Integreren Yoda en ResearchCloud identiteiten

Motivatie

Waarom willen we identiteiten koppelen?

- Gebruikers willen over meerdere applicaties heen dezelfde collegas kunnen herkennen, zodat zij over meerdere applicaties heen samen kunnen werken.

- ~~Applicaties willen een gebruiker herkennen zodat bijv. ResearchCloud een Yoda verbinding kan maken met het account van de gebruiker.~~
  Met voortschrijdend inzicht is dit niet het geval.

- Een gebruiker wil met hetzelfde account bij meerdere diensten inloggen, liefst SSO.

Huidige Situatie

Herkenning gebruikers

- Een Yoda gebruiker is herkenbaar aan zijn/haar email-adres, en de gebruiker van een ResearchCloud instantie aan UserName die in SRAM wordt gekozen. Gebruikers moeten voldoende informatie over hun collegas kennen om de relatie te leggen. Voor applicaties is de relatie momenteel niet te leggen.

Authenticatie

- Een gebruiker moe(s)t drie keer authenticeren:

Yoda	Email	Linux PAM + Radius (Intussen ondersteunt Yoda webportal OIDC)
SRAM en ResearchCloud Portal	Email of SOLIS-ID	SSO obv SAML / OIDC
ResearchCloud instantie(s)	UserName (SRAM)	LDAP icm PublicKey (SRAM) of Shared Secret (ResearchCloud)

Herkenning gebruikers (1/2)

Wat is de ideale username?

- We hanteren de volgende requirements:
  - Globally unique, zodat er geen twee gebruikers dezelfde username kunnen gebruiken.
  - Niet gescoped, zodat de oplossing onafhankelijk is van een bepaalde federatie.
  - Human Readable, zodat het username eenvoudig kan worden gebruikt.
- De volgende oplossingen voldoen niet:
  - Email, deze is (m.n. over de tijd) niet globally unique.
  - SRAM identifiers als Username of EduPersonUniqueID, deze zijn alleen uniek en dus toepasbaar binnen de scope van SRAM.
  - Gegenereerde GUIDs, deze zijn niet human readable.
- Conclusie, in overleg met SURF, is dat er geen enkelvoudige ideale username bestaat. We zullen consessies moeten doen, zoals werken met meerdere attributen.

Herkenning gebruikers (2/2)

Opties voor Yoda

- Haal extra attributen op van de IdP
  - Mogelijk zodra de OIDC koppeling
  - Extra attributen als ‘Fullname’ en/of ‘PlatformIdentifier’ (=EduPersonUniqueID) kunnen gebruikers en/of applicaties een gebruikers makkelijker herkennen.

- Nadelen:
  - Een SRAM attribuut als ‘PlatformIdentifier’ is gescoped op SRAM zelf. Dat impliceert dat gebruikers alleen binnen de context van SRAM uniek kunnen worden herkend.
  - Als de lokale IdP wordt gebruikt ontstaat een afhankelijkheid van de beschikbare attributen. Ook kan de globale uniekheid niet worden gegarandeerd.

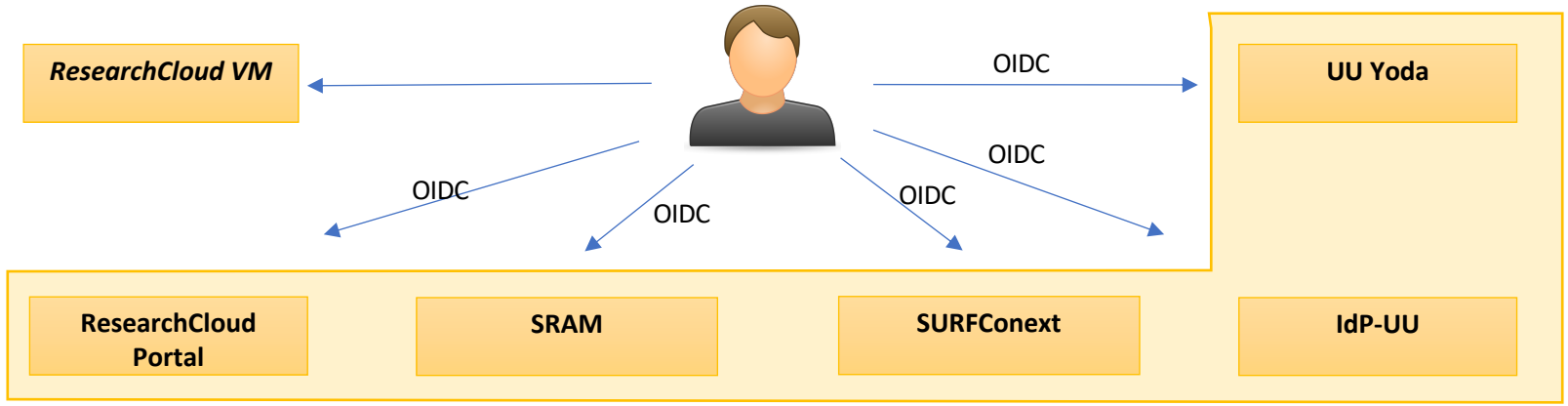
Authenticatie (1/2)

Wat is de beoogde authenticatie?

- Er is single-sign-on voor Yoda, SRAM, Researchcloud Portal en ResearchCloud instanties
- Er is ondersteuning voor alle interfaces (web, terminal, WebDAV)

Oplossingen

- Zodra Yoda OIDC ondersteunt is SSO met SRAM en ResearchCloud mogelijk.
- SSO met een ResearchCloud instantie is in principe niet realiseerbaar, omdat dit niet de bestaande browser-sessie herbruikt, en omdat de ResearchCloud VM niet federatief met de IdP is gekoppeld.



Authenticatie (2/2)

Wat is dàn de gewenste situatie?

- De belangrijkste behoefte is dat er vanaf een ResearchCloud VM kan worden geauthenticeerd (en geautoriseerd) bij Yoda. Dat wordt niet middels SSO gerealiseerd, maar betreft feitelijk ‘gedelegeerde autorisatie’ van de gebruiker aan de ResearchCloud VM bij Yoda.
- Dergelijke autorisatie wordt opgelost middels tokens, zoals die van OIDC.

Status

- De nieuwste Yoda-release ondersteunt OIDC authenticatie voor het webportal, en voor iRods (via WebPortal). Er is een afhankelijkheid van de nieuwste iRods release, die op korte termijn beschikbaar komt.
- In Yoda is de mogelijkheid gebouwd om access-tokens aan te maken, zoals ResearchDrive dat doet. Op deze manier kan ResearchCloud ipv ResearchDrive ook Yoda mounten.
- Er is een oplossingsrichting met SURF uitgedacht om dergelijke tokens via SRAM te kunnen provisionen naar ResearchCloud. Zo kan een veilige en gebruiksvriendelijke manier ontstaan om vanaf een ResearchCloud instantie toegang te krijgen tot Yoda Resources.

Knelpunt:

- De positionering van SRAM tov een instellingsdiensten als Yoda is niet triviaal. Zie deliverable “Yoda user provisioning and SRAM”.

Conclusies en Aanbevelingen

- De IAM koppeling tussen Yoda en ResearchCloud, en SRAM, blijkt een complex vraagstuk. Het kost veel tijd om het probleem, de diensten en de oplossingen goed te begrijpen. Dit is extra lastig omdat er veel verschillende spelers bij betrokken zijn.
- Het koppelen van identiteiten over onafhankelijke diensten niet vanzelfsprekend en heeft slechts beperkte meerwaarde.
- Met delegated autorisation kunnen Yoda resources worden benaderd vanuit ResearchCloud. Er zijn ideeen met SURF ontwikkeld waarbij SRAM hierin kan faciliteren. Deze ideen sluiten aan op lopende ontwikkelingen maar hebben een hoog innovatief karakter.

➔Zorg voor een duidelijke positionering van Yoda in relatie tot SRAM.

➔Committeer je samen met SURF aan het verkennen en ontwikkelen van mogelijkheden om onderzoeksdata uit bijvoorbeeld Yoda eenvoudig toegankelijk te maken voor onderzoeksdiensten zoals ResearchCloud.

Appendices

Short inventory of how someones identity is currently registered in the different services

ResearchCloud VM

Synced from Portal to local LDAP

- Username
- public Key
- Shared Secret

provision

UU Yoda

Added manually by group-administrator

- University email

Ext User Service

- email
- password

ResearchCloud Portal

User-Generated using Google Auth

- Shared secret for totp

Provisioned by SRAM:

- Name
- Firstname
- Surname
- Email adress
- Username
- Public Key
- eduPrincipalName
- voPersonsorid
- isMemberOf
- eduPersonuniqueid
- Academic Affiliations
- Entitlements
- Community affiliations
- Identity Assurance

provision

https://cm.sram.surf.nl/consent/27ed8a9a2468619 8dea9423cbb096a3ffaa6e2c46603adcdcc05db2f1759383

SRAM

Added manually by user:

- Short Username
- Public Key

Created by SRAM

- Group & CO memberships
- Platform identifier
- Short Platform identifier
- Platform affiliation

Provisioned by SURF:

- Status
- Name
- Firstname
- Surname
- Email adress
- Institutional identifier
- Institutional affiliation

https://wiki.surfnet.nl/display/SRAM/Attributes+in+SRAM

provision

https://dashboard.surfconext.nl/apps/8164/saml20_sp/attribute_policy

SURFConext

- Display Name
- Full Name
- Affiliation
- Scoped Affiliation
- Surname
- First Name
- Email Address
- Institutional User ID
- Identifier *(pseudonym)*
- User ID
- Unit Name
- Member of Organization
- Preferred Language
- Organization Type
- Organization
- Entitlement

https://wiki.surfnet.nl/display/surfconextdev/Attributes+in+SURFconext en https://profile.surfconext.nl/my-profile

provision

IdP-UU

- Full Name
- First Name
- Initials
- Last name
- Language
- E-mail
- Username
- Roles
- Status

https://mysolisid.uu.nl/account

Legend

- Added manually
- Provisioned or created by system