Levels of Assurance

OGF Activity

Michael Helm

ESnet/LBNL

27 Feb 2007

Goals

- What are levels of assurance?
- Introduce LoA activities just begun at OGF
- Test interest here – draw in co-authors for OGF documents/other activities

What Are Levels of Assurance?

Parse the phrase….

- Assurance – Assurance about what?

About identity – about trust assertions – about an authentication token &c

- Levels – Some “levels” are above/below others ➔ some better/worse than others (for what? to whom?)
- Implicit – levels represent a class; a bundle of attributes; perhaps attributes of some equivalence in value?

Examples of LoA

- LoA in Grids
  - IGTF Certificate Authority “profiles”
- LoA in US Government PKI
  - OMB definitions
  - NIST specifications

IGTF LoA

- “Classic” X.509 CA profile
  - Latest: http://www.eugridpma.org/guidelines/IGTF-AP-classic-20050930-4-0.html
  - Early: http://www.eugridpma.org/guidelines/CACG-minimum-requirements-v1.txt
  - Originally – one size fits all; over time has added features, become more precise (and restrictive)
  - Proposal to split – provide a profile with less government ID-based ID proofing, reduce face to face requirement
- SLCS (Short lived Certification Service) profile
  - Based on site ID management service

US Government Authentication LoA

- Reference URL's
  - OMB:
    - **OMB M-04-04**

http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

  - NIST
    - **NIST 800-63**

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

- Long history of evolution

  Ning Zhang at OGF mentioned the year 2000, but the idea was around in the mid -90's. Warwick Ford?

OMB Definition

- Level 1:

  Little or no confidence in the asserted identity's validity.
- Level 2:

  Some confidence in the asserted identity's validity.
- Level 3:

  High confidence in the asserted identity's validity.
- Level 4:

  Very high confidence in the asserted identity's validity.

➢ Important to read this whole document, including the risk assessment content and the advisory material.

OMB Definition (2)

Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as

1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and
2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

NIST 800-63

- Revised fairly regularly (annually?)
- **Level 1** – self assertion; no plaintext passwords on the network; assertions about identity are cryptographically authenticated, or obtained from a trusted provider thru trusted methods
- **Level 2** – add some identity proofing; eavesdropping, online guessing, replay prevented; assertions about claimants validated (rules)
- **Level 3** – 2 factor, proof of possession of private key, or OTP required ; validation of identity documents/process; add MITM protection
- **Level 4** – hardware token required; “All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.”

NIST 800-63 (2)

Table 1. Identity Proofing Requirements by Assurance Level

	In-Person	Remote
Level 2		
Basis for issuing credentials	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport)	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
RA actions	Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	• Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • Address confirmation and notification: a) Sends notice to an address of record confirmed in the records check or; b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or c) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.
Level 3		
Basis for issuing credentials	Possession of verified current primary Government Picture ID that contains applicant's picture and either address of	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number

NIST 800-63 (3)

	In-Person	Remote
	record or nationality (e.g. driver's license or passport)	(e.g., checking account, savings account, loan or credit card) with confirmation via records of both numbers.
RA actions	Inspects Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DoB. If ID is valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record	• Verifies information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. • Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Level 4		
Basis for issuing credentials	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application	Not Applicable
RA actions	• *Primary Photo ID:* Inspects Photo-ID and verify via the issuing government agency,	Not applicable

NIST 800-63 (4)

- That's 2/3 pages of the ID proofing section
- Also protocol requirements, mapping to other related infrastructure, threat model, &c
- Relationship to other Federal/US programs
  - Incommon (Shibboleth) has a set of levels
  - US Gov Fed Bridge PKI has ~5 levels
  - Similar … subtle differences/asynchrony

Relevance

- What LoA are appropriate for Grids?
- Is the concept useful? Have modern authorization concepts superceded it?
- What about interoperability?
- Do existing LoA standard cover things of interest to Grids (eg hosts, authorization, delegation)? [Ans: No, or poorly?]
- These issues are among those that motivated Ning Zhang to organize an LoA BOF at OGF-19

What Should Grid LoA Look Like?

- What are our relevant security use cases ?
- Existing debate in IGTF PMAs on related subjects
  - Meaning of/process behindhost & service certifications
  - Face to face proof of identity
  - Government ID vs project ID
- Surprise when IGTF tried to map onto US Fed PKI
  - The more rigorous IGTF classic X.509 CA profile doesn’t map to US Fed levels (or one could say, maps to the lowest possible level, with problems)

LoA Activites in OGF

BoF arrived at rough consensus for:

OGSA-AUTHN – issues related to protocol; delivery of LoA attributes; should be much interest in MSWG?

LOA-RG – Use cases, survey of existing LoA standards for relevance to Grids, examination of gaps in existing LoA, missing features

CAOPS – Either specification of levels, or application / utilization of levels - a little unclear

- Providing use cases, and discussing “bundling”, is a critically important activity – any contributors in the house?

LoA at OGF – Conclusion

- LoA RG leaders
  - Ning Zhang (nzhang@cs.man.ac.uk)
  - Yoshio Tanaka (yoshio.tanaka@aist.go.jp)
- OGSA-AUTHN (status?)
  - Alan Sill (Alan.Sill@ttu.edu)
- CAOPS WG

http://www.ogf.org/gf/group_info/view.php?group=caops-wg

- Need authors/contributors to a use-case paper