Security and Privacy for the Smart Grid

James Bryce Clark, OASIS
Robert Griffin, RSA
Hal Lockhart, Oracle
Agenda

• Security and privacy for the Smart Grid
• Key management standards for the Smart Grid
• Authentication and authorization standards for the Smart Grid
OASIS Standards to be Described

- **SAML**: Security Assertion Markup Language
  - A framework for the exchange of security-related information between trusting parties
  - The key standard for federated identity systems
  - Widely used today for cross-domain single sign-on

- **XACML**: eXtensible Access Control Markup Language
  - Language for expressing Access Control Policies
  - Also defines Network Req/Resp Protocol for Access decisions
  - Technology and domain-specific profiles

- **SAML 2.0 & XACML 2.0** are also ITU-T Recommendations
SAML assertions

- Assertions are declarations of fact, according to a trusted party
- XML Format
- SAML defines assertions about:
  - Authentication
  - Attribute
  - Authorization decision
- SAML can be extended to express other types of facts
- Assertions can be digitally signed and/or encrypted
- All SAML assertions have the same header info
SAML Architectural Entities

- Identity-attesting entities
- Identity Provider (IdP)
- Service Provider (SP)
- Identity-relying entities
- Identity-wielding entities
- User

Identity data
SAML components and how they relate to each other

Profiles
Combinations of assertions, protocols, and bindings to support a defined use case (also attribute profiles)

Bindings
Mappings of SAML protocols onto standard messaging and communication protocols

Protocols
Requests and responses for obtaining assertions and doing identity management

Assertions
Authentication, attribute, and entitlement information

Authentication Context
Detailed data on types and strengths of authentication

Metadata
Configuration data for identity and service data providers
SAML protocol for getting assertions

- Asserting Party
- Request for Assertion of Certain Type
- SAML
- Response Assertion
- Relying Party
SAML Features

- Multiple Web SSO Profiles
- Robust identity federation and management
- Identity provider discovery
- Basic session management and global logout
- Fine-grained description of authentication mechanisms
- Standard Attribute Profiles
- Metadata for simplified configuration
- Federation with Privacy protections
- Name Identifier Update Protocol
SAML in Web Services Security (WSS)

- Provides protection of SOAP messages
- SOAP header element `<Security>`
- Digital signatures and encryption
- Greater flexibility than SSL/TLS
- Supports multiple Security Token types
  - Username/password
  - Binary: X.509 and Kerberos
  - XML: SAML with or without keys
Additional SAML Profiles - 1

• Metadata Profiles
• Third-Party Requests
• Protocol Requesting Authentication Context
• Shared Credentials
• Challenge/Response Authentication
• X.500/LDAP/X.509 Profiles
• Simplified Digital Signatures
• Identity Provider Discovery Service Protocol
• Kerberos Profiles
• XSPA (Healthcare) Profile
• Delegation Restriction
• SSL/TLS Profiles
• Identity Assurance
What is XACML?

• XML language for access control
• Coarse or fine-grained
• Extremely powerful evaluation logic
• Superset of Permissions, ACLs, RBAC, etc
• Ability to use any available information
• Scales from PDA to Internet
• Federated policy administration
Powerful Policy Expression

• “Anyone can use web servers with the ‘spare’ property between 12:00 AM and 4:00 AM”
• “Salespeople can create orders, but if the total cost is greater that $1M, a supervisor must approve”
• “Anyone view their own 401K information, but nobody else’s”
• “The print formatting service can access printers and temporary storage on behalf of any user with the print attribute”
• “The primary physician can have any of her patients’ medical records sent to a specialist in the same practice.”
XACML Benefits

• Standard Policy Language
  – Investment protection
  – Skills reuse

• Leverage XML tools

• Policy not in application code
  – Reduce cost of changes
  – Consistent application
  – Enable audit
XACML Architecture
XACML Current Status

• XACML 2.0 OASIS Standard – Feb 2005
• XACML 3.0 In progress
  – Core & base profiles currently in 2nd Public Review
    • Administration/delegation {New}
    • Hierarchical resource {Enhanced}
    • Multiple resource {Enhanced}
    • SAML {Enhanced}
    • Digital Signature
    • Privacy
    • RBAC
  – Additional profiles under development
    • XSPA, Obligation families, Export Compliance, Policy Distribution, Metadata, WS-XACML
• OGC GeoXACML Standard Profiles and Extends XACML
OpenAZ Open Source Project

• AzAPI – API for requesting access decisions
  – Not specified by XACML Standard
  – Multiple languages (Java & C++ so far)
  – Enable full power of XACML

• Attribute Manifest Format (AMF)
  – Specifies attributes needed for access decision
  – Additional attribute type information for tools

• Goal is to provide ready to use code examples
Authorization API Benefits

• Needed for call to local PDP
  – Local PDP required for low latency calls
  – Inefficient to serialize data to and from XML
  – XML form not required by the standard

• Also useful to have standard API for remote requests
  – Common code to build message

• API can be used over legacy authorization schemes
  – JAAC, proprietary, etc.
  – Facilitates deployment: Application 1st or Infrastructure 1st
The Input Attributes Problem

- XACML Policies operate on data provided
- Only PDP sees/evaluates policies
- What attributes should be provided?
- Where can attributes be obtained from?
- How can the proper instance value be obtained?
Attribute Manifest File

• File in XML format identifies attributes to be added to Request Context
• Name of Attribute, Issuer, datatype, location, access method, other attribute to use as key
• Not all fields may be present
• Three usecases:
  – PDP advertizes required attributes
  – PIPs are configured to add attributes to Request Context
  – Policy authoring tools use attribute name & format
For More Information

- OASIS Security Services Technical Committee  
  – http://www.oasis-open.org/committees/security
- OASIS XACML Technical Committee  
  – http://www.oasis-open.org/committees/xacml
- OpenAZ Open Source Project  
  – http://www.openliberty.org/wiki/index.php/Main_Page#OpenAz
Questions?

Jamie.Clark@oasis-open.org
Robert.Griffin@rsa.com
Hal Lockhart@oracle.com