
SWAMID
Swedish Academic Identity Federation

SWAMID

Multifaktorinloggning via SWAMID

SWAMID Operations

Pål Axelsson, Björn Mattsson, Paul Scott och Eskil Swahn

SUNET

SWAMID

Varför multifaktorinloggning via SWAMID?

- Lösenordsinloggning är alltmer utsatt för flera olika hot, t.ex. lösenordsfiske och lösenordstestning
- Datainspektionen har ställt krav på att endast avsedda mottagare ska kunna ta del av känsliga personuppgifter i det för lärosätena gemensamma systemet Nais
  - Datainspektionen exemplifierar uppfyllande med e-legitimation
- Forskningsprojekt och –infrastrukturer börjar ställa krav på bättre inloggningsmetoder än endast lösenordsinloggning

SWAMID

Egenregistrerad multifaktor

- Stärker inloggningen så att du vet att ingen annan använder ditt användarkonto
- Löses idag oftast genom att lösenordet kompletteras med en särskild autentiseringsapp i mobilen, s.k. Authenticator
- Finns idag i de större privata tjänsterna
  - Tvåstegsverifiering hos Google, tvåstegsverifiering i Office 365 och tvåfaktorsautentisering i Facebook
- eduID har stöd för detta genom standarden U2F
  - Fungerar f.n. bara för Chrome och ev. Firefox

https://www.sunet.se/swamid/policy/al2mfa/

SWAMID

Personverifierad multifaktor

- Stärker inloggningen så att den tjänst du loggar in i vet att det är du som loggar in
- Tillitsprofil för personverifierad multifaktorinloggning
  - Både organisationen och användaren måste vara godkända för SWAMID AL2
  - Multifaktorn måste uppfylla vissa tekniska och säkerhetsmässiga krav
  - Två nivåer på personverifiering
    - Multifaktorn har delats ut till användaren enligt samma metoder som SWAMID AL2
    - Multifaktorn delas ut med metoder som motsvarar identitetskontroll med identitetskort och pass
  - Hur multifaktorinloggning hanteras beskrivs i organisationens Identity Management Practice Statement (IMPS), dvs. utökning av den som skrivits för SWAMID AL2
  - Att personverifierad multifaktor har använts signaleras via den federativa standarden REFEDS MFA

Hur tar organisationen ansvar för utdelning av multifaktor?

SWAMID

- Krav ställs på hur användaren får tillgång till multifaktorinloggning
  - Multifaktorn måste knytas till användaren som person med samma rutiner som definieras i SWAMID AL2 eller bättre beroende på behov.
- Krav ställs på att användaren kan byta ut en multifaktor
- Krav ställs på att användarens multifaktor ska kunna stängas av vid förlust eller missbruk

Exempel på utdelningsprocesser (1)

Online autentisering med hjälp av annan IdP (5.2.2 punkt 1,2,3)

Exempel på utdelningsprocesser (2)

Fysisk utdelning av engångskod (5.2.2 punkt 4,5)

Exempel på utdelningsprocesser (3)

Fysisk utdelning av andra faktor (5.2.2 punkt 4,5)

Exempel på utdelningsprocesser (4)

Engångskod skickad till användare (5.2.2 punkt 6)

Exempel på utdelningsprocesser (5)

Andra faktor skickad till användare (5.2.2 punkt 7)

Tekniska grundkrav på personverifierade multifaktorer i SWAMID

SWAMID

- Multifaktorn måste uppfylla minst samma nivå av inloggningssäkerhet som kraven i aktuell tillitsprofil men samtidigt tillföra ökat skydd
- Multifaktorn måste bindas till en fysisk enhet
- Multifaktorn får inte vara kopierings- eller kloningsbar
- Multifaktorn måste skyddas mot gissningsattacker
- Klientbaserade krypteringsnycklar måste lagras säkert i den enhet som hanterar multifaktorn
- Serverbaserade krypteringsnycklar, om de används, måste lagras säkert i verifieringsservern

SWAMID

Val av multifaktorteknik

SUNET

SWAMID

Vad innebär multifaktorinloggning?

För att logga in använder man inte bara lösenord utan en kombination av minst två av faktortyperna

- Något man vet
  - Exempel: Lösenord eller pinkod
- Något man har
  - Exempel: Google Authenticator, Yubikey och Smartcard
- Något man är *(endast i kombination med något man har)*
  - Exempel: Fingeravtryck och ansiktsigenkänning
- ~~Något man gör *(väldigt svår att använda på ett säkert sätt samt endast i kombination med något man har)*~~
  - ~~Exempel: Hur man skriver på tangentbordet och tittar på skärmen~~

SUNET

SWAMID

Multifaktor men på olika sätt…

- Fullständig multifaktor
  - Multifaktorn består av något man har där användaren måste låsa upp användningen med en pinkod eller via fingeravtryck för att använda multifaktorn
- Kombinerad multifaktor (lösenord + andra faktor)
  - Användaren loggar in med användaridentitet och lösenord och kompletterar sedan med en fristående andra faktor av typen något man har

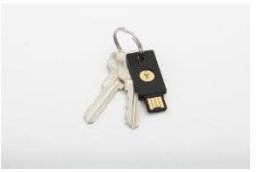
SWAMID

Exempel på fullständiga multifaktorer

- Smartcard *(eller Personal Identity Verification (PIV) card)*
  - Det klassiska PKI-baserade inloggningskortet med kortläsare
  - Kräver kortläsare med koppling till datorn och särskild kontroll av att det är ett kort och inte på datorn lagrade certifikat som används
- Multifaktor OTP
  - Inloggningsservern skickar en kontrollkod till användaren som denne matar in på OTP-dosan tillsammans med sin personliga pinkod för att få en svarskod som användaren sedan skriver in på inloggningssidan
  - Finns inbyggd säkerhetsrisk genom att OTP-dosan inte är fysiskt bunden till användarens webbläsare

SWAMID

Exempel på den andra faktorn

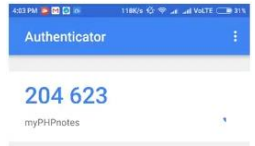


- Universal 2nd Factor (FIDO U2F)
  - En liten hårdvarubaserad nyckel med hög säkerhetsnivå som aktiveras med enkel tryckning på nyckeln
  - Webbläsarstödet är f.n. begränsat till Chrome, Opera och Firefox (manuell aktivering)
- FIDO2 – W3C Web Authentication (WebAuthn) + Client-to-Authenticator Protocol (CTAP)
  - Ny standard som beslutades i våras som främst kommer att användas för lösenordsfri inloggning men kompletteras även ibland med lösenord för att uppnå MFA
  - Finns stöd i Chrome och Firefox och senare i höst i Edge

SUNET

SWAMID

Exempel på den andra faktorn



- Tidsbaserad andra faktor - OTP (TOTP)
  - Användaren installerar och konfigurerar en Authenticatorapp som visar en engångskod som ändras ofta (normalt var trettionde sekund)
  - Enkel för användarna att använda och förstå men Authenticator och inloggningsservern delar på en gemensam hemlighet
  - Finns inbyggd säkerhetsrisk genom att OTP-appen inte är fysiskt bunden till användarens webbläsare

Beroende på säkerhetsrisker kommer OTP fasas ut som godkänd metod för personverifierad multifaktorinloggning i SWAMID inom några år

SUNET

SWAMID

Dåliga exempel på andra faktorn

- Engångslösenord/pinkod via SMS
  - SMS kan idag dyka upp på fler enheter än den avsedda, t.ex. på mobiltelefonen och datorn samtidigt
  - SIM-kortet kan flyttas över till annan mobiltelefon
- Automatiserad uppringning
  - Telefonsamtal kan kopplas över till en eller flera telefoner
- Pushnotifiering till mobilapp
  - Inloggningen kopplas inte tydligt och synligt ihop med den inloggning som görs

Får absolut inte användas för personverifierad multifaktor i SWAMID

SWAMID

Hur kräver och kontrollerar en webbtjänst personverifierad multifaktorinloggning i SWAMID?

SUNET

Hur begär en tjänst personverifierad multifaktorinloggning?

SWAMID

Tjänsten begär i sin inloggningsförfrågan

- att personverifierad multifaktorinloggning ska används
  - I Shibboleth SP sätter man authnContextClassRef=”https://refeds.org/profile/mfa” i SAML2 SessionInitiator
- att ny inloggning ska genomföras, dvs. inte lita på SSO
  - I Shibboleth SP sätter man forceAuthn=”true” i SAML2 SessionInitiator

Alternativt direkt via URL i en webbserver som använder Shibboleth SP:
https://sp.example.org/Shibboleth.sso/Login?forceAuthn=true&authnContextClassRef=
https%3A%2F%2Frefeds.org%2Fprofile%2Fmfa&target=https%3A%2F%2Fsp.example.org%2FservicePage

Hur kontrollerar en tjänst att personverifierad multifaktorinloggning har genomförts? 1(2)

Tjänsten ska efter inloggningen kontrollera att identitetsutfärdaren

1. uppfyller kraven för SWAMID AL2
   - Metadata Assurance Certification* innehåller http://www.swamid.se/policy/assurance/al2
2. a. uppfyller kraven för personverifierad MFA med särskild identitetskontroll alternativt
   - Metadata Assurance Certification* innehåller värdet http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi
2. b. uppfyller kraven för personverifierad MFA i SWAMID
   - Metadata Assurance Certification* innehåller värdet http://www.swamid.se/policy/authentication/swamid-al2-mfa

* I Shibboleth SP konfigureras att metadata attribut hämtas görs tillgängligt för webbservern

Hur kontrollerar en tjänst att personverifierad multifaktorinloggning har genomförts? 2(2)

SWAMID

Tjänsten ska efter inloggningen kontrollera att användaren

1. har loggat in med personverifierad multifaktor (REFEDS MFA)
   - I Shibboleth och Apache att Shib-AuthnContext-Class är https://refeds.org/profile/mfa
2. har loggat in precis nu (+/-(60 sekunder plus definierad max klockdrift))
   - I Shibboleth och Apache jämför Shib_Authentication_Instant med aktuell tidsstämpel
3. uppfyller kraven för SWAMID AL2
   - Attributet eduPersonAssurance innehåller värdet ”http://www.swamid.se/policy/assurance/al2”
4. uppfyller för kraven för personverifierad MFA med särskild identitetskontroll om detta krav finns
   - Attributet eduPersonAssurance innehåller värdet ”http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi”

SWAMID

Vilka identitetsutgivare går att använda för personverifierad multifaktorinloggning?

SUNET

Shibboleth Identity Provider

SWAMID

- Shibboleth 3 har ett särskilt autentiseringsflöde för multifaktorinloggning där man kombinerar olika inloggningsmetoder för att uppnå en multifaktorinloggning
- Det finns flera olika tekniska varianter implementerade och dokumenterade på Shibboleths Wiki
- SWAMID Operations har tittat på tre olika lösningar
  - Lösenord + FIDO U2F
  - Lösenord + TOTP
  - Mutifaktorinloggning via extern IdP

ADFS

SWAMID

- **ADFS går förnärvarande inte att använda för personverifierad multifaktorinloggning i SWAMID!**
  - Verifierat under förra vecka med Microsofts ADFS team på Microsoft Ignite
  - Microsofts ADFS team skapar change request för att detta ska fungera i framtiden
- ADFS kan inte hantera andra Authentication Context Class än de som redan är definierade i ADFS
  - Microsoft har en egen Authentication Context Class för att aktivera multifaktorinloggning men vi kan inte använda den eftersom forskartjänster kommer att använda REFEDS MFA
  - Multifaktorvarianterna i Microsofts Azure AD är byggda för egenregistrerade multifaktorer

eduID

SWAMID

- eduID har idag stöd för egenregistrerad multifaktorinloggning via FIDO U2F
- Under hösten kommer detta stöd utvidgas till att U2F-nykeln kopplas till användaren med FREJA eID på sådant sätt så att kraven för personverifierad multifaktorinloggning uppfylls

- Kan användas av de lärosäten som själva inte hinner eller kan implementera personverifierad multifaktor
- eduID kommer framöver att implementera FIDO2

SWAMID

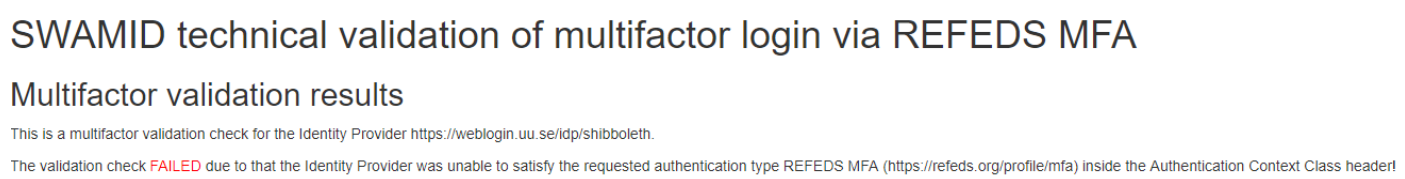
SWAMIDs testverktyg för personverifierad multifaktorinloggning

https://mfa-check.swamid.se

SUNET

SWAMIDs testverktyg mfa-check.swamid.se

Exempel på en IdP som inte kan hantera begäran om multifaktorinloggning enligt REFEDS MFA



SWAMIDs testvektyg mfa-check.swamid.se

Exempel på en IdP som kan hantera begäran om multifaktorinloggning via REFEDS MFA men som ännu inte är godkänd för SWAMID personverifierad multifaktorinloggning

Detta är också resultatet om en IdP inom eduGAIN som har stöd för REFEDS MFA testar mot tjänsten

SWAMID technical validation of multifactor login via REFEDS MFA

Multifactor validation results

This is a multifactor validation check for the Identity Provider (https://weblogin-test.kau.se/idp/shibboleth).

There are four different possible outcomes of the technical validation check:

- **PASSED:** The Identity Provider has passed the technical validation check,
- **MAY PASS:** The Identity Provider has passed all test except there is no information in the Identity Provider metadata that fulfils the SWAMID criteria for REFEDS MFA (please contact SWAMID Operations) or the user doesn't fulfil the requirments for SWAMID AL2-MFA-HI,
- **FAILED:** The Identity Provider has failed one or more test, please see below for the reason, and
- **FAILED (INCOMPLETE TEST):** The Identity Provider has failed one or more test due to missing information, please see below for the reason.

Technical validation summary:	**MAY PASS!**
	PASS 4, WARN 3, FAIL 0
Check for the SWAMID compliance criteria of the SWAMID AL2-MFA (http://www.swamid.se/policy/authentication/swamid-al2-mfa) inside the Assurance certification metadata attribute:	WARN
Check for the SWAMID compliance criteria of the SWAMID AL2-MFA-HI (http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi) inside the Assurance certification metadata attribute:	WARN
Check for the SWAMID compliance criteria of the assurance profile SWAMID AL2 (http://www.swamid.se/policy/assurance/al2) inside the Assurance certification metadata attribute:	PASS
Check for the user assurance value of SWAMID AL2-MFA-HI (http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi) inside the eduPersonAssurance attribute:	WARN
Check for the user assurance value of SWAMID AL2 (http://www.swamid.se/policy/assurance/al2) inside the eduPersonAssurance attribute:	PASS
Check for used authentication type REFEDS MFA (https://refeds.org/profile/mfa) inside the Authentication Context Class header:	PASS
Checks for freshness of authentication, i.e. authentication must complete within 60 seconds. Time since authentication was 1 seconds:	PASS

SWAMIDs testverktyg mfa-check.swamid.se

Exempel på en IdP och en användare i denna som uppfyller alla krav för personverifierad multifaktorinloggning

SWAMID technical validation of multifactor login via REFEDS MFA

Multifactor validation results

This is a multifactor validation check for the Identity Provider (https://idp.dev.eduid.se/idp.xml).

There are four different possible outcomes of the technical validation check:

- **PASSED:** The Identity Provider has passed the technical validation check,
- **MAY PASS:** The Identity Provider has passed all test except there is no information in the Identity Provider metadata that fulfils the SWAMID criteria for REFEDS MFA (please contact SWAMID Operations) or the user doesn't fulfil the requirments for SWAMID AL2-MFA-HI,
- **FAILED:** The Identity Provider has failed one or more test, please see below for the reason, and
- **FAILED (INCOMPLETE TEST):** The Identity Provider has failed one or more test due to missing information, please see below for the reason.

Technical validation summary:	**PASSED!**
	PASS 7, WARN 0, FAIL 0
Check for the SWAMID compliance criteria of the SWAMID AL2-MFA (http://www.swamid.se/policy/authentication/swamid-al2-mfa) inside the Assurance certification metadata attribute:	PASS
Check for the SWAMID compliance criteria of the SWAMID AL2-MFA-HI (http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi) inside the Assurance certification metadata attribute:	PASS
Check for the SWAMID compliance criteria of the assurance profile SWAMID AL2 (http://www.swamid.se/policy/assurance/al2) inside the Assurance certification metadata attribute:	PASS
Check for the user assurance value of SWAMID AL2-MFA-HI (http://www.swamid.se/policy/authentication/swamid-al2-mfa-hi) inside the eduPersonAssurance attribute:	PASS
Check for the user assurance value of SWAMID AL2 (http://www.swamid.se/policy/assurance/al2) inside the eduPersonAssurance attribute:	PASS
Check for used authentication type REFEDS MFA (https://refeds.org/profile/mfa) inside the Authentication Context Class header:	PASS
Checks for freshness of authentication, i.e. authentication must complete within 60 seconds. Time since authentication was 23 seconds:	PASS

SWAMID

Exempel på hur man kan implementera personverifierad multifaktorinloggning

SUNET

Yubico u2fval (1/3)

SWAMID

- Standalone valideringsserver för U2F devices, t.ex. Yubikeys, troligtvis andra U2F nycklar
- Licenserat under BSD-2-Clause, skrivit av Yubico själv
- Python baserat server som presenteras ett REST API via Apache med WSGI stöd
- Yubico har skrivit exempel connectors i PHP och Python som kan integreras i befintlig kontohanteringsplattform. Det finns inget management GUI.
- Shibboleth modulen finns och är testat med u2fval och IdPv3. Modulen är skrivit av någon som tidigare jobbat på Yubico som SWAMID operations har kontakt med. Koden kommer att fortsätta underhållas.

Yubico u2fval (2/3)

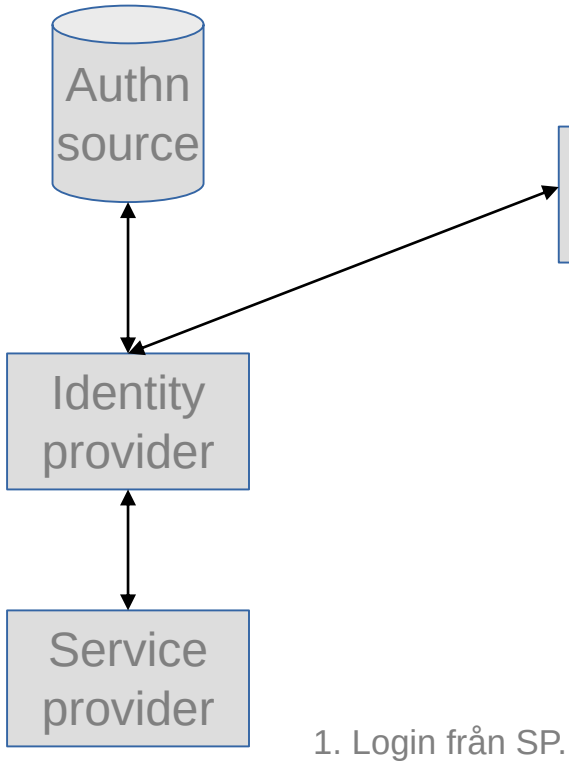
SWAMID

- SWAMID Operations har testat u2fval, PHP connectorn och Shibboleth IdP-modulen
- https://developers.yubico.com/U2F/
- https://github.com/Ratler/shibboleth-mfa-u2f-auth
- https://wiki.sunet.se/display/SWAMID/Setting+up+U2F+Multi-factor+authentication+with+Shibboleth+IdP+for+use+within+SWAMID

Yubico u2fval (3/3)

SWAMID

Login till tjänst som kräver MFA

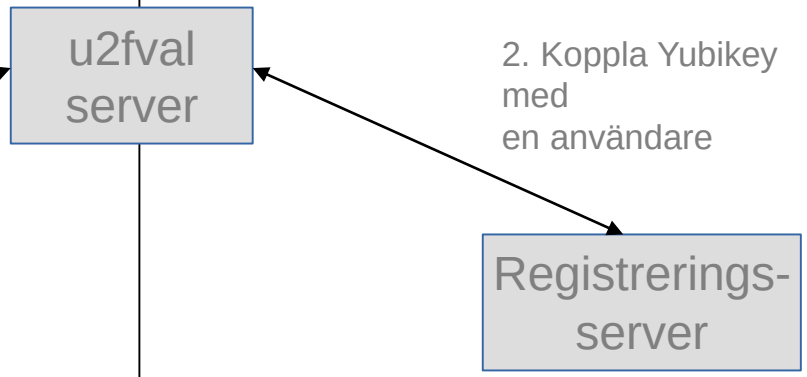


2. IDPn kräver lösenordet och sedan knapptryckt på Yubikey

3. IdPn slå ihop svaren och skicka tillbaka till SPn

1. Login från SP. SPn kräver Refeds MFA som context

Vid helpdesk



2. Koppla Yubikey med en användare

1. Registreringen utförs på helpdesk av supportpersonal möt uppvisning av legitimation.

SUNET

LinOTP (1/3)

SWAMID

- Linux baserad enterprise-level OTP plattform
- Licenserat under AGPLv3 och GPLv2 som ”community edition”
- Server och GUI komponenter som kan integreras med LDAP, AD mm
- Kan köpa support och färdigt virtual appliances från KeyIdentity GmbH
- SWAMID operations har testat med LDAP, Google Authenticator (TOTP) och Shibboleth IdP

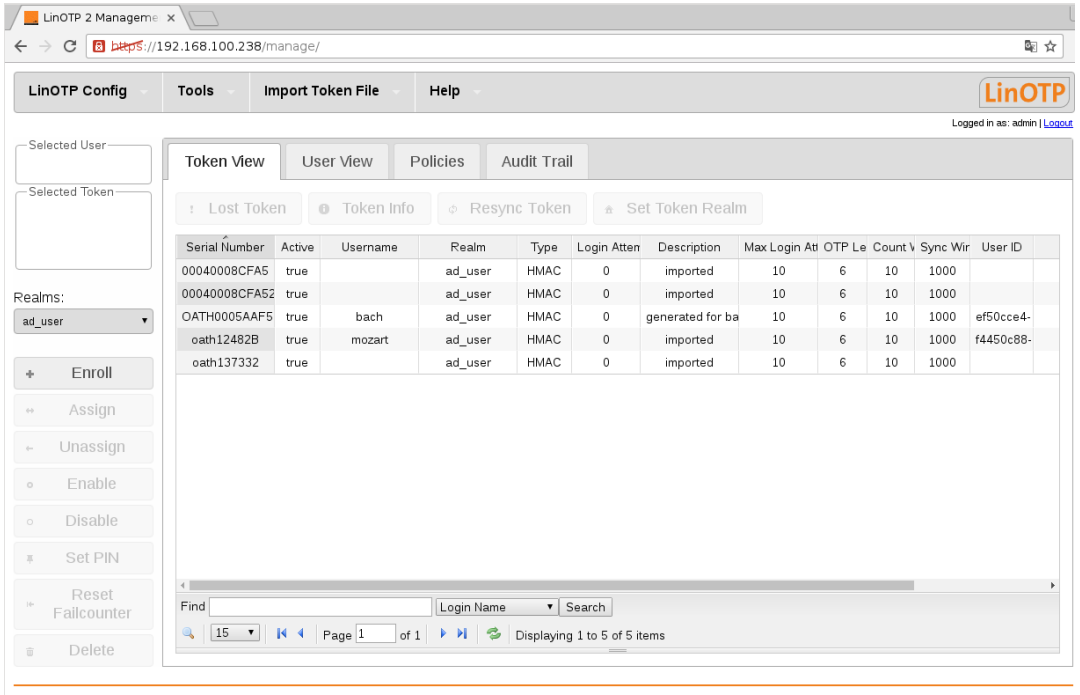
LinOTP (2/3)

SWAMID

- https://www.linotp.org
- https://github.com/cyber-simon/idp-auth-linotp
- *Oklart om stöd för denna Shibboleth modul – SWAMID har tagit kontakt med KeyIdentity och inväntar svar*

Beroende på säkerhetsrisker kommer OTP fasas ut som godkänd metod för personverifierad multifaktorinloggning i SWAMID inom några år

LinOTP (3/3)



Exempel på Web UI features

- Provisioning av realms (koppling till backend)
- Token view och provisioning (dock inte för all typer av tokens)
- https://www.linotp.org/doc/latest/part-management/introduction.html

Mpassid shibboleth-idp-authn-shibsp (1/2)

SWAMID

- Utvecklas av våra kollegor på CSC i Finland
- Fungerar som en SAML proxy
- Förfrågningar som kommer in och kräver https://refeds.org/profile/mfa skickar användaren vidare till en annan IdP som stödjer detta. Skulle kunna vara eduID.
- Svaret som kommer i retur berikas med uppgifter från den egna katalogen.

Mpassid shibboleth-idp-authn-shibsp (2/2)

SWAMID

- Fungerar med hjälp av en auth-modul som måste kompileras upp
- Kräver att det finns en Shibb SP som kan ta emot svaret från den externa IdP:n
- Auth-modulen använder EPPN eller liknande i svaret till SP:n för att koppla till en användare i den lokala katalogen.

Intressant teknisk lösning som dock är väldigt tekniskt komplex och svår att implementera. Detta kan enklare att använda istället använda Satosa för all federativ inloggning.

SWAMID

Swedish Academic Identity Federation

SWAMID

Vad är på gång nu?

SWAMID

- SWAMID Operations kommer att hålla ett antal webinarer och workshops runt multifaktorinloggning
- SWAMIDs Wiki kommer att få mer information om personverifierad multifaktorinlogging inkl. exempel
- eduID kommer att under hösten driftsätta stöd för personverifierad multifaktorinloggning via U2F

SUNET

SWAMID

Swedish Academic Identity Federation

SWAMID