PRIVACY COMPANY

Microsoft Double Key Encryption

Analyse voor SLM Microsoft Rijk en het NBV van de AIVD

13 januari 2021

Inhoudsopgave

Samenvatting

Microsoft biedt met de dienst *Double Key Encryption* (DKE) een nieuwe manier van versleuteling aan waarbij de klant zelf een sleutel beheert, en alleen de klant toegang zou moeten hebben tot die sleutel en de daarmee versleutelde inhoud, maar Microsoft niet. SLM Microsoft Rijk en de afdeling NBV van de AIVD willen graag weten of het mogelijk is om gegevens in Microsoft Office 365 met behulp van DKE te beveiligen tegen toegang door Microsoft als clouddienstverlener. Deze analyse gaat over de risico's, in weerwil van het doel van de dienst, dat een systeembeheerder bij Microsoft onrechtmatig in de gegevens kijkt, dat verkeer naar Microsoft wordt afgetapt, of dat Microsoft wordt gedwongen gegevens te overhandigen aan een inlichtingen- of opsporingsdienst.

Privacy Company beantwoordt deze hoofdaanvraag in deze analyse in tien deelvragen en antwoorden. In de inleiding wordt de juridische achtergrond geschetst, waarom het toepassen van encryptie belangrijk is om gegevens te kunnen (blijven) doorgeven naar cloudproviders in de Verenigde Staten.

Het antwoord op de hoofdvraag kan niet met een eenvoudig Ja of Nee worden beantwoord, omdat eventuele ongewilde toegang door Microsoft sterk samenhangt met het eigen risicoprofiel van de organisatie, van de gebruikte Office applicatie, en met de technische configuratie van de versleutelingsdienst.

DKE is alleen beschikbaar op Windows desktops en laptops, waarbij alleen Word, PowerPoint en Excel een automatische integratie hebben met DKE. Dat betekent dat er nog veel platforms zijn die gebruikt worden door overheidsmedewerkers waarop DKE niet te gebruiken valt.

Om de inhoud van bestanden met DKE zo goed mogelijk te beschermen tegen onrechtmatige toegang door Microsoft als cloudprovider, adviseert Privacy Company beheerders om zeven technische en organisatorische maatregelen te treffen. Deze maatregelen helpen echter niet tegen eventuele backdoors op Microsofts Azure AD-servers, in de DKE Service software of in de eindgebruikersclient (de *Azure Information Protection Unified Labeling Client*). Privacy Company gaat niet uit van kwade wil van Microsoft, maar in sommige omstandigheden is het conform de eisen van de BIO nodig om rekening te houden met eventuele kwade wil van beheerders, bevel van een overheid, of hacks. Organisaties kunnen dit risico alleen voorkomen door hun netwerk volledig los te koppelen van internet, of door versleutelingsmaatregelen te treffen.

Los van de adviezen aan beheerders adviseert Privacy Company het Rijk om een test set-up met DKE in te richten, en het gebruik van de verschillende Connected Experiences afzonderlijk te testen. Ook zou het Rijk een commitment moeten vragen aan Microsoft om quantum-bestendige asymmetrische algoritmen toe te passen in DKE zodra die beschikbaar komen.

De aanbevolen maatregelen zijn:

1. Rol de DKE Service uit via een hosting-oplossing waar Microsoft geen directe invloed op kan uitoefenen. Een *on-premises* installatie van de DKE Service ligt daarbij het meest voor de hand. Hosting bij een externe hostingpartij is ook een optie, mits de overheidsorganisatie kan uitsluiten dat een dreigingsactor die toegang kan krijgen tot de Azure dienstverlening, ook toegang kan krijgen tot deze hostingpartij.

2. Gebruik een sleutellengte van minimaal 3072 bit, vanwege het relatief hoge dreigingsniveau waartegen Office 365 DKE zou moeten beschermen, of sluit minimaal aan bij het

bestaande beleid van de organisatie met betrekking tot het gebruik van cryptografische sleutels.

3. Autoriseer gebruikers gebaseerd op hun rol (lid van het onderzoeksteam), en niet op basis van hun e-mail adres. *Role Authorization* zorgt ervoor dat het beheer van autorisaties op een centrale plek kan worden bijgehouden. Als de beheerder gebruik maakt van een administratieve indeling van medewerkers per groep, hoeft hij de autorisaties niet per inkomende en vertrekkende medewerker bij te houden.

4. Sta bij gebruik van DKE alleen synchronisatie toe van de *on premises* AD naar de Azure AD, en niet omgekeerd. Om gebruik van Microsoft DKE mogelijk te maken, is het noodzakelijk om de eigen *on-premises* Active Directory te synchroniseren met Microsoft's centrale online AD. Dat synchroniseren kan twee kanten op lopen. Dat kan de beheerder instellen. Als de beheerder kiest voor synchronisatie van de Azure AD naar de *on premises* AD, dan kan Microsoft in theorie de autorisaties voor zowel de *Azure Information Protection Service*s als de DKE Service beïnvloeden.

5. Scherm de DKE Service zodanig af dat die niet te benaderen is via het publieke internet, maar bijvoorbeeld alleen via het interne netwerk of via een VPN. Dit om te voorkomen dat bestanden buiten het netwerk kunnen worden ontsleuteld, als bepaalde gebruikersaccounts eventueel gecompromitteerd raken. Dit is een aanvullende maatregel op maatregel 4, omdat voor toegang tot de private sleutel zowel autorisatie nodig is, als toegang tot de DKE Service.

6. Adviseer gebruikers om géén persoonsgegevens of vertrouwelijke gegevens op te nemen in bestandsnamen.

7. Zet de telemetrie-verzameling voor Windows uit. Configureer de telemetrieverzameling bij Office 365 op het laagste niveau '*Required'* en beoordeel of de gedocumenteerde telemetrieverzameling acceptabel is. Als een overheidsorganisatie twijfelt of de contractuele waarborgen van Microsoft over het gebruik van die we services in het privacy-amendement van Rijk voldoende garantie bieden, schakel de Connected Experiences dan volledig uit.

8. Contractuele opdracht aan SLM Microsoft Rijk: vraag Microsoft om een commitment, wanneer quantum-bestendige asymmetrische algoritmen beschikbaar komen, om te onderzoeken of zij ondersteuning voor deze algoritmes kan toevoegen aan de DKE Service en de *Azure information Protection Unified Labeling Client*.

Dit rapport bevat een analyse van de werking van DKE , op basis van de informatie die Microsoft ter beschikking stelt, inclusief antwoord op een aantal specifieke vragen van Privacy Company. Deze analyse is niet gebaseerd op een technische analyse van de feitelijke werking van DKE op de server en in de gebruikersclients. De scope van dit rapport omvat géén toetsing aan de BIO-vereisten, juist omdat dat alleen effectief mogelijk is in combinatie met technisch onderzoek naar de client en de service. Dit rapport kan, omdat er geen broncode analyse is gedaan en geen audit op de feitelijke implementatie van DKE, ook geen uitspraken doen over de cryptografische betrouwbaarheid en effectiviteit van de tool of de eventuele aanwezigheid van backdoors. De conclusies bevatten wel aanbevelingen voor nader technisch onderzoek.

Inleiding

Microsoft biedt met de dienst *Double Key Encryption* (DKE) een nieuwe manier van versleuteling aan waarbij de klant zelf een sleutel beheert, en alleen de klant toegang zou moeten hebben tot die sleutel en de daarmee versleutelde inhoud, maar Microsoft niet. De hoofdvraag van dit rapport is of het mogelijk is om gegevens in Microsoft Office 365 met behulp van DKE te beveiligen tegen toegang door Microsoft als clouddienstverlener.

Overheidsorganisaties in Nederland maken veel en intensief gebruik van allerlei Microsoft-diensten. Een deel van de persoonsgegevens die overheden daarmee verwerken, wordt verwerkt op servers van Microsoft. Ook als overheden kiezen voor het gebruik van *on-premises* lokale servers, verzamelt Microsoft nog steeds persoonsgegevens in de Verenigde Staten over de gebruikers en het gebruik van de online diensten. Zelfs als overheden die datastromen minimaliseren, en de inhoudelijke gegevens exclusief alleen (laten) opslaan in datacentra in de EU, bestaat er nog steeds een risico dat Microsoft als cloudprovider op onrechtmatige wijze toegang krijgt tot de inhoudelijke gegevens.

In haar Online Servicevoorwaarden (inclusief aparte verwerkersovereenkomst)[1] garandeert Microsoft dat de inhoudelijke gegevens *at rest* alleen in datacentra in de EU worden opgeslagen.[2] Maar Microsoft biedt geen mogelijkheid aan beheerders om de diagnostische gegevens en de telemetriegegevens over het gebruik van Office 365, of de authenticatiegegevens uit de (online) Azure AD, in de EU te laten verwerken. Bovendien biedt opslag in de EU geen sluitende waarborg tegen onrechtmatige toegang tot de gegevens, dat wil zeggen: toegang in strijd met de Algemene Verordening Gegevensbescherming (AVG).

Dit rapport analyseert het risico van onrechtmatige toegang door Microsoft in de volgende drie omstandigheden, in weerwil van het doel van deze dienst, namelijk om juist tegen onrechtmatige toegang te beschermen:

- Een systeembeheerder van Microsoft bekijkt en kopieert gegevens (al dan niet na omkoping, chantage of hacking, ,)
- Microsoft moet gegevens verstrekken aan een opsporings- of inlichtingendienst zonder dat zij haar klant mag informeren
- Gegevens die Microsoft verwerkt, worden zonder medewerking van Microsoft onderschept, inclusief hacking van de supply chain of hacking via een vijandelijke statelijke actor

De vraag naar adequate encryptie van gegevens is zeer actueel geworden door de nieuwe conceptrichtsnoeren van het Europees Comité voor Gegevensbescherming (European Data Protection Board, hierna: EDPB) over technische maatregelen die verantwoordelijken moeten treffen bij doorgifte van persoonsgegevens naar een land met een niet passend dataprotectie niveau.[3] Encryptie speelt in deze richtsnoeren een belangrijke rol, om de gevolgen van

[1] Microsoft Voorwaarden voor Online Diensten, augustus 2020, URL: https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=Dutch

[2] Microsoft definieert deze als Customer Data.

[3] Europees Comité voor Gegevensbescherming (hierna: EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Consultation version adopted on 10 November 2020, Consultation between 11 November and 21 December 2020, URL: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en , en: EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020, URL: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

onrechtmatige toegang te minimaliseren. Bij een juiste toepassing worden de gegevens immers onbruikbaar.

Volgens Microsoft zou toepassing van DKE betrouwbare en controleerbare end-to-end beveiliging opleveren, die voldoet aan de hoge norm van de EDPB. Daarmee zou het mogelijk worden voor het Rijk om niet openbare informatie te plaatsen in de Microsoft cloud, mogelijk zelfs BIO BBN2 informatie (buiten scope van deze analyse).

Juridische achtergrond: Schrems II-arrest

Het advies van de EDPB is een reactie op het Schrems II-arrest van het Europese Hof van Justitie. Het EU Hof oordeelt daarin dat het doorgeven van persoonsgegevens naar de Verenigde Staten problematisch is, omdat er in de VS geen adequaat (*essentially equivalent*) beschermingsniveau is voor persoonsgegevens.

Het Schrems II-arrest is de uitkomst van de rechtszaak die Max Schrems heeft gevoerd tegen Facebook Ierland en de Ierse dataprotectie autoriteit. In een eerdere rechtsgang van Schrems tegen Facebook Ierland, in 2015, verklaarde het Europees Hof de Safe Harbor overeenkomst tussen de EU en de VS al ongeldig. Dat was de voorloper van het Privacy Shield. Ook het Privacy Shield zelf is met onmiddellijke ingang ongeldig verklaard.

Het EU Hof noemt als belangrijkste redenen dat de beperkingen van de privacy die voortvloeien uit de Amerikaanse regelgeving onvoldoende zijn afgebakend en disproportioneel zijn en daarom een te grote inbreuk op de privacy vormen. Concreet beschrijft het Hof de risico's van massa surveillance (bulksgewijze gegevensverzameling) door de Amerikaanse inlichtingendiensten op grond van de surveillanceprogramma's PRISM en Upstream op basis van section 702 FISA en op basis van E.O. 12333, en het gebrek aan effectieve en afdwingbare rechten voor inwoners van de EU bij het gebruik van die gegevens door de Amerikaanse overheidsinstanties.[4] De Amerikaanse opsporingsautoriteiten kunnen daarnaast ook toegang eisen tot gegevens van Amerikaanse bedrijven die elders in de wereld worden verwerkt, op grond van de US CLOUD Act.

Persoonsgegevens mogen vanuit de EU ook legitiem aan een derde land worden doorgegeven op grond van Standard Contractual Clauses (hierna: SCC, of modelbepalingen). De SCC zijn vastgesteld door de Europese Commissie op grond van de (vorige) Privacyrichtlijn.[5] Deze modelbepalingen zorgen contractueel voor een hoog beschermingsniveau. Hoewel het EU Hof de geldigheid erkent van het besluit van de Europese Commissie waarmee zij de SCC heeft vastgesteld, en gegevensoverdracht op basis van deze bepalingen in principe dus nog steeds is toegestaan, geldt dat niet voor systematische doorgifte van persoonsgegevens naar de Verenigde Staten op basis van de huidige modelbepalingen. Elke verantwoordelijke moet namelijk zelf beoordelen of het contractueel afgesproken beschermingsniveau in het land van ontvangst wel waargemaakt kan worden.
Het Hof schrijft:

[4] Europees Hof van Justitie, C-311/18, Data Protection Commissioner tegen Facebook Ireland Ltd en Maximillian Schrems (Schrems-II), 16 juli 2020, ECLI:EU:C:2020:559, URL: http://curia.europa.eu/juris/document/document.jsf;jsessionid=CF8C3306269B9356ADF861B57785FDEE?text=&docid=228677&pageIndex=0&doclang=NL&mode=req&dir=&occ=first&part=1&cid=9812784. Zie met name r.o. 165 en r.o. 178-185.

[5] Inmiddels heeft de Europese Commissie nieuwe concept SCC gepubliceerd, met een reactiemogelijkheid tussen 12 november en 10 december 2020. Zie: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries Het is niet bekend wanneer de Europese Commissie de definitieve nieuwe SCC publiceert

> *"Bij de beoordeling die daartoe in het kader van een dergelijke doorgifte vereist is, moet met name rekening worden gehouden met zowel de contractuele bepalingen die zijn overeengekomen tussen de in de Unie gevestigde verwerkings-verantwoordelijke of zijn in de Unie gevestigde verwerker en de in het betrokken derde land gevestigde ontvanger van de doorgifte, als, wat een eventuele toegang van de overheidsinstanties van dat derde land tot de doorgegeven persoonsgegevens betreft, de relevante aspecten van het rechtsstelsel van dat derde land."*[6]

SLM Microsoft Rijk heeft op 22 juli 2020 een openbaar memo opgesteld over de gevolgen van het Schrems II-arrest, gericht aan de CIO Rijk, CIO Beraad, CIO Raad, CTO Raad, CTO Overleg, deelnemers SLM Microsoft Rijk en geïnteresseerden. Hierin schrijft SLM Microsoft Rijk dat Microsoft alleen nog de SCC gebruikt voor haar online diensten onder Enterprise licentie, maar dat de uitspraak ook gevolgen kan hebben voor de toelaatbaarheid van doorgiftes op basis van de SCC naar de Verenigde Staten. SLM Microsoft Rijk wacht op een visie van de AP en de samenwerkende Europese toezichthoudende autoriteiten, maar zal zich ook zelfstandig een oordeel vormen, in afstemming met alle verwerkingsverantwoordelijken die zijn aangesloten bij de MBSA.[7]

Microsoft gebruikte tot nu toe een combinatie van de twee doorgifte-maatregelen naar de VS: het Privacy Shield en de EU Standard Contractual Clauses (SCC). Microsoft gebruikte de SCC al voor de doorgifte van diagnostische en inhoudelijke persoonsgegevens vanuit de zakelijke online diensten (Business en Enterprise licenties) zoals de Office 365 mobiele, desktop en web apps, Exchange Online en de Processor Connected Experiences. Microsoft baseerde de doorgifte van diagnostische persoonsgegevens afkomstig uit de Controller Connected Experiences echter op het EU-VS Privacy Shield. Microsoft heeft zichzelf gecertificeerd onder dit instrument.[8] Verantwoordelijke overheidsorganisaties (en andere zakelijke klanten van Microsoft) kunnen deze gegevensverwerking overigens zelf stopzetten, door het gebruik van de Controller Connected Experiences centraal te blokkeren.

Uit de hierboven aangehaalde beoordeling door het Hof van de bulkbevragingen door de veiligheidsdiensten in de VS blijkt dat gebruik van de SCC inderdaad geen soelaas biedt voor structurele doorgifte van persoonsgegevens naar de VS.

Reactie Microsoft op Schrems II

Microsoft belooft in reactie op Schrems II om zich principieel altijd tegen elke vordering te verzetten. Bovendien belooft Microsoft om elke klant die door een dergelijke vordering wordt getroffen, een schadevergoeding te betalen. Microsoft's VP voor privacy, oud-FTC commissioner Julie Brill, legt in een officiële blogpost uit:

---

[6] Europees Hof van Justitie, Schrems-II, r.o. 104

[7] SLM Microsoft Rijk, Nota over de gevolgen van de uitspraak ECJ over de doorgifte van persoonsgegevens naar landen buiten de Europese Unie op gebruik het gebruik van Microsoft producten en diensten, 22 juli 2020.

[8] Microsoft is (nog steeds) een actieve deelnemer aan het Privacy Shield Framework. Zie: https://www.privacyshield.gov/participant?id=a2zt000000KzNaAAK&status=Active. De FTC legt uit dat de ongeldigverklaring van het Privacy Shield de deelnemers niet ontslaat van de aangegane verplichtingen. "(…)*the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. That decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework.*" FTC informatie Privacy Shield, https://www.privacyshield.gov/Program-Overview

> *"First, we are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.*
>
> *Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure."*[9]

Toch zijn deze vernieuwende toezeggingen van Microsoft op zichzelf onvoldoende. Microsoft kan als bedrijf weinig beginnen tegen het juridische ontbreken van de vereiste vier essentiële Europese garanties voor dataprotectie in het Amerikaanse recht. Technische maatregelen zijn daarom ook nodig, om gevoelige gegevens onbruikbaar te maken voor onbevoegde derde partijen. Dat kan door de gegevens op zodanige wijze te versleutelen dat Microsoft zelf geen toegang heeft tot de sleutel, en dus alleen toegang kan krijgen tot versleutelde, en dus onbruikbare data.

Microsoft was goed voorbereid op de uitkomsten van de rechtszaak, en heeft al op 21 juli 2020 bekend gemaakt dat zij met DKE een nieuwe zware vorm van encryptie mogelijk ging maken in bepaalde Office 365 producten.[10]

Tien subvragen

De secties 1 tot en met 10 van dit rapport geven antwoord op de tien subvragen. De tien subvragen zijn:

1. Hoe werkt Double Key Encryption?
2. Welke diensten van Office 365 kunnen gebruik maken van DKE? En welke dus niet, voor zover gedocumenteerd?
3. Welke functionaliteiten werken niet als je DKE aanzet, volgens beschikbare documentatie?
4. Is er verschil tussen de verschillende platformen waarop de vijf kerndiensten draaien, dat wil zeggen, tussen de iOS en Android mobiele applicaties, de browser-versie en de MacOS en Windows desktop applicaties?
5. Welke encryptiefunctionaliteit zit bij elk van deze platforms in de client, en welke in de verschillende back-ends, namelijk: de lokale back-end server en de remote cloud back-end in Azure?
6. Binnen de vijf kerndiensten van Office (namelijk: Word, PowerPoint, Excel, Teams en Outlook): welke functionaliteiten vallen wel onder de end-to-end encryptie, en welke niet?
7. Welke opties en keuzemogelijkheden bestaan bij de inzet van DKE en welke hiervan bieden maximale afscherming van gebruikersgegevens tegen Microsoft als clouddienstverlener?
8. Hoe werkt het sleutelbeheer? Wat is exact het beveiligings- en encryptiemechanisme achter DKE? Wie heeft er toegang tot de sleutels, en onder welke omstandigheden? Hoe verhoudt DKE zich tot reeds bestaande Microsoft functies als BYOK en HYOK?

[9] Blog Julie Brill, New Steps to Defend Your Data, 19 november 2020, URL: https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

[10] Microsoft blogpost, Announcing public preview of Double Key Encryption for Microsoft 365, URL: https://techcommunity.microsoft.com/t5/microsoft-security-and/announcing-public-preview-of-double-key-encryption-for-microsoft/ba-p/1534451

9. Inventarisatie van de risico's en aannames dat Microsoft als clouddienstverlener geen toegang meer heeft tot de gebruikersinformatie. Waar zitten de kwetsbaarheden in de architectuur, en de afhankelijkheden?
10. Is DKE een '*proprietary*' oplossing enkel voor Microsoft gebruik (en applicaties) of maakt Microsoft hier een volledige *open source* oplossing van?

Buiten scope

De afbakening van deze analyse tot de vraag naar mogelijkheden voor onbevoegde toegang door Microsoft betekent dat een aantal risico's buiten scope valt. Dit zijn risico's die altijd kunnen optreden bij het gebruik van encryptie. Andere risico's die buiten scope vallen zijn hacking van de apparatuur van overheidsmedewerkers, afpersing van medewerkers, meekijken op het scherm door onbevoegden en andere risico's die niet direct gerelateerd zijn aan het gebruik van Office 365 DKE.

1. Hoe werkt Double Key Encryption?

Microsoft Office 365 DKE is onderdeel van Microsoft's *Azure Information Protection* (AIP) dienst. Met AIP kunnen organisaties informatie classificeren met behulp van labels. Microsoft noemt deze dienst sinds eind maart 2020 overigens geen AIP meer, maar *unified labeling*.[11] Voorbeelden van dergelijke labels zijn: '*vertrouwelijke gegevens*' of '*openbare gegevens*'.

De overheid werkt met drie beveiligingsniveaus: BBN1, BBN2 en BBN3, waarbij BBN staat voor Basis Beveiligings Niveau. Op grond van het Voorschrift Informatiebeveiliging Bijzondere Informatie (VIRBI) rubriceert de Rijksoverheid vertrouwelijke informatie in vier categorieën. Voor deze analyse is de alleen de categorie Departementaal Vertrouwelijk van belang.[12] Per categorie wordt een beveiligingsniveau opgelegd aan de beheerder van de vertrouwelijke informatie. Het niveau BBN1 is het minimum vereiste beveiligingsniveau voor overheidsinstellingen. BBN2 is alles tot het niveau Departementaal Vertrouwelijk en BBN3 "*richt zich op de bescherming van als Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie, waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistent Threats (APT's), die uitgaat van statelijke actoren en beroepscriminelen.*"[13]

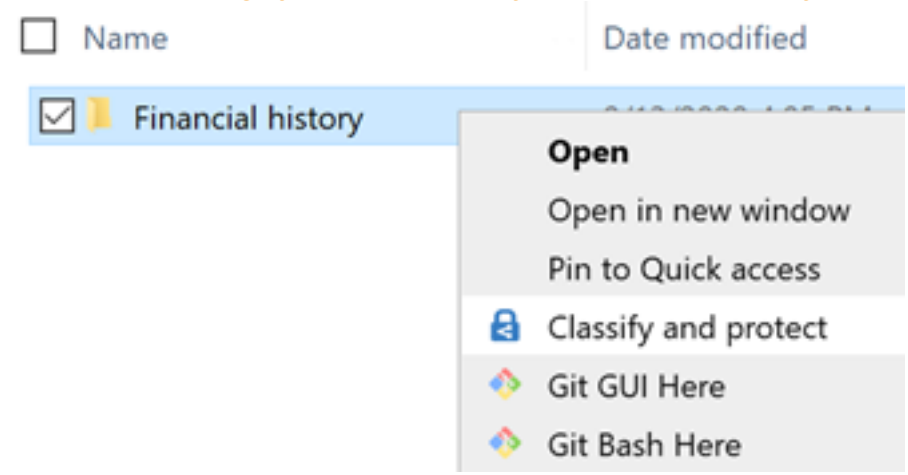
Beheerders zouden de vertrouwelijkheidsrubricering letterlijk als labels kunnen toevoegen aan AIP, maar ze kunnen ook kiezen voor naamgeving die praktisch aansluit op de werkzaamheden van medewerkers, zoals interne besluitvoering, openbare informatie of financiële informatie.

Beheerders kunnen op basis van de toegewezen labels beleid afdwingen voor toegangscontrole en versleuteling. Op basis van kenmerken zoals bestandslocatie of -inhoud kan een beheerder beleid configureren voor het automatisch toekennen van labels. Daarmee kan een beheerder de versleuteling met DKE dus afdwingen op basis van verschillende eigenschappen van bestanden. Het beleid wordt dan afgedwongen via de *Azure Information Protection Unified Labeling Client* die is geïnstalleerd op de (Windows) werkplek van de eindgebruiker. Beheerders kunnen er ook voor kiezen om gebruikers op basis van dit soort regels alleen aanbevelingen te doen om DKE toe te passen.

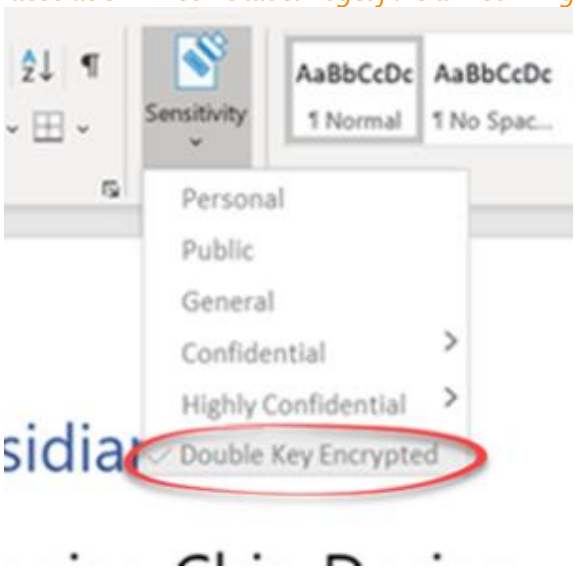
Eindgebruikers kunnen ook op eigen initiatief bestanden versleutelen met DKE. Dat kan op twee verschillende manieren: (i) vanuit de *Azure Information Protection Unified Labeling Client* (zie Illustratie 1), of (ii) vanuit een gevoeligheidskeuzemenu in Word, PowerPoint en Excel (Zie Illustratie 2). In de praktijk ziet het er voor gebruikers uit als een nieuw label onder het tabblad 'Gevoeligheid' ('*Sensitivity*'), dat standaard de naam krijgt '*Double Key Encrypted*'. Als gebruikers dat nieuwe label kiezen, wordt het bestand versleuteld met twee verschillende sleutels.[14] Een van deze twee sleutels wordt beheerd door de organisatie zelf, zodat zelfs Microsoft, die de andere sleutel beheert, de bestanden niet kan ontsleutelen.

[11] Microsoft, Azure Information Protection labels migreren naar Unified sensitiv-labels, 9 november 2020, URL: https://docs.microsoft.com/nl-nl/azure/information-protection/configure-policy-migrate-labels
[12] Besluit van de Minister-President, Minister van Algemene Zaken van 1 juni 2013, nr. 3124134, houdende voorschrift informatiebeveiliging Rijksdienst – bijzondere informatie 2013 (VIRBI 2013), Staatscourant 2013, 15497, URL: https://wetten.overheid.nl/BWBR0033507/2013-06-01
[13] BIO versie 1.04, p. 18.
[14] Office Watch, Double Key encryption coming to Microsoft 365, 27 augustus 2020, URL: https://office-watch.com/2020/double-key-encryption-coming-to-microsoft-365/

Illustratie 1: Labelmogelijkheid in de Azure Information Protection Unified Labeling Client[15]



Illustratie 2: Nieuwe labelmogelijkheid in sommige Office applicaties



Microsoft heeft Office 365 DKE ontworpen voor organisaties met een relatief klein aantal bestanden waarvan de inhoud zo gevoelig is dat zelfs de contractuele afspraken met Microsoft niet voldoende worden geacht om de risico's van onrechtmatige toegang tot de bestanden te mitigeren. Deze risico-analyse gaat uit van de mogelijkheid dat (medewerkers van) Microsoft mogelijk niet te vertrouwen zijn, ook al is dat in de meeste situaties geen redelijke aanname.

[15] Microsoft, URL: https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

2. Welke diensten van Office 365 kunnen gebruik maken van DKE?

Het gebruik van DKE is, volgens documentatie van Microsoft[2], afhankelijk van:

- Een Microsoft 365 E5 of Office 365 E5 licentie.
- *Azure Information Protection*: nodig voor het toekennen en beheren van DKE gevoeligheidslabels.
- Microsoft Office Apps for Enterprise versie *.12711 of hoger. DKE is alleen te gebruiken op de geïnstalleerde desktop versies van Word, PowerPoint en Excel op Windows.
- *Azure Information Protection Unified Labeling Client* versie 2.7.93.0 of hoger.

Microsoft DKE is dus niet beschikbaar voor Outlook en Teams, of andere Office 365-applicaties.

DKE voor Word, PowerPoint en Excel is niet beschikbaar voor de webapplicaties, niet voor de iOS en Android apps en niet voor de macOS-applicaties. De versleutelde bestanden kunnen zonder (technische) beperkingen worden opgeslagen op verschillende opslagmedia, *on-premises* netwerkopslag of in cloud-opslag zoals Microsoft OneDrive of Microsoft Sharepoint. Met DKE versleutelde bestanden kunnen ook per e-mail verstuurd worden, ook via Outlook, of gedeeld via Teams. De bestanden kunnen dan alleen ontcijferd worden, en dus bruikbaar gemaakt, door ontvangers die in de interne Azure AD staan van de versleutelende organisatie, en in de online AD van de organisatie. Dat hoeven niet perse medewerkers van de eigen organisatie te zijn: een organisatie kan ook gastgebruikers toevoegen aan de AD. De organisatie moet de gastgebruiker wel dubbel autoriseren voor het gebruik van de sleutel, zowel in de interne AD, als in de Azure AD. Die dubbele autorisatie wordt nader uitgelegd in het antwoord op paragraaf 8 van dit rapport. Technisch behoort de gastgebruiker dan tot hetzelfde domein als de andere medewerkers.

Via de *Azure Information Protection Unified Labeling Client* kunnen bijna alle soorten bestanden worden versleuteld.[16] Maar om te voorkomen dat het functioneren van de computer wordt gehinderd door versleutelen van essentiële uitvoeringsbestanden, heeft Microsoft een aantal bestands-typen en mappen uitgezonderd.

Van DKE uitgesloten bestandstypen:

- .lnk, .exe, .com, .cmd, .bat, .dll, .ini, .pst, .sca, .drm, .sys, .cpl, .inf, .drv, .dat, .tmp, .msp, .msi, .pdb, .jar

Van DKE uitgesloten (Windows) mappen:

- Program Files (\Program Files en \Program Files (x86))
- \ProgramData
- \AppData (voor alle gebruikers)

Omdat DKE alleen beschikbaar is binnen Word, Excel en Powerpoint, is alleen voor de bestandstypen die worden ondersteund door deze drie applicaties 'native' encryptie beschikbaar.

[16] Privacy Company heeft Microsoft per mail van 8 december 2020 gevraagd: "*Are there any (publicly) know alternative implementations of either the AIP Service or the AIP Unified Labeling Client, or are the protocols documented in such a way that an alternative implementation is feasible? For example, for the purpose of supporting additional file formats, client applications or cloud-services. I'm aware of the PowerShell API for the Unified Labeling Client.*" Microsoft Nederland heeft per mail van 10 december 2020 gereageerd met een verwijzing naar publieke informatie over de AIP client, Microsoft Admin Guide: File types supported by the Azure Information Protection classic client, 11 maart 2020, URL: https://docs.microsoft.com/en-us/azure/information-protection/rms-client/client-admin-guide-file-types

Dat betekent dat gebruikers de bestanden direct kunnen openen, zonder extra handelingen. Dit geldt ook voor bestanden in PDF-formaat. De AIP Unified Labeling Client ondersteunt dit formaat.[17] Er is geen openbare documentatie over andere bestandsformaten die door deze drie Office applicaties worden ondersteund, of die andere bestandsformaten *native* in de applicatie kunnen worden versleuteld en ontsleuteld. Hier is technisch onderzoek voor nodig.

3. Welke functionaliteiten werken niet als je DKE aanzet?

De belangrijkste functionaliteit die niet werkt bij gebruik van DKE, is de verwerking van gegevens door online diensten die toegang nodig hebben tot de inhoud van documenten. Het is wel mogelijk om met DKE-versleutelde bestanden op te slaan in bijvoorbeeld Microsoft SharePoint en OneDrive for Business, of om ze te mailen. Maar de versleutelde documenten kunnen pas worden geopend op een Windows-computer met de *Azure Information Protection Unified Labeling Client* en de relevante Office applicatie.

In de Office applicaties blijven Add-ins en Connected Experiences werken, met uitzondering van de functies waarvoor het document zelf in Azure moet staan. Microsoft geeft in haar documentatie over DKE de volgende voorbeelden van online diensten die niet-compatibel zijn:

- Transport rules inclusief anti-malware en anti-spam voor zover die afhankelijk zijn van de inhoud van bijlagen
- Microsoft Delve
- eDiscovery
- Content search en indexing
- Office Web Apps en co creatie (live samenwerken aan hetzelfde document)

Microsoft noemt geen andere voorbeelden en geeft geen limitatieve opsommingen in haar publieke documentatie. Dat betekent dat de vraag alleen goed beantwoord kan worden door een test set-up met DKE in te richten, en de verschillende Connected Experiences afzonderlijk te testen.

Er kunnen aanvullende problemen optreden als bijvoorbeeld de antivirus software, of een spamfilter, alle e-mails blokkeren met bijlages die niet gescand kunnen worden. Dergelijke blokkades kunnen ertoe leiden dat gebruikers van Office 365 in de praktijk besluiten om geen versleuteling toe te passen, om dergelijke blokkades te omzeilen.

Privacy Company heeft Microsoft gevraagd of het gebruik van DKE in de Office 365 applicaties leidt tot wijzigingen in de functionaliteit van de client. Bijvoorbeeld, als privacy-instellingen met betrekking tot de diagnostische gegevens worden aangepast, of als bepaalde Connected Experiences niet meer werken. Microsoft heeft uitgelegd dat het gebruik van DKE niet leidt tot wijzigingen in de configuratie van de Office apps.[18]

4. Is er verschil tussen de verschillende platformen waarop de vijf kerndiensten draaien?

Microsoft stelt DKE op dit moment alleen beschikbaar voor het Windows platform, via (i) de *Azure Information Protection Unified Labeling client* op Windows, en (ii) via Word, Excel en

[17] Idem, antwoord op vraag 3 van Privacy Company.
[18] Antwoord Microsoft Nederland van 10 december 2020 op vragen Privacy Company over DKE.

PowerPoint voor Office 365, in een Enterprise licentie. Microsoft ondersteunt op dit moment geen andere platformen. Privacy Company heeft geen informatie van of over Microsoft gevonden of het bedrijf plannen heeft om de beschikbaarheid van DKE uit te breiden.

5. Welke encryptiefunctionaliteit zit bij elk van deze platforms in de client, en welke in de verschillende back-ends?

De *Azure Information Protection Unified Labeling Client* is (alleen) beschikbaar voor Windows-werkplekken. Deze client is verantwoordelijk voor het toepassen van het geconfigureerde encryptiebeleid. Binnen DKE is de *AIP Unified Labeling Client* de enige component die verantwoordelijk is voor het versleutelen en ontsleutelen van de inhoud van documenten.

Daarnaast heeft de DKE service (die draait op een server van de organisatie) toegang tot de encryptiesleutel die voor elk document uniek is. In antwoord op vraag 8 wordt uitgelegd dat er in totaal drie sleutels een rol spelen bij de versleuteling. De derde sleutel is een asymmetrische sleutel waarmee de organisatiesleutel weer wordt versleuteld.

De server met de DKE Service heeft géén toegang nodig tot de inhoud van versleutelde documenten. Hoewel de DKE Service is geschreven door Microsoft, heeft Microsoft niet perse toegang tot de geïnstalleerde DKE Services. Dat is niet het geval als de organisatie het advies opvolgt uit dit rapport (zie Illustratie 3) om de DKE service *on-premises* of bij een vertrouwde hostingprovider onder te brengen, in ieder geval niet bij Microsoft. De DKE service bevat de sleutels om de documenten te ontsleutelen, het klant-stuk van de sleutel. Als je ook het klant-stuk van de sleutel (de *private key*) ergens bij Microsoft onderbrengt (bijvoorbeeld via hosting in Microsoft Azure), kan Microsoft zichzelf in theorie toegang verschaffen tot beide sleutels.

6. Binnen de vijf kerndiensten: welke functionaliteiten vallen wel onder de end-to-end encryptie, en welke niet?

Met deze vraag wil het Rijk weten of elk onderdeel van een applicatie waarin je DKE kunt gebruiken, versleuteld wordt met DKE, of dat er uitzonderingen zijn naar gelang de aard van de communicatie (tekst of cijferbestand, video, gesprek, chat, videoconferentie, et cetera).

Microsoft Office 365 DKE is op twee manieren beschikbaar: (i) via de *Azure Information Protection Unified Labeling client* op Windows, en (ii) via de AIP Unified Labeling Client, via Word, Excel en PowerPoint voor Office 365, in een Enterprise licentie, en alleen op Windows. Andere platformen en applicaties worden niet ondersteund.

Medewerkers van overheidsorganisaties kunnen wel andere applicaties gebruiken, zoals Teams en Outlook, om met Office 365 DKE versleutelde bestanden op te slaan of uit te wisselen.

7. Welke opties en keuzemogelijkheden bestaan bij de inzet van DKE?

Bij de inrichting van Office 365 DKE kan een organisatie kiezen waar zij de DKE Service installeert. In de configuratie-documentatie geeft Microsoft voornamelijk uitleg hoe een organisatie DKE kan uitrollen in Microsoft's cloudhostingdienst Azure.[4] Als organisaties dat doen (en geen gebruik maken eigen *on-premises* hosting) leidt dat ertoe dat Microsoft, in theorie, nog steeds toegang heeft tot beide sleutels die nodig zijn om de documenten te ontsleutelen.

Beheerders hebben verschillende keuzemogelijkheden bij de inzet van DKE. Privacy Company adviseert, op grond van de openbare documentatie, om de volgende maatregelen te treffen om DKE zo veilig mogelijk in te zetten.

1. Privacy Company raadt aan om de DKE Service uit te rollen via een hosting-oplossing waar Microsoft geen directe invloed op kan uitoefenen. Een *on-premises* installatie van de DKE Service ligt daarbij het meest voor de hand. Hosting bij een externe hostingpartij is ook een optie, mits de overheidsorganisatie kan uitsluiten dat een dreigingsactor die toegang kan krijgen tot de Azure dienstverlening, ook toegang kan krijgen tot deze hostingpartij. Microsoft heeft in een blogpost een configuratie-voorbeeld gepubliceerd voor organisaties die de DKE Service *on-premises* willen installeren. [19]

2. Bij de configuratie van de DKE Service maakt een organisatie zelf een RSA-keypair aan. De sleutellengte die Microsoft in haar configuratievoorbeeld[5] adviseert, is 2048-bits. Deze sleutellengte wordt over het algemeen als voldoende gezien voor RSA-sleutels. Vanwege het relatief hoge dreigingsniveau waartegen Office 365 DKE zou moeten beschermen raadt Privacy Company aan om een sleutellengte van minimaal 3072 bit te hanteren. In ieder geval moet de organisatie aansluiten bij haar bestaande beleid met betrekking tot het gebruik van cryptografische sleutels.

3. Voor de toegangscontrole is de DKE Service afhankelijk van een Active Directory service. Beheerders kunnen gebruikers op twee manieren autoriseren: gebaseerd op hun rol (lid van het onderzoeksteam), of op basis van hun e-mail adres. Privacy Company raadt aan om gebruik te maken van *Role Authorization* omdat dit het beheer van autorisaties op een centrale plek houdt. Als de beheerder gebruik maakt van een administratieve indeling van medewerkers per groep, hoeft hij de autorisaties niet per inkomende en vertrekkende medewerker bij te houden.

4. Om gebruik van Microsoft DKE mogelijk te maken, is het noodzakelijk om de eigen *on-premises* Active Directory te synchroniseren met Microsoft's centrale online AD. Dat synchroniseren kan twee kanten op lopen. Dat kan de beheerder instellen. Als de beheerder kiest voor synchronisatie van de Azure AD naar de *on premises* AD, dan kan Microsoft in theorie de autorisaties voor zowel de *Azure Information Protection Service*s als de Double Key Encryption Service beïnvloeden. Daarom adviseert Privacy Company om alleen de andere kant op te synchroniseren bij gebruik van DKE: van de *on premises* AD naar de Azure AD.

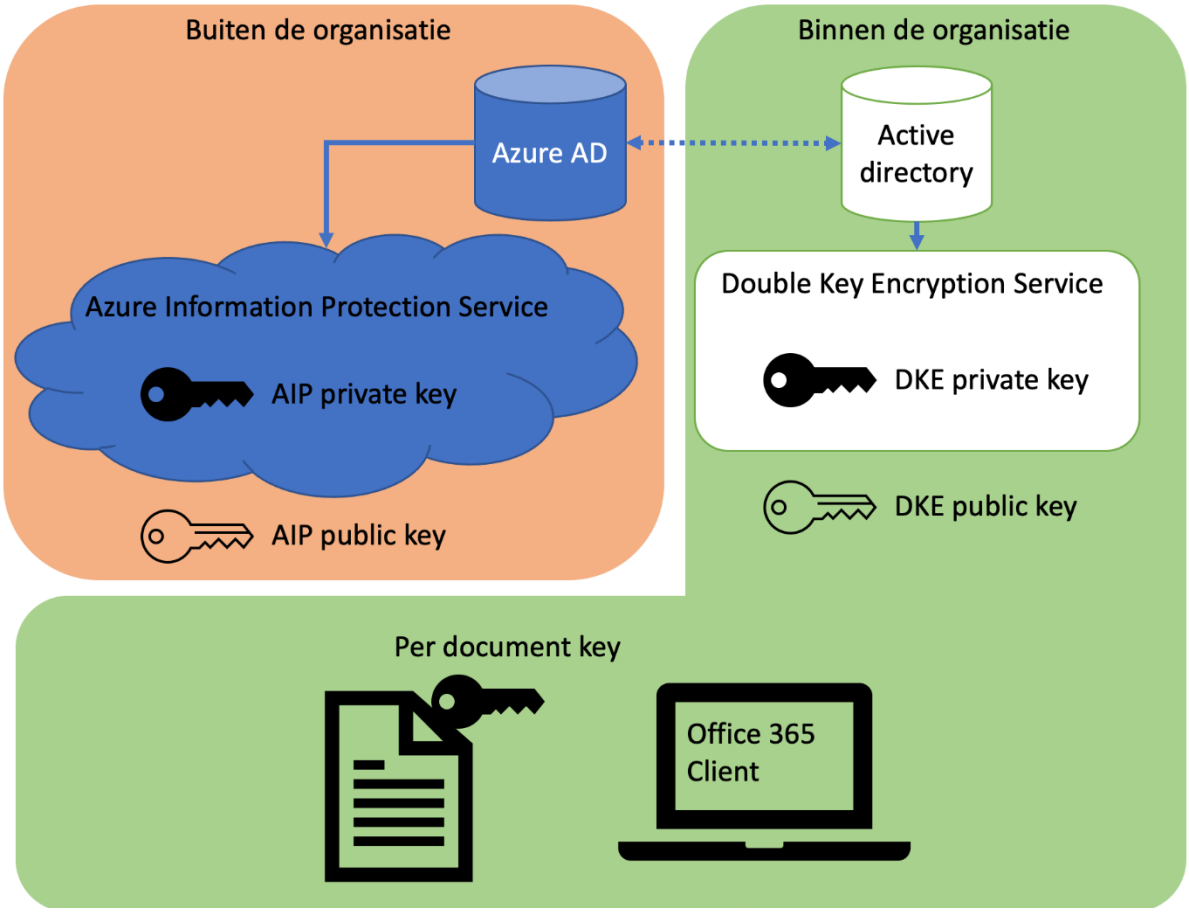
[19] Microsoft, Host DKE on IIS, using an on-premises server, 22 oktober 2020, URL: https://techcommunity.microsoft.com/t5/microsoft-security-and/host-dke-on-iis-using-an-on-premises-server/ba-p/1811046

5. Tenslotte adviseert Privacy Company dat de DKE Service niet te benaderen is via het publieke internet, maar bijvoorbeeld alleen via het interne netwerk of via een VPN. Dit om te voorkomen dat bestanden buiten het netwerk kunnen worden ontsleuteld, als bepaalde gebruikersaccounts eventueel gecompromitteerd raken. Dit is een aanvullende maatregel op maatregel 4, omdat voor toegang tot de private sleutel zowel autorisatie nodig is, als toegang tot de DKE Service.

8. Hoe werkt het sleutelbeheer?

DKE past een tweede laag van versleuteling toe door middel van de DKE Service. Daardoor hoeft de beheerder niet meer te vertrouwen op een HSM in Azure (*Hardware Security Module*[20]) voor het afschermen van het sleutelmateriaal. Maar het nadeel is dat diensten binnen Azure ook geen toegang meer hebben tot de (onversleutelde) inhoud.

Illustratie 3: Werking van het DKE sleutelbeheer



Het sleutelbeheer van Office 365 DKE vindt plaats in drie gescheiden omgevingen. Organisaties kunnen twee van deze omgevingen binnen de eigen organisatie plaatsen, zoals getoond in Illustratie 3. In deze illustratie is ervoor gekozen om de DKE service 'binnen' de organisatie te

[20] Dit rapport bevat geen analyse hoe Microsoft de HSM's beheert en configureert, maar een antwoord op de vraag wat klanten kunnen doen om hun gegevens te beschermen zonder te hoeven vertrouwen op de beloftes van Microsoft over de opslag van de sleutels in, en het proces van gegevensverwerking naar de HSM's.

hosten. Een organisatie kan er ook voor kan kiezen om die service 'buiten' onder te brengen (bij een vertrouwde hostingaanbieder, anders dan Microsoft, zie ook het antwoord op vraag 5).

1. De werkplek van de gebruiker met, in ieder geval, Microsoft Windows, Office 365 apps for Enterprise versie *.12711 of later, en de *Azure Information Protection Unified Labeling Client* versie 2.7.93.0 of hoger.
2. De DKE Service. Microsoft heeft de DKE Service (het onderdeel van de DKE server dat het *on-premises* sleutelbeheer verzorgt) gepubliceerd als open-source software onder een MIT-licentie.[8] Iedereen kan deze server software dus downloaden, configureren en compileren. De resulterende executables kunnen in eigen beheer worden uitgerold en gehost op verschillende locaties. Dat kan in Microsoft's Azure cloud, maar ook bij elke andere hosting-provider of *on-premises* op eigen hardware of virtuele machines.
3. De versleutelingsdiensten in de *Azure Information Protection Service* (AIP). De AIP-dienst is onderdeel van Microsoft's Azure cloudomgeving en is afhankelijk van Azure Active Directory (Azure AD). Zowel AIP als Azure AD zijn niet te beperken tot een geografische regio in Europa.

Het versleutelen van bestanden gebeurt in de volgende stappen:

- De Office 365 client versleutelt het document met een per document unieke symmetrische sleutel.
- De Office 365 client versleutelt de symmetrische sleutel met de publieke sleutel van de Double Key Encryption Service.
- De Office 365 client versleutelt het resultaat van stap 2 met de publieke sleutel van *Azure Information Protection Service*.
- De dubbel versleutelde sleutel wordt aan de metadata van het document toegevoegd.
- Het versleutelde document kan *on-premises* worden opgeslagen, of in een cloud-opslag.

Het ontsleutelproces verloopt vrijwel hetzelfde, maar dan in omgekeerde volgorde:

- De header van het versleutelde document bevat de encryptiesleutel en wordt losgekoppeld van de inhoud.
- De Office 365 Client authenticeert zich bij de *Azure Information Protection Service* die met behulp van de AIP Private Key de sleutel in de header ontsleutelt.
- De Office 365 Client authenticeert zich bij de DKE Service die met behulp van de DKE Private Key de sleutel in de header ontsleutelt.
- De drie relevante Office 365-applicaties kunnen met behulp van de sleutel in de ontsleutelde header het document ontsleutelen.

In reactie op een vraag van Privacy Company naar de *key length*, heeft Microsoft aangegeven dat Microsoft gebruik maakt van dezelfde cryptografische algoritmes en sleutels voor DKE als voor de andere *Azure Information Protection* diensten.[21]

De cryptografische algoritmes en sleutels voor de AIP diensten zijn:

- Versleuteling van inhoud met AES met 128 of 256-bit sleutels.
- Versleuteling van de document-sleutels met RSA met een 2048-bit sleutel
- SHA-256 voor cryptografische handtekeningen.[22]

[21] E-mail van Microsoft Nederland aan Privacy Company van 10 december 2020.
[22] Microsoft, How does Azure RMS work? Under the hood, 11 augustus 2020, URL: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#cryptographic-controls-used-by-azure-rms-algorithms-and-key-lengths

Dat betekent dat de inhoud en sleutels toegankelijk zijn vanuit verschillende omgevingen, mits DKE technisch inderdaad werkt zoals gespecificeerd in de openbare documentatie.

Tabel 1: overzicht sleutelbeheer vanuit de drie omgevingen die toegang hebben tot DKE

	Werkplek	DKE Service	AIP Service
Document inhoud	x		
Per document key	x	x	
DKE Public Key	x	x	
DKE Private key		x	
AIP Public Key	x		x
AIP Private Key			x

Tabel 1 toont welke informatie beschikbaar is vanuit elk van de drie omgevingen. Om documenten te kunnen ontsleutelen is controle nodig over beide *private keys*, en daarom is het belangrijk om de DKE service af te schermen tegen toegang door Microsoft.

Microsoft heeft twee andere diensten voor het versleutelen van documenten: *Bring Your Own Key* (BYOK) en *Hold Your Own Key* (HYOK). Hieronder wordt kort toegelicht waarin deze diensten verschillen van de nieuwe DKE dienst.

Met BYOK kan de klant een eigen sleutel beheren in een Azure Key Vault. De sleutel kan volgens Microsoft *on-premises* worden aangemaakt en opgeslagen in een HSM in de Azure cloud. Beheerders kunnen de sleutels ook direct in de Azure Key Vault aanmaken.

HYOK wordt door Microsoft vanaf 31 maart 2021 niet meer ondersteund.[23] Deze service kan gezien worden als de voorloper van Office 365 DKE. HYOK maakt net als DKE gebruik van twee sleutels om de inhoud van documenten te beschermen. Een van de sleutels wordt beheerd door Microsoft en opgeslagen in de Azure cloud. De andere sleutel wordt door een organisatie zelf beheerd en opgeslagen in de Active Directory Rights Management Service. Dat kan in de cloud of *on-premises*. Door de tweede sleutel buiten controle van Microsoft te houden, kan zelfs Microsoft geen toegang krijgen tot de inhoud van bestanden. Dit terwijl organisaties gebruik kunnen maken van de verschillende Microsoft clouddiensten voor de opslag en uitwisseling van bestanden.

Verschillen DKE en HYOK

Het belangrijkste verschil tussen Office 365 DKE en HYOK is dat HYOK is gebaseerd op verouderde software. Het gaat om de Active Directory Rights Management Service en de vorige AIP Unified Labeling Client. De Active Directory Rights Management Service die verantwoordelijk is voor het sleutelbeheer, is bijvoorbeeld géén open source, in tegenstelling tot de nieuwe DKE Service. Een ander belangrijk verschil is dat HYOK op meer platformen kon worden gebruikt dan DKE. HYOK is beschikbaar in de Office 365, Office 2019, Office 2016 en Office 2013 applicaties Word, PowerPoint, Excel en Outlook op Windows met beperkte functionaliteit om beschermde inhoud te bekijken. Sommige HYOK functionaliteiten zijn ook beschikbaar voor macOS, maar dan alleen als *read-only*. Op iOS en Android is HYOK helemaal niet beschikbaar voor Outlook. [24]

[23] Microsoft, Hold your own key (HYOK) details for Azure Information Protection, 13 October 2020, URL: https://docs.microsoft.com/en-us/azure/information-protection/configure-adrms-restrictions

[24] Microsoft, Hold your own key (HYOK) details for Azure Information Protection, 13 October 2020, URL: https://docs.microsoft.com/nl-nl/azure/information-protection/configure-adrms-restrictions#supported-applications-for-hyok

Verschillen DKE en BYOK
Het belangrijkste verschil tussen Office 365 DKE en BYOK zit in het aantal encryptiestappen, wie de sleutels beheert en het aantal diensten waar de encryptiedienst kan samenwerken. Vergeleken met BYOK is een belangrijk nadeel dat je de sleutel die door Azure wordt beheerd, niet zelf kunt beheren.

9. Inventarisatie van de risico's

Privacy Company beoordeelt in deze analyse alleen risico's die specifiek voortkomen uit het gebruik van Office 365 DKE en de bijbehorende software. Zoals toegelicht in de inleiding zijn andere risico's buiten scope die niet direct gerelateerd zijn aan het gebruik van Office 365 DKE.

9.1 Backdoors in client-software

Op de werkplek van de eindgebruiker hebben het besturingssysteem, de *Azure Information Protection Unified Labeling Client* en de Office 365 applicaties toegang tot de onversleutelde inhoud van documenten en de sleutel waarmee de versleutelde documenten ontsleuteld kunnen worden. In theorie is het mogelijk dat deze software de documenten of het sleutelmateriaal exfiltreert.

Er zijn tegenmaatregelen denkbaar tegen dit exfiltratie risico, maar deze maatregelen lijken geen effectieve oplossing te bieden.

- Het volledig ontkoppelen van de werkplekken van het internet is geen oplossing tegen deze dreiging omdat het functioneren van Office 365 DKE afhankelijk is van een online dienst in de Azure Cloud.

- Een andere mogelijke maatregel tegen dit risico is het (laten uitvoeren van) een audit op de software om het bestaan van backdoors uit te sluiten. Deze maatregel is waarschijnlijk niet haalbaar vanwege de complexiteit van alle componenten en de hoeveelheid updates.

- Monitoring op netwerkcommunicatie om eventuele exfiltratie van sleutels of vertrouwelijke inhoud te detecteren is waarschijnlijk evenmin praktisch uitvoerbaar. Een beheerder kan weliswaar monitoren of er afwijkingen optreden in de communicatie met bekende hosts, maar dergelijke monitoring biedt weinig zekerheid. De hosts waar de legitieme communicatie mee plaatsvindt (de *Azure Information Protection Service*) zijn eigendom van Microsoft, en als de client een backdoor zou hebben naar Microsoft, zou het verkeer nog steeds naar de vertrouwde servers van Microsoft kunnen lopen.

Het gebruik van Office 365 DKE biedt dus geen effectieve bescherming tegen het risico van een door Microsoft bewust ingebouwde backdoor in de client. Als risico's op backdoors onaanvaardbaar zijn voor een organisatie, kan de organisatie beter géén gebruik maken van Office 365 DKE. Bij het gebruik van DKE is het immers niet mogelijk om werkplekken los te koppelen van het internet als maatregel om de impact van eventuele backdoors in te perken, omdat DKE afhankelijk is van het gebruik van enkele Azure diensten.

De meerwaarde van DKE ten opzichte van oplossingen zoals *Azure Information Protection* (de labeling en gewone versleuteling van gegevens) is dat het voor sommige inhoud niet acceptabel is om Microsoft toegang te geven tot de sleutels waarmee de data ontsleuteld kan worden. Door de inzet van DKE heeft Microsoft geen toegang tot het sleutelmateriaal, maar nog wel toegang tot de code van Windows, Office 365 applicaties en de *Azure Information Protection Unified Labeling Client*.

Microsoft kan, in theorie, via deze applicaties of updates die later worden geïnstalleerd, toegang krijgen tot sleutelmateriaal of tot de ontsleutelde inhoud.

9.2 Telemetrie in Windows en Office

DKE informatie zou eventueel bij Microsoft kunnen belanden via de stroom diagnostische gegevens die Microsoft verzamelt vanuit Windows en Office. Microsoft verzamelt via zowel Windows[25] als de Office 365[26] applicaties telemetrie over het gebruik van Windows en Office. Voor Windows Server, Windows 10 Enterprise en Windows 10 Education is het inmiddels mogelijk om de telemetrie volledig uit te schakelen (Diagnostic data off[27]). Voor Office is het niet mogelijk om het verzamelen van telemetrie uit te schakelen. Privacy Company adviseert om in ieder geval de telemetrie-verzameling voor Windows uit te zetten en bij Office 365 te configureren op het laagste niveau '*Required*' en te beoordelen of de gedocumenteerde telemetrieverzameling acceptabel is.

Microsoft kan de inhoud van de telemetrie dynamisch aanpassen. De telemetrie kan, afhankelijk van de instellingen, ook gedeeltelijk inhoud van documenten en tekstinvoer bevatten. Gebruikers kunnen zien welke telemetriegegevens Microsoft verzamelt via de Diagnostic Data Viewer[12]. Deze Diagnostic Data Viewer is echter niet geschikt voor beheerders, om al het uitgaande verkeer gecentraliseerd of geautomatiseerd te monitoren en is ook niet geschikt om specifieke telemetrie te blokkeren.

Als een overheidsorganisatie de verzending van telemetrie niet volledig blokkeert, is er geen effectieve methode om te voorkomen dat Microsoft door een aanpassing in de telemetrie-configuratie alsnog vertrouwelijke inhoud of metadata verzamelt. Uiteraard biedt Microsoft contractuele garanties onder het Rijks privacy-amendement dat zij dit niet doet, maar deze analyse beschrijft het risico dat Microsoft deze garanties omzeilt. Bovendien kunnen eindgebruikers via de Diagnostic Data Viewer controleren welke informatie Microsoft verzamelt. Die maatregel biedt wel enige zekerheid over de informatie die Microsoft verzamelt. Hiermee kan de organisatie achteraf beoordelen of dit acceptabel is voor het vereiste beschermingsniveau.

9.3 Connected Experiences in Office

De Office 365 applicaties bevatten een aantal categorieën Connected Experiences.[28] Dit zijn mini-functionaliteiten in Office die afhankelijk zijn van online diensten, zoals spelling of het invoegen van

---

[25] Microsoft, Configure Windows diagnostic data in your organization, 13 oktober 2020, URL: https://docs.microsoft.com/nl-nl/windows/privacy/configure-windows-diagnostic-data-in-your-organization

[26] Microsoft, Required diagnostic data for Office, 26 november 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/required-diagnostic-data

[27] Toen Privacy Company onderzoek deed voor SLM Microsoft Rijk naar de diagnostische gegevens uit Windows 10 Enterprise, was de laagst mogelijke telemetrie-instelling 'Security'. Inmiddels biedt Microsoft de mogelijkheid aan beheerders om de telemetrie in Windows volledig uit schakelen. Microsoft schrijft: "*Diagnostic data off-*
This setting was previously labeled as ***Security****. When you configure this setting, no Windows diagnostic data is sent from your device. This is only available on Windows Server, Windows 10 Enterprise, and Windows 10 Education. If you choose this setting, devices in your organization will still be secure.*" Bron: Microsoft, Configure Windows diagnostic data in your organization, 13 oktober 2020, URL: https://docs.microsoft.com/nl-nl/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostische-gegevens-uitdiagnostic-data-off.

[28] Microsoft noemt deze diensten in het Nederlands 'verbonden ervaringen', maar in dit rapport wordt de Engelstalige term Connected Experiences aangehouden.

3D -animaties.[29] Als een organisatie DKE toepast, zijn de Connected Experiences nog steeds beschikbaar in Office.

Microsoft maakt onderscheid tussen Connected Experiences waarvoor zij optreedt als verwerker, en Connected Experiences waarvoor zij optreedt als zelfstandige verantwoordelijke. In haar rol als verwerker mag Microsoft de persoonsgegevens maar voor drie functionele doelen verwerken, voor zover noodzakelijk. In haar rol als verantwoordelijke behoudt Microsoft zich het recht voor de gegevens ook voor allerlei commerciële doelen te verwerken, zoals benoemd in haar algemene (consumenten) privacyverklaring.[30]

Microsoft stelt beheerders niet in staat om de verschillende Connected Experiences individueel toe te staan of uit te schakelen. In plaats daarvan biedt Microsoft de volgende vier beleidsinstellingen:[31]

- Het gebruik van Connected Experiences in Office toestaan waarmee inhoud wordt geanalyseerd
- Het gebruik van Connected Experiences in Office toestaan waarmee online-inhoud wordt gedownload
- Het gebruik van aanvullende, optionele Connected Experiences in Office toestaan
- Het gebruik van Connected Experiences in Office toestaan

Daarbij heeft Microsoft drie categorieën Connected Experiences gedefinieerd:

- Connected Experiences die uw inhoud analyseren[32]
- Connected Experiences die online-inhoud downloaden[33]
- Overige Connected Experiences[34]

Alle categorieën Connected Experiences bevatten functionaliteit waarmee gebruikers actief inhoudelijke gegevens kunnen doorgeven aan een webservice. Als een overheidsorganisatie twijfelt of de contractuele waarborgen van Microsoft over het gebruik van die web services in het privacy-amendement van Rijk voldoende garantie bieden, raadt Privacy Company aan om het gebruik van de Connected Experiences volledig uit te schakelen. In alle andere gevallen kunnen de beheerders volstaan met het uitschakelen van de aanvullende, optionele Connected Experiences.

9.4 Gekoppelde autorisaties voor toegang tot sleutels

De DKE Service kan op twee manieren geconfigureerd worden om gebruikers te autoriseren voor toegang; op basis van het e-mailadres of op basis van de rol waarmee de betreffende gebruiker in de Active Directory geconfigureerd staat.

---

[29] Microsoft, Connected experiences in Office, 30 oktober 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/connected-experiences

[30] Microsoft, Privacyverklaring van Microsoft, november 2020, URL: https://privacy.microsoft.com/nl-nl/privacystatement .

[31] Microsoft, Policy settings for connected experiences, 7 november 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/manage-privacy-controls#policy-settings-for-connected-experiences

[32] Microsoft, Connected experiences that analyze your content, 30 oktober 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/connected-experiences#connected-experiences-that-analyze-your-content

[33] Microsoft, Connected experiences that download online content, 30 oktober 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/connected-experiences#connected-experiences-that-download-online-content

[34] Microsoft, Other connected experiences, 30 oktober 2020, URL: https://docs.microsoft.com/nl-nl/deployoffice/privacy/connected-experiences#other-connected-experiences

In de praktijk is het gebruikelijk dat de lokale Active Directory gekoppeld is aan de Azure Active Directory zodat lokale gebruikers toegang hebben tot de online dienstverlening van Azure. Dat wil zeggen dat de organisatie gebruik maakt van een hybride Active Directory waarbij de Azure AD en de *on-premises* AD gekoppeld zijn. Bij opslag in de cloud heeft Microsoft toegang tot de Azure AD. Wanneer een organisatie toestaat dat veranderingen in de Azure AD worden gesynchroniseerd naar de *on-premises* AD betekent dat dat Microsoft ook invloed kan uitoefenen op de *on-premises* AD. Er is een risico dat een hacker of gecompromitteerde medewerker van Microsoft toegang krijgt tot de Azure AD, en via de synchronisatie, tot de lokale AD service. Via de synchronisatie van de AD's krijgen Microsoft en eventuele kwaadwillende third parties weliswaar geen onmiddellijke toegang tot de DKE Service, maar deze synchronisatie betekent wel dat Microsoft in 'haar' Azure AD de bestaande autorisaties in de lokale AD kan verhogen. Microsoft zou vervolgens toegang kunnen krijgen tot de sleutels als aan een tweede voorwaarde is voldaan, dat de DKE service publiek te benaderen valt. De server met de DKE service kan publiek benaderbaar zijn als een organisatie de server in de cloud host, of als er op een andere wijze toegang is verkregen tot het interne netwerk. Dat risico kan zich voordoen als een organisatie medewerkers toestaat om onderweg toegang te krijgen tot het netwerk, als ze op een laptop met Wifi zijn verbonden, en niet via een VPN.

Samenvattend, indien een organisatie kiest voor een hybride identiteit, kunnen aanpassingen in gebruikersaccounts in de Azure AD leiden tot aanpassingen in de *on-premises* AD. In een dergelijke configuratie kan iemand met voldoende toegang tot de Azure AD autorisaties beïnvloeden voor de beide keyservices.

Om dit risico tegen te gaan, adviseert Privacy Company om:

- De Double Key Encryption Service niet via het publieke internet benaderbaar te maken; en
- Geen veranderingen vanuit Azure AD te synchroniseren met de *on-premises* AD die de Double Key Encryption Service gebruikt voor autorisatie.

9.5 Post-quantum dreiging

Office 365 DKE is afhankelijk van de veiligheid van RSA om de vertrouwelijkheid te waarborgen. Voor bestanden waarvan de inhoud voor meer dan tien of twintig jaar vertrouwelijk moet blijven en waarvoor het bestaan van kwantumcomputers als reële dreiging gezien wordt, moet de organisatie afwegen of Office 365 DKE het risico voldoende afdekt.[35]

Wanneer quantum-bestendige asymmetrische algoritmen beschikbaar komen, adviseert Privacy Company om Microsoft te vragen een commitment aan te gaan om te onderzoeken of zij ondersteuning voor deze algoritmes aan de DKE Service en de *Azure information Protection Unified Labeling Client* kan toevoegen.

9.6 Bestandsnamen en metadata

Office 365 schermt en inhoud van documenten af, maar niet de bestandsnamen. Organisaties die Office 365 DKE implementeren dienen hun medewerkers duidelijk te instrueren dat de bestandsnamen geen vertrouwelijke inhoud of persoonsgegevens mogen bevatten. Een dergelijke instructie is wel foutgevoelig. Er is een grote kans dat medewerkers deze instructie af en toe vergeten na te leven.

Het gebruik van de *Azure Information Protection Service* laat ook een extra spoor van metadata na bij Microsoft over het benaderen van bestanden. Ook als een organisatie kiest voor lokale opslag

[35] AIVD, Bereid u voor op de komst van de quantumcomputer, 13 april 2015, URL: https://www.aivd.nl/documenten/publicaties/2015/04/15/bereid-u-voor-op-de-komst-van-de-quantum-computer

van bestanden kan Microsoft in theorie gegevens verzamelen over werkpatronen omdat de *Azure Information Protection Service* benaderd moet worden voor elk bestand dat geopend wordt. Deze verwerking van deze gegevens is contractueel beperkt in het privacy-amendement van het Rijk met Microsoft, omdat Microsoft in haar rol als verwerker de persoonsgegevens uit de online-diensten alleen voor drie afgesproken functionele doelen mag verwerken, voor zover noodzakelijk.

10. Is DKE een '*proprietary*' oplossing enkel voor Microsoft gebruik?

Office 365 DKE is niet te gebruiken zonder closed-source software, namelijk in de drie Office 365 Apps voor Enterprise, op het *proprietary* besturingssysteem Windows en met gebruik van de *Azure Information Protection Unified Labeling Client*.

Daarnaast is het gebruik van Office 365 DKE afhankelijk van de *Azure Information Protection Service*, een cloud-dienst die alleen door Microsoft wordt aangeboden. Eén component van Office 365 DKE is wel open source: de DKE Service.[36] Microsoft heeft deze component gepubliceerd onder de open-source MIT-licentie. De primaire functie daarvan is dat een cruciale component in het sleutelbeheer makkelijker geaudit kan worden. Toch maakt deze open source licentie het gebruik van Office 365 DKE buiten de Microsoft -cloud om nog niet mogelijk.

Conclusies

Kunnen overheidsorganisaties gegevens in Microsoft Office 365 met behulp van DKE beveiligen tegen toegang door Microsoft als clouddienstverlener? Er is geen makkelijk Ja of Nee antwoord mogelijk op deze vraag, omdat eventuele ongewilde toegang door Microsoft sterk samenhangt met het eigen risicoprofiel van de organisatie, de gebruikte applicatie, en met de inrichting van de versleutelingsdienst.

DKE is alleen beschikbaar op Windows desktops en laptops, waarbij alleen Word, PowerPoint en Excel een automatische integratie hebben met DKE. Dat betekent dat er nog veel platforms zijn die gebruikt worden door overheidsmedewerkers waarop DKE niet te gebruiken valt.

Om de inhoud van bestanden met DKE zo goed mogelijk te beschermen tegen onrechtmatige toegang door Microsoft als cloudprovider, adviseert Privacy Company beheerders om zeven technische en organisatorische maatregelen te treffen. Deze maatregelen helpen echter niet tegen eventuele backdoors op Microsofts Azure AD-servers, in de DKE Service software of in de eindgebruikersclient (de *Azure Information Protection Unified Labeling Client*). Organisaties kunnen dit risico alleen voorkomen door hun netwerk volledig los te koppelen van internet, of door andere versleutelingsmaatregelen te treffen.

Los van de adviezen aan beheerders adviseert Privacy Company het Rijk om een test set-up met DKE in te richten, en het gebruik van de verschillende Connected Experiences afzonderlijk te testen.

[36] De broncode is beschikbaar via Github, URL: https://github.com/Azure-Samples/DoubleKeyEncryptionService

Ook zou het Rijk een commitment moeten vragen aan Microsoft om quantum-bestendige asymmetrische algoritmen toe te passen in DKE zodra die beschikbaar komen.

De aanbevolen maatregelen zijn:

1. Rol de DKE Service uit via een hosting-oplossing waar Microsoft geen directe invloed op kan uitoefenen. Een *on-premises* installatie van de DKE Service ligt daarbij het meest voor de hand. Hosting bij een externe hostingpartij is ook een optie, mits de overheidsorganisatie kan uitsluiten dat een dreigingsactor die toegang kan krijgen tot de Azure dienstverlening, ook toegang kan krijgen tot deze hostingpartij.

2. Gebruik een sleutellengte van minimaal 3072 bit, vanwege het relatief hoge dreigingsniveau waartegen Office 365 DKE zou moeten beschermen, of sluit minimaal aan bij het bestaande beleid van de organisatie met betrekking tot het gebruik van cryptografische sleutels.

3. Autoriseer gebruikers gebaseerd op hun rol (lid van het onderzoeksteam), en niet op basis van hun e-mail adres. *Role Authorization* zorgt ervoor dat het beheer van autorisaties op een centrale plek kan worden bijgehouden. Als de beheerder gebruik maakt van een administratieve indeling van medewerkers per groep, hoeft hij de autorisaties niet per inkomende en vertrekkende medewerker bij te houden.

4. Sta bij gebruik van DKE alleen synchronisatie toe van de *on premises* AD naar de Azure AD, en niet omgekeerd. Om gebruik van Microsoft DKE mogelijk te maken, is het noodzakelijk om de eigen *on-premises* Active Directory te synchroniseren met Microsoft's centrale online AD. Dat synchroniseren kan twee kanten op lopen. Dat kan de beheerder instellen. Als de beheerder kiest voor synchronisatie van de Azure AD naar de *on premises* AD, dan kan Microsoft in theorie de autorisaties voor zowel de *Azure Information Protection Service*s als de DKE Service beïnvloeden.

5. Scherm de DKE Service zodanig af dat die niet te benaderen is via het publieke internet, maar bijvoorbeeld alleen via het interne netwerk of via een VPN. Dit om te voorkomen dat bestanden buiten het netwerk kunnen worden ontsleuteld, als bepaalde gebruikersaccounts eventueel gecompromitteerd raken. Dit is een aanvullende maatregel op maatregel 4, omdat voor toegang tot de private sleutel zowel autorisatie nodig is, als toegang tot de DKE Service.

6. Adviseer gebruikers om géén persoonsgegevens of vertrouwelijke gegevens op te nemen in bestandsnamen.

7. Zet de telemetrie-verzameling voor Windows uit. Configureer de telemetrieverzameling bij Office 365 op het laagste niveau '*Required'* en beoordeel of de gedocumenteerde telemetrieverzameling acceptabel is. Als een overheidsorganisatie twijfelt of de contractuele waarborgen van Microsoft over het gebruik van die we services in het privacy-amendement van Rijk voldoende garantie bieden, schakel de Connected Experiences volledig uit.

8. Contractuele opdracht aan SLM Microsoft Rijk: vraag Microsoft om een commitment, wanneer quantum-bestendige asymmetrische algoritmen beschikbaar komen, om te onderzoeken of zij ondersteuning voor deze algoritmes kan toevoegen aan de DKE Service en de *Azure information Protection Unified Labeling Client*.

Als het Rijk nader technisch onderzoek wil laten uitvoeren, dan adviseert Privacy Company de volgende stappen:

1. Controleer de AIP labeling client met een cryptografische audit en controleer technisch of de client geen telemetrie of andere gegevens naar Microsoft verzendt;
2. Controleer de DKE service met een cryptografische audit en controleer technisch of de client geen telemetrie of andere gegevens naar Microsoft verzendt;
3. Voer een audit uit bij Microsoft hoe ze omgaat met sleutels en updatebeleid (worden de updates gecontroleerd/gecertificeerd dat er geen backdoors in zitten?).

Dit rapport is opgesteld door senior technoloog Floor Terra, in samenwerking met senior adviseur Sjoera Nas

Vragen?

www.privacycompany.eu
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
Den Haag

KvK 63080052