Standardization of Entity Authentication Assurance

5th ETSI Security Workshop
20-22 January 2010
ETSI, Sophia Antipolis, France

Erika McCallister, Esq., CIPP/G
Computer Scientist, Computer Security Division
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
Acting Editor, ISO/IEC 29115
erika.mccallister@nist.gov
Agenda

- Introduction to ISO/IEC 29115 | ITU-T X.eaa
- Importance of the Standard
- U.S. Government Case Study
  - Overview of Problem and Proposed Solution
  - National Institutes of Health Pilot Study
- Overview of ISO/IEC 29115 | ITU-T X.eaa
  - Important Points
  - Scope
  - Overview of Contents
- Applicability to Other Contexts

Disclaimer: Any mention of commercial products within this presentation is for informational purposes only; it does not imply recommendation or endorsement by the U.S. Department of Commerce (NIST).
Introduction

- **Entity Authentication Assurance Framework***
  - Joint work of ISO JTC1/SC 27/WG5 and ITU-T SG 17/Q.10
  - Expected to reach Committee Draft status this year
- Standardizes **four** Levels of Assurance (LoAs) to promote trust, improve interoperability, and facilitate identity federation across organizations and borders

* Pending approval to add “Framework” to existing title.
Why Is This Standard Important?

- Provides a consistent basis for trust
- Promotes identity federation
- Helps organizations make informed decisions
- Enables credential re-use in different contexts
- Promotes efficiency and reduces costs
- Enables cross-organization and cross-border services
- Provides framework for further standardization
U.S. Government Case Study: Government to Citizen Interactions

Pilot Study:
National Institutes of Health
U.S. Department of Health and Human Services
U.S. Government Case Study:
The Problem

- Most U.S. government agencies want to offer more online applications to citizens:
  - Research, grant proposals, taxes, benefits, data sharing
- Authentication is a large barrier to deployment:
  - There is no universal citizen credential
  - Application-specific credentials are difficult and expensive:
    - Identity proofing
    - Forgotten passwords from infrequent usage
    - Help desks and other maintenance overhead
    - Multiple collections of personally identifiable information (PII)
U.S. Government Case Study: The Proposed Solution

- Government agencies can act as the Relying Party (RP) rather than the Identity Provider (IdP) and accept credentials issued by “trusted” external organizations.
- Based on NIST Special Publication 800-63, the U.S. government developed a Trust Framework Adoption Process, which defines IdP requirements for the LoAs.
  - Started an IdP certification program based on the Trust Framework.
- The U.S. government is currently running pilot studies to use open standards credentials from several certified IdPs.
National Institutes of Health (NIH): Pilot Study

- NIH is the primary agency for conducting and supporting medical research
  - Requires authentication of over 35,000 external researchers from various hospitals, universities, and other governmental bodies
- Using the Trust Framework, NIH has started a pilot study to enable the use of OpenIDs and Information Cards issued by external IdPs (e.g., Google, PayPal, Yahoo) for NIH applications
NIH demonstrated the benefits of standardized LoAs:
- Many types of credentials issued by multiple IdPs can be used for a single application
- Increased user flexibility by providing choice of IdPs and not requiring a pre-existing relationship with NIH
- Trust in the technical and organization processes of the IdPs
- Reduced costs to NIH

The pilot study is a small-scale example of the potential benefits of ISO/IEC 29115 | ITU-T X.eaa
ISO/IEC 29115 | ITU-T X.eaa
Entity Authentication Assurance Framework

An Overview
Important Points

- The standard brings together existing work in this area and will not “re-invent the wheel”:
  - Kantara Initiative, ITU-T, NIST standards efforts
  - New Zealand, Australian, U.S., European, and Canadian e-government efforts
  - EU research efforts (STORK, IDABC, etc.)
- There is an emerging global consensus on four levels
- There is alignment with existing industry and government standards (e.g., Kantara Initiative)
- The 4 LoAs can be mapped to other entity authentication schemes (e.g., InCommon)
Scope*

- ISO/IEC 29115 | ITU-T X.eaa provides a framework for managing entity authentication assurance in a given context. In particular, it:
  - specifies four levels of entity authentication assurance;
  - specifies criteria and guidelines for each of the four levels of entity authentication assurance;
  - provides guidance concerning controls that should be used to mitigate authentication threats;
  - provides guidance for mapping the four levels of assurance to other authentication assurance schemes;
  - provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

* Pending approval to change existing scope.
Structure and Contents

- Four Levels of Assurance
- Entity Authentication Assurance Framework
- Management and Organizational Considerations
- Threats Based on Framework Components
- Required Controls for Each LoA
- Privacy and Protection of PII
- Operational Service Assurance Criteria
## 4 Levels of Assurance

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Low</td>
<td>Little or no confidence in the asserted identity</td>
</tr>
<tr>
<td>2 - Medium</td>
<td>Some confidence in the asserted identity</td>
</tr>
<tr>
<td>3 - High</td>
<td>High confidence in the asserted identity</td>
</tr>
<tr>
<td>4 – Very High</td>
<td>Very high confidence in the asserted identity</td>
</tr>
</tbody>
</table>
EAA Framework Overview

- **Authorization**
  - LoA Selection
  - Risk Assessment
  - Rights, Access Controls, etc.

- **Usage**
  - Authentication

- **Enrollment**
  - Proofing
  - Verification
  - Registration

- **Record-Keeping**

- **Credential Management**
  - Binding
  - Revocation
  - Issuance

- Scope boundary of this standard
Applicability to Other Contexts

- “A Roadmap for a Pan-European eIDM Framework by 2010” states that authentication levels are a building block for European eID federation and requires:
  - A definition of the authentication levels on a European level, along with the requirements demanded at each level
  - A mapping of existing authentication mechanisms in the Member States to a specific level, based on their conformity to the definitions above
  - An autonomous decision by the Member States regarding the authentication level required for each e-government service

- ISO/IEC 29115 | ITU-T X.eaa could help in meeting these objectives
Questions?

- For additional information:
  - **ISO Acting Editor**
    - Erika McCallister – erika.mccallister@nist.gov
  - **ITU-T Editor**
    - Richard Brackney - rcbrack@verizon.net
References

- Federated Authentication at NIH, Slides prepared by Debbie Bucci, November 2009.