

Sources of Authority Discussion

**Tao of Attributes
9/28/09**

Chris Loudon

Agenda

2 Discussions:

- ❑ Sources of Authority
 - delegation
- ❑ Levels of Assurance

Sources of Authority

What are the sources of Authority for Attributes?

- ❑ “Natural Authority”
 - Employer for employment
 - SSA for SSN
 - Department of Motor Vehicles for drivers license number
- ❑ “Proper Diligence”
 - Service provider checked appropriate sources, gathered appropriate evidence, etc
- ❑ “Trusted Administrator”
 - Administrator sets the role & “they ought to know”
 - Often used for delegation
 - “Superuser” grants access to Administrators, they set up others
- ❑ Others?

Sources of Authority

Issues

- ❑ What role does the subject have?
 - What if the SSA says you're dead?
 - Does the subject always reconcile with the source?
 - Can the subject reconcile with "Proper Diligence" authority?
- ❑ What do authorities bind attributes to?
 - Common name?
 - Authenticated Session?
 - Credential Identifier?
- ❑ Can Authorities delegate?
 - Do delegates necessarily inherit authority?

- ❑ Other Issues?

Sources of Authority

Needs & Tools

- ❑ How do you anchor attribute trust?
 - Common trust anchor for attributes and identity?
 - Different anchors for different namespaces?
- ❑ Do standards allow different authorities for attributes & identity?
 - Can the products do that?
- ❑ Example view from the RP...
 - Verify the identity claim & that the IDP is trusted
 - Find the attribute authority & request an attribute claim
 - Verify the attribute claim & that the authority is trusted for this claim
 - Verify these claims are bound to this session?
 - Verify this attribute is bound to this identity?
- ❑ Other Needs & Tools?

Agenda

2 Discussions:

- ✓ Sources of Authority
- Levels of Assurance

Levels of Assurance

Do we need Levels of Assurance for attributes?

2 sides to LOA:

- ❑ Assurance needed by the RP
- ❑ Assurance provided by the authority

Levels of Assurance

Assurance Needed by the RP

- ❑ Sometimes the attribute matters more than others
 - Convenience for the user “Welcome John”
 - Basis of Access Control
 - Attributes are often more important than identity...
 - All police officers can carry a gun
 - All “John Smith” can carry a gun
- ❑ How sure does the RP need to be in this situation?
 - Generally risk based
 - Specifically the risk of a false positive
 - This person is not really a police officer

Levels of Assurance

- Is M-04-04 Adoptable for Attributes?

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Levels of Assurance

What effects Assurance provided by the authority?

- ❑ Type of Authority
 - Natural versus Diligence versus Administrator
- ❑ Practices used to establish the attribute values
- ❑ Practices used to maintain the values
- ❑ Proper controls to protect the attribute database
 - Basic security controls for data integrity
 - Subject access controls?
- ❑ Trustworthiness of the bindings
 - Attribute bound to a common name?
 - Attribute bound to a session context?
- ❑ What Else?

Levels of Assurance

Needs & Tools

- ❑ Do we need an 800-63 equivalent?
- ❑ Maybe just best practices for Natural Authorities?
- ❑ Do we need an *AuthN Context* equivalent?

Agenda

2 Discussions:

- ✓ Sources of Authority
- ✓ Levels of Assurance