegevens veilig worden bewaard, en de duur van de bewaarperiode. Versleutelde gegevens die vandaag worden gestolen, worden in 2033 mogelijk ontcijferd. Als er nu maatregelen worden genomen zijn alle gegevens vanaf vandaag beschermd, maar gegevens die eerder dan vandaag zijn opgeslagen zijn onbeschermd, zonder dat we daartegen kunnen optreden. Als we later dan vandaag maatregelen nemen dan wordt deze kwetsbare tijdsduur langer.



Afb. 3
'Nu bewaren, later ontsleutelen'

Een omgeving waarin de hoogste categorie van gegevensbeveiliging noodzakelijk is[2], is daarom gebaat bij een gegevensuitwisseling- en opslag op kwantumniveau.
Er bestaan heden ten dage al PKI oplossingen die kwantum-proof zijn. Er worden nieuwe standaarden voor versleutelingsalgoritmen ontwikkeld onder de naam Post-Quantum Cryptography. Quantum Key Distribution (QKD)[1] is een methode voor het uitwisselen van een geheime sleutel op basis van kwantummechanica principes. Bij QKD is het uitermate lastig om onopgemerkt afgeluisterd te worden vanwege de natuurkundge eigenschappen van in de communicatie gebruikte kwantumdeeltjes[4].

Techniek en proces

De 'I' in PK 'Infrastructure' gaat over techniek én proces. De software ondersteunt de menselijke beslissing. Uiteindelijk worden certificaten gekoppeld aan personen en organisaties. De configuratie van deze koppeling verandert vaak en veel. Mensen komen in dienst, krijgen een rol in de informatiebeveiliging, verwerken gegevens en maken nieuwe, en vervolgens verlaten ze de organisatie. Organisaties zelf veranderen ook van samenstelling en grootte. De verantwoordelijkheid voor de aansturing van de processen die de certificaten uitdelen en intrekken ligt uiteindelijk bij mensen. Een hoog veiligheidsniveau betekent daarom niet alleen adequate techniek, maar ook: audit en monitoring van processen en personen.

Een belangrijk punt bij het opstellen en uitbreiden van de procedures is dat ze realistisch zijn om te implementeren en haalbaar voor de mensen om zich er aan te houden[5]. De personen die de hoofdcertificaten beheren hebben doorgaans ieder een deel van de verantwoordelijkheid bij een noodverhandeling in geval van gecompromitteerde certificaten. In zo'n geval dienen deze personen op korte termijn aanwezig te zijn. Dit betekent dat het belangrijk is om functies en verantwoordelijkheden af te wegen, tezamen met de snelheid om fysiek in het gebouw aanwezigheid te zijn. Als een betrokkene een functie heeft waarbij hij/zij geregeld moet reizen of te ver weg woont, is die persoon wellicht niet de meest geschikte kandidaat.

Verder moet nagedacht worden wie eventueel deze persoon kan vervangen in geval van verlof, ziekte of plotseling overlijden. Ook voor deze reservepersoon dienen afwegingen gemaakt te worden. Het mag niet zo zijn dat deze persoon als reservist voor meerdere collega's waarneemt in het proces, omdat dit de scheiding van verantwoordelijkheden vermindert.

Conclusie

Het inrichten van een PKI is geen kwestie van plug-and-play. Een degelijke PKI is een PKI die is ontworpen op basis van praktische ervaring. In het ontwerp wordt rekening gehouden met drie zaken.

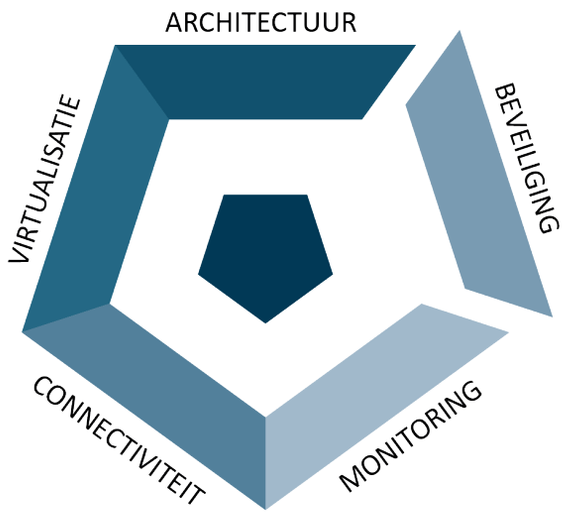
Allereerst de complexiteit van de organisatie en het aantal assets in- en de configuratie van het netwerk van devices en systemen. Op welke manier kan dit worden gesegmenteerd zodat enerzijds de impact van een mogelijk beveiligingslek wordt verkleind en anderzijds de distributie van de certificaten, controleerbaarheid en optimale fysieke bereikbaarheid mogelijk maakt.

Ten tweede: de bewaartijd en het beveiligingsniveau van de gegevens. Hierop wordt de versleutel methode (kwantumveilig of niet) en de levensduur van de certificaten gebaseerd.

Tenslotte: de organisatie. Selecteer de sleutelbewaarders zorgvuldig en implementeer een methode voor governance. Een Trusted Third Party (TTP) inschakelen behoort hierbij ook tot de mogelijkheden.

Waarom PKI bij Tedas

Vanwege onze jarenlange ervaring met klanten uit opsporings-, inlichtingen & veiligheidsdomein en Defensie snappen wij als geen ander dat veiligheid en gemak lastig samengaan. Wij hebben onze oplossing Bastion daarom zo ontworpen, dat door middel van flexibele maatregelen toch een veilige én werkbare oplossing is gemaakt. Gepokt en gemazeld als we zijn verbazen we ons niet meer over de creativiteit van criminelen én de snelheid van technologische ontwikkelingen. Wij denken vooruit en maken het veilig.



Afb. 4
PKI valt onder het onderdeel Beveiliging van Bastion

Referenties

[1] ETSI- Quantum Key Distribution | Quantum cryptography, August 2020. Library Catalog: www.etsi.org.
[2] bio overheid.nl. Home NL- bio-overheid, 2019.
[3] Fox-IT B.V. Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach, 2012.
[4] Artur K. Ekert. Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6):661–663, August 1991.
[5] Amir Jafri and June Leung. PKI Deployment – Business Issues. page 15,2005.
[6] I.S. Kabanov, R.R. Yunusov, Y.V. Kurochkin, and A.K. Fedorov. Practical cryptographic strategies in the post-quantum era. arXiv:1703.04285 [quantph],page 020021, 2018. arXiv: 1703.04285.3
[7] Michael J.D. Vermeer and Evan D. Peet. Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption, 2020. Library Catalog: www.rand.org Publisher: RAND Corporation.4

TEDAS
SENSE FOR SAFETY

info@tedas.nl | www.tedas.nl