Higher Assurance Authentication for the Enablement of Federated Online Trust

Abbie Barbir, PhD
ITU-T Study Group 17
Rapporteur, Identity Management
Abbie.Barbir@ties.itu.int
Scope

- Overview of International Telecommunication Union (ITU-T) Study Group 17 (SG 17)
- Overview of Entity Authentication Assurance
- Enhancing Cybersecurity through Open Trust Frameworks
- Some Legal Concerns
- Conclusions
ITU-T Overview

History

- Established 17 May 1865
- CCIF and CCITT formed in 1924 and 1925, merged into CCITT in 1956, became ITU-T in 1992
- Decisions by consensus (voting almost never occurs)
- Participation through national Government channels
- Telecom does not mean that focus is only on Telecom
M i s s i o n  a n d  L e g a l  S t a t u s

M i s s i o n

• s t u d y  t e c h n i c a l ,  o p e r a t i n g  a n d  t a r i f f  q u e s t i o n s  a n d  i s s u e  n o n - b i n d i n g  i n t e r n a t i o n a l  s t a n d a r d s  t o  e n s u r e  c o m p a t i b i l i t y  o f  s t a n d a r d s  o n  w o r l d w i d e

L e g a l  S t a t u s

• U N  s p e c i a l i z e d  a g e n c y
• L e g a l  b a s e :  C o n s t i t u t i o n  a n d  C o n v e n t i o n ;  h a v e  t r e a t y  s t a t u s  a m o n g  t h e  s i g n a t o r y  s t a t e s
• 1 9 2  U N  M e m b e r  S t a t e s  a r e  s i g n a t o r y  m e m b e r s
• A p p r o x .  7 0 0  S e c t o r  M e m b e r s  ( o p e r a t o r s ,  m a n u f a c t u r e r s ,  e t c . )
ITU-T Structure

Workshops, seminars, symposiums, ...

WSA
World Telecommunication Standardization Assembly

TSA G

JCA
Promo.

GSI

WP
WP
WP
WP

SG

Question: Develop Recommendations

Regional group

Flagship group

IPR
<table>
<thead>
<tr>
<th>Study groups (2009-2012)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SG 2</strong></td>
</tr>
<tr>
<td><strong>SG 3</strong></td>
</tr>
<tr>
<td><strong>SG 5</strong></td>
</tr>
<tr>
<td><strong>SG 9</strong></td>
</tr>
<tr>
<td><strong>SG 11</strong></td>
</tr>
<tr>
<td><strong>SG 12</strong></td>
</tr>
<tr>
<td><strong>SG 13</strong></td>
</tr>
<tr>
<td><strong>SG 15</strong></td>
</tr>
<tr>
<td><strong>SG 16</strong></td>
</tr>
<tr>
<td><strong>SG 17</strong></td>
</tr>
</tbody>
</table>
Q 10/17 collaboration on identity management

Advancing open standards for the information society
IdM Drivers

- For Financials
- Meeting customer needs
  - Safe, secure
  - Simple, seamless, convenient access
  - Active customers
The threat: Cyber crime
Cyber crime losses are growing

FBI: Fraud losses 2001-09
Identity crime affects all sectors
Identity Management Drivers

Financial Institutions Identity Theft Drivers

- Laws, Regulations & Guidance
  - Regulatory Risk
    - Privacy
    - Information Protection
    - Anti-Money Laundering
    - FACT Act
    - FFIEC
    - Additional Legislation
  - Standards, Policies, & Programs
  - Reputation Risk
    - Consumer Focused
    - Consumer Protection Groups
    - Rising Rate of ID Theft
    - Market Volatility
    - Growth Through Relationships
  - Current Environment
  - Financial Impacts
    - Financial Risks
      - Credit Risk
        - Identity Theft/Fraud Losses
        - Customer Dissatisfaction
        - Fines, Penalties, Litigation
      - Third Party Risk
        - Suppliers
        - Privacy Breaches
        - Mass Compromises
    - Operational Risk
      - Privacy
      - Information Protection
      - Anti-Money Laundering
      - Supply Chain Management
      - Fraud
      - Returned Mail
    - Legal/Contractual Obligations
Q 1 0 f o c u s i s T o w a r d s

S t r o n g I d e n t i t y , P o r t a b l e R e p u t a t i o n a n d
E n h a n c e d T r u s t

N e e d f o r B e t t e r I d e n t i t y A s s u r a n c e

T e c h n o l o g y
S t a n d a r d s a n d
G u i d e l i n e s

B u s i n e s s a n d
P r i v a c y G u i d e l i n e s

A n E c o s y s t e m o f
I n t e r o p e r a b l e P r o d u c t s
& S e r v i c e s

I d e n t i t y A s s u r a n c e
F r a m e w o r k & A s s e s s o r s

A s s u r a n c e

L I B E R T Y A L L I A N C E
P R O J E C T
Q 10/17

Entity Authentication Assurance

- Joint work with ISO JTC 1/SC 27/WG 5 and ITU-T SG 17/Q 10

- Standardizes four Levels of Assurance (LoAs)
  - to promote trust,
  - improve interoperability, and
  - facilitate identity federation across organizations and borders
Why do the work?

- Provides a consistent basis for trust
- Promotes identity federation
- Enables credential re-use in different contexts
- Promotes efficiency and reduces costs
- Enables cross-organization and cross-border services
- Provides framework for further standardization
- Establishes foundation for liability and other legal aspects
- 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.)
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)
Possible Solutions

- Government agencies can act as the Relying Party (RP) rather than the Identity Provider (IdP) and accept credentials issued by "trusted" external organizations.

- Standard is used to develop Trust Framework Adoption Process, that defines IdSP requirements for the LoAs.
  - Started an IdP certification program based on the Trust Framework.

- NIH pilot studies to use open standards credentials from several certified IdPs.
ISO/IEC 29115 | ITU-T X. e a a p r o v i d e s a f r a m e w o r k f o r m a n a g i n g e n t i t y a u t h e n t i c a t i o n a s s u r a n c e i n a g i v e n c o n t e x t. I n p a r t i c u l a r, i t:

• s p e c i f i e s f o u r l e v e l s o f e n t i t y a u t h e n t i c a t i o n a s s u r a n c e;

• s p e c i f i e s c r i t e r i a a n d g u i d e l i n e s f o r e a c h o f t h e f o u r l e v e l s o f e n t i t y a u t h e n t i c a t i o n a s s u r a n c e;

• p r o v i d e s g u i d a n c e c o n c e r n i n g c o n t r o l s t h a t s h o u l d b e u s e d t o m i t i g a t e a u t h e n t i c a t i o n t h r e a t s;

• p r o v i d e s g u i d a n c e f o r m a p p i n g t h e f o u r l e v e l s o f a s s u r a n c e t o o t h e r a u t h e n t i c a t i o n a s s u r a n c e s c h e m e s;

• p r o v i d e s g u i d a n c e f o r e x c h a n g i n g t h e r e s u l t s o f a u t h e n t i c a t i o n t h a t a r e b a s e d o n t h e f o u r l e v e l s o f a s s u r a n c e.
S t r u c t u r e  a n d  C o n t e n t s

- Four Levels of Assurance
- Entity Authentication Assurance Framework
  - Human and non-human
- 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>
What consumers are willing to give up

- Move from anonymous to identity enabled
- Internet transactions are still anonymous or low trust
- Value transactions are widely identity based
- Enable Identity while protecting privacy (PII)
  - Isolation of Issuer and target Identity
  - Enable the right to forget
  - Identity dashboard for user to keep control identity
- Enable audit, accountability and policy enforcement
Some Implications

- Simplify the Task of Authentication
  - who are you (context based)

- Attributes
  - what are you
  - This is where the beef is

- Proof of validity
  - ID Source and/or Reputation

- Towards Open Identity Trust Frameworks

- Need better understanding of Legal Issues and liabilities

- How about consumer protection?
Current Basic “Trust Triangle”

- User has direct trust relationship with IDSP and RP
- How can the IDSP and RP trust each other?

* Source OIX
Where trust Frameworks Fit

Market Expansion & Adoption

Usability (User Experience Ceremonies)

Policy Interoperability (Trust Frameworks)

Technology Interoperability (Identity Protocols)

Hardware Devices (Security Capabilities)

* Source OIX
Open Identity Framework Model

Trust Community

Identity service providers

1

OIF Trust Framework Provider

2

Identity assessors & auditors

3

Dispute resolvers

4

Relying parties

5

User

Trust framework agreements

TOS agreements

* Source OIX
How Can UNCITRAL Help

- Identify possible legal issues and determine how they relate locally and internationally
- What are the liabilities of IdSP and RPs
- What are the legal requirements for trust among the participants
- How can this be enforced across international boundaries
Conclusions

- Strong Identity and higher assurance authentication is key for enabling online trust and enhancing Cybersecurity
  - Interoperable federated frameworks
  - Multiple methods
  - End-to-end identification
  - Higher-level authentication

- Need for better National and International understanding legal and assume liabilities and policies
Acknowledgments

- Some slides are based on presentation on X.eaa by the editor ISO editor Erika McCallister and the ITU-T Editor Richard Brackney
- Some slides are based on presentation on OIX by Don Thibeaux