2-faktorsinloggning via SAML2-baserad Proxy-IdP

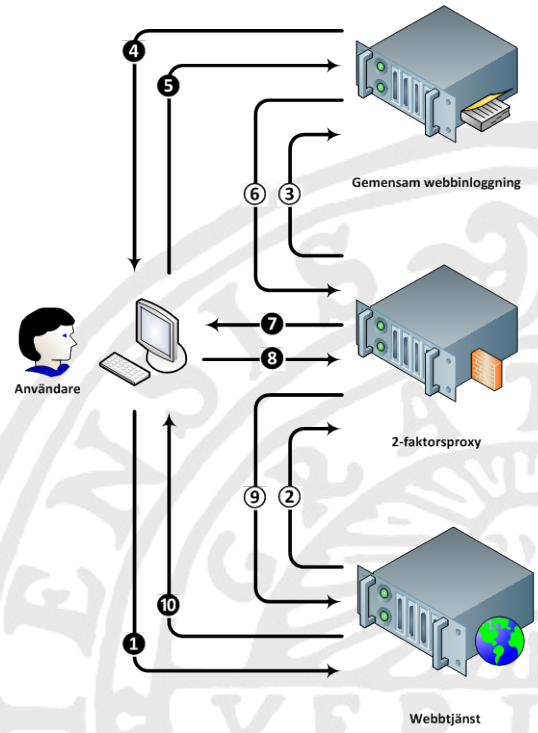
UPPSALA UNIVERSITET

Upplägg för pilot

- Uppsala universitet genomför en sex månader lång 2-faktorspilot tillsammans med partnern 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)

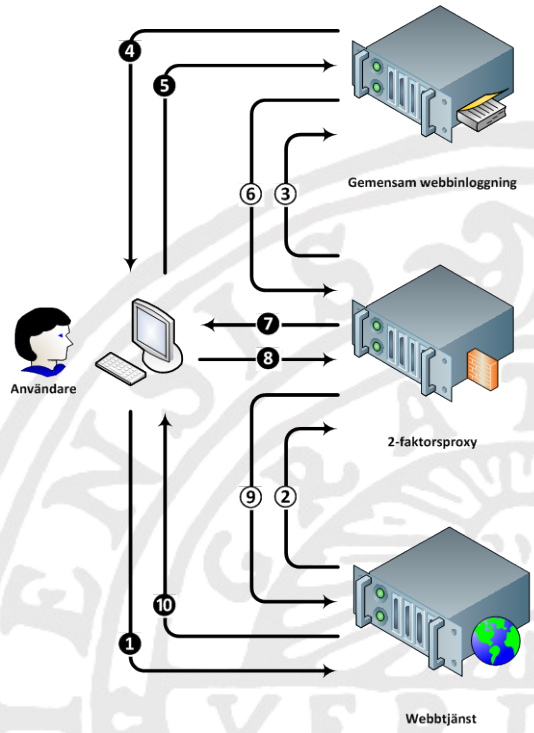
Flöde för SAML2-inloggning med 2-faktorsproxy

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.



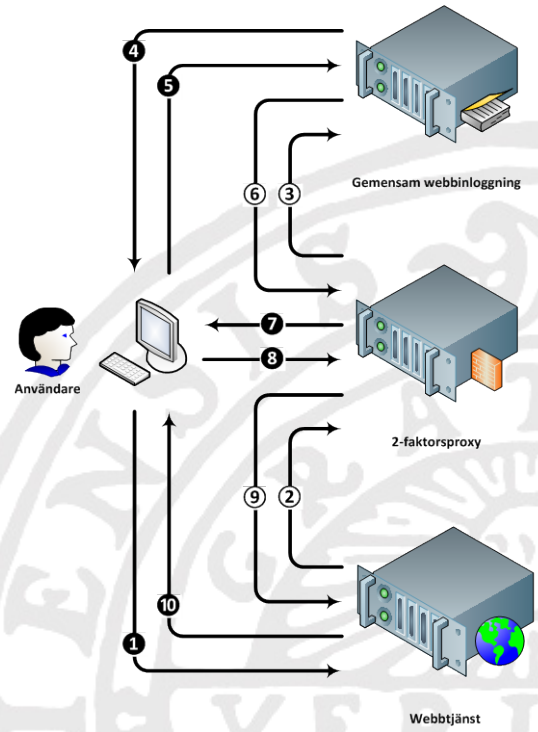
Flöde för SAML2-inloggning med 2-faktorsproxy

6. Användare omdirigeras automatiskt till 2-faktorsproxyn med information om användaridentitet, ytterligare attribut som ska skickas till webbtjänsten, 2-faktorsbärare samt om 2-faktors-inloggning 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.



UPPSALA UNIVERSITET

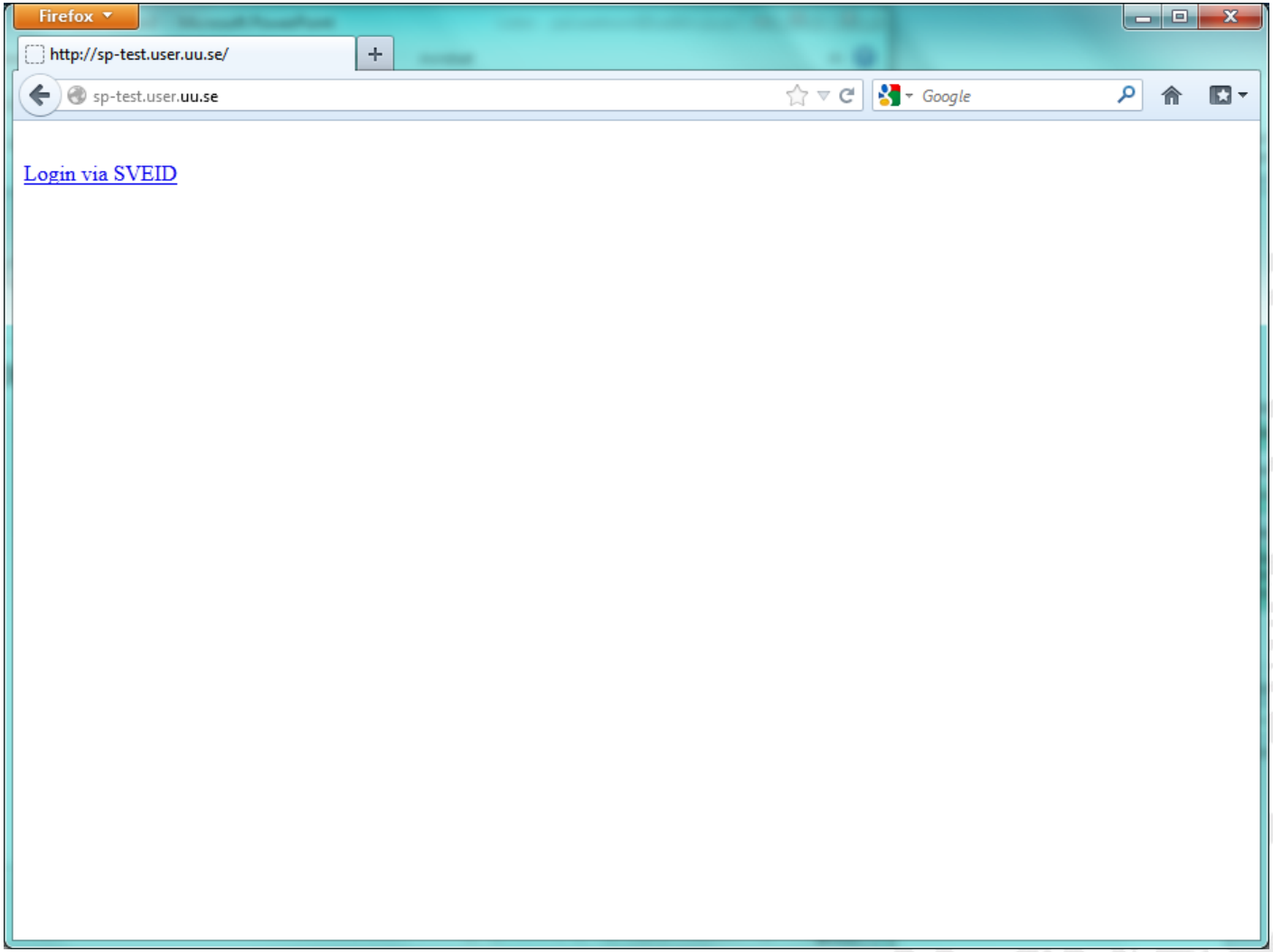
Särskilda 2-faktorsattribut

- 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*

DEMO

UPPSALA UNIVERSITET

Skärmbild från demo

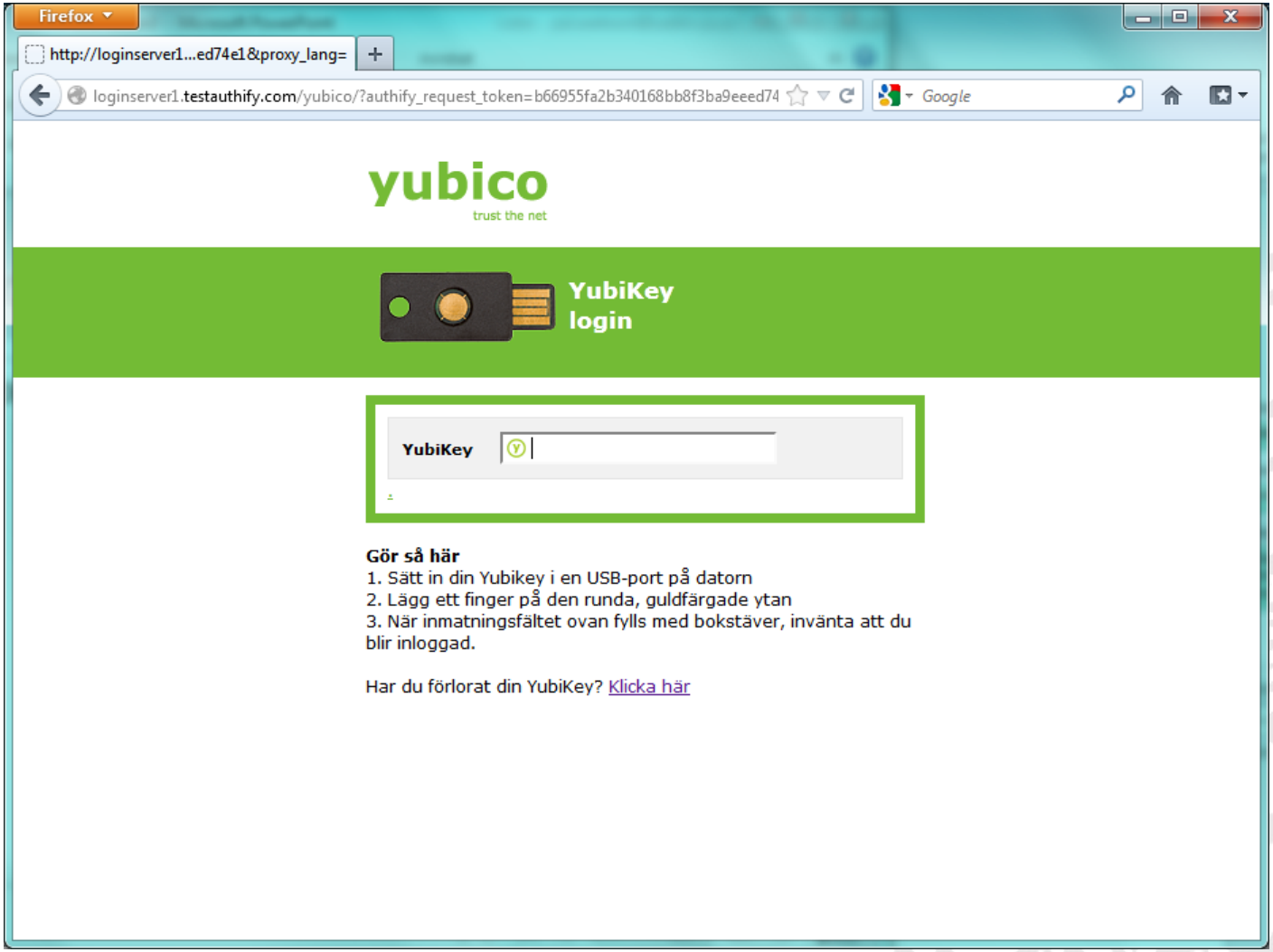


UPPSALA UNIVERSITET

Skärmbild från demo

UPPSALA UNIVERSITET

Skärmbild från demo



UPPSALA UNIVERSITET

Skärmbild från demo