Privacy By Default

CPDP 2013

Ronny Bjones
Director Cloud Identity & Privacy Services
Azure Active Directory
Microsoft Corporate

Looking Back…

- Déjà Vu
  - Predictions of huge security problems mid 90thees
  - Security was not on the industry’s radar

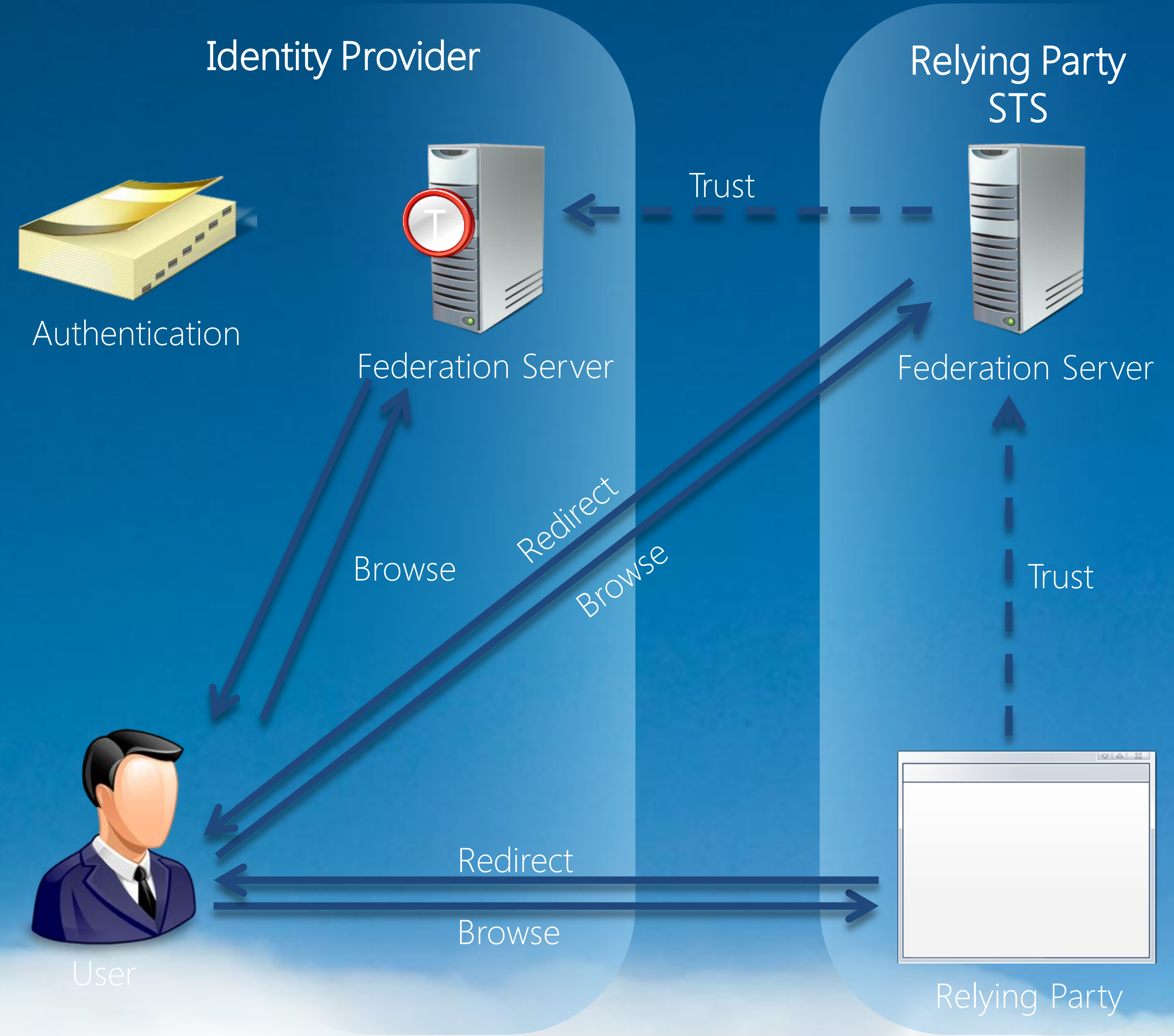
- Are we seeing the same now with Privacy?
  - Industry must be proactive
  - Privacy has to be at the core of new Cloud developments

Privacy By Default

- Privacy must be part of the design/development process
  - Examples are
    - Microsoft's Trustworthy Computing Security Development Lifecycle SDL
    - OASIS Privacy by Design TC
  - Area of emerging standards

- New Privacy innovations
  - Key Area – Prevent linking of transactions
  - Privacy needs to addressed on the whole infrastructure
    - IPv6 Privacy Extensions
    - Internet Explorer Do Not Track
    - Cloud Identity Do Not Track
    - Privacy Attribute-Based Credentials

Identity Federation has Security, Scalability and Privacy problems



- There is an explicit trust between the Identity Provider and other federation servers. The relying party trust its STS
- Insiders of the federation server can impersonate anybody in the relying parties
- If one of the federation servers go down it replicates to all relying parties within the trust ecosystem
- Federation Servers learn user claims and the user's relationship with the relying party
- Current federation protocols:
  - Solve a host of important problems
  - Need to be completed with mechanisms that offer better privacy and multi-lateral security.
- We are creating Cloud Identity and Privacy Services to give federation protocols these broader capabilities.

Attribute-Based Credentials Privacy Features

- Untraceability
  - Identity Provider can’t correlate issuance and presentations of claims
- Minimal Disclosure
  - Only show those claims needed for the transaction to succeed
- Unlinkability
  - Different relying parties can’t correlate presentation of claims

References

- http://www.microsoft.com/security/sdl/resources/publications.aspx
- OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC
- Identitity Blog
  Kim Cameron: Identity Management As A Service
  http://www.identityblog.com/?p=1205

Microsoft®

Be what's next.™

Microsoft®