SWAMID

Swedish Academic Identity Federation

ADFS Toolkit MFA Workshop

Johan Peterson

Tommy Larsson

SWAMID

Agenda

- Introduction – What is ADFS Toolkit?
- Azure Template Specs
- Installation, Configuration
- RefedsMFA
- ADFSTkStore
- ADFSTk-Health
- Tools
- Q&A

SWAMID

What is the ADFS Toolkit?

- PowerShell Module
- PowerShell Gallery
- GitHub
- Import eduGAIN Metadata to ADFS in a “professional” way
- Gives you tools to handle day-to-day tasks and issues

SWAMID

Entity Categories

- No Entity Category
- R&S
- CoCo v1 and v2
- Anonymous Authorization
- Pseudonymous Authorization
- Personalized Authorization
- Federation specific Entity Categories and/or overrides

SWAMID

Subject ID Request

- SP can save what ID to use in the Metadata
  - subject-id
  - pairwise-id
  - none
  - any
    - We will choose the attribute with least personal data = pairwise-id

SWAMID

Override default attribute release

- Attributes added to release list
- Attributes added/overwritten to release list
- Attributes added/overwritten to/in release list
- Attributes added/overwritten to/in release list
- Attributes added/overwritten to/in release list

SWAMID

Azure Template Specs

- Azure Template in GitHub
- Deploys
  - AD DS
  - DNS (.local)
  - AD FS
  - Claims X-Ray
- Only for test purposes!

SWAMID

Installation

- Install ADFS Toolkit
  - Install-Module ADFSToolkit
- Create ADFS Toolkit Configuration
  - New-ADFSTkConfiguration
- Import Federation Defaults
  - Get-ADFSTkFederationDefaults -URL https://github.com/fedtools/federation-settings/archive/refs/heads/main.zip -InstallDefaults
- Create Institution Configuration
  - New-ADFSTkInstitutionConfiguration
- Install Additional modules
  - Install-ADFSTkStore
  - Install-ADFSTkMFAAdapter –RefedsMFA

SWAMID

Configuration files

WHERE get attributes from?

HOW build and release attributes?

WHAT should be released?

SWAMID

Configuration files

WHERE

Institution Config

C:\ADFSToolkit\config\institution\Config.[federation].xml

- Four Stores
  - Active Directory
  - SQL
  - Custom Store
  - Static
- Restricted values
- Groups (Name/SID)
- Transform value
  - Append, Prepend, Regexreplace
- allowedRegistrationAuthorities
- ADFSTk Store

SWAMID

HOW WHAT

Configuration files

HOW

Local Transform Rules

`C:\ADFSToolkit\config\institution\Get-ADFSTkLocalTransformRules.ps1`

- Add new attributes
- Override the way an attribute is build/released

SWAMID

WHERE WHAT

Manual overrides

WHAT

Local Manual SP Settings

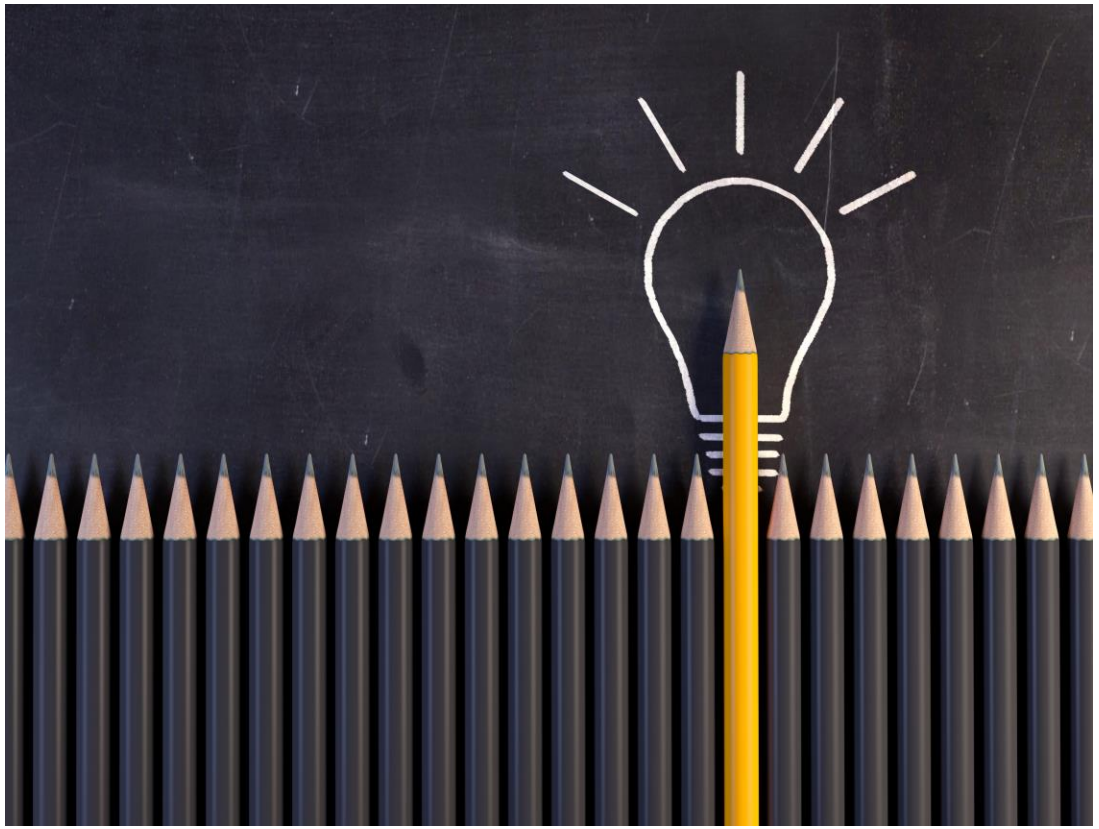
`C:\ADFSToolkit\config\institution\Get-ADFSTkLocalManualSpSettings.ps1`

- Targets:
  - A single SP
  - All SP's ending on DNS… (all SP's from the university)
  - All SP's
- Add attribute(s)
- Change attribute release(s)
- "Remove" attribute(s)

SWAMID

WHERE HOW

Federation Defaults



- Institution Config Defaults
- “Federation Local”
  - Entity Categories
  - Entity Category overrides
- Look at GitHub
- Put on GitHub or local URL

```
Get-ADFSTkFederationDefaults -URL https://github.com/fedtools/federation-settings/archive/refs/heads/main.zip -InstallDefaults
```

SWAMID

REFEDS MFA – how we beat the system

- ADFSTkMFAAdapter
  - Microsoft's own code
  - Easy to add other contexclasses if needed
- AccessControlPolicy
  - Force MFA if refedsMFA is requested
- ClaimRules
  - Are the correct methods used?
  - Number of Methods >1

  - Relese RefedsMFA

SWAMID

Azure MFA as Refeds MFA provider

- Configure Azure MFA in ADFS (see link below)
- Install-ADFSTkMFAAdapter
  - On *all* ADFS servers!
- If you allow other methods than number-matching you need to configure MFA methods in LocalManualSPSettings.ps1

https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa

SWAMID

Custom MFA providers

- DUO
- Yubikey
- BankID
- Freja eID+
- eduID
- Azure Passwordless (Nope)

SWAMID

BankID as MFA provider

- Install the BankID MFA adapter
  - On *all* ADFS servers!

SWAMID

Freja eID+ as MFA provider

- Install the Freja eID+ MFA adapter
  - On *all* ADFS servers!

SWAMID

eduID as MFA provider

- Install the eduID MFA adapter
  - On *all* ADFS servers!
  - Requires a ProxyWeb that redirects to EduID
  - Requires that popups are allowed.

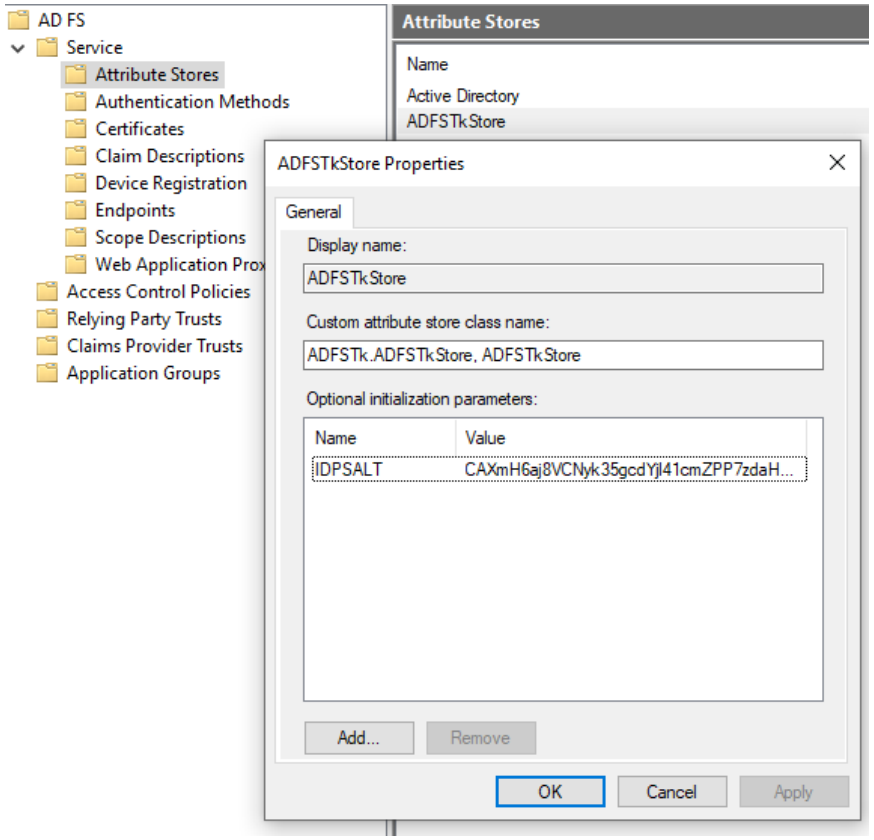
SWAMID

ADFS Toolkit Store

- Used for calculations/transformations that ADFS can't handle internally
- Calls C# .NET code for execution
- Used in the config.[*federation*].xml file

SWAMID

ADFS Toolkit Store - Installation



- Install-ADFSTkStore
  - Run on *all* ADFS servers!
- Generate Hash Salt or enter it manually on first Server

SWAMID

ADFS Toolkit Store - Configuration

```
<attribute type="urn:oasis:names:tc:SAML:attribute:pairwise-id" store="Active Directory" name="norEduPersonLIN" >
  <transformvalue adfstkstorefunction="pairwiseid" />
</attribute>

<attribute type="urn:oasis:names:tc:SAML:attribute:subject-id" store="Active Directory" name="samaccountname" >
  <transformvalue adfstkstorefunction="subjectid" />
</attribute>

<attribute type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" store="Active Directory" name="mail">
  <transformvalue adfstkstorefunction="tolower" />
</attribute>
```

- Add `<transformvalue adfstkstorefunction="storefunction" />` to the attribute where you want to use the ADFS Toolkit Store
- Store Functions:
  - pairwiseid
  - subjectid
  - toupper/tolower
  - hash
  - base32

SWAMID

Test Your Installation

- ADFSTkTools
  - $Rules = Get-ADFSTkToolsIssuanceTransformRules –entityId [myEntityID]
- Claims X-Ray
  - https://adfshelp.microsoft.com/ClaimsXray
- Import one SP
  - Import-ADFSTkMetadata -EntityId [myEntityID] -ConfigFile C:\ADFSToolkit\config\institution\config.[Federation].xml
- Import all Release Check SP's
- Attention:
  Don't forget the Cache!

SWAMID

Caching in ADFS Toolkit

- Global variables
- $global:ADFSTk*
  - $global:ADFSTkManualSPSettings
- Remove-ADFSTkCache

SWAMID

ADFSTk-Health

- Get-ADFSTkHealth
  - Runs at every sync
- Health Checks
  - CheckSignature*
  - CheckConfigVersion*
  - MFAAccesControlPolicy*
  - RemovedSPsStillInSPHash
  - MissingSPsInADFS
  - ScheduledTaskPresent
- Run Get-ADFSTkHealth -HealthCheckMode Full after upgrade!

SWAMID

* Default Health Check

ADFSTk-Tools

- Get-ADFSTkTool*
  - EntityId
  - IssuanceTransformRules
  - SpInfoFromMetadata
- Copy-ADFSTkToolRules

SWAMID

Dissection of the ADFS Toolkit module

- C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit
- Public – stores all public cmdlets
- Private – stores all internal cmdlets
- Demo

SWAMID

Thank you for participing!

SWAMID