



IT-servicebeschrijving Centrale Authenticatie

Eigenaar
Versienummer

Architectuur RID-Utrecht
1.1



Algemene beschrijving

De IT-service Centrale Authenticatie maakt het mogelijk voor medewerkers en (interne) applicaties die onder de beheerverantwoordelijkheid van RID-Utrecht vallen aan te melden op applicaties die door leveranciers beschikbaar worden gesteld (meestal in de vorm van een SaaS-applicatie). Door deze IT-service in te zetten in combinatie met een externe (SaaS)-applicatie hoeven gebruikers slechts een keer in te loggen (ofwel op een interne werkplek, of bij een willekeurige externe applicatie) om toegang te krijgen tot alle applicaties die bij deze dienst zijn aangesloten (Single Sign On). De IT-service is erop ingericht om zoveel als mogelijk MFA (MultiFactor Authenticatie) toe te passen, waarbij de digitale identiteit van gebruikers op meerdere manieren kan worden geverifieerd.

Kwaliteitskenmerken

De IT-service heeft de volgende kwaliteitskenmerken:

Kwaliteitskenmerk	Waarde
beschikbaarheid	business critical
schaalbaarheid	up/down (trendmatig en piekbelasting, dynamisch)
integriteit	BBN2
verrekenbaarheid	gedeeld (gezamenlijke bekostiging)
servicewindow	24x7

Toepassing

De IT-service Centrale Authenticatie wordt gebruikt voor authenticatie van gebruikers en systemen/applicaties van de RID-Utrecht bij het aanmelden op externe applicaties van derden (SaaS-applicaties). Accounts van gebruikers in de voorziening die de Centrale Authenticatieservice levert worden geautomatiseerd opgevoerd door replicatie vanuit de interne Account Store (AD).

Richtlijnen voor gebruik

De volgende richtlijnen voor gebruik zijn van toepassing:

- Het wachtwoorden-/wachtzinnenbeleid dat door het Information Security Team is vastgesteld wordt gehanteerd.
- Bij toegang vanaf een apparaat buiten het (beheer)domein van de RID-Utrecht vindt authenticatie altijd plaats op basis van MultiFactor Authentication (MFA). Op zakelijke Windows-apparaten moeten gebruikers biometrische authenticatie en/of een pincode configureren waarmee ze in kunnen loggen waarna ze vervolgens automatisch geauthentiseerd zijn bij browser- en desktopapplicatie zoals Outlook, Teams en SharePoint Online. Op privé-apparaten is dit niet van toepassing. Daar wordt MFA afgedwongen vanuit de diverse Conditional Access policies.
- De externe leverancier dient een trust-relatie in te stellen met de Centrale Authenticatieservice van RID-Utrecht (SAML).
- Identity/account creation dient automatisch/'on the fly' te gebeuren bij het voor de eerste keer aanmelden van een gebruiker/systeem bij externe dienst. Hiervoor wordt een gebruiker toegewezen aan een Active Directory-groep, in beheer bij de RID. Indien dit niet werkt, dan dienen gebruikers actief beheerd te worden door de organisatie zelf en worden de (mutaties op) accounts van medewerkers die toegang dienen te hebben tot een applicatie door de afnemende organisatie aan de leverancier doorgegeven.
- Na 10 opeenvolgende mislukte aanmeldpogingen wordt een account vergrendeld.
- De token lifetime is ingesteld op 1 uur (access) en 90 dagen (refresh), de sessie-lifetime van browserapplicaties en mobiele apps op 14 dagen. Beheerders en gastgebruikers dienen na 10 uur opnieuw te authenticeren.
- Tokens worden ingetrokken door de volgende gebeurtenissen:

- Beeïndigen levensduur sessie.
- Verandering van IP-adres of netwerk
- Verwijderen of uitschakeling van gebruikersaccount
- Het verlopen van een wachtwoord
- Het wijzigen/opnieuw instellen van een wachtwoord door gebruiker/beheerder
- Het intrekken van de refreshtokens voor gebruiker(s) door beheerder
- Wanneer een inlogpoging van een gebruiker geëvalueerd wordt als een hoog/midden risico.

Hierbij wordt gebruik gemaakt van 'continue toegangsevaluatie'. Hierbij worden tokens direct of uiterlijk binnen 15 minuten (afhankelijk van de situatie) ingetrokken. Dit is vooral van belang bij access tokens.

Capabilities

De IT-service omvat de volgende capabilities:

Capability	Toelichting
Account Store (external)	Gecentraliseerde opslag van gebruikers- en serviceaccounts ten behoeve van externe identiteitsvalidatie. Accounts omvatten gebruikersnaam, wachtwoord en aanvullende attributen, zoals groepslidmaatschap(pen), adresgegevens, et cetera.
Account Store (internal)	Gecentraliseerde opslag van gebruikers- en serviceaccounts ten behoeve van interne identiteitsvalidatie en replicatie met externe account stores. Hiermee levert deze account store de primaire gegevensbron. Accounts omvatten gebruikersnaam, wachtwoord en aanvullende attributen, zoals groepslidmaatschap(pen), adresgegevens, et cetera.
Identity Validation	Zo onweerlegbaar mogelijk vaststellen dat de digitale identiteit waarmee een gebruiker zich presenteert geldig en actief is.
Identity Validation Throttling	Bij het valideren van een digitale identiteit wordt een oplopende tijdsinterval ingebouwd wanneer meerdere opeenvolgende malen foutieve credentials worden opgegeven.
Identity Validation Monitoring	Actief geautomatiseerd volgen van aanmeldpogingen en rapportage van verdacht gedrag/verdachte omstandigheden.
Account Replication	Het synchroniseren van accounts en accountgegevens vanuit de primaire account store richting secundaire (externe) account stores.
Account Handling Logging	Vastleggen van alle bewerkingen en gebruiksactiviteiten die op/met accounts worden uitgevoerd, zoals replicatie en aanmeldpogingen.
Identity Validation Monitoring	Toezicht houden op het identiteit validatieproces.
Identity Reporting	Presentatie van identiteitsevenementen en resultaten van geautomatiseerde analyses i.r.t. identiteitsvraagstukken.

Technische specificaties

Component/protocol	Toepassing
Azure AD	Account store (external) middels synchronisatie
Azure AD Premium Plan 1	Licentie voor ontsluiting minimaal benodigde beveiligingsfunctionaliteit Azure AD
Azure AD Premium Plan 2	Licentie voor ontsluiting volledige beveiligingsfunctionaliteit Azure AD
Active Directory	Account store (internal)
AD Connect	Hybride identiteit (identity store onafhankelijk) met gelijk wachtwoord middels synchronisatie
Microsoft Authenticator	Multi Factor Authenticatie
SAML	Federatieve (gedelegeerde) authenticatie en verstrekken tokens
SHA256	Secure Hash Algoritme / Encryptie authenticatieverkeer