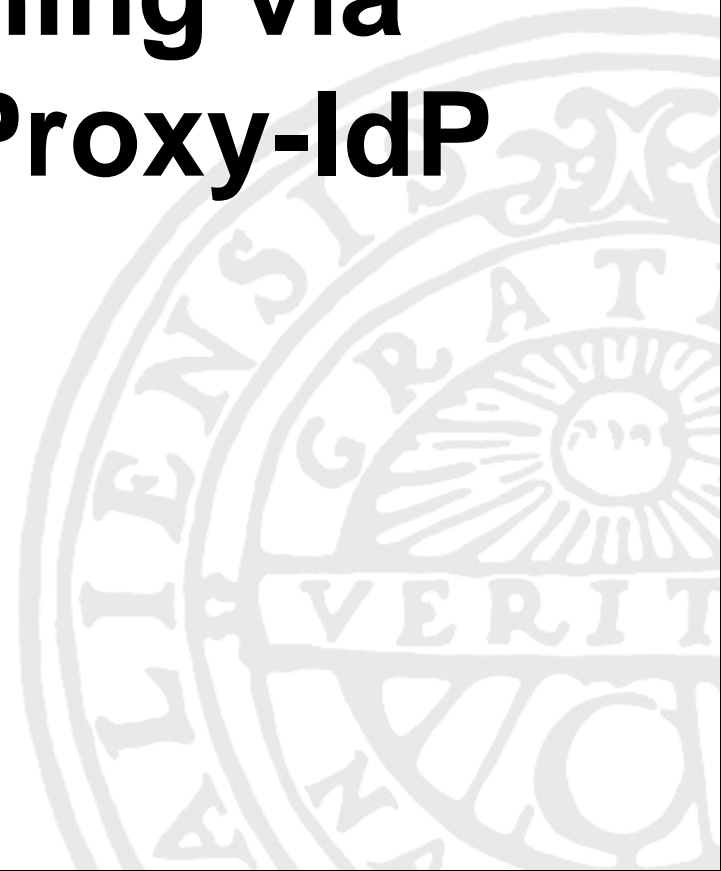




UPPSALA
UNIVERSITET

SWAMID Workshop 2012 3

2-faktorsinloggning via SAML2-baserad Proxy-IdP





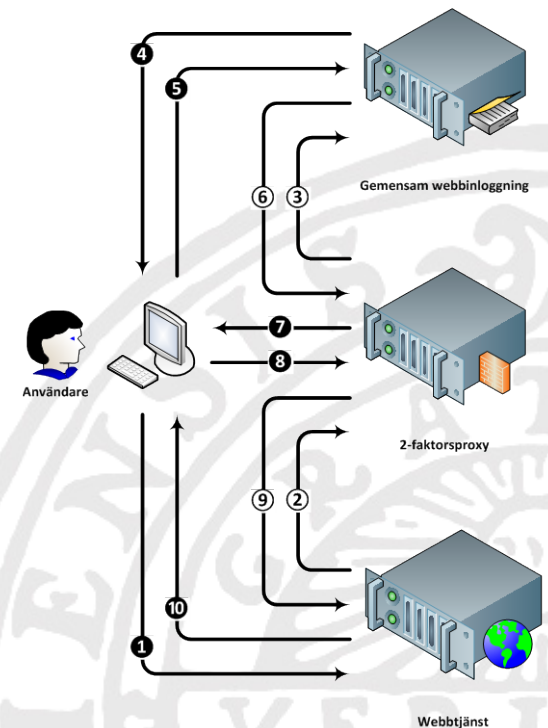
Upplägg för pilot

- Uppsala universitet genomför en sex månader lång 2-faktorspilot tillsammans med partneren Svensk e-identitet AB
 - Förberedelsefas med uppsättning och konfiguration av miljön ingår inte i de sex månaderna
- I piloten ingår att ett antal användare ska använda en Yubikey tillsammans med användaridentitet och lösenord för att logga in i en webbaserad administrativ applikation
 - Faktor 1: Användaridentitet och lösenord (något man vet)
 - Faktor 2: Yubikey (något man har)



Flöde för SAML2-inloggning med 2-faktorsproxy

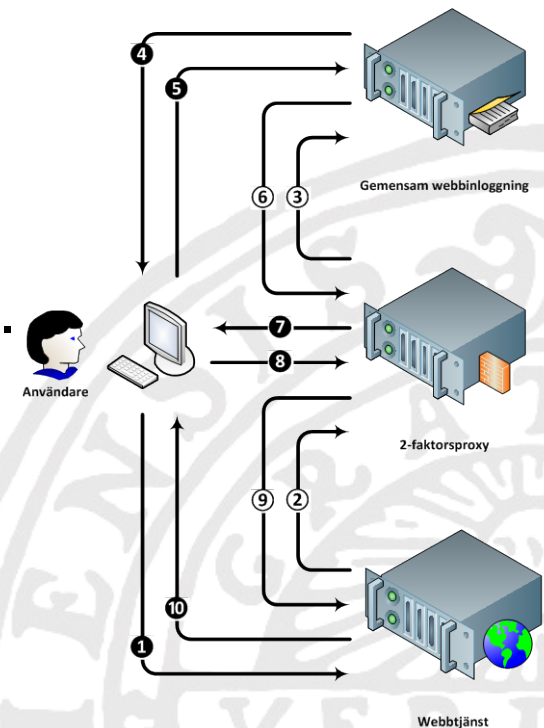
1. Användaren går till webbtjänstens webbadress och väljer att logga in.
2. Användaren omdirigeras automatiskt till 2-faktorsproxyn.
3. Användaren omdirigeras automatiskt till normal IdP med inloggning genom användaridentitet och lösenord.
4. Användaren får begäran om inloggning.
5. Användaren loggar in med användaridentitet och lösenord.





Flöde för SAML2-inloggning med 2-faktorsproxy

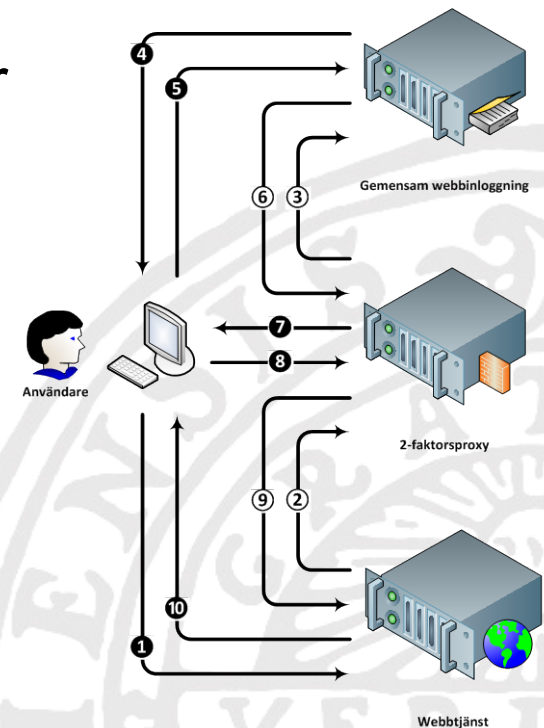
6. Användare omdirigeras automatiskt till 2-faktorsproxyn med information om användaridentitet, ytterligare attribut som ska skickas till webbtjänsten, 2-faktorsbärare samt om 2-faktorsinloggning krävs för någon webbtjänst.
7. Om 2-faktorsinloggning krävs för aktuell webbtjänst efterfrågas andra faktorn av användaren, annars, gå till steg 9.
8. Användaren loggar in med andra faktorn, dvs Yubikey.





Flöde för SAML2-inloggning med 2-faktorsproxy

9. Användaren omdirigeras automatiskt till webbtjänsten med information om inloggning skett med andra faktor eller med endast användaridentitet och lösenord samt användaridentitet och andra attribut som kommer från Gemensam webbinloggning.
10. Användaren är nu inloggad och kan börja använda tjänsten.





Särskilda 2-faktorsattribut

- Normal IdP skickar två (ev. tre) typer av styrattribut via eduPersonEntitlement till 2-faktorsproxyn
 - Serienummer på registrerad Yubikey:
`urn:mace:swami.se:gmai:2fakt:yubikey:sn=serienr`
 - Om användaren krävs på 2-faktor för viss applikation:
`urn:mace:swami.se:gmai:2fakt:applikation`
 - *Ev. särskilt genererat attribut för att säkerställa att 2-faktorsproxyn genomför omdirigering till normal IdP, ska skickas vidare till webbtjänsten som använder 2-faktorsproxyn*



UPPSALA
UNIVERSITET

SWAMID Workshop 2012 3

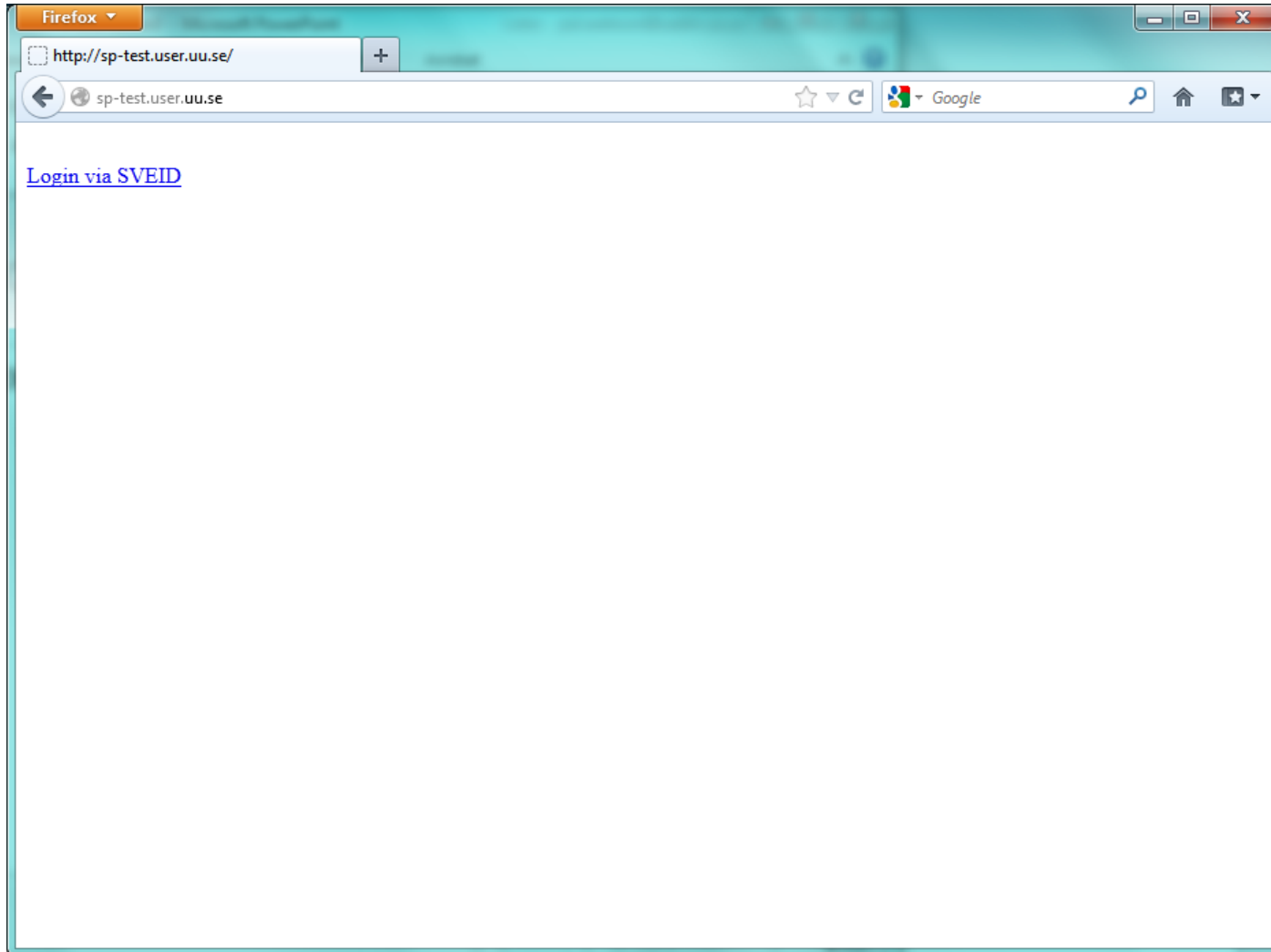
DEMO





UPPSALA
UNIVERSITET

Skärmbild från demo





Skärmbild från demo

Firefox

Gemensam webbinloggning

https://cas.user.uu.se/cas/login?service=https%3A%2F%2Fswamid.user.uu.se%2Fidp%2FAuthn!

Uppsala University logo

Gemensam webbinloggning

Lyssna English

Logga in i en webbtjänst


Webbtjänsten som du vill använda kräver inloggning.

Användaridentitet:

Lösenord A:

LOGGA IN

Har du glömt ditt lösenord? [Klicka här](#)
Vill du byta ditt lösenord? [Klicka här](#)

 Av integritets- och säkerhetsskäl bör du alltid **logga ut** och **stänga alla** webbläsarfönster när du är färdig med webbtjänsterna som kräver inloggning. Om du använder **Apple MacOS X** måste du **också stänga av hela** webbläsaren, inte bara fönstren. Använder du en **publik dator** är det **extra viktigt** att du stänger alla webbläsarfönster innan du lämnar datorn.

www.uu.se Uppsala universitet | Kontakt: Student, Anställd | Om gemensam webbinloggning



Skärmbild från demo


Firefox

http://loginserver1...ed74e1&proxy_lang=

loginserver1.testauthify.com/yubico/?authify_request_token=b66955fa2b340168bb8f3ba9eed74

Google

yubico
trust the net

 **YubiKey**
login

YubiKey

Gör så här

1. Sätt in din Yubikey i en USB-port på datorn
2. Lägg ett finger på den runda, guldfärgade ytan
3. När inmatningsfältet ovan fylls med bokstäver, invänta att du blir inloggad.

Har du förlorat din YubiKey? [Klicka här](#)



Skärmbild från demo

The screenshot shows a Firefox browser window with a single tab titled "Session Summary". The address bar displays the URL `https://sp-test.user.uu.se/Shibboleth.sso/Session`. The page content is as follows:

```
Miscellaneous
Client Address: 130.238.90.64
Identity Provider: https://callback-test.inloggning.se/simplesaml/saml2/idp/meta_92bb17d9a4f44040c524b5e3f895ec6e
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Authentication Time: 2012-10-09T18:30:51Z
Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
Authentication Context Decl: (none)
Session Expiration (barring inactivity): 480 minute(s)

Attributes
cn: Pål Axelsson
countryName: SE
displayName: Pål Axelsson
entitlement: urn:mace:swami.se:gmai:2fakt:akka2fakt;urn:mace:swami.se:gmai:2fakt:yubikey:uuAKKAextendedAuth2=01077
friendlyCountryName: Sweden
givenName: Pål
mail: pal.axelsson@uadm.uu.se
norEduOrgAcronym: UU
o: Uppsala universitet
sn: Axelsson
uid: palaxel|
```