Vragen/opmerkingen vooraf gesteld	Antwoord Microsoft
(Hoe) kan ik SaaS Solutions met M36 MFA beveiligen? En dan bedoel ik niet 'technisch' met vinkjes en instellingen, maar op CISO-niveau ;-)	Zie slide 11
Ik weet dat de sessie gaat over MFA op diensten van Microsoft, maar ik zou ook graag willen weten wat het standpunt is van MFA op apparaten (laptop/smartphones/tablets) en hoe dit ingevuld zou moeten worden. Wellicht kan Microsoft dat toelichten voor met name gebruik op Windows laptops en kan de IBD aangeven of dit veilig genoeg geacht wordt. Als dit niet de juiste sessie voor deze vraag is of er is geen tijd voor dan zou ik graag op een andere manier de vraag beantwoord krijgen.	Zie slide 16, type apparaat is minder relevant. Relevanter is de mate van vertrouwen (locatie/compliant)
Hoe om te gaan met applicaties waarbij er functies om e-mailadressen te onthouden worden aangeboden.	Tijdens sessie benoemd dat cachen van credentials geen manier is om MFA te omzeilen. Het gaat om vertrouwen
Wij gebruiken een 2FA oplossing van OneSpan (voorheen Vasco) kunnen we deze ook gebruiken voor 2fa op Office365.	Zie slide 14, meer info over requirements: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-oath-tokens#oath-hardware-tokens-preview
Ik ben benieuwd hoe en of de MFA ook doorwerkt op mobiele apparaten (O365 apps) zoals telefoons en ipads. En hoe dit samenhangt met conditional access.	Zie slide 16, type apparaat is minder relevant. Relevanter is de mate van vertrouwen (locatie/compliant)
Hoe zorgen we ervoor dat alle gebruikersgroepen dus ook buitendienst medewerkers of medewerkers zonder mobiel toestel. Gebruik kunnen maken van 2FA / MFA, als ze gebruik maken van een klein deel van de oplossingen.	Zie slide 14
Welke two-factor policy instelling geeft voldoende veiligheid zonder de gebruikers te frustreren waardoor ze achteloos gaan goedkeuren.	Zie slide 14
MFA in combinatie met Netscaler. Kunnen we dit ook koppelen aan VMware identity manager? Zodat we maar één MFA provider hebben.	Zie slide 11, https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/citrix-netscaler-tutorial Azure MFA biedt mogelijkheden voor externe intergatie. Bijvoorbeeld via Radius of NPS: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension
Kan Self Service Password Recovery meegenomen worden?	Meer info over SSPR: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
Indien MFA is ingeschakeld werkt outlookmail dan nog wel in andere mailapplicaties?	Outlook 2013 en later ondersteunt moderne authenticatie. MFA vereist moderne authenticatie
Hoe kun je het inloggen gebruiksvriendelijk houden? Hoe stel je bij conditional access bijvoorbeeld in dat mfa maar eens per 4 uur nodig is? En hoe ga je om met het gebruik van prive apparaten in vergelijking tot volledig beheerde apparaten (telefoons/laptops)?	Zie slide 16, CA heeft mogelijkheden de sessie-tijd te bepaken waamee je de frequentie van MFA reguleert.
Is het mogelijk om bij conditional access policies waarbij op basis van IP reeksen MFA niet wordt vereist (trusted zone) toch voor bepaalde (high privileged) accounts MFA af te dwingen?	Zie slide 21
Ik ben geïnteresseerd in de volgende punten: - welke licenties zijn nodig om MFA in te richten in een Citrix omgeving (intern geen 2-factor). - voldoet de MFA die standaard aangeboden wordt aan de eisen van de IBD	Zie slide 11, https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/citrix-netscaler-tutorial. Bij Microsoft is het niet bekend of IBD/VNG hier specifieke eisen aan stelt.
Nee geen specifieke vragen, Informatie inwinnen.	Ok, helder. We hopen dat de sessie hierin heeft bijgedragen.
Hoe kan een laptop met MFA/2FA in de Azure AD worden beveiligd?	Zie slide 15
Kan hierbij het gebruik van Intune betrokken worden?	Zie slide 32 en 33
Hoe voorkom je dat je medewerkers opzadelt met tig MFA challenges per dag, wat zijn daarvoor goede richtlijnen. Ook gezien vele SaaS toepassingen - dus andere webapplicaties.	Zie slide 16, CA heeft mogelijkheden de sessie-tijd te bepaken waamee je de frequentie van MFA reguleert.
Passwordless inloggen	Zie slide 15
Gebruik van ADFS servers en MFA servers, deze gaan op den duur uit de support, wat zijn de alternatieven voor het on-premis faciliteren voor 2fta.	Zie slide 12
Hoe kun je MDM en MAM zo inrichten dat het veilig is, maar dat er op het apparaat wel verschillende organisatie accounts naast elkaar gebruikt kunnen worden?	Zie slide 33
Koppeling op SSO voor andere clouddiensten zoals YouForce, Ibabs, etc etc etc en gebruik voor onprem applicaties en vervanging voor de SafeNet Token voor VDI/Citrix toegang.	Zie slide 11, https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/citrix-netscaler-tutorial
Wat zijn de mogelijkheden aangaande mfa icm een remote desktop cluster? Wat zijn de mogelijkheden om MFA toe te passen op onpremise applicaties / waar moeten deze applicaties aan voldoen / welke protocollen worden hiervoor gebruikt.	Zie slide 11, Application proxy, info voer protocollen: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-proxy#authentication
Zijn er persoonsgegevens (login, namen, enz) van onze medewerkers bij deze oplossing in het spel? Zo ja, verlaten die dat de EU? Is er een DPIA over dit oplossing gedaan (is volgens mij geen onderdeel van de MS-DPIA"s van SLM Microsoft Rijk)?	Informatie over locatie van data via trust.microsoft.com. https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-data-residency#data-stored-by-azure-ad-multifactor-authentication
Graag meer uitleg over de algemene werking van de 2FA en wat dat betekent voor het werken op verschillende apparaten.	Zie alle slides
Fijn om de achtergrond te zien. Mooi om het in relatie tot Azure en M365 mee te krijgen.	Ok, duidelijk. We hopen dat dit is gelukt tijdens de uitzending.
1: Microsoft MFA heeft de optie om authenticatieverzoeken goed te keuren via de APP, de APP notificatie te openen en op goedkeuren te klikken, deze moet je wel 2 keer ontgrendelen met je vingerafdruk of toegangscode van je device. Is dit veilig genoeg of raden jullie aan om de volledige eenmalige wachtwoordcode steeds in te vullen? 2: Is het aan te raden om MFA ook intern in te schakelen voor toegang tot de werkomgeving, of voldoet het IP adres van kantoor als veilige zone, om geen 2 factor te hanteren voor binnen het pand.	Zie slide 14 en 5
Wat is het verschil met andere MFA ontwikkelaars?	Zie alle slides
1. 2MFA voor 'e-mail only' accounts handig in te stellen? We hebben een aantal accounts waarbij de gebruiker alleen de e-mail gebruikt. Deze mensen zijn in gevallen externen. Zijn daar handige instellingen binnen office 365 voor; is daar ook een handleiding voor? 2. Er zijn heel vele mailboxen waar meerdere personen toegang krijgen. Het gaat dan om algemene zaken als privacy@hilversum.nl. Wanneer zij vanuit de organisatie toegang tot de mailbox krijgen; is het dan ook voor verschillende personen te bereiken met hun eigen MFA proces?	Zie slide 16, MFA begrijpt mailbox delegation en mailbox rechten

Geen specifieke vraag, ik vraag me wel iets af. Onze ICT afdeling wil laptops uitleveren met lokaal Office geinstalleerd icm OneDrive, terwijl we op dit moment 0 footprint laptops hebben die alleen een verbinding met onze Citrix servers kunnen maken, inloggen gebeurt met MFA. Als straks de laptops ook direct vanuit Office naar de OneDrive kunnen connecten hoe past MFA dan in dat verhaal? Of is het na inloggen op de laptop een kwestie van single sign-on? zoals je merkt snap ik het nog niet allemaal, gelukkig komt deze sessie er aan :)	Zie slide 16, type apparaat is minder relevant. Relevanter is de mate van vertrouwen (locatie/compliant) - compliant kan zijn (hybrid) AAD joined en daarme ook SSO
M365 heeft de nodige instellingen om 2FA in te stellen. Is er een best praktisch tussen security en gebruikersgemak? Om te voorkomen dat men tientallen keren goedkeuring via de app moet geven. Want daar wordt de security zwakker van. Immers worden de goedkeuringen zonder nadenken geaccepteerd.	Zie slide 14 en 5
Ik ben benieuwd in hoeverre Microsoft kan integreren met oplossingen van derden, vooral in combinatie met een hybride infrastructuur.	Zie slide 11 en 12
Benieuwd hoe we met de juiste afstemming met SAAS leveranciers zoveel mogelijk 2fa kunnen standaardiseren op MFA. Om te voorkomen dat we onze gebruikers straks met x-aantal authenticators moeten uitrusten om hun werkzaamheden te kunnen verrichten.	Zie slide 11
Hoe bruikbaar/gebruikersvriendelijk en de beheerlast ervaren van Biometrie als men deze wil inzetten als 2fa	Zie slide 5, biometrie vereist geen extra beheer vanuit techniek. Hoogstens gebruikerstraining
Moeten we MFA niet breder zien, bijv. Sso/device fingerprinting/locatie policy?	Zie slide 11, 14, 16
Is er één MFA oplossing die voor alle omgevingen/aspecten inzetbaar is	Zie slide 11
Hoe voorkomen we het uitlekken van tokens	Vraag is me niet helemaal duidelijk, tokens hebben ingebouwde tamper bescherming om uitlekken tegen te gaan
Welke MFA types zijn veilig, kunnen we bijv. nog sms tokens gebruiken?	Zie slide 14
Kunnen jullie een doorkijkje geven naar passwordless authenticatie?	Zie slide 15

Vragen/opmerkingen tijdens de uitzending	Antwoord Microsoft
Is het per applicatie een aparte Azure AD App Proxy? of 1 proxy voor meerdere applicaties?	1 app proxy kan meerdere applicaities bedienen. Kijk hier voor HA en load balance aandachtspunten: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-high-availability-load-balancing
vmware view vraagt eerst een token en dan een password waardoor dat niet werkt	Als vmware om een token vraagt is er al een mfa oplossing actief op vmware. Die uitschakelen en vmware koppelen met Azure MFA zou een optie zijn. Dat kan via Radius of NPS: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension
En hoe zorg je lokaal op de desktop voor MFA met deze oplossing?	Zie slide 15
Hoe zorg je dan voor activesync met passwordless inloggen?	Activesync is een legacy protocol en ondersteunt geen modern authentication. Advies om af te stappen van activesync en gebruik te maken van moderne authetnicatie. Dat is sneller, stabieler en veiliger.
Zijn de hard tokens nu wel of niet officieel gesupport? Op de Microsoft site staan deze nog steeds gemeld dat deze een Preview status hebben	Is nog in Preview op dit moment. GA datum nog niet bekend.
Is er integratie met 'know leaked passwords' zoals je nu ziet in o.a. Chrome.	Dit is in chrome een functionaliteit van de password manager. We bieden in Edge vergelijkbare functionaliteit. Echter, dit beperkt zich tot opgeslagen wachtwoorden. In plaats van wachtwoorden opslaan, leuenen we liever op SSO integratie en condtional access. Binnen condtional access kennen we user risk. Dat kijkt naar leaked credentials. Meer info: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#user-risk
Wat is de meerwaarde van oplossingen zoals Imprivata? en is dat een partner of een concurrent?	Imprivata is een partner van Microsoft. Met hun OneSign App kunnen ze heel goed on prem apps & devices voorzien van authenticatie middels pasjes (passwordless). Wordt met name toegepast voor Tap & Go voor VDI omgevingen vanuit een on prem infrastructuur.
Inloggen met Mifare kaart (personeelspas) kan dus wel mits je een geschikte reader hebt via usb?	Technisch zou dat wellicht kunnen. Dat noemen we smartcard authenticatie. Dergelijke oplossingen zijn vaak complex en kostbaar. De passwordless alternatieven die we op slide 13 noemen zijn eenvoudiger en goedkoper.
De gebruiker moet wel een pincode opgeven voor windows hello. Hoe veilig is dat dan?	Vele male veiliger dan een wachtwoord. Meer info: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password
Valt authenticatie met biometrische gegevens onder de toegestane mogelijkheden door de AP?	Er is hiervoor iets geregeld in de uAVG, je mag biometrische gegevens gebruiken voor authenticatie van bedrijfsnetwerken, als je eerst onderzocht hebt of er geen realistischer oplossingen zonder biometrie mogelijk zijn die hetzelfde doel bereiken, of als je (vrijelijk gegeven) toestemming hebt. De eerste optie is denk ik de beste, voor beide moet je als werkgever ook even langs de OR voor instemming. Overigens gaat het hier om gehashte en versleutelde persoonsgegevens die na de eerste opslag voor anderen niet meer te herleiden zijn naar een persoon. Voor meer informatie zie https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/av_sv/av15_sv.pdf. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie#mag-biometrie-worden-gebruikt-voor-toegangscontrole-6711. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie?qa=biometrie
Zijn er al organisaties die het aandurven om passwordless authentication door te voeren (dus verder gaan dan optionele keuze) op basis van biometrische informatie? Gezien AVG en AP?	Vele organisaties hebben de overstap naar passwordless reeds gemaakt. Passwordless is niet nieuw. Dagelijks gebruiken vele mijloenen werkplekken passwordless authenticatie om aan te melden. Ook in Nederland wordt al veelvuldig gebruik gemaakt hiervan. Voor meer informatie zie https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/av_sv/av15_sv.pdf
Hoe gaat zero trust om met TAB-NUC apparaten, en room account, met automatische login	Zie slide 16, type apparaat is minder relevant. Relevanter is de mate van vertrouwen (locatie/compliant)
Wij gebruiken al Azure AD. Heb nu een SAAS applicatie die nog werkt met sms code. Heb ze gevraagd om het mogelijk te maken dat we via Azure AD kunnen inloggen. Volgens hen is dit niet mogelijk. Kan dit kloppen of willen ze gewoon niet? Of te wel, hoe krijgen we SAAS leveranciers bereid om hier aan te voldoen?	Dit is afhankelijk van de app. Als de app web authenticatie spreekt dan zou het mogelijk moeten zijn om te koppelen voor SSO en dus ook in Conditional Access mee te nemen
Hoe kunnen we het beste omgaan met apps die credentials cachen? Bv de Team desktop app onthoudt je (MFA) credentials als je die afsluit in plaats van uit te loggen. De volgende keer log je automatisch in zonder credentials in te geven.	Tijdens sessie benoemt dat cachen van credentials geen manier is om MFA te omzeilen. Het gaat om vertrouwen.

Hoe verzorg je MFA binnen je onprem omgeving specifiek voor beheerder binnen een nieuwe omgevinge nu MFA server niet meer wordt ondersteund?	Zie slide 11 en 12 koppel de app aan Azure AD
Hoe zorg je ervoor dat je niet de hele dag gevraagd wordt om mfa, hoe is de geldigheidsduur van een mfa authenticatie in te stellen? Is de proxy functionaliteit ook geschikt voor niet web applicaties?	Zie slide 16, CA heeft mogelijkheden de sessie-tijd te bepaken waamee je de frequentie van MFA reguleert. Er zijn bepaalde use cases die niet-webapps publishing mogelijk maken: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-proxy#other-use-cases
MFA toepassen op een app, bijv. wachtwoordenkluis, binnen de Citrix omgeving (waar al MFA op actief is) voegt dat iets toe?	MFA toepassen op een app met wachtwoordkluis via Condtional Access voegt zeker iets toe. Azure AD biedt ook wachtwoordkluis functionaliteit.
Hoe kan ik het beste MFA toepassen op onprem server omgevingen en dan specifiek voor admin accounts	Meer info over securing privileged access: https://docs.microsoft.com/en-us/security/compass/privileged-access-accounts
Hoe kan je omgaan met MFA voor samenwerkingspartners/leveranciers die op afstand moeten inloggen? We hebben de situatie dat een bedrijf wordt ingehuurd om werkzaamheden m.b.t. leerlingenvervoer voor de gemeente uit te voeren.	Gebruik MFA voor externe gebruikers/guests, dit kan geconfigureerd worden in het MFA/Conditional Access dashboard van Azure AD.
Is er een mogelijkheid om activesync devices MFA toe te passen zonder Exchange online?	Activesync is een legacy protocol en ondersteunt geen modern authentication. Advies om af te stappen van activesync en gebruik te maken van moderne authenticatie. Dat is sneller, stabieler en veiliger.
Kan de link naar de standaard CA policies gedeeld worden?	Zie: aka.ms/caascode