

SWAMID+NyA IDP-dagen

Övningar med SAML och NyA IdP

Syfte (varför vi är här)

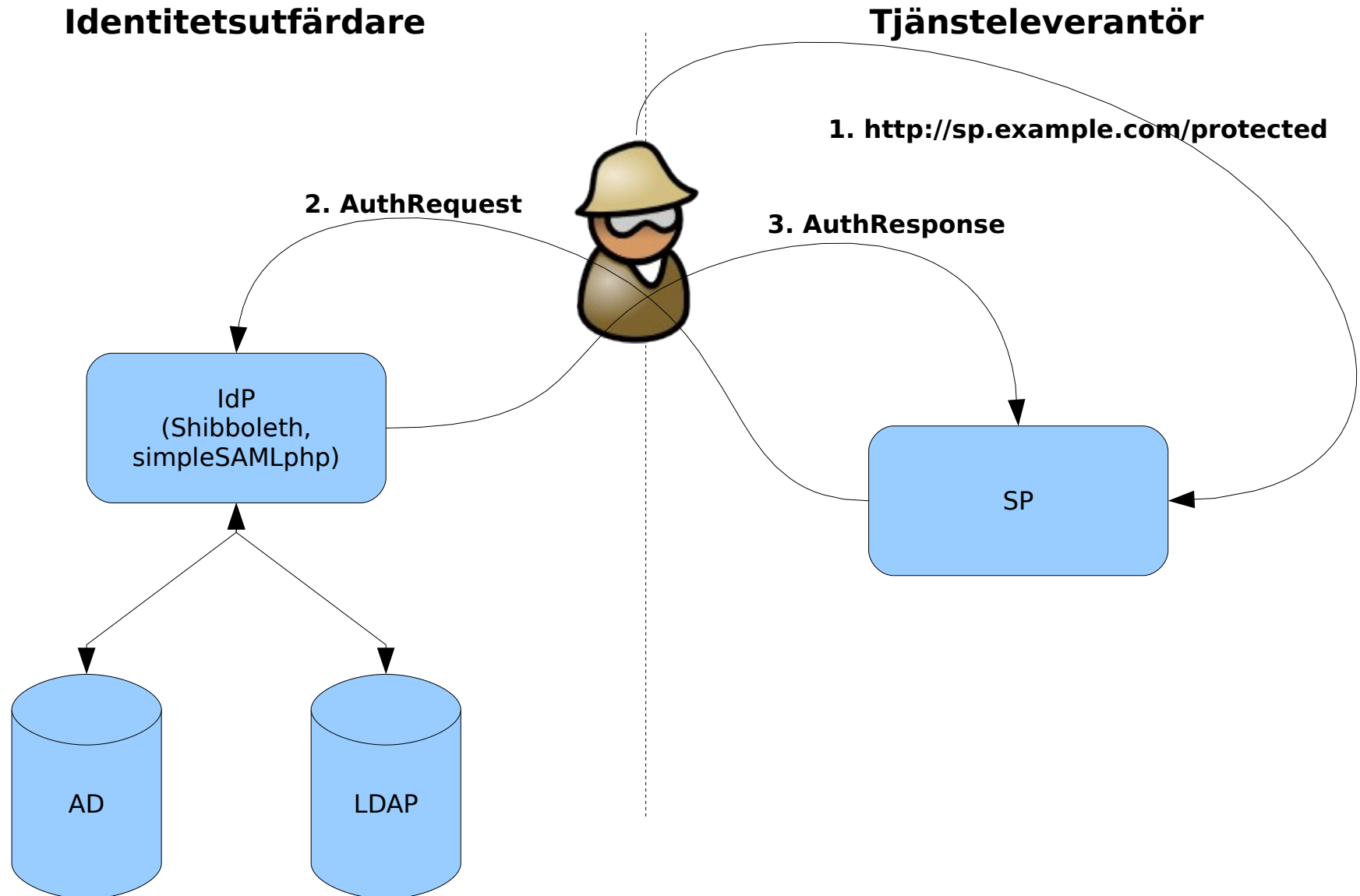
Sänka våra kostnader för IDM
(och lära oss något nytt)

Mål (vad vi ska göra idag)

- Repetera SAML och ID federationer
- Förstå var NyA IdP passar in i bilden
- "Hands-on" med NyA IdP och SAML
 - Shibboleth 2.2 SP
 - simpleSAMLphp

Håll i er för nu börjar det!

SAML



Säkerhet

- Protokollmeddelanden signeras och (ibland) krypteras för att auktorisera avsändare och mottagare.
- Transporter skyddas (ibland) med TLS.

Två centrala problem...

- Nyckeldistribution
- Att hitta resurser ("discovery")

Problem 1: Nyckeldistribution

- Om A ska kryptera ett meddelande till B så...
 - behöver A hitta B's nyckel!
- Om A ska signera ett meddelande till B så ...
 - behöver B veta A's nyckel
- Slutsats: Alla måste ha allas nycklar
- Lösningar:
 - 1) Bygg PKI
 - 2) Lista över allas nycklar

Problem 2: Discovery

- Hur vet en SP vilken IdP som den ska skicka sin AuthnRequest till?

Metadata

- löser nyckeldistributionsproblemet genom att lista alla nycklar i federationen
- bygger "trust" genom att vara signerad
- löser "discovery-problemet" genom att lista alla IdP:er

Vad är en Identitetsfederation?

- Svar: metadata
 - och lite policy
 - men mest metadata!

Var passar NyA IdP in?

NyA IdP är en SAML Web Browser SSO IdP baserad på Shibboleth 1.x som använder NyAs CAS och LDAP som SSO och AA

SAML – liten ordlista (1)

- Relying party (förlitande part)
 - En mottagare av SAML-meddelanden
- SAML assertion
 - SAML meddelande som förmedlar ett påstående om ett subjekt utfärdat av en (vanligen) IdP
- SAML protokoll
 - Beskrivning av hur SAML-meddelanden skickas mellan producerande och konsumerande parter.

SAML – liten ordlista (2)

- SAML protokoll bindning
 - En konkret representation av ett SAML-protokoll, tex till SOAP eller HTTP+POST
- SAML profil
 - Beskrivning av hur protokoll, bindning och assertion sitter ihop för att uppfylla ett användningsfall.
- XML-dsig & XML-enc
 - SAML är XML. Skydd av meddelanden kan ske genom signering och kryptering av XML

SAML – liten ordlista (2)

- SAML Metadata
 - XML-dokument som beskriver medlemmar i en federation. Signerad XML ger tillförlitlighet till listan.
- Web Browser Single Sign-On Profile
 - En profil som beskriver web-inloggning med SAML
- Lightweight Web Browser SSO Profile
 - Bara Browser/POST och Browser/GET

Dagens Övning

Sätt upp en miljö och genomför en inloggning med ett test-konto mot NyA IdP (test)

Checklista (1)

- Få igång vmware-image
 - starta apache och shibd
- Gå igenom konfigurationen och fixa certifikat
 - shibboleth2.xml
- Prata med federationsoperatören och få in din SP i test-metadata (Leif)
 - metadata uppdateras ofta!
- Ordna med attributrelease från IdPn (Kristina)

Checklista (2)

- Skapa en SessionInitiator för NyA IdP
- Få shib-echo.cgi att fungera!

Överkurs

- MSFT Geneva
- Egen IdP