Fallstudie runt införande av SWAMIDs multifaktorinloggning vid ett lärosäte

Paul Scott (paul.scott@kau.se)
Karlstads universitet
SWAMID operations

Behov av MFA på Karlstads universitet

- Krav för införande av multifaktorautentisering för Nais
- Kravet gäller bara få anställda idag som jobbar i Nais
- Kravet (och lösningen) gäller enbart anställda, dvs vi har inget stöd i dagsläget för MFA för studenter

En Proof of Concept

- SWAMID operations tog på sig uppdraget att testa olika lösningar som skulle fungera tillsammans med Shibboleth

- Jag gjorde en Proof of Concept som presenterades i på Sunetdagar HT18:
  - Shibboleth Identity Provider v3
  - Yubico u2fval valideringsserver + exempel connector bibliotek
  - Shibboleth U2F MFA plugin med stöd för u2fval
  - Yubico Security Key (andra typer av U2F finns!)

Yubico u2fval & connector bibliotek

- u2fval är en standalone server licensierat under BSD 2-clause och körs i en webbserver med WSGI stöd (ex Apache)

- u2fval tillåter registrering och autentisering via ett enkelt JSON REST API

- Yubico har skrivit exempel connectors i PHP och Python som kan integreras i befintligt identitetshanteringsystem för att hantera registrering och avregistrering av MFA nycklar

Shibboleth MFA U2F plugin

- En Shibboleth plugin som knyter ihop u2fval med IdPs egen MFA login flow
- Pluginen är skrivit av någon som tidigare jobbat på Yubico som SWAMID operations har kontakt med. Koden kommer att fortsätta underhållas.
- Länkar:

  Yubico u2fval: https://developers.yubico.com/u2fval/
  Connector bibliotek: https://developers.yubico.com/Software_Projects/FIDO_U2F/U2FVAL_Connector_Libraries/
  Shibboleth plugin: https://github.com/Ratler/shibboleth-mfa-u2f-auth
  Installation cookbook: https://bit.ly/2Un50TP (Länk till SWAMIDs wiki - finns under IdP best current practice)

En ganska små steg att driftsätta i produktion

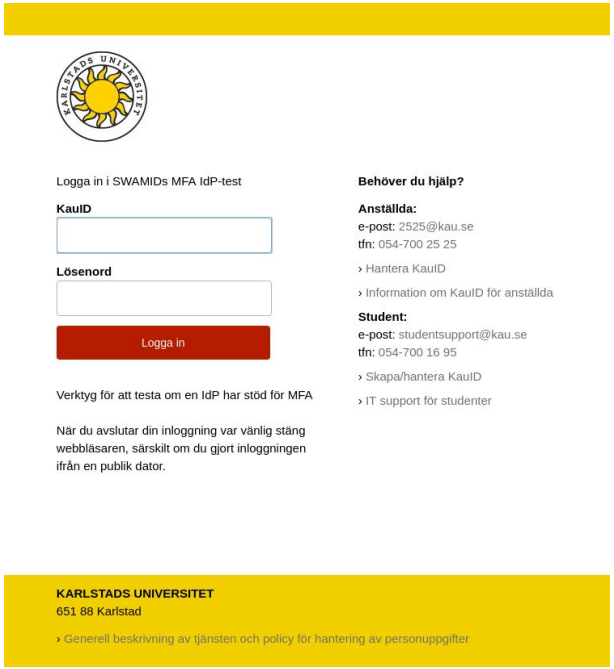
- Byter från SQLite till en produktionsdatabas för u2fval server
- Driftsätta konfig från test IdPn till produktion och skapa en u2f view
- Göra en registreringsgränssnitt utifrån Yubicos PHP connector bibliotek
    - Lägger till Shibboleth inloggning
    - Kontroll av användare (inloggning, anställd på AL2)
    - Byter till KAUs admintema
- Från Proof of Concept till produktion tog ~ 20h

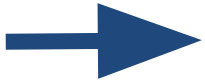
För- och nackdelar med U2F för KAU

- Fördelar med denna lösning:
  - Fungerar som MFA lösning för vår Shibboleth IdP
  - Våra anställda kan använda sina KauID tillsammans med Yubikeyn
  - Enkel knapptryck att aktivera den andra faktorn
  - Kan användas för andra KAU webbtjänster samt federerade webbtjänster

- Nackdelar med denna lösning:
  - Webbläsarstöd är begränsat till Chrome, Opera och Firefox
  - U2F är redan gammal teknik, FIDO2 WebAuthn är nu beslutad av W3C
  - Löser inte alla tänkbara behov av MFA

Enkel inloggning för användarna





Registrering av MFA nyckeln

- Vi har använt Yubicos PHP connector bibliotek för registrering/avregistrering av MFA nycklar

- Gränssnittet har en enkel flöde:
  - Administratören loggar in i gränssnittet (som själv kräver MFA) och starta processen för att registrera en ny MFA nyckel
  - Användaren autentisera sig för att bevisa att de innehar KauID:t som ska tilldelas en MFA nyckel
  - Systemet kollar att användaren är en anställd som redan ligger på AL2
  - Användaren legitimerar sig med godkänt ID handling
  - Administratören kopplar en ny MFA nyckel till användarens KauID

Registreringsgränssnitt

Multifaktoradministration

Administratör inloggning Paul Scott (paulscot@kau.se) [Logga ut] Tid kvar: 4 minut(er)

Registrera en ny MFA nyckel

För att påbörja registrering av en ny MFA nyckel måste användaren autentisera sig med sitt KauID och lösenord. När du klickar på knappen "Registrera en ny MFA nyckel" nedan, så kommer du omdirigeras till den vanliga KauID inloggning. Lämna över tangentbordet till användaren och klicka på den gröna knappen. Efter inloggning tar du som administratör tillbaka kontrollen på datorn för nästa steg.

Registrera en ny MFA nyckel

Avregistera en MFA nyckel

För att ta bort en MFA nyckel, behöver användaren inte vara på plats. Detta används om användaren har t.ex tappat bort sin MFA nyckel eller om det har skett en säkerhetsincident med användarens konto.

Avregistrera en MFA nyckel

Administratör inloggning Paul Scott (paulscot@kau.se) [Logga ut] Tid kvar: 5 minut(er)

Följande information skickades av IdPn vid inloggning:

affiliation	employee@kau.se;member@kau.se
assurance	http://www.swamid.se/policy/assurance/al1;http://www.swamid.se/policy/assurance/al2
cn	Paul Scott
eppn	paulscot@kau.se
mail	paul.scott@kau.se
personnummer	19[redacted]

Utföra legitimationskontroll innan du fortsätter med registrering av en MFA nyckel!

Att utföra legitimationskontroll

Följande typer av legitimation är godkända (enligt Skatteverket)

Medborgare i Sverige

- id-kort utfärdat av Skatteverket
- svenskt pass med vinröd pärm
- svenskt nationellt id-kort
- svenskt körkort
- svenskt SIS-märkt id-kort utfärdat av till exempel en bank, ett företag eller en myndighet
- svenskt tjänstekort utfärdat av en statlig myndighet.

Medborgare i ett EU-/EES-land

Medborgare i övriga länder

Registrera en ny MFA nyckel för paulscot

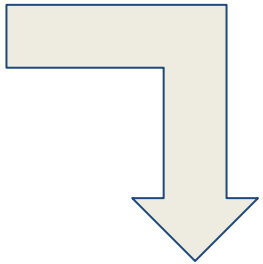
Starta om

Multifaktoradministration

Administratör inloggning Paul Scott (paulscot@kau.se) [Logga ut] Tid kvar: 5 minut(er)

Registrera MFA nyckel

Sätta in MFA nyckeln i en USB port, vänta tills den börjar blinka, sedan tryck på knappen.



Karlstads universitet
651 88 Karlstad

Följande MFA nycklar är kopplade till KauID: paulscot

Security Key by Yubico

Registrerad: 2019-01-12 17:39:15
Senaste använt: 2019-03-28 11:26:47

Avregistrera

SWAMID technical validation of multifactor login via REFEDS MFA

Multifactor validation results

This is a multifactor validation check for the Identity Provider (https://weblogin.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:	**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 1 seconds:	PASS

Användarupplevelser

- Det har gått bra!

> *“Jag har nu gått in i Nais med säkerhetsnyckeln, och kan tala om att det gick jättelätt! Jag gick in i Nais som vanligt, klickade på Personal och Lärosäte, loggade in med mitt KauID och ombads sedan sätta i säkerhetsnyckeln och trycka på knappen som blinkade. Sedan kom jag in i Nais utan vidare.*
>
> *Var det något mer jag skulle tänka på? Är det bara att dra ut nyckeln när man kommit in i Nais?”*

- Men man måste kom ihåg att använda rätt webbläsare!

Uppdateringar av IMPS

- Man måste skicka i en uppdaterad IMPS till SWAMID operations för att bli godkänd för SWAMID Person-Proofed Multi-Factor Profile

- Finns två nivåer
  - Person-Proofted Multi-Factor (AL2-MFA)
  - Person-Proofted Multi-Factor with high identity assurance (AL2-MFA-HI)

- KAU delar enbart ut SWAMID AL2-MFA-HI
  - Delas ut personligt hos IT-avdelningens reception mot uppvisning av godkänd legitimation samt att personen själv loggar in som en del av registreringsprocessen

Sammanfattning

- Det här har varit en jättebra sätt att lära sig MFA-teknik i en produktionsmiljö
- Enkel för användarna att använda en Yubikey tillsammans med sitt KauID
- Vi kan deploya MFA till flera webbtjänster men det är inte bestämt i dagsläget vilka interna tjänster kommer att börja kräva MFA
- För de användarna som redan har en hårdvarunyckel så kommer dessa att fungera med eventuella WebAuthn lösningar framöver