Smart Card Alliance

Assurance Levels Overview and Recommendations

This document briefly lays out an interpretation for the four assurance levels outlined in the Office of Management and Budget (OMB) M04-04, *E-Authentication Guidance for Federal Agencies*.[1]

OMB M04-04 states the following levels for authentication:

"2. Assurance Levels and Risk Assessments

2.1. Description of Assurance Levels

This guidance describes four identity authentication assurance levels for e-government transactions. 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. The four assurance levels are:

- *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"*

From this OMB guidance, the Smart Card Alliance interpretation and position on the definition of these levels follow.

Assurance Level 1

Level 1 appears to be positioned as an identifier[2] rather than an actual identity[3]. An identifier can be used to present information on a consistent basis and can be, but does not have to be, loosely associated with an individual. An identifier can therefore be anonymous or pseudo-anonymous in nature. A Level 1 identifier is likely to be some type of account and will consist of one or more elements (such as an email address and password). Examples of Level 1 identifiers include email addresses (e.g., Gmail, Yahoo, Hotmail) or usernames and passwords. Level 1 accounts may or may not be created with a person's actual name (e.g., WhiteKnight99@gmail.com). Although an email address is owned by an individual, or a group of individuals if shared, there is little way of identifying the person or persons behind the identifier.

GSA has recently endorsed OpenID as a valid Level 1 identifier. This approach allows one identifier to be associated with the Open ID account. However, an OpenID can be translated to different, consistent, repeatable, unique identifiers when using it to access other services, allowing an individual to be recognized when returning to a service over time, but preventing tracking across services. A Level 1 credential has little value and therefore presents doubt and risk that an individual cannot be held accountable for the information. In the case where traceability is needed, a legal vehicle may be needed to create a linkage to a real person.

[1] http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

[2] An identifier is a minimal set of information attributes which may or may not be directly attributable to an individual. An identifier is not required to disclose any personally identifiable information.

[3] An identity is a defined set of attributes which define an individual's claimed and verified identity information. An identity requires the inclusion of such items as the individual's name, credential expiry date, issuing authority, role, and affiliation.

A Level 1 identifier can be self-asserted by an individual and verification of the identifier is minimal.

Assurance Level 2

Level 2 assurance is provided when a secret token or key is memorized by one or more parties allowing a trusted relationship to exist, without the specific need for full identification. Knowing the shared secret enables an assertion of an identifier to another party (who also knows the shared secret) and enables a level of trust for establishing an interaction. Level 2 could be interpreted as a soft token and not require any specific hardware protection. Level 2 would not utilize PKI. SAML is an example of Level 2 assurance.

Assurance Level 3

Level 3 could be best described as an account-based credential with additional verification. An account number is used to register for services and uses a username and password. This account may be linked to a person’s actual identity, but the use of the account does not directly imply the known identity is actually present. An example is a mobile phone account. The information about the person responsible for account payment is on record with the telecommunications provider, but that person may not be using the phone at a particular time. A Level 3 identity would require some registration and enrollment with relying parties to reduce the risk of fraud. The addition of an out-of-band authentication channel (e.g., sending a one-time password to a registered user’s phone) can bring a higher degree of trust once the person is enrolled and verified.

A Level 3 identity can be self-asserted by an individual. To confirm the validity of the information in the context of usage, relying parties should undertake some verification of the identification information. Some enrollment is required and verification of the enrollment information is needed to confirm the claimed identity.

Level 3 is starting to be deployed to protect online accounts, such as personal online banking accounts and premium web site user account protection.

Assurance Level 4

Level 4 implies knowledge of a person’s identity with personal identifiable information (PII) required and present. The Level 4 credential is meant to hold an individual accountable for their access and actions. A Level 4 credential would be used in situations requiring knowledge of a person’s established identity as part of a transaction or interchange of information. For there to be a non-repudiable chain of trust, this credential must provide two or three factor authentication. Authentication factors are: "something you are" (e.g., biometric); "something you have" (e.g., token or smart card); "something you know" (e.g., PIN or password). A Level 4 credential would require a strong enrollment and identification verification process prior to the credential being issued to the individual requesting the credential. Level 4 credentials in use today include HSPD-12 Personal Identity Verification (PIV) cards and Department of Defense Common Access Cards (CAC). The use of a Level 4 credential would significantly reduce the risk of a fraudulent transaction, since the device has the ability to electronically authenticate both the rightful credential owner and the relying parties’ services.

A Level 4 identity must be enrolled and rigorously verified by the issuer prior to credential issuance and activation. The verification process will vary according to the issuer’s policy.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.