Voorwoord Albert de Ruiter

Policy Authority PKIoverheid, Logius

Behorend bij Whitepaper:

Meer dan 60% van de publieke web certificaten in gebruik bij gemeenten voldoet niet aan de BIO2.0

Voorwoord

Vertrouwen komt te voet en gaat te paard. Dat was vroeger al zo en zal niet snel veranderen. En het vakgebied waar ik me op focus? Dat gaat over vertrouwen pur sang.

Vroeger was het relatief gemakkelijk om iemand te vertrouwen. Want je zag elkaar, kwam op visite, had een band met een individu en schudde handen waardoor je wist met wie je zakendeed. Tegenwoordig ligt de hele wereld binnen handbereik én wordt een groot deel daarvan digitaal georganiseerd. De hamvraag is dus niet alleen hoe je dit vertrouwen (ook internationaal) gaat organiseren, maar ook hoe je dit aantoont en borgt. Dát is mijn passie.

Unieke rol

Nederland is een van de weinige landen in Europa waar een publiek private samenwerking rondom Public Key Infrastructure (PKI) voor de overheid is georganiseerd en is samengevat in een stelsel (PKIoverheid). Daarbij wordt samengewerkt met Qualified Trust Service Providers (QTSP-en), toezichthouders en overige belanghebbenden om de betrouwbaarheid van de digitale communicatie tussen de overheden, bedrijfsleven en burgers te waarborgen. In Amerika, Afrika en Azië kennen we soortgelijke constructies van Federale overheids PKI's waarin een publiek-private samenwerking plaatsvindt.
Als Policy Autoriteit (PA) speel je een sleutelrol als het gaat om vertrouwen. Mijn rol komt vooral neer op het bewaken van de samenhang qua wetgeving, het maken van beleid en het toezichthouden op het stelsel van PKI.
Om dat goed te doen kijken we naar alle wetgevingen, naar standaarden en naar bewegingen die zich plaatsvinden (nationaal en internationaal).

Over certificaten, cryptografie en quantumcomputers

Met de komst van Quantum computers die in potentie veel meer verwerkingskracht kennen dan traditionele computers (meerdere taken gelijktijdig kunnen uitvoeren) kunnen in de toekomst nieuwe toepassingen worden ontwikkeld op het gebied van medicijnen, energie, gezondheidszorg en financial services.
Dat levert, naast de genoemde kansen ook potentiële bedreigingen op, namelijk dat deze quantumcomputers de bestaande cryptografietechnieken de we gebruiken kunnen kraken. PKI heeft veel raakvlakken met cryptografie omdat certificaten hier gebruik van maken om digitale communicatie te beveiligen. Denk bijvoorbeeld aan digitale encryptie, de digitale handtekening of andere vormen van digitale authenticatie. Alle zaken die je digitaal doet en beveiligd worden met cryptografie kunnen, vooralsnog in theorie, in de toekomst gekraakt worden met een quantumcomputer. Ook dat is een reden waarom je je nú al bewust moet zijn van dit soort zaken, zodat je tijdig kunt reageren. Een voorbeeld hiervan is Apple die onlangs bekend heeft gemaakt dat hun berichtenapp iMessage inmiddels als quantumproof kan worden beschouwd door het aanpassen van Quantum Safe cryptografie (PQ3).

Het gaat om bewustzijn én actie

Uiteindelijk, en daar levert dit whitepaper een bijdrage aan, gaat het erom dat men zich bewust is van de dreigingen die met dit soort ontwikkelingen gemoeid gaan. Dat betekent ook dat je na moet denken over welke acties je kunt organiseren. En dat is waar we vanuit de overheid dag in, dag uit mee bezig zijn. Vanuit mijn rol werk ik samen met

organisaties als TNO, CWI, Microsoft en veel andere partijen. Zo ook in HAPKIDO, een Hybrid Approach-oplossing om organisaties te helpen met de transitie richting quantumveilige PKI's. Ook neem ik deel aan de post quantum werkgroepen van het PKI-consortium, het programma Quantumveilige Cryptografie van de Rijksoverheid en ben ik enthousiast driver en medeorganisator van het Post Quantum congres. Tot slot zijn we ook betrokken bij PKIoverheid producenten, waar veel mooie ontwikkelingen gaande zijn. Uitdagingen zijn er ook: de veranderende wet- en regelgeving en de policy-wijzigingen vanuit de browserpartijen, de NIS2 en de nieuwe versie van de eIDAS-verordening die op stapel staat, waarin onder meer remote identification een rol speelt. Kortom, er is beleid nodig: wéér een raakvlak met het whitepaper dat voor je ligt.

Het digitaal waarborgen van vertrouwen: dáár gaat het om

Bij PKI-landschappen is het belangrijk dat je een drietal zaken structureel in ogenschouw houdt: veiligheid, soevereiniteit en interoperabiliteit. Dat laatste zegt iets over hoe goed er onderling samengewerkt wordt, het gaat over helder communiceren en over kwalitatieve gegevensuitwisseling. In die drie pijlers wil je een balans vinden.

Dit betekent dat je rekening houdt met elkaars belangen, zowel internationaal als nationaal. Nederland is een handelsnatie: we richten ons volop op digitaal zakendoen met de wereld om ons heen. We hebben de plicht om dit als overheid zo veilig mogelijk te kunnen waarborgen. Daarom werken we vanuit beleid en houden we toezicht. Maar het is uiteindelijk aan de lokale overheden zélf om aan de slag te gaan.

En werk aan de winkel in bredere zin is er continu: ook rondom de opleidingen en audits. Zo merk ik bijvoorbeeld dat er een onderscheid is tussen de eisen die voortvloeien vanuit de wetgeving en de technische eisen. De technische eisen, die bijvoorbeeld gaan over hoe je een PKI opzet, die zijn anders dan de eisen die aan de processen gesteld worden. Het is belangrijk om die twee samen te brengen. Een PKI-omgeving opzetten is op zich zo gebeurd, maar het gaat erom dat je volledig vertrouwen kan hebben in het gehele systeem.

Over Europa en eIDAS

Verder zijn er verschillende initiatieven rondom digitaal samenwerken: EU-burgers moeten eenvoudig grensoverschrijdend kunnen werken. Stel dat iemand bij een instantie in het buitenland inzage nodig heeft in een bepaald register, dan kan dat bijvoorbeeld goed geregeld worden met een EU-wallet die toegang verleent. Dit soort ontwikkelingen vergemakkelijken het om digitaal zaken te kunnen doen, dit betekent ook dat bedrijven digitaal moeten kunnen ondertekenen. De grondlegging voor een dergelijke wallet is, hoe kan het ook anders, het certificaat. Wederom geldt dat het ecosysteem zo veilig mogelijk gehouden moet worden. Hoe je dat doet? Door goed te kijken naar de balans tussen de drie termen die ik eerder noemde: veiligheid, soevereiniteit en interoperabiliteit.

Nationale beweging de BIO2.0, de Baseline Informatiebeveiliging Overheid

Veiligheid is minstens zo belangrijk als de mogelijkheid hebben om interoperabel met elkaar te zijn. Dat geldt natuurlijk ook voor overheden die nauwe relaties hebben met haar burgers en bedrijfsleven. Daarvoor is een elektronische identificatie noodzakelijk. Je wilt uiteindelijk onomstotelijk vast kunnen stellen met wie je zakendoet.

Zo is er voor overheidsorganen een nieuwe handreiking ontwikkeld (de BIO2.0), de Baseline Informatiebeveiliging Overheid. Daarin wordt bijvoorbeeld gesteld dat de minimale vereiste om certificaten in zetten die van het niveau Organization Validated (OV) moeten zijn. Concreet betekent dit dat de organisaties gevalideerd dienen te worden en

ingeschreven staan bij de Kamer van Koophandel en de informatie zichtbaar wordt meegenomen in het certificaat. Hiermee is het voor eenieder zichtbaar dat het om vertrouwde partijen gaat. Naast OV-certificaten zijn er ook nog DV-certificaten (Domain Validated), EV-certificaten (Extended Validated) en QWAC- certificaten (Qualified Web Authentication). Je leest er meer over in dit whitepaper.

Goed huisvaderschap onmisbaar

Samenvattend, het belangrijkste is dat je de zaken goed organiseert, je processen in kaart brengt, dat je weet wat je doet en beseft waar je afhankelijkheden liggen. En dat je in staat bent om op een veilige manier digitaal zaken te doen en daarop toetst. Pas goed op jezelf, zou ik willen zeggen! Het tonen van goed huisvaderschap, met oog voor due dilligence en due care is onlosmakelijk verbonden met goed op jezelf passen.

Vertrouwen komt te voet en gaat te paard

Het in Nederland ontworpen PKIoverheid -stelsel is erg krachtig en we genieten, met ons land, volop vertrouwen en hebben met dit stelsel internationaal naamsbekendheid. Het stelsel werd al ontwikkeld voordat de eIDAS-verordeningen zijn intrede deed. Dat zegt wel wat. Met eIDAS (Electronic Identification and Trust Services) wil Europa bijdragen aan het wegnemen van digitale grenzen tussen landen uit de Europese Economische Ruimte. Zo kan de veiligheid van digitale systemen gewaarborgd worden en de privacy van mensen beschermd.

Het is zaak dat er, met de komst van alle nieuwe ontwikkelingen en eventuele bijbehorende eisen er continue gekeken wordt of je eraan voldoet om daarmee het aantoonbaar vertrouwen te genieten. En de oplossing? Die is simpel: beleid. Je past toe óf je legt uit waarom dit niet nodig is. Meer info in het whitepaper.
Ik opende dit voorwoord met een spreekwoord en sluit daar ook graag mee af: vertrouwen komt te voet en gaat te paard. En geloof mij, het is beter om aan te tonen dat hetgeen je zegt en biedt écht klopt, dan dat je klant, relatie of collega er maar op moet vertrouwen dat het zo is.

Albert de Ruiter

Policy Authority PKIoverheid, Logius
Dienst Digitale Samenleving
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De motivatie voor dit onderzoek

Door Ton Oosterwijk

De hypothese vond zijn oorsprong in 2020 toen duidelijk werd door een maatregel van het CA/B platform dat Logius, beheerder van PKIoverheid waaronder het uitgeven van Staat der Nederlanden webcertificaten, in 2021 geen scherp antwoord had op de risico's. Zij kwamen enkel met een algemeen advies over dat alle certificaten eender waren en elke overheid (nationaal en lokaal) zelf een eigen risico-inventarisatie moest doen. Oftewel niks anders dan de (hoogste) en helder afgekaderde norm PKIoverheid: pas toe of laat varen[10]. Deze stelling werd stelliger gesteund en uitgedragen als gevolg van de publicatie van NSCS[11]; die weliswaar dekkend was; maar tegelijkertijd geen stelling in nam wat nu werkelijk een alternatief was voor de tot dan toe geldende harde "PKIoverheid - pas toe of leg uit".

Het werd aan de partijen en de certificaatproducenten (TSP) overgelaten, er was geen regie-duiding en partijen hadden maar één zorg... dat de servers/site's en apps bereikbaar bleven. Ongeacht welke certificaten daarvoor ingezet werden; van elk authenticiteit niveau. Een inleidend onderzoek liet al snel zien dat Lokale Overheden veelal geen bewuste keuzes maakten voor welk type vervangende certificaten, maar dat een flink aantal ministeries, enkele gemeenten en ZBO's duidelijk, generiek en rigoureus kozen voor de EU variant QWAC, terwijl dit niet nodig of voorgeschreven was en ook niet door Logius, NCSC en de toen geldende BIO de norm was.

Nu met de komst van BIO2.0 wel een duidelijk minimaal niveau werd gesteld, kwam de vraag: hoe groot is de schade of achterstand opgedaan in de afgelopen 3 jaar? Welk achterstallig werk moet worden gerepareerd door de letterlijk honderden CISO's in een periode minder dan een jaar? Welke ketens moeten op orde worden gebracht met welke normen voor certificaten en het beheer daarvan? Brengt vergrijzing en de gang naar de cloud (meer ketenpartijen) een verhoogd risico met zich mee, zoals de de IBD beschreven in het Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten[12] (Gevaren in ketens uit het zicht)?

Al deze zorgen en met name onbeantwoorde onduidelijkheden werden en worden nog steeds, door IT medewerkers geuit, maar zij voelen zich niet gehoord. Mede ook door onbekendheid op bestuursniveau en door gebrek aan onderbouwde kennis bij belangenorganisaties, toezichthouders, adviseurs en IT-auditors.

10 Logius - Uitfasering uitgifte publiek vertrouwde webcertificaten PKIoverheid.

11 Logius - Factsheet NCSC over uitfasering webcertificaten van PKIoverheid.

12 Informatiebeveiligingsdienst Nederland (IBD)(2022) - Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023-2024.

PKI partners®

Seinstraat 22
1223 DA Hilversum
PKIpartners.nl

T 085 90 20 820
E info@pkipartners.nl

Dit whitepaper is voorzien van een eIDAS gekwalificeerd bedrijfszegel (QCert for ESeal) en gekwalificeerd tijdzegel (QTimestamp).

PKI partners®