

Technology for Consideration: SAML

Overview of SAML, Identity Management and
Why it is Important to the SmartGrid

Why is He Standing Here?

- Kyle Meadors, Principal of Drummond Group
- Rik Drummond
 - Co-founder of Drummond Group Inc (DGI)
 - Chairman of GridWise Architecture Council
- Mission to Drive Adoption of Standards and Technology through Certification Testing
- Responsible for Interoperability Testing of SAML

And Why Should We Listen?

- Understand Identity Management in the Digital World
- Understand How SAML is Used for Secure Identity Management
- How Government Agencies and other Deployers are Using SAML
- How SAML can be used for the Evolving SmartGrid

Identity Management in the Real World

- Compare to a Airport Check-In with Drivers License
 - You = Subject
 - Airline = Service Provider
 - License = Assertion/Credential
 - Information on License (Name, Height, Birthdate, etc.) = Attributes
 - State = Identity Provider/Authority
 - Trustworthiness = Level of Assurance

Unique Identity Challenges for Digital World

- Far Less Direct Contact with Person
 - Trustworthiness is Diminished
 - Minimize Business Opportunities
- Information is Far Harder to Control
 - Loss of Privacy
- Service Providers Need Different Credentials
 - Confusing for User to Maintain Multiple Passwords

Advantages of SAML

- Secure Exchange of Identity Information
 - Better Security/Privacy
- Managing Passwords/Credentials
 - Better User Experience
 - Reduced Scope for Service Providers
- Federated Identity
 - Enhanced User Operations
 - New Business Opportunities

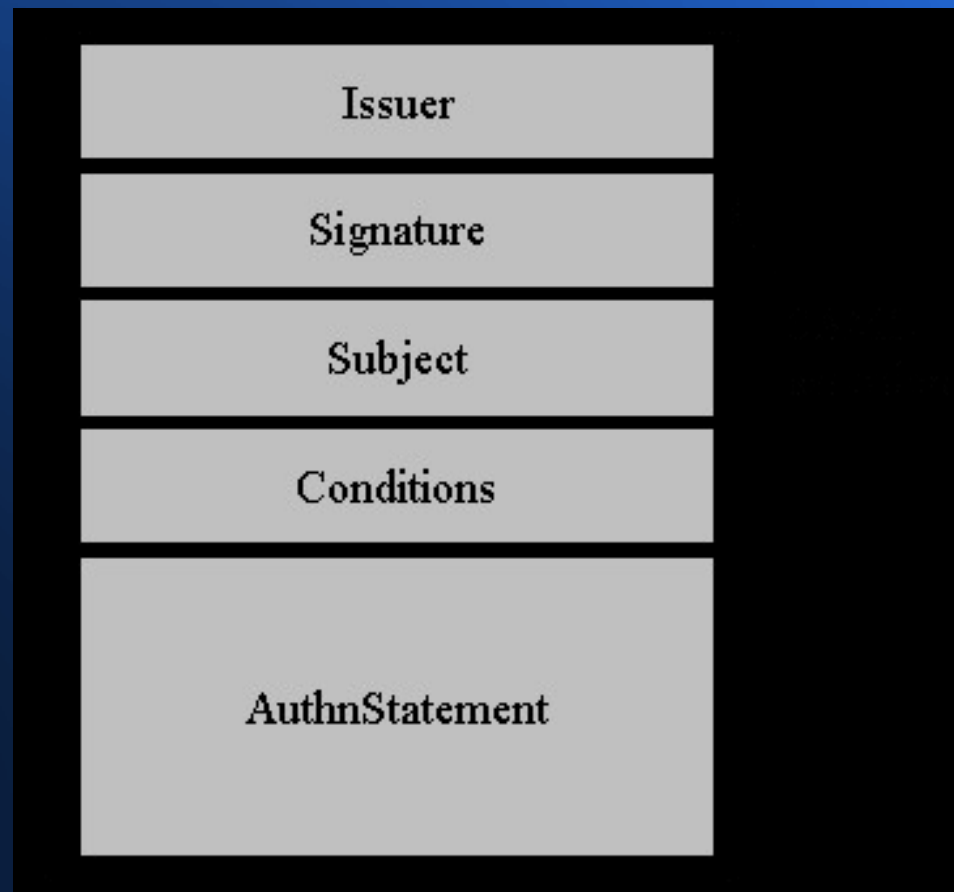
SAML History

- Security Assertion Markup Language
- SAML 1.0 developed through OASIS in 2002
- SAML 2.0 evolved taking input from Liberty Alliance's Identity Federation Framework and higher education's Shibboleth Initiative
- SAML 2.0 is mature (finished in 2005) with much of the new work on specific profiles

SAML Components

- Actors: SP, IdP and User Agent (typically browser)
- Message Core (Assertions, etc.)
- Protocols (AuthnRequest, more)
- Profiles (SSO, SLO, more)
- Bindings (HTTP POST, SOAP Artifact, etc.)
- Metadata (Deployment Description)

SAML Assertion



SAML – Single Sign One

- User Presents Credentials to Identity Authority
- Identity Authority Makes Assertions of the User
- Service Provider Consumes User Assertions and Grants Service based on User Attributes and Identity Assurance
- User Reuses Assertion with Multiple Service Providers

Other Use Case for SAML

- Single Logoff
 - Simultaneous Logout of All Service Provider Sessions
- Attribute Statements
 - Assertion Makes Statement of User's Attribute Status
 - Example: Kyle Has Admin Privileges

SAML Deployment

- Many Government Deployments: US, Canada, France, Denmark, New Zealand
 - GSA and International eGov Profile
- Shibboleth for High Education System
- Financial and Banking
- Google and other Web 2.0 Work

Value for Utilities and SmartGrid

- Evolution of Electric Grid to Smart Grid Means Becoming an Information Network
- Needs ID Management Just Like Other Information Networks
- Specific Industry Use Cases
 - Engineer Connecting to Different Substations
 - Smart Meters Communicating with Utilities

Recommendations for UtiliSec

- Familiarize with SAML and other Identity Management Initiatives
- Profiling for Unique Needs of Utilities and Energy Actors
- Certified Products

Questions