SWAMID

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

SUNET

Agenda

SWAMID

- 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

SUNET

Välkomna och presentation av alla deltagare

SWAMID

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?

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

SUNET

Nyheter ADFS 2019

SWAMID

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

SUNET

Förbättringar

SWAMID

- 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://adfshelp.microsoft.com/

ADFS och MFA

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

SWAMID

SUNET

ADFS Anpassning

SWAMID

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

SWAMID

Swedish Academic Identity Federation

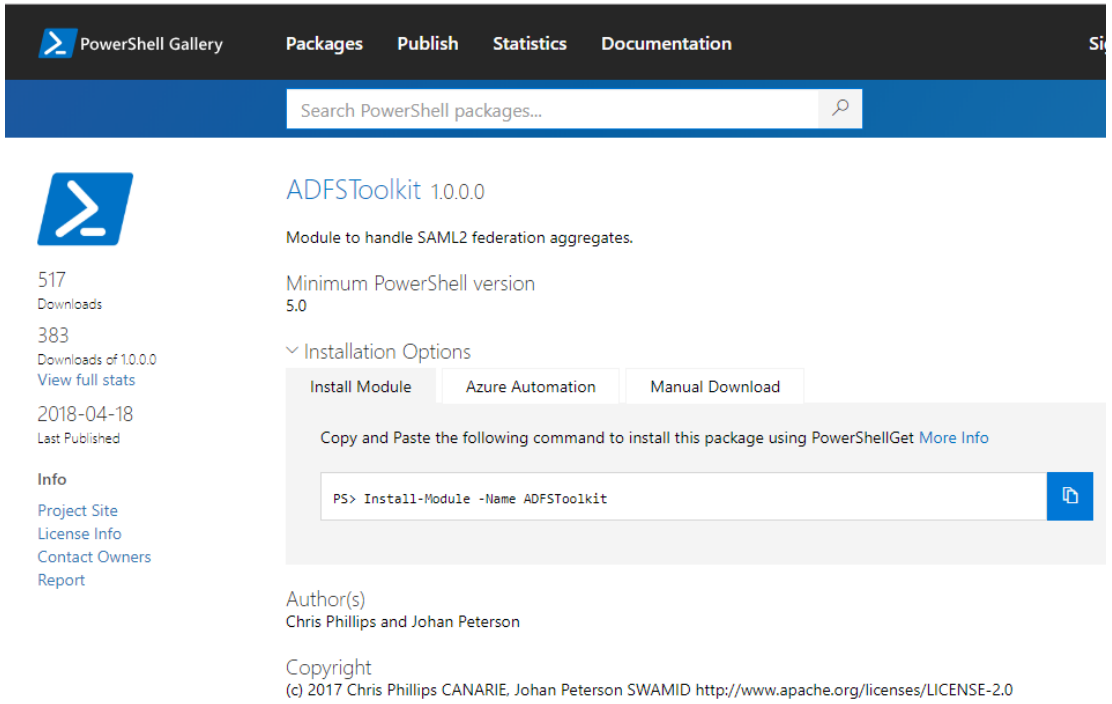
Fikatajm!

SUNET

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



SUNET

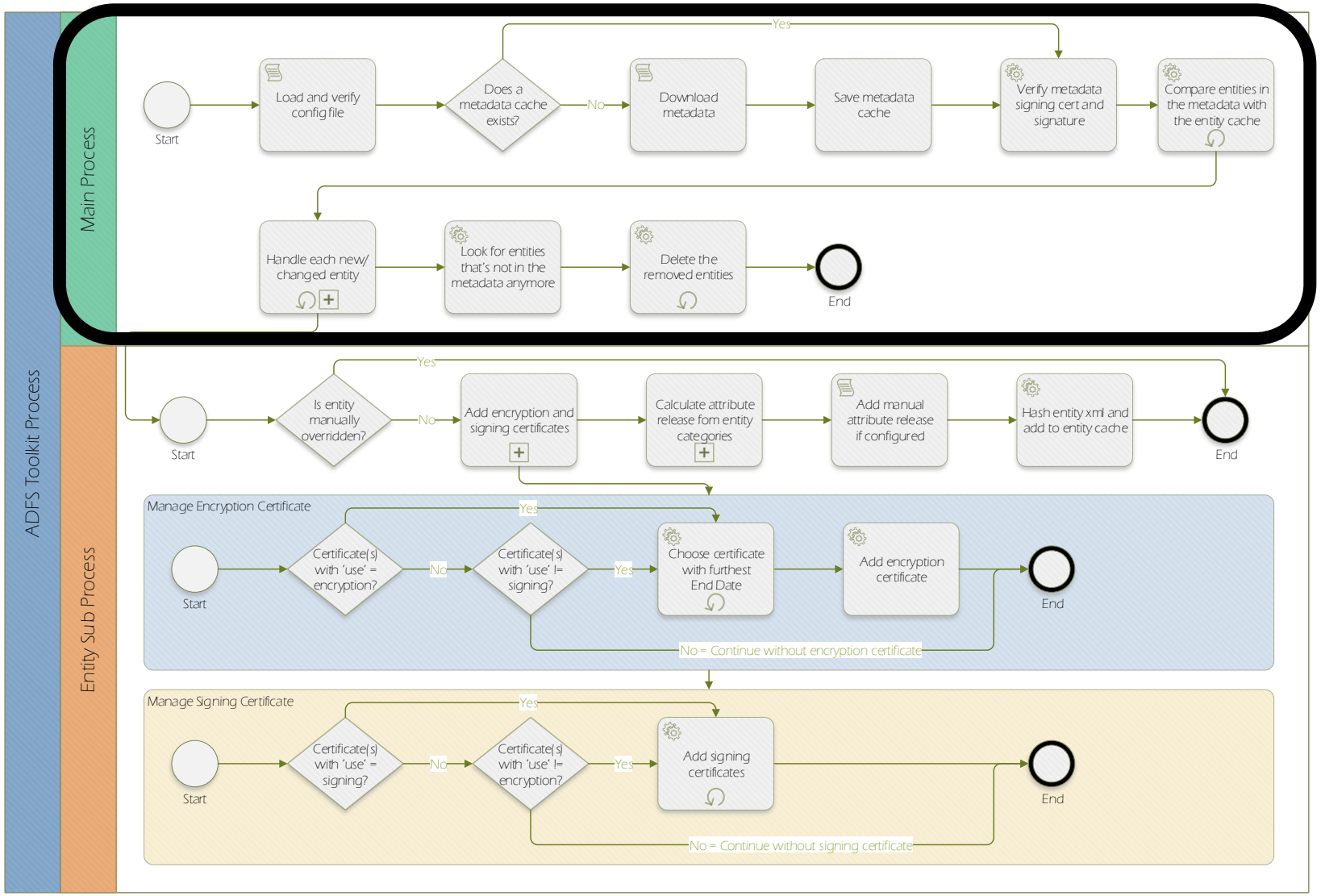
Att tänka på

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

SWAMID

SUNET

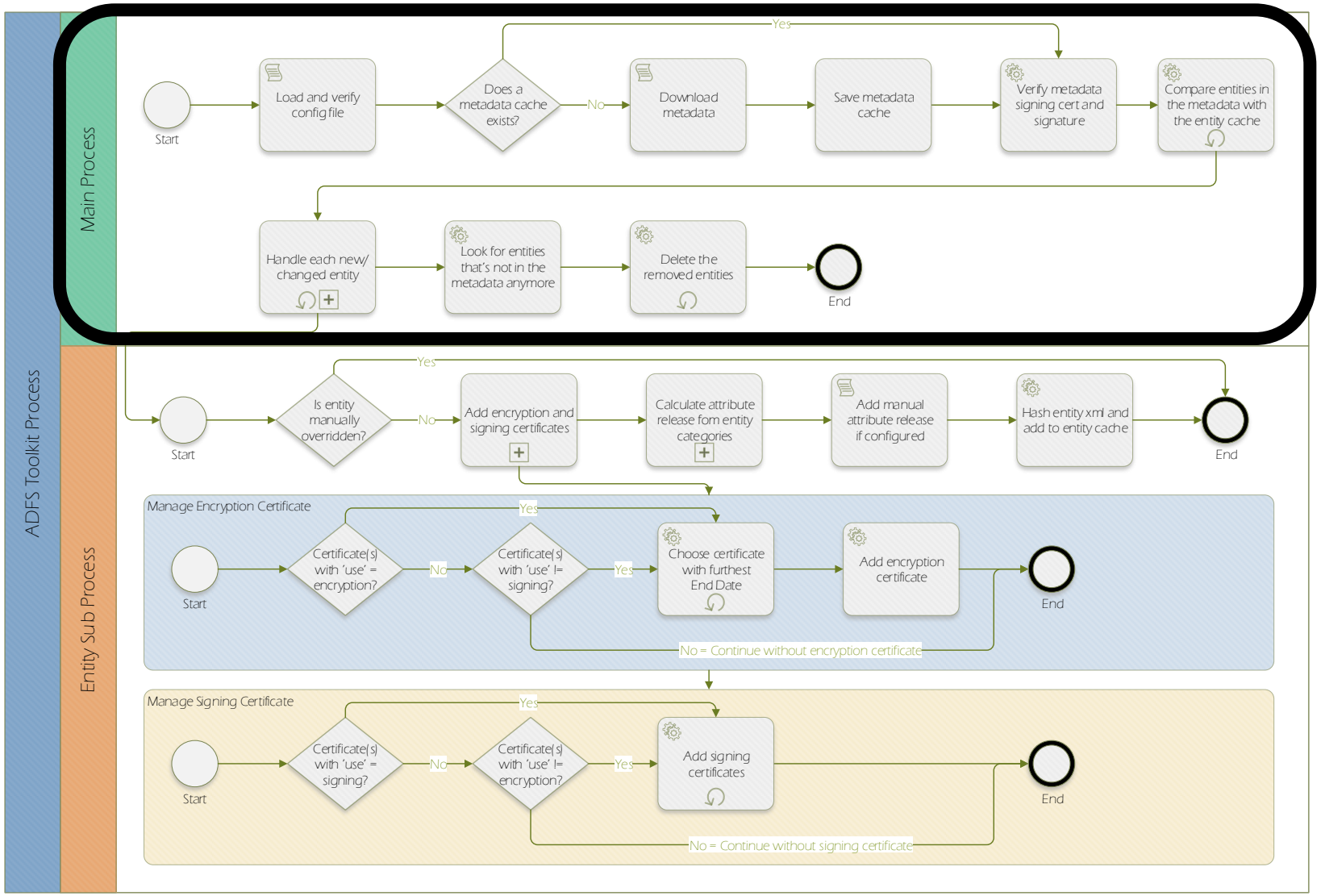
ADFS Toolkit – hur funkar det?



SUNET

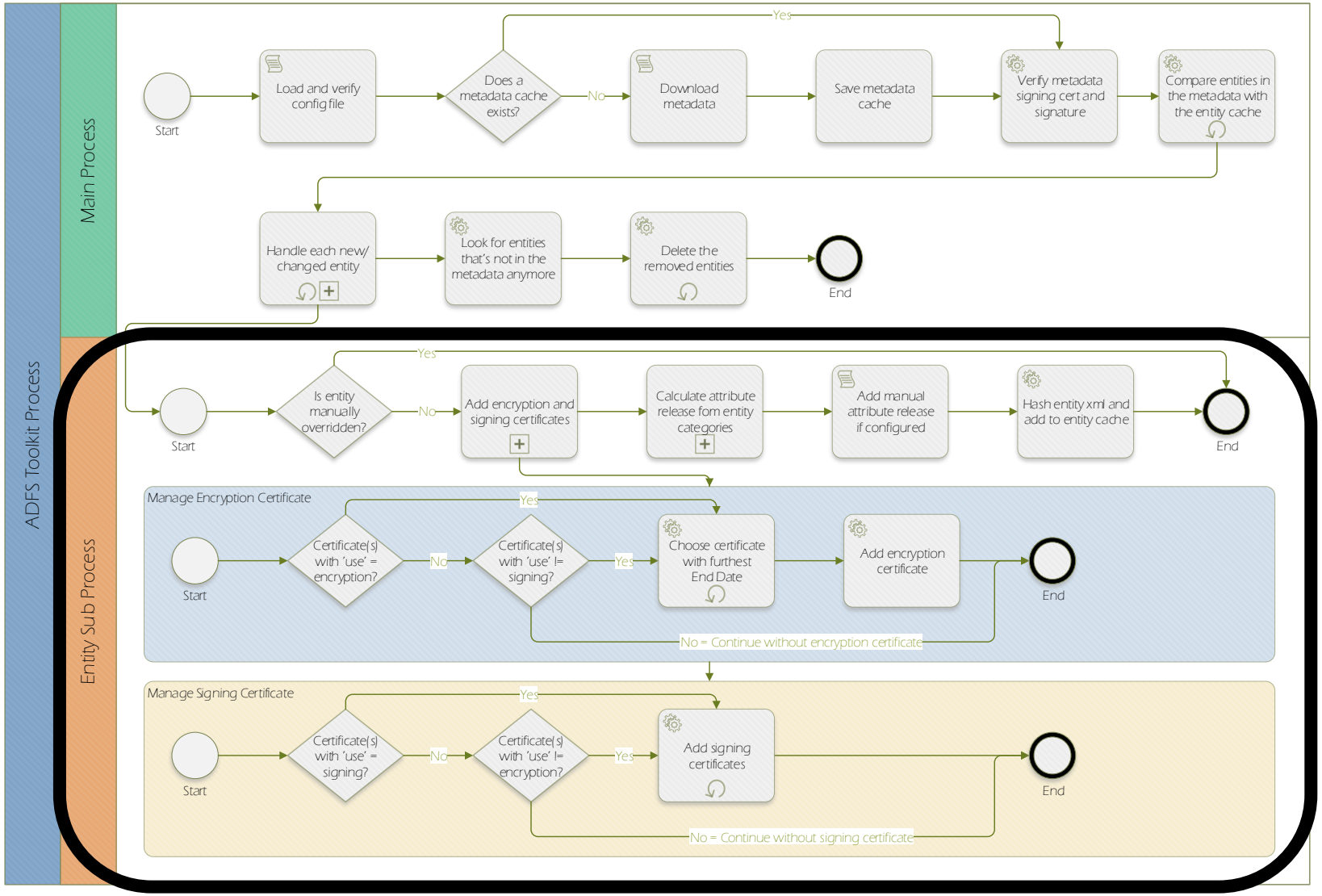
Huvudprocessen

ADFS Toolkit – hur funkar det?

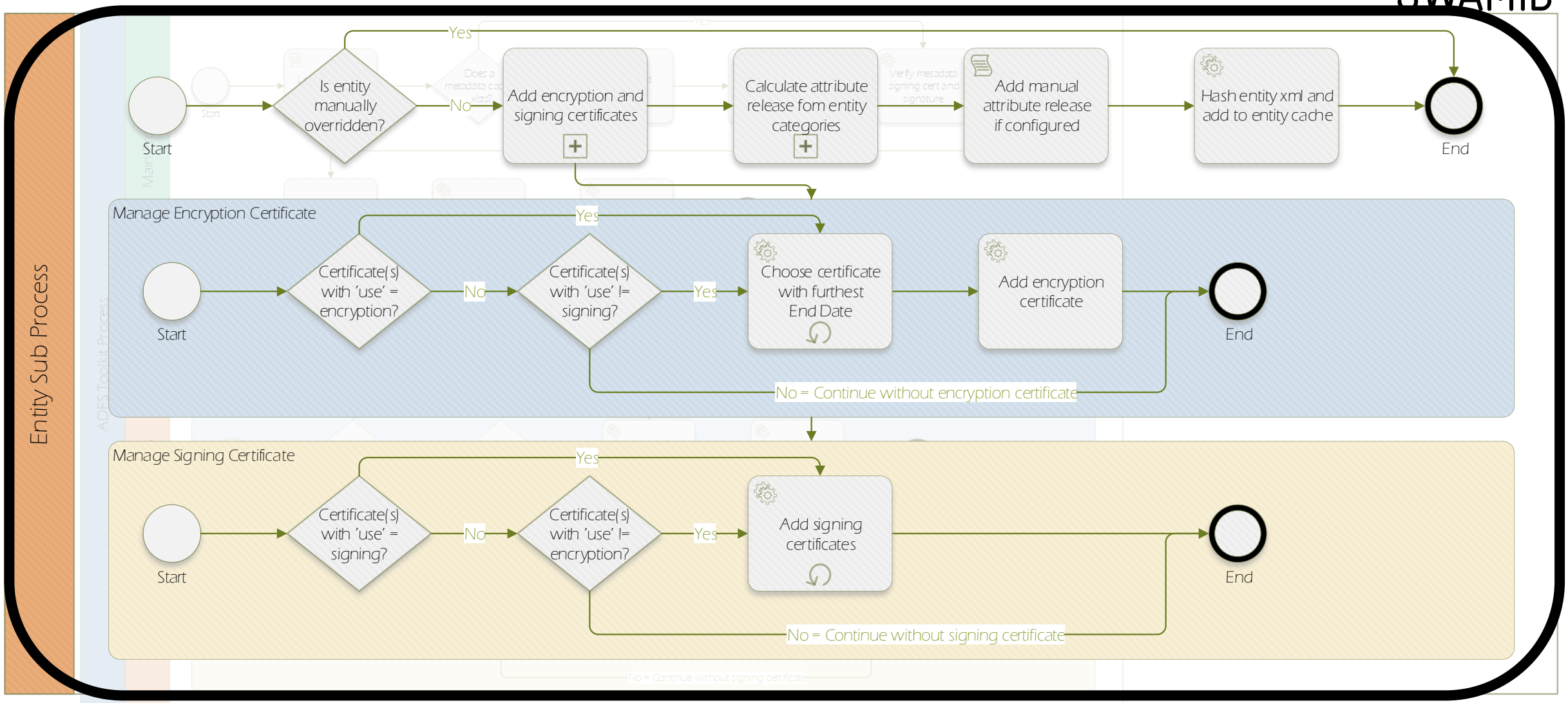


SUNET

ADFS Toolkit – hur funkar det?



Per entitetsprocessen



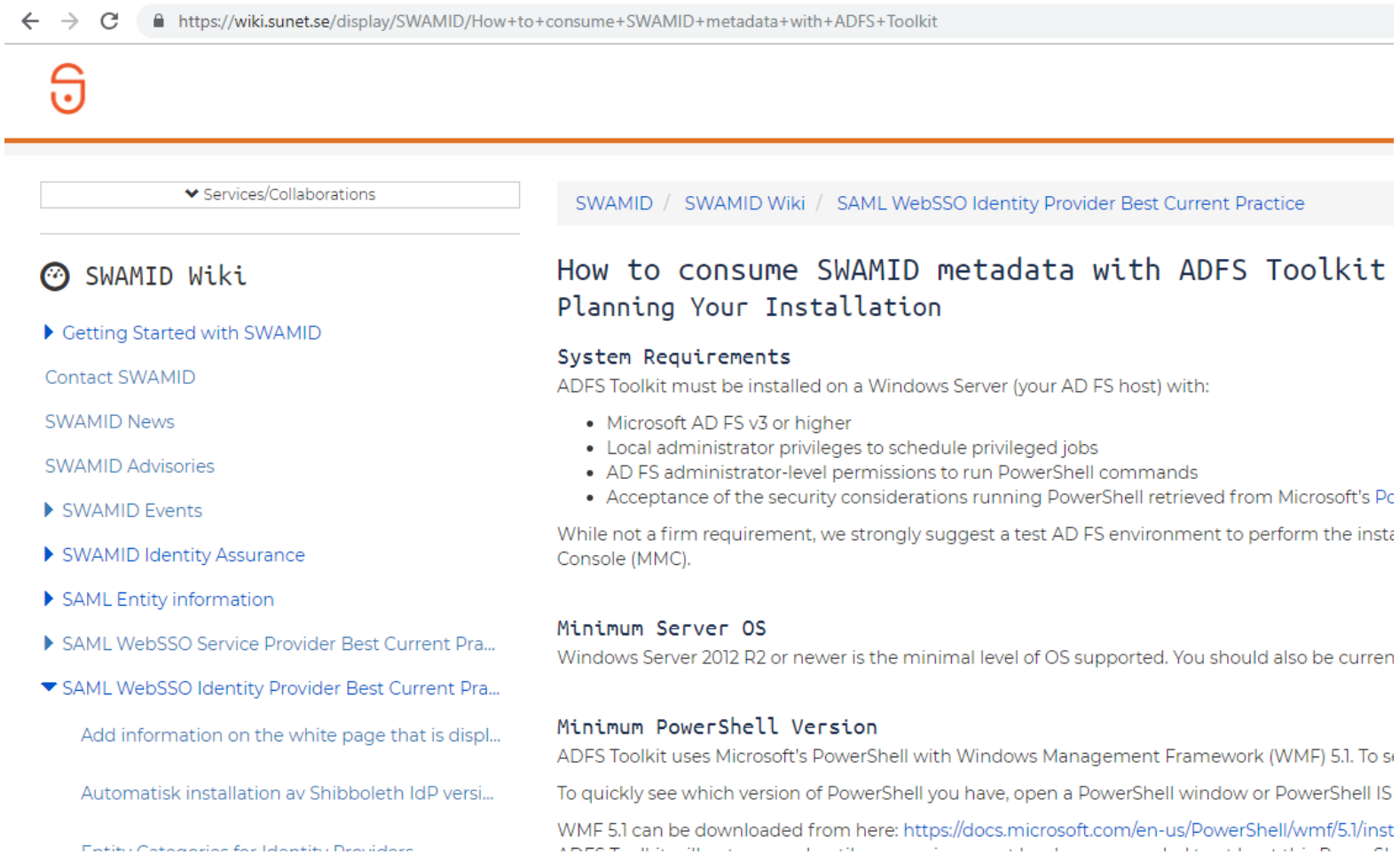
Dags för DEMO!

- Men först…
- …ett offer till demogudarna!

SWAMID

SUNET

Titta på SWAMIDs wiki!



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

Installation och konfiguration

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

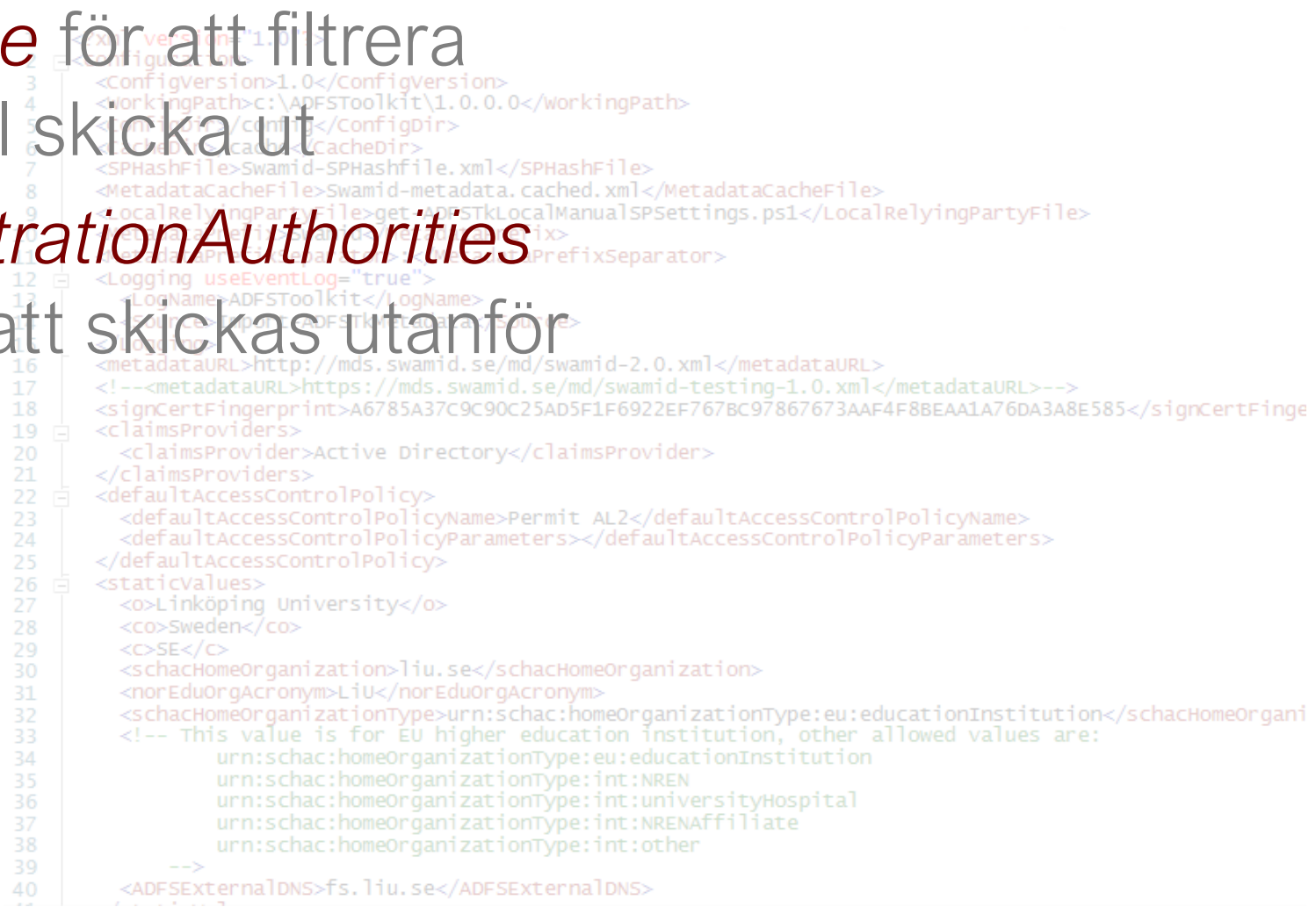
```
PS C:\Published Powershell Scripts> Install-Module ADFSToolkit

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
ADFSExternalDNS: The DNS name of your ADFS (adfs.institution.edu).
Please provide a value for ADFSExternalDNS: 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

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



Hjälp-cmdlets

SWAMID

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