



SWAMID



SWAMID

Swedish Academic Identity Federation



SWAMID

ADFS som IdP i SWAMID

Workshop om hur Microsoft Active Directory Federation Services (ADFS) fungerar på ett bra sätt som identitetsutgivare (IdP) i SWAMID

Tommy Larsson & Johan Peterson

tommy.larsson@umu.se resp. johan.peterson@liu.se



SWAMID

Agenda

- Välkomna och presentation av alla deltagare
- Mål med eftermiddagen
- Nyheter i ADFS 2019
- MFA
 - Refeds/Azure/Custom (additional authentication rules)
- Custom Claims Provider
- ADFS Toolkit

Välkomna och presentation av alla deltagare



Laget runt

- Vem är du?
- Var kommer du ifrån?
- Vad förväntar du dig av dagen?
- Hur mycket erfarenhet har du av SWAMID?
- Hur mycket erfarenhet har du av ADFS?



SWAMID

Mål med eftermiddagen

- Dela med oss SWAMIDs kunskap
- Dela med sig av alla deltagares kunskap
- Diskutera vad som är vägen framåt för ADFS i SWAMID



SWAMID

Nyheter ADFS 2019

- Externa providers som primär autentisering
- Lösenord som andra faktor
- Plugins för "Threat protection"
- ESL (Extranet Lockout Protection) förbättringar
- [Nyheter från Ignite](#)



SWAMID

Förbättringar

- Remote PSH med smarta kort
- Specificera andra faktor per RP (genom grupper)
- Hantera TLS device auth för applikationer
- MFA freshness, parameter i Azure
AD kan prompta återinloggning med bara andra faktorn
- Paginerad inloggning
- Bättre support för "Modern apps"
- Bättre säkerhet i Oauth flödet med en "code verifier"
- <https://adfs-help.microsoft.com/>



SWAMID

ADFS och MFA

- Refeds MFA
 - AuthContextClass Microsoft
- Azure MFA
 - Microsoft Authenticator
 - TOTP dosa
- Custom/third party MFA Provider





SWAMID

ADFS Anpassning

- Logo
- Bakgrundsbild
- Help + Privacy länk
- OnLoad.js
- Export-AdfsWebTheme
 - Name DefaultAdfs2019
 - DirectoryPath
- Set-AdfsWebConfig
 - ActiveThemeName custom



SWAMID



SWAMID

Swedish Academic Identity Federation

Fikatajnm!



SWAMID

ADFS Toolkit


- En PS modul för att konsumera SWAMIDs metadata
- Samarbete mellan SWAMID och CAF
- Förenklar attributrelease och hantering av RP:s i din ADFS miljö
- Finns på PowerShell Gallery

<https://www.powershellgallery.com/packages/ADFSToolkit>

The screenshot shows the PowerShell Gallery interface for the ADFS Toolkit package. The page title is "ADFSToolkit 1.0.0.0". The description is "Module to handle SAML2 federation aggregates." The minimum PowerShell version is 5.0. The installation options are "Install Module", "Azure Automation", and "Manual Download". The "Install Module" option is selected, and the command to install the package is shown in a text box: "PS> Install-Module -Name ADFSToolkit". The author(s) are listed as "Chris Phillips and Johan Peterson". The copyright information is "(c) 2017 Chris Phillips CANARIE, Johan Peterson SWAMID http://www.apache.org/licenses/LICENSE-2.0".

PowerShell Gallery Packages Publish Statistics Documentation

Search PowerShell packages...

 ADFSToolkit 1.0.0.0

Module to handle SAML2 federation aggregates.

Minimum PowerShell version
5.0

Installation Options

Install Module Azure Automation Manual Download

Copy and Paste the following command to install this package using PowerShellGet [More Info](#)

```
PS> Install-Module -Name ADFSToolkit
```

Author(s)
Chris Phillips and Johan Peterson

Copyright
(c) 2017 Chris Phillips CANARIE, Johan Peterson SWAMID <http://www.apache.org/licenses/LICENSE-2.0>

517 Downloads
383 Downloads of 1.0.0.0
[View full stats](#)
2018-04-18 Last Published

Info
[Project Site](#)
[License Info](#)
[Contact Owners](#)
[Report](#)



SWAMID

Att tänka på

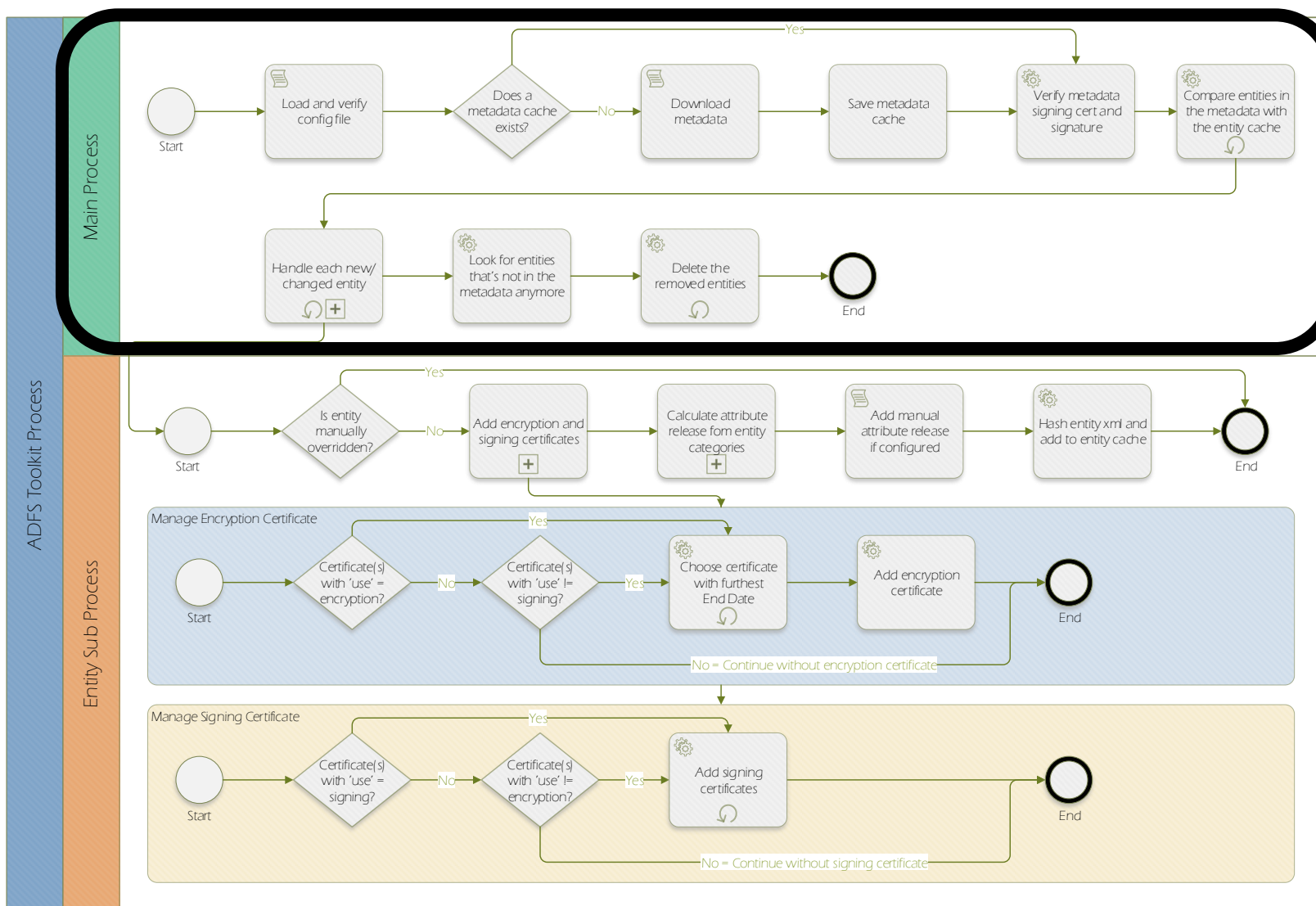
- 1% installation
- 10% konfiguration
- 88% förberedelse och planering av attributrelease
- 1% WTF?!



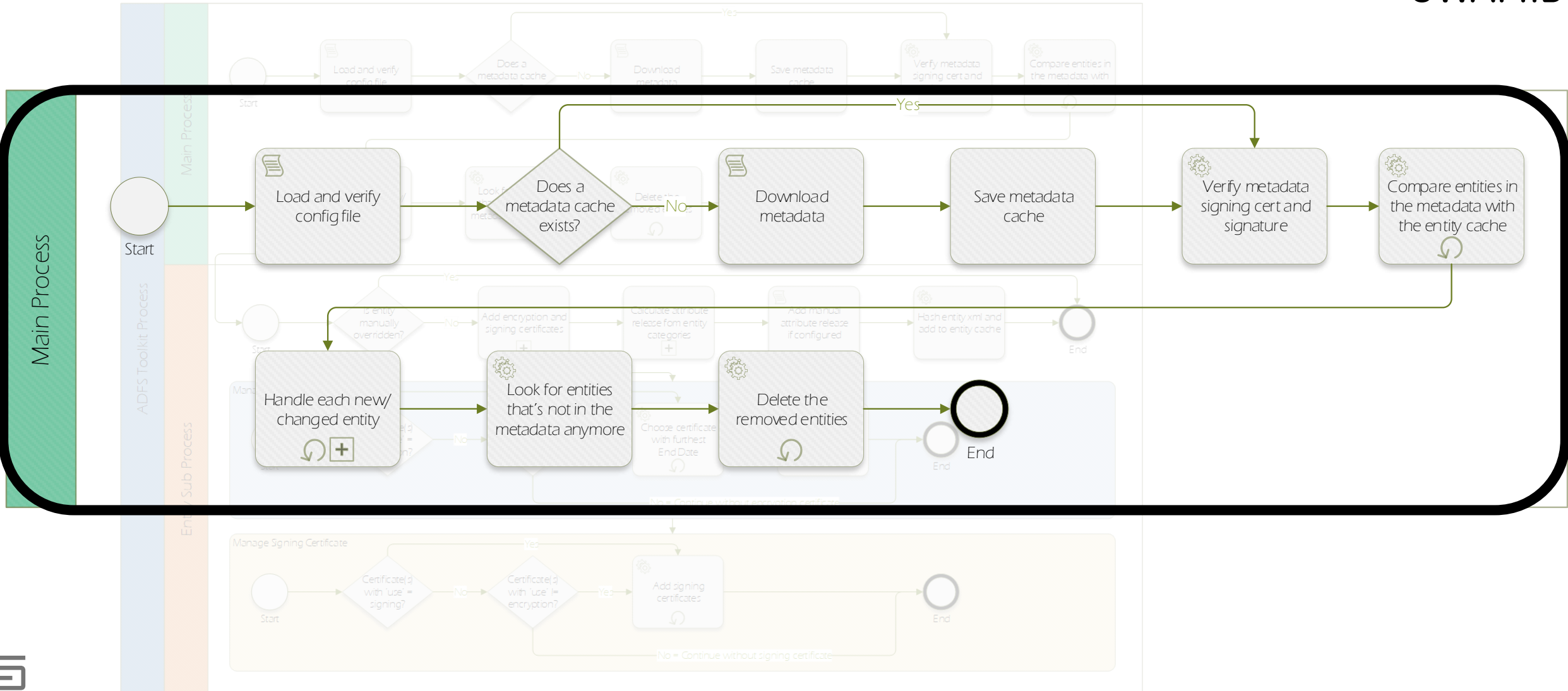


SWAMID

ADFS Toolkit – hur funkcar det?



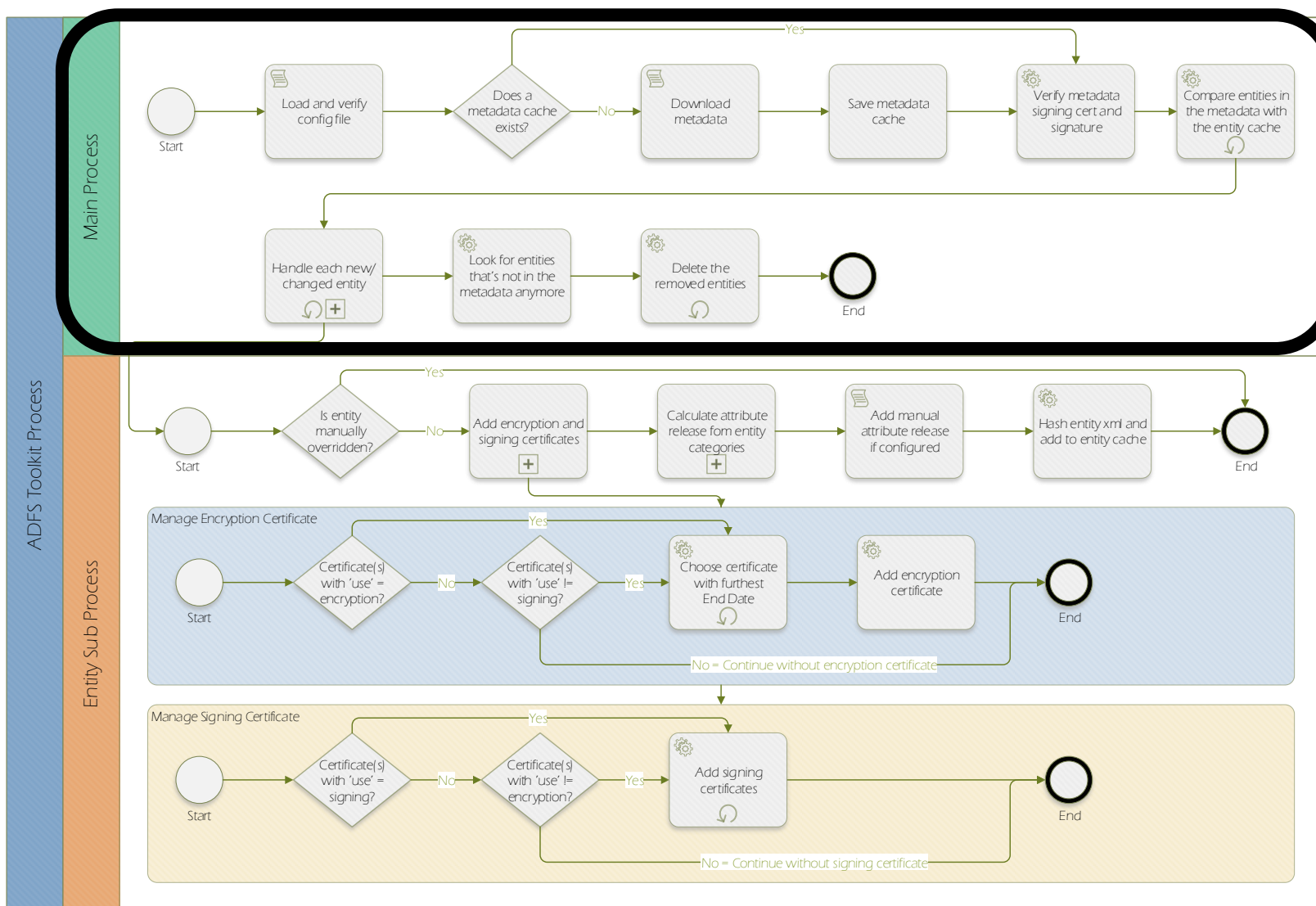
Huvudprocessen



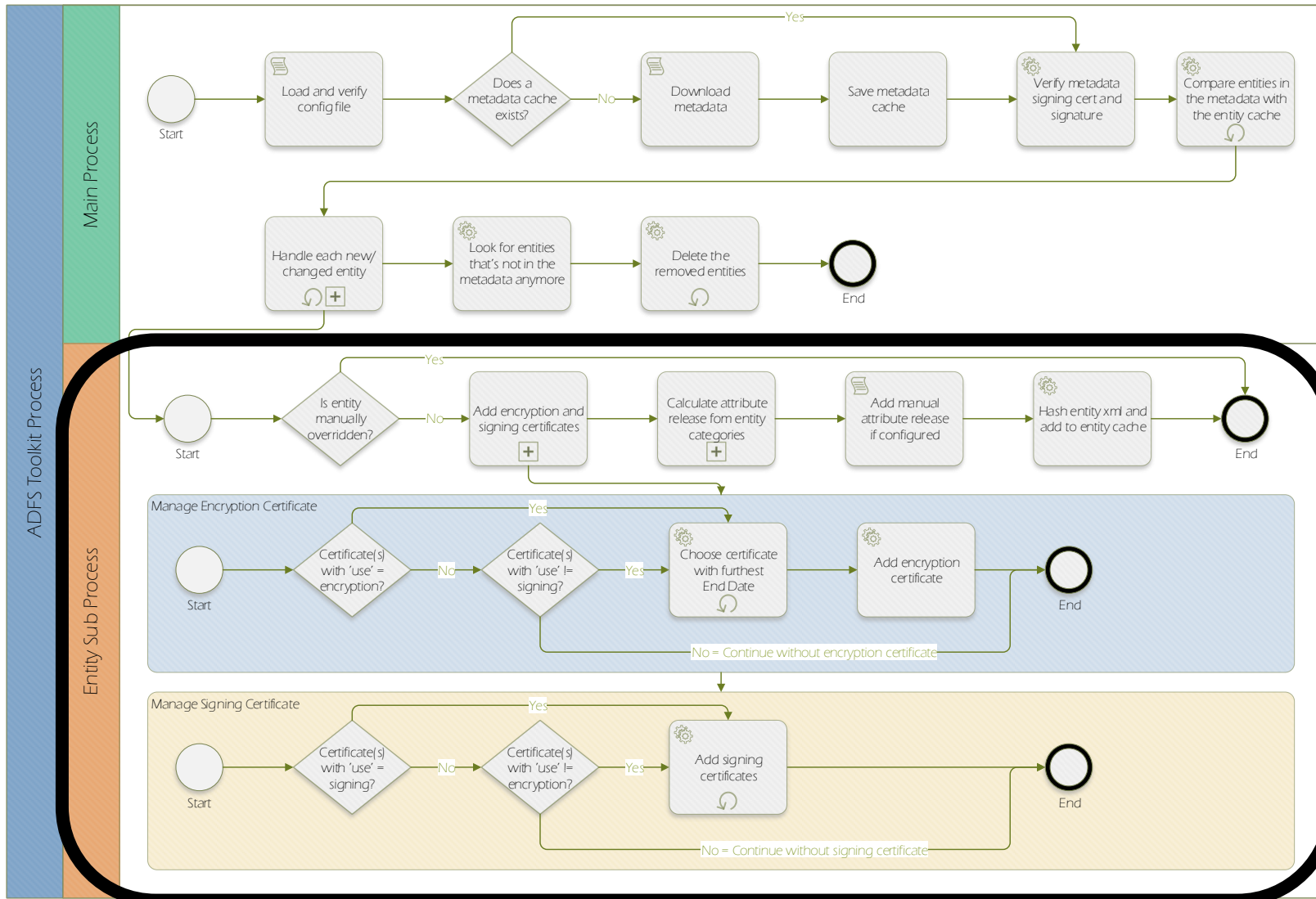


SWAMID

ADFS Toolkit – hur funkar det?



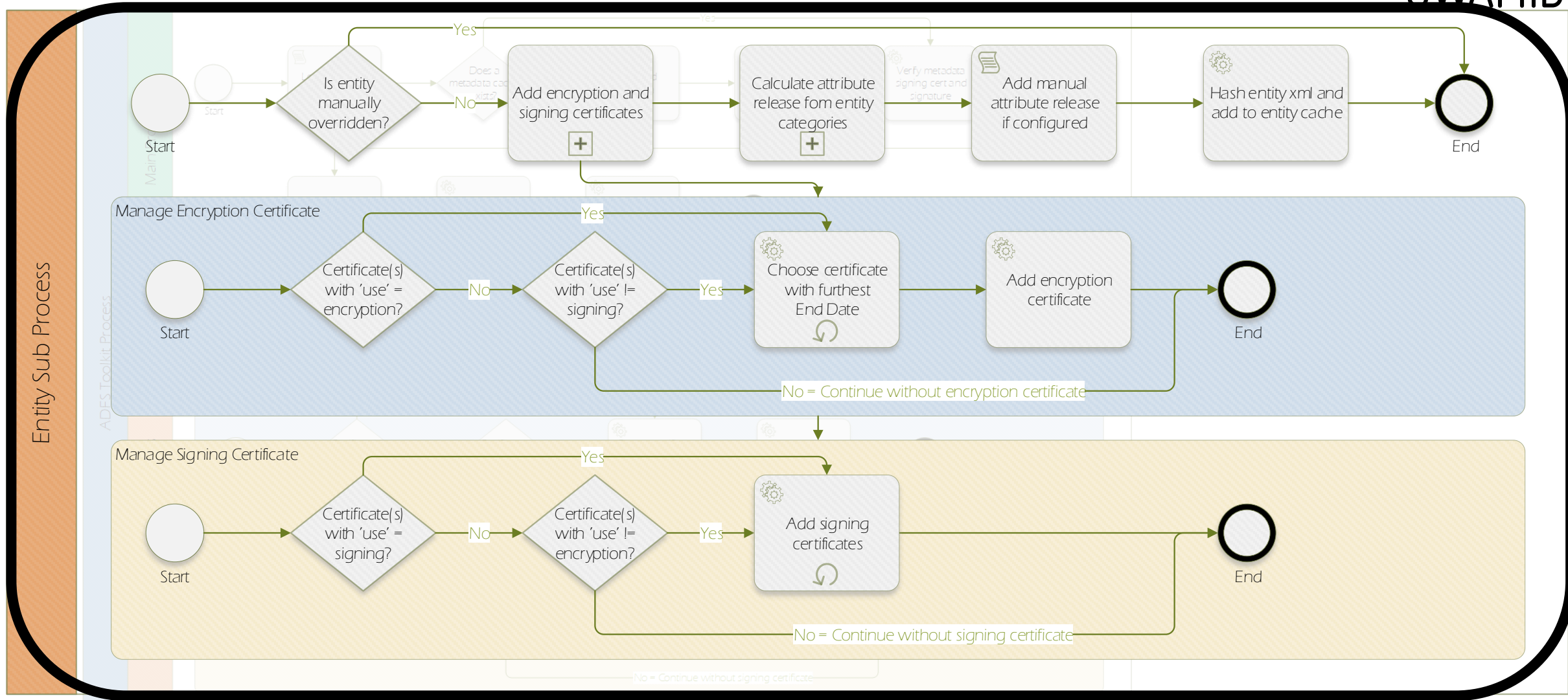
ADFS Toolkit – hur funkar det?



Per entitetsprocessen



SWAMID





SWAMID

Dags för DEMO!

- Men först...
- ...ett offer till demogudarna!






SWAMID


Titta på SWAMIDs wiki!

← → ↻ <https://wiki.sunet.se/display/SWAMID/How+to+consume+SWAMID+metadata+with+ADFS+Toolkit>



Services/Collaborations

[SWAMID](#) / [SWAMID Wiki](#) / [SAML WebSSO Identity Provider Best Current Practice](#)

 **SWAMID Wiki**

- ▶ [Getting Started with SWAMID](#)
- [Contact SWAMID](#)
- [SWAMID News](#)
- [SWAMID Advisories](#)
- ▶ [SWAMID Events](#)
- ▶ [SWAMID Identity Assurance](#)
- ▶ [SAML Entity information](#)
- ▶ [SAML WebSSO Service Provider Best Current Pra...](#)
- ▼ [SAML WebSSO Identity Provider Best Current Pra...](#)
 - [Add information on the white page that is displ...](#)
 - [Automatisk installation av Shibboleth IdP versi...](#)
 - [Entity Categories for Identity Providers](#)

How to consume SWAMID metadata with ADFS Toolkit Planning Your Installation

System Requirements

ADFS Toolkit must be installed on a Windows Server (your AD FS host) with:

- Microsoft AD FS v3 or higher
- Local administrator privileges to schedule privileged jobs
- AD FS administrator-level permissions to run PowerShell commands
- Acceptance of the security considerations running PowerShell retrieved from Microsoft's Pc

While not a firm requirement, we strongly suggest a test AD FS environment to perform the insta Console (MMC).

Minimum Server OS

Windows Server 2012 R2 or newer is the minimal level of OS supported. You should also be curren

Minimum PowerShell Version

ADFS Toolkit uses Microsoft's PowerShell with Windows Management Framework (WMF) 5.1. To s

To quickly see which version of PowerShell you have, open a PowerShell window or PowerShell IS

WMF 5.1 can be downloaded from here: <https://docs.microsoft.com/en-us/PowerShell/wmf/5.1/inst>

<https://wiki.sunet.se/display/SWAMID/How+to+consume+SWAMID+metadata+with+ADFS+Toolkit>



SWAMID

Installation och konfiguration

- Installera ADFS Toolkit från PS Gallery
 - Install-Module ADFSToolkit
- Konfigurera ADFS Toolkit
 - New-ADFSTkConfiguration
- Kontrollera det automatiskapade schemalagda jobbet

```
PS C:\Published Powershell Scripts> Install-Module ADFSToolkit
PS C:\Published Powershell Scripts> New-ADFSTkConfiguration
-----
You are about to create a new configuration file for ADFSToolkit.

You will be prompted with questions about metadata, signature fingerprint
and other question about your institution.

Hit enter to accept the defaults in round brackets

If you make a mistake or want to change a value after this cmdlet is run
you can manually open the config file or re-run this command.
-----
metadataURL: The URL to the federated metadata (https://metadata.federationOperator.org/path/to
Please provide a value for metadataURL: http://mds.swamid.se/md/swamid-2.0.xml
signCertFingerprint: The fingerprint of the certificate that signs the metadata (0123456789ABCD
Please provide a value for signCertFingerprint: A6785A37C9C90C25AD5F1F6922EF767BC97867673AAF4F8
MetadataPrefix: A prefix that are added to the Service Provider's name in AD FS Console (ADFSTk
Please provide a value for MetadataPrefix: Swamid
o: The name of your institution (ABC University).
Please provide a value for o: Linköping University
co: The name of your Country (Canada, Sweden).
Please provide a value for co: Sweden
c: Country Code (CA, SE).
Please provide a value for c: SE
schacHomeOrganization: The DNS name of your institution (institution.edu).
Please provide a value for schacHomeOrganization: liu.se
norEduOrgAcronym: The short name of your institution (CA).
Please provide a value for norEduOrgAcronym: Liu
ADFSEternalDNS: The DNS name of your ADFS (adfs.institution.edu).
Please provide a value for ADFSEternalDNS: fs.test.ad.liu.se
```



Genomgång av utökad konfiguration

➤ Fyra olika attributstores

- Static
- Active Directory
- SQL
- Custom Store

➤ Använd *useGroups* för att basera ett attribut på medlemskap i grupper

➤ *claimOrigin* styra om gruppen ska styra på namn eller SID

```
<?xml version="1.0"?>
<configuration>
  3 <ConfigVersion>1.0</ConfigVersion>
  4 <workingPath>c:\ADFSToolkit\1.0.0.0</workingPath>
  5 <ConfigDir>/config</ConfigDir>
  6 <CacheDir>/cache</CacheDir>
  7 <SPHashFile>Swamid-SPHashfile.xml</SPHashFile>
  8 <MetadataCacheFile>Swamid-metadata.cached.xml</MetadataCacheFile>
  9 <LocalRelyingPartyFile>get-ADFSTkLocalManualSPSettings.ps1</LocalRelyingPartyFile>
 10 <MetadataPrefix>Swamid</MetadataPrefix>
 11 <MetadataPrefixSeparator>:</MetadataPrefixSeparator>
 12 <Logging useEventLog="true">
 13 <LogName>ADFSToolkit</LogName>
 14 <Source>Import-ADFSTkMetadata</Source>
 15 </Logging>
 16 <metadataURL>http://mds.swamid.se/md/swamid-2.0.xml</metadataURL>
 17 <!--<metadataURL>https://mds.swamid.se/md/swamid-testing-1.0.xml</metadataURL-->
 18 <signCertFingerprint>A6785A37C9C90C25AD5F1F6922EF767BC97867673AAF4F8BEAA1A76DA3A8E585</signCertFinge
 19 <claimsProviders>
 20 <claimsProvider>Active Directory</claimsProvider>
 21 </claimsProviders>
 22 <defaultAccessControlPolicy>
 23 <defaultAccessControlPolicyName>Permit AL2</defaultAccessControlPolicyName>
 24 <defaultAccessControlPolicyParameters></defaultAccessControlPolicyParameters>
 25 </defaultAccessControlPolicy>
 26 <schacHomeOrganization>
 27 <schacHomeOrganizationType>urn:liu.se:schac:homeOrganization
 28 <schacHomeOrganizationType>urn:liu.se:schac:homeOrganization
 29 <!-- This value is for EU higher education institution, other allowed values are:
 30 urn:schac:homeOrganizationType:eu:educationInstitution
 31 urn:schac:homeOrganizationType:int:NREN
 32 urn:schac:homeOrganizationType:int:universityHospital
 33 urn:schac:homeOrganizationType:int:NRENAffiliate
 34 urn:schac:homeOrganizationType:int:other
 35 -->
 36 </schacHomeOrganization>
 37 <ADFSEExternalDNS>fs.liu.se</ADFSEExternalDNS>
 38
 39
 40
```




SWAMID

Genomgång av utökad konfiguration

➤ Använd *restrictedvalue* för att filtrera bort värden du inte vill skicka ut

➤ Använd *allowedRegistrationAuthorities* för att hindra attribut att skickas utanför SWAMIDs federation

```
1 <!-- ConfigVersion -->
2 <ConfigVersion>1.0</ConfigVersion>
3 <workingPath>c:\ADFSToolkit\1.0.0.0</workingPath>
4 <configDir>c:\ADFSToolkit\1.0.0.0</configDir>
5 <cacheDir>c:\ADFSToolkit\1.0.0.0\cache</cacheDir>
6 <SPHashFile>Swamid-SPHashfile.xml</SPHashFile>
7 <MetadataCacheFile>Swamid-metadata.cached.xml</MetadataCacheFile>
8 <LocalRelyingPartyFile>get-ADFSTkLocalManualSPSettings.ps1</LocalRelyingPartyFile>
9 <LocalRelyingPartyFile>get-ADFSTkLocalManualSPSettings.ps1</LocalRelyingPartyFile>
10 <LocalRelyingPartyFile>get-ADFSTkLocalManualSPSettings.ps1</LocalRelyingPartyFile>
11 <LocalRelyingPartyFile>get-ADFSTkLocalManualSPSettings.ps1</LocalRelyingPartyFile>
12 <Logging useEventLog="true">
13 <LogName>ADFSToolkit</LogName>
14 <LogPath>c:\ADFSToolkit\logs</LogPath>
15 </Logging>
16 <metadataURL>http://mds.swamid.se/md/swamid-2.0.xml</metadataURL>
17 <!--<metadataURL>https://mds.swamid.se/md/swamid-testing-1.0.xml</metadataURL-->
18 <signCertFingerprint>A6785A37C9C90C25AD5F1F6922EF767BC97867673AAF4F8BEAA1A76DA3A8E585</signCertFinge
19 <claimsProviders>
20 <claimsProvider>Active Directory</claimsProvider>
21 </claimsProviders>
22 <defaultAccessControlPolicy>
23 <defaultAccessControlPolicyName>Permit AL2</defaultAccessControlPolicyName>
24 <defaultAccessControlPolicyParameters></defaultAccessControlPolicyParameters>
25 </defaultAccessControlPolicy>
26 <staticvalues>
27 <o>Linköping University</o>
28 <co>Sweden</co>
29 <c>SE</c>
30 <schacHomeOrganization>liu.se</schacHomeOrganization>
31 <norEduOrgAcronym>LIU</norEduOrgAcronym>
32 <schacHomeOrganizationType>urn:schac:homeOrganizationType:eu:educationInstitution</schacHomeOrgani
33 <!-- This value is for EU higher education institution, other allowed values are:
34 urn:schac:homeOrganizationType:eu:educationInstitution
35 urn:schac:homeOrganizationType:int:NREN
36 urn:schac:homeOrganizationType:int:universityHospital
37 urn:schac:homeOrganizationType:int:NRENAffiliate
38 urn:schac:homeOrganizationType:int:other
39 -->
40 <ADFSEternalDNS>fs.liu.se</ADFSEternalDNS>
```



SWAMID

Hjälp-cmdlets

- `Get-ManualADFSIssuanceTransformRulesFromADFSTk`
- `Import-ADFSTkMetadata -ConfigFile [config] -EntityId [id]`