Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Babylonische spraakverwarring in de cryptografie

Werken aan de basis. Van Nederland en ons Koninkrijk.

Inleiding

De migratie naar quantumveilige cryptografie is nodig om jouw organisatie (en diensten) digitaal veilig te houden. Belangrijke, toonaangevende publicaties – zoals het PQC-migratiehandboek – helpen je om wegwijs te worden in de wereld van quantumveilige cryptografische algoritmes, protocollen, standaarden en parameters. Waar deze termen voor de meesten herkenbaar zijn, valt op dat niet iedereen hieraan dezelfde betekenis geeft vanuit de eigen rol en expertise. Wat de één ziet als een primitieve, kent de ander als een algoritme, en wat de ene ziet als een standaard ziet de ander als een richtlijn.

Dit soort *Babylonische spraakverwarringen* maakt de dialoog tussen verschillende stakeholders over cryptografie onnodig complex en verwarrend. En dat kan een extra obstakel vormen in de tijdige migratie naar quantumveilige cryptografie. Maar hoe begrijp je elkaar als je andere dialecten spreekt? En hoe kan je hier het beste mee omgaan?

Om hier een antwoord op te geven beginnen we dit artikel met een (fictief) voorbeeld, waarmee we schetsen hoe dit soort verwarringen zich uiten in de praktijk. Vervolgens beschrijven we een referentiemodel, ontwikkeld binnen de werkgroep *crypto-agility* van het programma Quantumveilige Cryptografie NL (QVC-NL), dat aangeeft hoe dit soort spraakverwarringen ontstaan. Tenslotte geven we je een aantal praktische tips om te voorkomen dat je dezelfde termen gebruikt, maar toch langs elkaar heen praat. Dat draagt bij aan slagvaardigheid in de migratie naar quantumveilige cryptografie.

Een praktijkvoorbeeld: TLS in softwareontwikkeling

Laten we beginnen met een illustratief voorbeeld. Een bedrijf wil een nieuwe dienst ontwikkelen. Klanten kunnen gebruik maken van deze dienst via een app, die toegang geeft tot functionaliteit die draait op de backend systemen van het bedrijf. Het bedrijf ontwikkelt en beheert de dienst zelf. Verschillende rollen zijn betrokken bij de ontwikkeling: een producteigenaar, software architect en een ontwikkelaar. In dit voorbeeld heeft de opdrachtgever enige basiskennis van informatiebeveiliging en stelt in de opdracht expliciet dat de verbinding tussen de app en server beveiligd moet worden conform *de standaard*. Als ondersteuning voor zijn productontwikkelteam betrekt hij zelfs een cryptograaf bij de ontwikkeling.

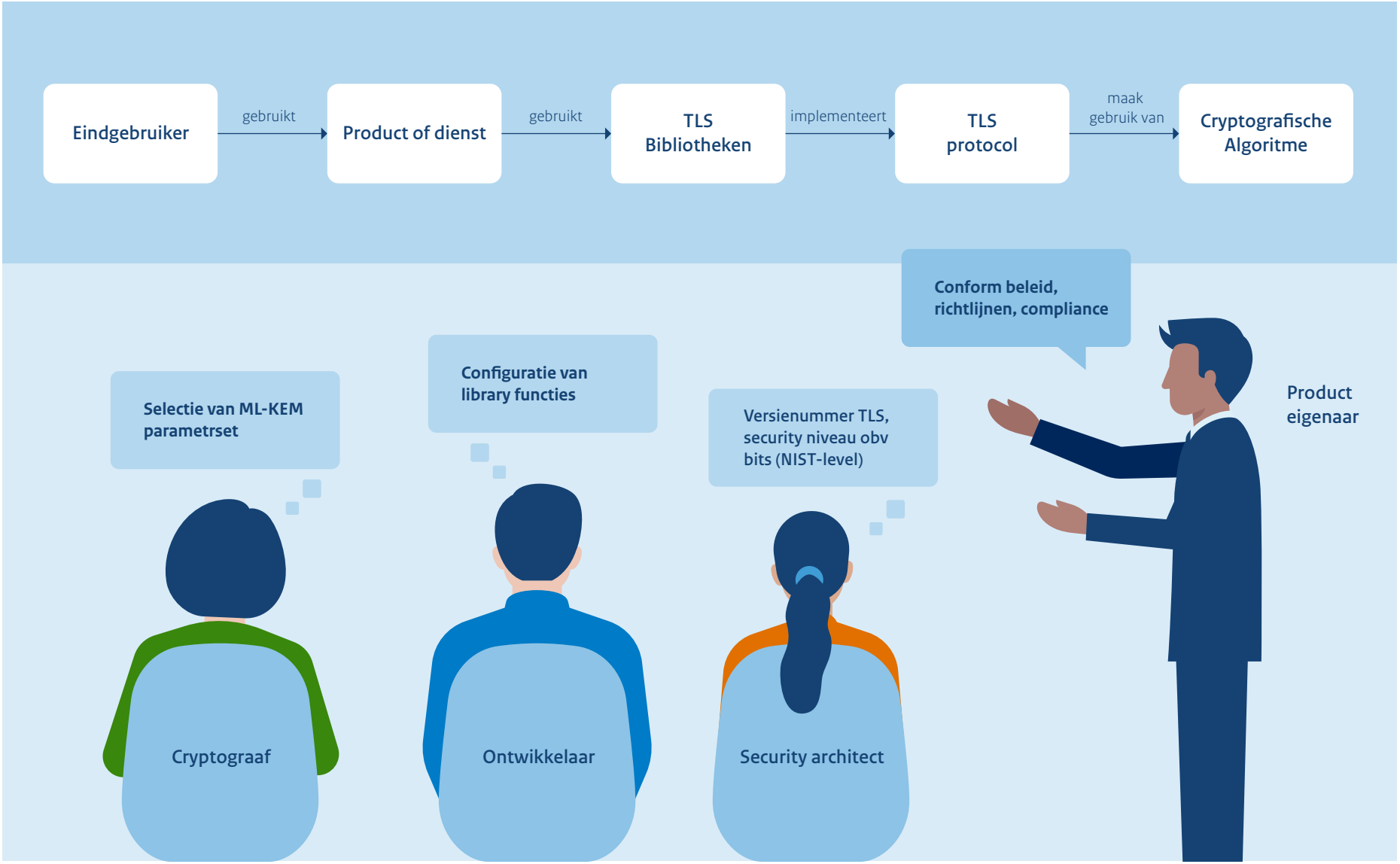
Het is uiteraard fantastisch dat de opdrachtgever zo vroeg in het ontwikkelproces denkt aan beveiliging! Maar de vraag lonkt: Wat is *de standaard*? Zonder verdere discussie gaan de verschillende betrokkenen aan de slag met de opdracht vanuit hun eigen expertise. De producteigenaar weet uiteraard dat de *standaard* refereert naar *standaard* informatiebeveiligingsdoelen die passen bij een digitale verbinding en formuleert zijn eisen in algemene termen zoals “vertrouwelijkheid” en “integriteitsbescherming”. De architect zoekt het meer in een *standaard* beveiligingsraamwerk en *standard practices* volgen. De ontwikkelaar vindt een set aan *de facto standaard* TLS-softwarebibliotheken, inclusief een aantal aanbevolen (gouden *standaard*) extensies.

En de cryptograaf kan niet wachten om de NIST-standaarden voor quantumveilige cryptografie te verwerken in het product.

Vanuit hun eigen expertise weten de verschillende betrokkenen invulling te geven aan hun opdracht. In de wandelgangen wordt vaak gesproken over hun activiteiten, maar pas later in het traject komen ze erachter dat ze met iets heel anders bezig waren dan beoogd. Ze trekken het recht, maar hadden ze dit eerder door, dan had ze dat veel tijd en moeite bespaard.

Juist in veelgebruikte termen, zoals parameter, standaard en algoritme, zit een valkuil verstopt. Mocht je niet weten hoe jouw gesprekspartner een dergelijke term gebruikt, dan loop je kans dat je er beide een andere invulling aangeeft.

Figuur 1: TLS standaarden vanuit verschillende perspectieven.



Begrijp de meerdere dialecten in cryptografie met het referentiemodel

Om inzicht te geven in de verschillende 'dialecten' die dezelfde (cryptografische) termen net iets anders gebruiken is een referentiemodel ontwikkeld. Met het referentiemodel wordt de complexe wereld van cryptografie toegankelijk gemaakt en vanuit diverse perspectieven belicht. Dat bevordert de samenwerking op het gebied van cryptografie. Het referentiemodel, geïllustreerd in *Figuur 2*, bestaat uit vijf lagen en is afgeleid van de onderwerpen die ook te vinden zijn in het PQC-migratiehandboek:

1. **Risicomanagement**: Op deze laag zullen nog geen aan cryptografie gerelateerde termen voor komen. Hier wordt wel de basis gelegd voor de eisen aan de onderliggende lagen.
2. **Informatiebeveiligingsdoelen** zijn een doorvertaling van algemene doelen en risicomanagement eisen naar doelen die een relatie hebben met informatiebeveiliging. Veel, maar niet alle, doelen hebben een relatie met cryptografie.
3. **Cryptografische functionaliteiten** zijn functionaliteiten die gerealiseerd kunnen worden met cryptografische protocollen. Deze dragen bij aan het halen van informatiebeveiligingsdoelen.
4. **Implementatie** is een concrete uitwerking van de cryptografische functionaliteiten, waarbij gebouwd wordt op cryptografische primitieven.
5. **Cryptografische primitieven** zijn elementaire bouwblokken die de basis vormen voor elk cryptografisch ontwerp en implementatie daarvan.

Figuur 2: Referentiemodel cryptografie. Per laag zijn veelvoorkomende termen beschreven.

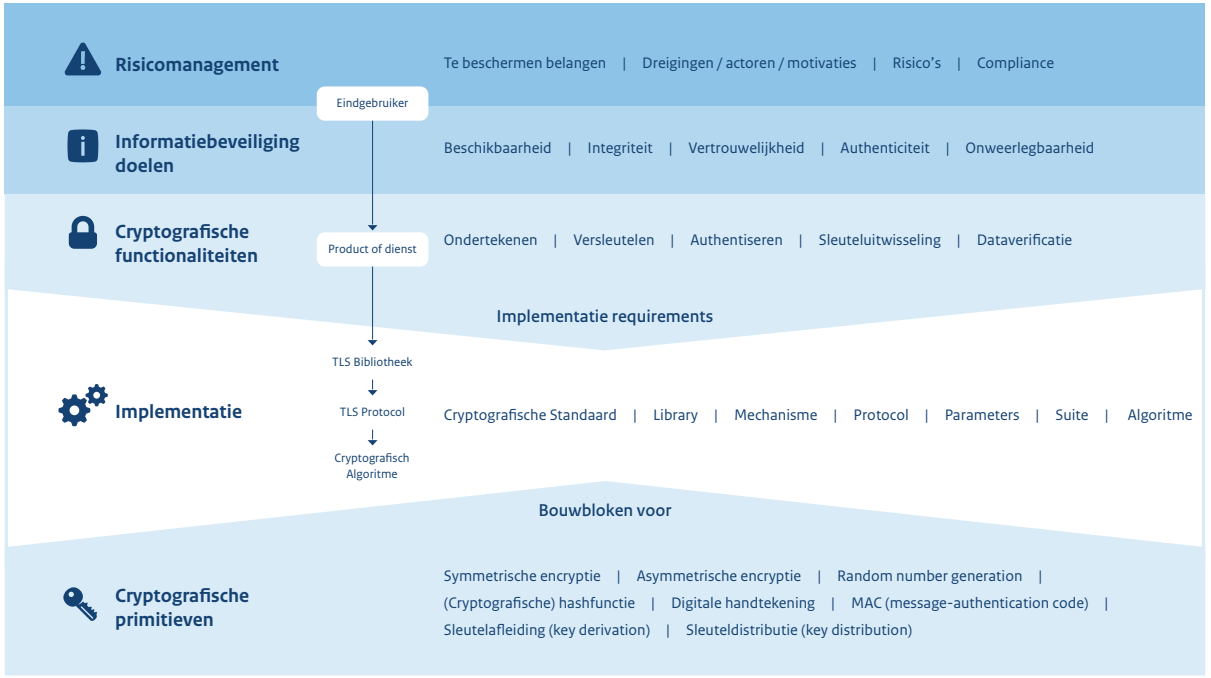
NB: Een PDF-versie met hoge resolutie van dit model is te vinden op https://www.digitaleoverheid.nl/quantumveilige-cryptografie/handige-linkjes/

In praktijk zien we de meeste verwarring ontstaan in de onderste lagen van dit diagram. Zo worden termen uit de lagen **cryptografische functionaliteiten, cryptografische primitieven** en **Implementatie** ogenschijnlijk door elkaar gebruikt, zelfs binnen vakliteratuur. Dat is ergens ook logisch: stakeholders met verschillende achtergronden en rollen zullen de termen herkennen, maar deze vanuit hun eigen expertise gebruiken. Dat zien we terug als we het eerdergenoemde voorbeeld rondom TLS spiegelen op dit referentiemodel in *Figuur 3*.

In dit figuur valt een aantal zaken op. Allereerst is er een duidelijke relatie tussen de wensen die op de risico-management laag worden beschreven en de impact hiervan op de implementatie. Onrealistische of niet goed omschreven wensen kunnen leiden tot een zwakke/ onvolledige uitwerking op implementatieniveau.
Het gebruik van een 'gemeenschappelijk taal' kan helpen om de verwachtingen over en weer te managen.

Verder is te zien dat het TLS voorbeeld binnen de implementatie laag diverse expertise en kennis vereist om tot een gewenst eindresultaat te komen. Zelden is slechts één persoon bezig met zowel het inrichten van de architectuur, het ontwikkelen van de functionaliteit en het verwerken van cryptografie. Dit is vaak een team prestatie van specialisten uit verschillende vakgebieden en organisatieonderdelen. Het niet spreken van dezelfde 'taal' kan leiden tot ongewenste of onjuiste toepassing van cryptografie.

Figuur 3: Het TLS voorbeeld getoetst op het referentiemodel.



Omgaan met Babylonische spraakverwarringen

Met bovenstaande in ogenschouw kun je je vast situaties herinneren waarin jij en je collega's langs elkaar heen praatten. Mogelijk heeft dat er toe geleid dat jullie activiteiten (en resultaten) niet conform verwachting waren, met als gevolg dat je langer bezig was met een project dan nodig.

Hoe herken je dit soort babylonische spraakverwarringen tijdig en hoe ga je hiermee om? Een eenduidig antwoord is er niet, maar de volgende tips kunnen je helpen.

- → Bespreek met elkaar de cryptografische begrippen die voor dit project aan bod komen en verkrijg duidelijkheid over elkaars opvattingen en taakinvulling. Spiegel deze aan het referentiemodel.
- → Documenteer binnen het project wie welke betekenis geeft aan relevante termen. Een voorbeeld is het onderstaande tabel. Daardoor weet iedereen precies wat bedoeld wordt en wat de afspraken zijn.
- → Het is niet altijd een probleem dat je, vanuit jouw eigen perspectief, een andere definitie hanteert. Gebruik het referentiemodel om de verschillende definities en interpretaties expliciet te maken. Zo houd je babylonische spraakverwarringen buiten de deur.
- → Beschrijf de uitkomst van dit overleg en deel dit met de projectgroep, zodat bij iedereen helderheid is over de invulling van de taken en wie welke rol daarin vervuld.
- → Werk je samen met externe leveranciers en dienstverleners? Ook zij kunnen een eigen opvatting hebben over begrippen en definities! Neem ze mee in dit proces en krijg met elkaar helderheid over wat de bedoeling is.

Rol	Definitie	Waarde/parameter
Product eigenaar	Standaard	Volgens de good practice
Security Architect	Standaard	Aanbevolen ciphers volgens TLS-richtlijnen
Ontwikkelaar	Standaard	Standaard software library
Cryptograaf	Standaard	Sterke ciphers volgens NIST

Tijdens de diverse bijeenkomsten rond de totstandkoming van dit artikel en het hierin getoonde referentiemodel, kwam de groep experts verschillende interpretaties van definities tegen. Dit werd al snel onderwerp van discussie. Deze expertgroep had soms zichtbaar moeite om het eens te worden over het definiëren van begrippen en de onderlinge samenhang scherp te krijgen. Het laat zien hoe complex dit werkveld door de jaren heen is geworden.

Niet vreemd dus, dat een gemiddelde organisatie worstelt met cryptografische vraagstukken. Deze uitdaging is te overkomen met wat aandacht voor wat we bedoelen met de termen die we gebruiken. Heel praktisch, bijvoorbeeld met vragen als: 'Hebben we het nu over hetzelfde?' en 'Wat bedoel je precies?'. Zo voorkomen we babylonische spraakverwarring en werken we efficiënter toe naar cryptografische oplossingen voor quantumveiligheid.

Deze publicatie is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011 | 2500 EA Den Haag
t (070) 426 64 26

November 2025