ECK-iD verwerken en opslaan in een userstore in eigen beheer

Dit document is bedoeld als een handreiking voor onderwijsinstellingen, met betrekking tot het opslaan en verwerken van het ECK-iD in het identity management systeem. De focus ligt hierbij op instellingen die zelf hun userstore geschikt moeten maken voor het ontvangen, opslaan en verzenden van het ECK-iD, zoals bijvoorbeeld een Active Directory of Azure AD.

De ICT architectuur van instellingen is nooit helemaal het zelfde. Deze handreiking beschrijft dan ook op functioneel niveau wat een instelling met AD / ADFS / Azure AD als identity provider moet doen om het ECK iD. Deze handreiking is ook tot stand gekomen met medewerking van vertegenwoordigers van middleware partijen DWE-ICT en RedSpider en tevens besproken met Tools4Ever. Scholen die hier gebruik van maken kunnen zich richten op deze partijen om na te gaan op welke wijze deze partijen de verschillende scenario's in dit document ondersteunen.

Uitgangspunten en voorschriften

De onderstaande uitgangspunten en voorschriften zijn gebaseerd op het document 'Voorschriften verwerken ECK-iD'. Deze bevat technische en organisatorische beveiligingsvoorschriften met als doel het voorkomen van het onbevoegd gebruik of misbruik van het ECK-iD. Door het volgen van deze handreiking bij het verwerken en opslaan van het ECK iD, wordt voldaan aan de voorschriften ECK iD-2 en ECKiD-5

Voor wat betreft informatiebeveiliging en het minimaliseren van de impact van eventuele datalekken, moet het ketenpseudoniem (ECK-iD) op geëncrypte wijze vastgelegd worden in de systemen van de scholen en met name in de systemen waarin zowel personalia als het ketenpseudoniem vastgelegd zijn. Afhankelijk van de gekozen oplossing kan encryptie plaatsvinden op het attribuut of op de database in zijn geheel. Daarnaast wordt voor alle oplossingen geadviseerd om encryptie op disk niveau toe te passen.

Het niet kunnen herleiden van personen na koppeling van gegevens is ook in de AVG opgenomen als belangrijke eigenschap van goede pseudonimisering.

Voorschrift ECKID-2:

- Bij de opslag van het ketenpseudoniem (ECK-iD) in administraties wordt encryptie toegepast
- Elke partij past zijn eigen encryptie toe, die voldoet aan de minimumvoorschriften, zodat er geen koppelrisico voor gegevens ontstaat. De eisen voor encryptie zijn:
    - Gebruikte encryptie algoritmen zijn bewezen veilig
    - Gebruikte sleutellengten zijn128-bits (symmetrisch) of meer
    - Algoritmen hebben geen structurele zwakheden
    - Algoritmen zijn uitvoerig bestudeerd en gestandaardiseerd
- Voorbeelden van op dit moment geaccepteerde encryptiealgoritmen zijn AES-128 en Camellia.

Verder is er een logische scheiding tussen gegevens vereist. Dit betekent dat de opgeslagen pseudoniemen niet herleidbaar zijn zonder toegang tot de encryptiesleutel en / of het gebruikte salt. Hiervoor worden private encryptiesleutels en / of salts opgeslagen met de meest minimale set aan toegangsrechten:

- Alleen leestoegang voor het serviceaccount dat gebruikt wordt voor versleuteling of ontsleuteling
- Toegang tot dit account is beperkt en wordt gelogd.

Voorschrift ECKID-5:

Dit voorschrift wordt toegepast als het ketenpseudoniem getransporteerd wordt via systeem-systeem koppelingen binnen een onderwijsorganisatie, in situaties waarbij de koppeling over het publieke internet

zonder additionele veiligheidsmaatregelen. Dit kan bijvoorbeeld het geval zijn bij cloud-oplossingen zoals Azure AD. Voor deze koppelingen geldt:

- Gebruik alleen TLS versie 1.2 of hoger.
- Kies goede cyphersuites voor de server
- Kies voldoende lengte van parameters en sleutels

Edukoppeling 1.2 voldoet aan dit voorschrift.

Aanvullend voorschrift
Als aanvullend voorschrift (door scholen gesteld bij optekenen van deze handreiking) is gesteld dat servers minimaal een A rating dienen te behalen op https://www.ssllabs.com/ssltest/.

Transport ECK-iD vanuit SIS of LAS

De uitwisseling van het ECK-iD tussen het SIS en het authenticatie systeem van de school gebeurt op basis van SCIM 2.0 (System for Cross-domain Identity Management). De SCIM koppeling bestaat uit een REST API die JSON gebruikt als Content-Type. De beveiliging van deze koppeling gebeurt op basis van oAuth2.

De implementatie zal plaats vinden op basis van push berichten vanuit het SIS. De koppeling komt naast bestaande koppelingen voor de uitwisseling van data. De onderwijsinstelling zal deze koppeling moeten realiseren in samenwerking met het SIS, waarbij voldaan wordt aan de voorwaarden voor systeem-systeem koppelingen.

Voor de uitwisseling van de data wordt een EduUser profiel geïntroduceerd waarin de volgende velden worden opgenomen:

1. Id
2. EduUser: Identificatiesleutel
3. EduUser: ECK-iD
4. EduUser:name: Achternaam
5. EduUser:name: Tussenvoegsel
6. EduUser:name: Roepnaam

De identificatiesleutel wordt gebruikt om de leerling/student of docent mee te identificeren over de systemen heen. Deze sleutel wordt beheerd door het administratiesysteem (SIS/LAS).

LET OP: *Het is belangrijk dat de onderwijsinstelling de gebruikte identificatiesleutel afstemt met de leverancier van het LAS/SIS. Voorstel is om hiervoor het* studentnummer *voor te gebruiken, aangezien deze in de verschillende systemen beschikbaar zal zijn.*

Het SIS zal volgens de voorschriften voor het verwerken van het ECK-iD deze versleuteld opslaan. Voor transport zal deze echter door het SIS worden ontsleuteld.

Opslag ECK-iD

Voor de opslag van het ECK-iD in het authenticatie systeem zijn drie mogelijke scenario's voorzien:

1. Het ECK-iD wordt in een aparte en afdoende beveiligde database opgeslagen.
2. Het ECK-iD wordt geëncrypt opgeslagen in Active Directory.
3. Het ECK-iD wordt geëncrypt opgeslagen in een Azure Active Directory omgeving.

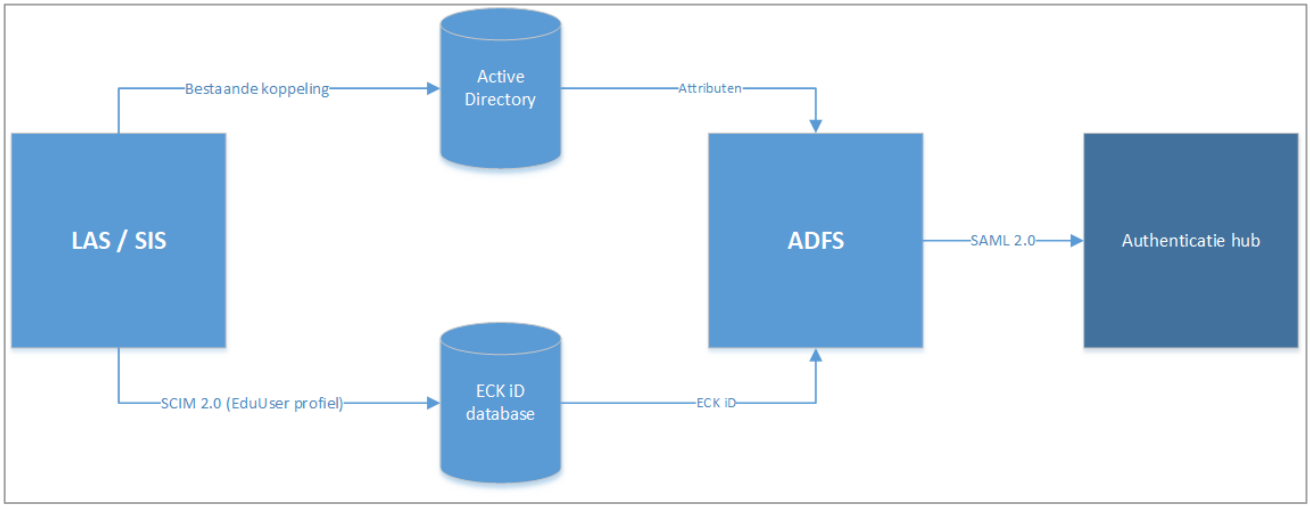
Scenario 1: ECK iD in aparte database naast Active Directory

In dit scenario wordt het ECK-iD bij ontvangst uit het SIS opgeslagen in een afzonderlijke database (naast een Active Directory). Als identificerende sleutel binnen het authenticatie systeem wordt het veld 'identificatiesleutel' uit het EduUser profiel opgeslagen bij het ECK-iD.

De database zelf is voldoende beveiligd doordat alleen een service account toegang heeft. Bovendien moet de database geëncrypt zijn. Belangrijk is dat de database een high availability en een high performance heeft. De requirements hiervoor moeten gelijk zijn aan de bestaande Active Directory van de onderwijsinstelling.

Richt ADFS in dit scenario zodanig in, dat bij het beantwoorden van een authenticatieverzoek attributen uit zowel de Active Directory als de database met ECK iD's wordt gehaald.

De meeste ketenpartijen richten hun systemen op gelijksoortige wijze in. Het scenario heeft de voorkeur wanneer met een on-premise user store wordt gewerkt.



Figuur 1: ECK iD in aparte database naast Active Directory

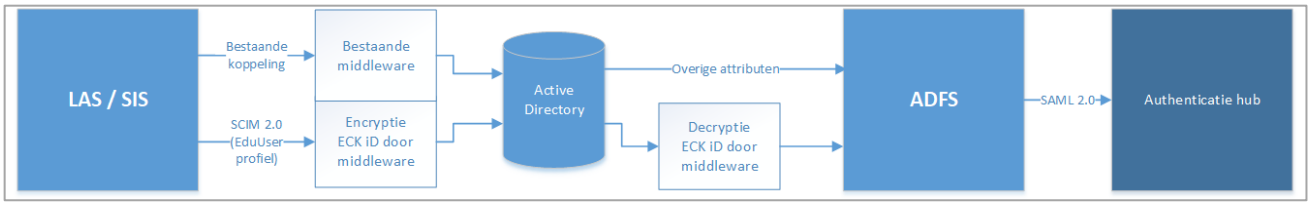
Scenario 2: ECK iD versleuteld opslaan in Active Directory

In dit scenario wordt het ECK-iD bij ontvangst uit het SIS geëncrypt en vervolgens wordt deze waarde opgeslagen in de Active Directory (on-premises of SaaS).

Aangezien Active Directory zelf geen data-encryptie ondersteunt zal voor dit scenario een aparte middleware applicatie moeten worden ingezet. Deze applicatie verzorgt de encryptie van het ECK-iD voordat het wordt opgeslagen in de Active Directory. De gebruikte encryptie dient hierbij te voldoen aan de eisen zoals beschreven in Voorschrift ECKID-2.

Dezelfde middleware applicatie kan het ECK-iD decrypten op het moment dat deze nodig is voor authenticatie in de educatieve content keten (zie 1.4).

Het belangrijkste aandachtspunt voor dit scenario is de performance van het decrypten voor het beantwoorden van een authenticatieverzoek. Hierbij moet rekening gehouden worden met de piekmomenten gedurende een dag. Afhankelijk van het aantal gebruikers bij de onderwijsinstelling kan het aantal authenticatieverzoeken op deze momenten aanzienlijk zijn.



Figuur 2: ECK iD versleuteld opslaan in Active Directory

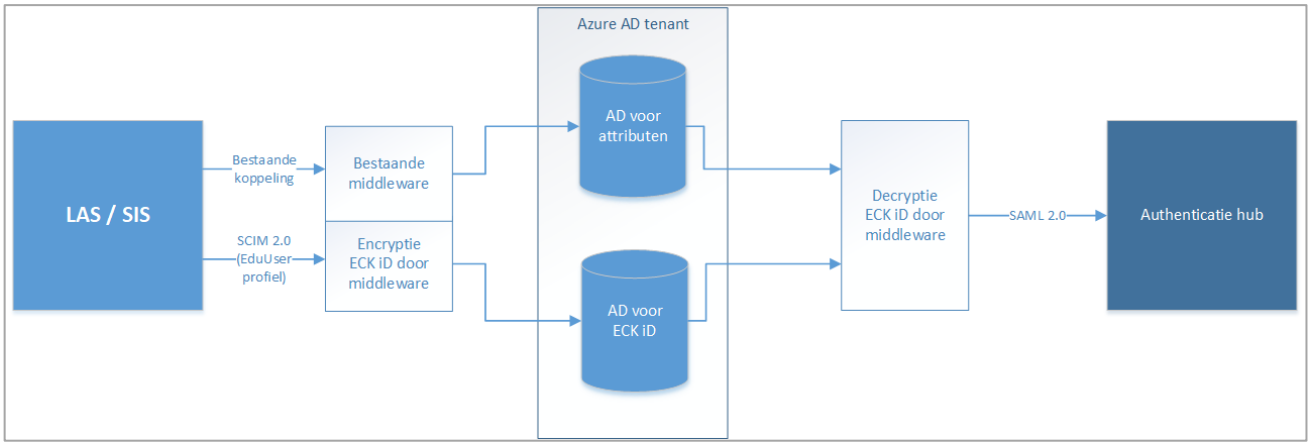
Scenario 3: ECK iD versleuteld in Azure AD.

Dit scenario is vergelijkbaar met scenario 1. Bij ontvangst uit het SIS wordt het ECK-iD encrypted opgeslagen in een aparte database binnen de Azure AD omgeving van de onderwijsinstelling, dus gescheiden van de overige gebruikersattributen. Toegang tot deze database is alleen mogelijk via een service account.

Ook in dit scenario zal er gebruik moeten worden gemaakt van een middleware applicatie, die zorgt voor het encrypten van het ECK-iD en het opslaan in de database. Tevens zal deze applicatie zorgen voor de decryptie voor het beantwoorden van een authenticatieverzoek.

Aanvullend moet Azure AD geconfigureerd worden om de standaard disk level encryption te gebruiken (https://www.microsoft.com/en-us/microsoft-365/blog/2017/09/05/how-we-secure-your-data-in-azure-ad/).

Vanwege het geëncrypt opslaan van het ECK-iD moet bij dit scenario ook rekening gehouden worden met de performance van het decrypten voor het beantwoorden van authenticatieverzoeken.



Figuur 3: ECK iD versleuteld in Azure AD

Gebruik ECK-iD tijdens authenticatie

Uiteindelijk wordt het ECK-iD in de educatieve content keten uitgeserveerd via een authenticatie volgens het SAML2 protocol. In het authenticatie response bericht, dat het authenticatiesysteem van de onderwijsinstelling naar de centrale authenticatie hub verzendt, wordt het ECK-iD opgenomen als een attribuut.
LET OP: de naam van dit attribuut in het SAML bericht is 'eckId', zie ook https://developers.wiki.kennisnet.nl/index.php?title=KNF:Attributen_overzicht_voor_Identity_Providers.

In de applicatie die de rol van Identity Provider vervult (bijvoorbeeld ADFS) moet dit attribuut geconfigureerd worden. Aansluitend bij de drie hiervoor genoemde scenario's betekent dit:

1. *Scenario 1: ECK iD in aparte database naast Active Directory.*
   De ADFS haalt het ECK-iD uit de externe database en de overige attributen komen uit de Active Directory. Voor informatie over het gebruik van meerdere datastores: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-attribute-stores

2. *Scenario 2: ECK-iD versleuteld opslaan in Active Directory.*
   De middleware applicatie die het ECK-iD heeft geëncrypt zal de decryptie uitvoeren waarna het onversleutelde ECK-iD beschikbaar komt in ADFS.

3. *Scenario 3: ECK iD versleuteld in Azure AD*
   De middleware applicatie die het ECK-iD heeft geëncrypt zal de decryptie uitvoeren waarna het onversleutelde ECK-iD beschikbaar is voor authenticatie.