HVERNIG STÝRIR ÞÚ AÐGENGI AÐ GEIMSKIPINU ÞÍNU?

SITT LÍTIÐ AF HVERJU UM FEDERATED IDENTITY

JÖRG P. KÜCK & EDWARD JÓHANNESSON

EFNI

- Auðkenningarvandi nútímans
- Identity
- Federated Identity (FI)
- Identity & Access Management (IAM)
- Azure Active Directory (AAD)

AUÐKENNINGARVANDI NÚTÍMANS

- Sótt í utanaðkomandi þjónustur (SaaS) í vaxandi mæli
  - Þjónustur með eigin notandaupplýsingar
  - Mörg auðkenni og lykilorð
  - Heilindum áfátt
  - Stjórnleysi

IDENTITY

- Einkennandi fyrir hlut, persónu o.s.frv.
  - Physical identity
  - Digital identity

IDENTITY

- Authentication er til þess að bera kennsl á hlut, persónu o.s.frv.
- Authentication er tvíþætt
  - Identification – auðkenning
  - Validation, verification – sannvottun
- Grundvöllur allrar sannvottunar er traust

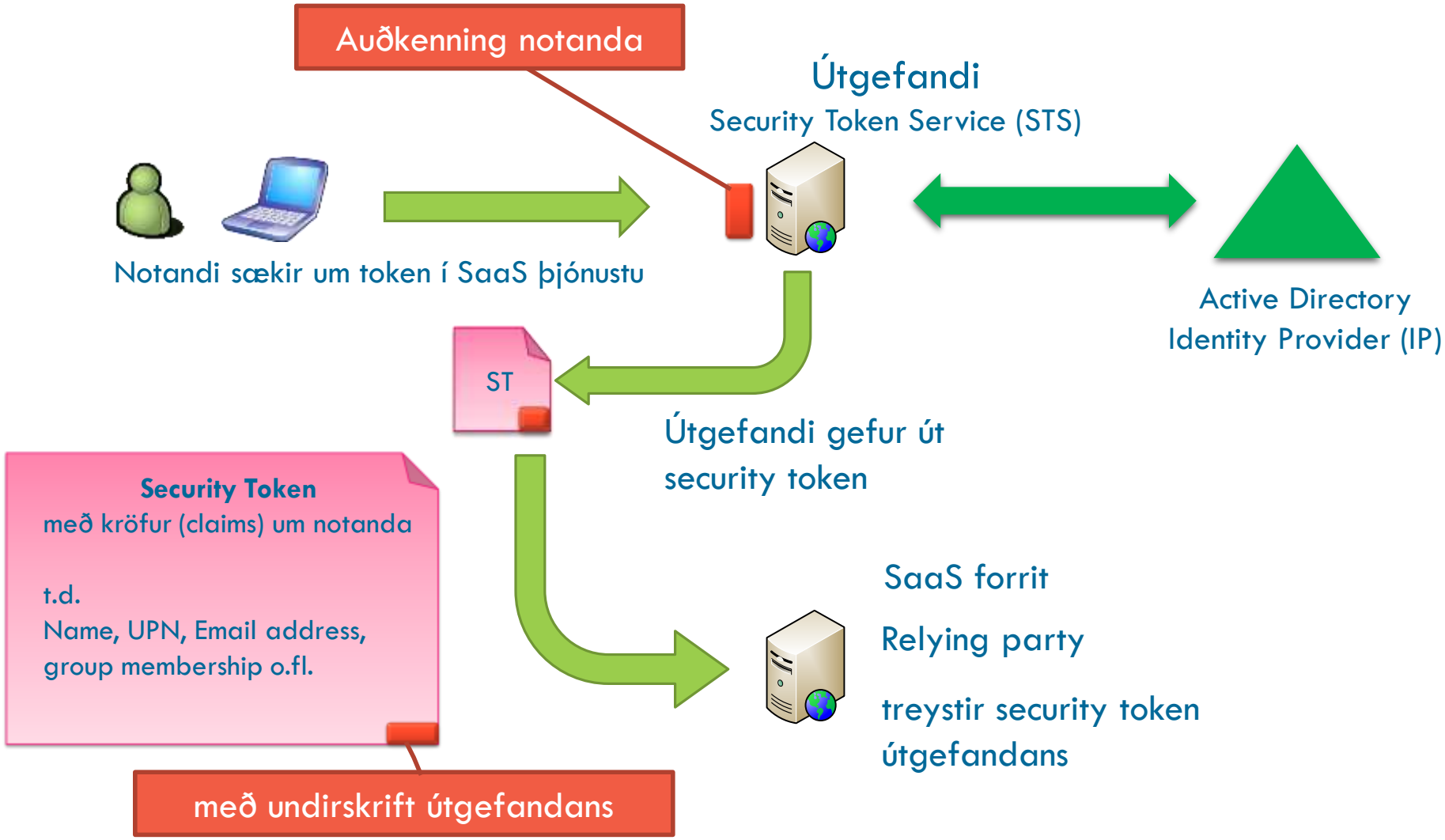
FEDERATED IDENTITY

- Aðgangur að ótengdum þjónustum án endurvottunar
- Traustur sannvottunaraðili
- Ákveðin eigindi
- Jarteikn (security token)
- Rafræn undirskrift

„Og með því að Hlöðvir kóngur var sjálfur góðviljaður og sá og heyrði sannar **jarteinir** almáttugs Guðs og hans heilagra manna [...] þá tók hann skírn og rétta trú.“

FEDERATED IDENTITY

- Hugtök
  - Identity Provider
  - Service Provider (Relying Party)
  - Security Token Service


Auðkenning notanda
Útgefandi
Security Token Service (STS)
Notandi sækir um token í SaaS þjónustu
Active Directory
Identity Provider (IP)
ST
Útgefandi gefur út
security token
Security Token
með kröfur (claims) um notanda
t.d.
Name, UPN, Email address,
group membership o.fl.
SaaS forrit
Relying party
treystir security token
útgefandans
með undirskrift útgefandans

FEDERATED IDENTITY

- Auðkennum fækkað
- Aukin heilindi
- Aukið öryggi
- Gagnsætt auðkenningarferli
- Staðsetning sannvottunar
- Einn aðgangur að þjónustum
- Innleiðing og ferlar
- Þekking

FEDERATED IDENTITY

- Margar lausnir
  - Microsoft, IBM, Oracle, OneLogin, Okta o.fl.
- Open source
  - Shibboleth, Gluu, Keycloak o.fl.
- On-premises eða í skýinu (IDaaS)
- Tvær lausnir frá Microsoft: AD FS og Azure Active Directory

IDENTITY & ACCESS MANAGEMENT

- Réttur aðgangur á réttum tíma á réttum forsendum
- Misleitt tækniumhverfi
- Síharðnandi kröfur um hlítingu
- Mikilvægur þáttur í öryggi
- Krefst þekkingar á rekstri auk UT

IDENTITY & ACCESS MANAGEMENT

Gartner criteria for IAM systems 2017

- User authentication
- Federated SSO
- Password vaulting & forwarding
- Step up authentication
- Security token services
- Autherization enforcement
- Security Analytics & Reporting
- User Provisioning

Figure 1. Magic Quadrant for Access Management, Worldwide

Source: Gartner (June 2017)

AZURE ACTIVE DIRECTORY

- Auðkenning notanda
- Samþætting við AD on-premises
- SSO virkni fyrir fleiri en 3.000 SaaS þjónustur
- Margþætt auðkenning
- Skilyrtur aðgangur
- Auðkennisvernd

AZURE ACTIVE DIRECTORY

- Office 365 krefst AAD
- Samþætting við AD on-premises / AD Connect
  - Password hash synchronization (PHS)
  - Pass-through authentication (PTA)
  - Federation (AD FS)
  - Seamless SSO

AZURE ACTIVE DIRECTORY

- Federated SSO
  - WS-FED
  - SAML 2.0
  - OpenID Connect, OAuth2
- Password-based SSO
  - notandaupplýsingar vistaðar í Azure AD
- Linked sign-on
  - URL vísun í Azure AD portal inn á federated token services annars staðar (t.d. AD FS)

TAKK FYRIR OKKUR