SAML 2.0
Authentication Context Introduction

Frederick Hirsch

Nokia Mobile Phones

03-09-09

NOKIA

Authentication

- Mechanism commonly discussed
  - E.g. X.509 cert
- Not meaningful without additional considerations
  - Self-signed unknown CA…
  - Private key not secret…

NOKIA

Authentication Context

- Identification
  - Quality of due diligence at time of credential issuance
- Technical protection
  - How is secret (e.g. key) kept secure?
- Operational protection
  - Audits, record keeping, Keygen procedure, expiration periods, etc
- Authentication mechanism
  - Password, smartcard, …
- Governing Agreements
  - Legal framework, liability agreements, etc.

Authentication Context

- Can be too complex to analyze for SP
- Many combinations

NOKIA

Authentication Context Classes

- Create categories to determine “quality” of authentication
- SP can ignore details and review appropriateness of class
- Class includes schema that provides details
  - “Password over SSL” is a class, so is “Smartcard PKI”
  - “Internet Protocol” (IP source), “Time-Sync-Token”

NOKIA

Use

- Authentication Statement (FF 1.2)
  - Extension of saml:AuthenticationStatementType
  - Includes authentication context
  - Indicate quality and details of authentication with authentication statement
- AuthnRequest – authentication request
  - Can include 1 or more
  - Indicate desired quality of authentication
  - IDP evaluates
  - Processing rules:
    - Exact – exact match of one of
    - Minimum – at least as strong as any one
    - Better – stronger than any specified

Defined Authentication Classes

- Mobile Contract
- Mobile Digital ID
- Mobile Unregistered
- Password
- Password-Protected Transport
- Previous Session
- Smartcard
- Smartcard PKI
- Software PKI
- Time-Sync-Token
- Internet Protocol
- Internet Protocol + Password

NOKIA