Levels of Assurance

What are levels of assurance?

Levels of assurance are an important part of the trust fabric of Tuakiri. Tuakiri participants use a framework to describe the level of assurance associated with an instance of authenticating a particular user. This framework allows an identity provider to indicate to a service provider how much trust is behind the authentication event. Service providers, based on their own needs and assessment of risks, determine what level of assurance they require in an authentication event in order to allow the user access.

The framework used within Tuakiri is based on the NIST Electronic Authentication Guideline – NIST SP 800-63-2. The NIST guideline forms the basis of many assurance frameworks used internationally and was selected with a view to being interoperable with other federations.

Within Tuakiri, assurance is separated into two concepts:

- The strength of the processes used to identify the user at the time of user registration. This is the concept of identity assurance and is indicated by the value asserted in the eduPersonAssurance attribute.
- The strength of the authentication method(s) used in this particular authentication instance. This is the concept of authentication assurance and is indicated by the value asserted in the AuthenticationMethod attribute.

While identity assurance (eduPersonAssurance) is a stable attribute associated with the user, authentication assurance (AuthenticationMethod) might be different each time a user logs in, depending on what method(s) they used to authenticate.

There are four levels of identity assurance in the framework, expressed as a value from 1 to 4. Likewise there are four levels of authentication assurance, expressed as a value from 1 to 4. The relying party – the service provider – determines what levels they require in order to allow access to their service. Level 1 will be sufficient for many service providers; however, some may require additional assurance, regarding identity, authentication strength, or both.

What do the different levels mean?

The following is a brief summary of the levels. For further details, please refer to NIST SP 800-63-2.

Level 1 – Identity assurance
There is no identity proofing requirement at this level. However, the fact that the user is able to authenticate to the identity provider gives some assurance. It means the identity provider has some relationship with the user because they have issued them a credential (username and password or cryptographic key).

Level 1 – Authentication assurance
This level allows a wide range of authentication technologies. For example, simple password challenge-response protocols are allowed. Successful authentication requires that the user prove through a secure authentication protocol that he or she controls the token (password). Plain text passwords or secrets are not transmitted across a network at Level 1. However, this level does not require cryptographic methods that block offline attacks by an eavesdropper. Any of the authentication methods accepted for Levels 2, 3, or 4 also satisfy Level 1.

Level 2 – Identity assurance
At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. Both in-person and remote registration are permitted. For in-person registration the applicant must be in possession of a primary government photo ID (such as a driver's license or passport). For remote registration, the applicant submits the references of and attests to current possession of at least one primary government photo ID and a second form of identification. The applicant must provide to the registration authority at a minimum their name, date of birth, and current address or personal telephone number.

Level 2 – Authentication assurance
Level 2 provides single factor remote network authentication. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented. Passwords must be strong.

Level 3 – Identity assurance
At this level, identity proofing procedures require verification of identifying materials and information. Both in-person and remote registration are permitted. Level 3 requires the same evidence for issuing credentials as Level 2; however, at this level verification of the documents or references through record checks is required.

Level 3 – Authentication assurance
Level 3 authentication is based on proof of possession of a cryptographic key using a cryptographic protocol. Three kinds of tokens may be used to meet Level 3 requirements: "soft" cryptographic token, "hard" token, or "one-time password" device token. Level 3 authentication assurance requires cryptographic strength mechanisms that protect the primary authentication token against compromise by eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. Level 3 also requires two factor authentication; in addition to the key, the user must employ a password or biometric to activate the key.

Level 4 – Identity assurance
Remote registration is not permitted at this level. The applicant must appear in person before the registration officer. Presentation and verification of two independent ID documents or accounts is required, meeting the requirements of Level 3, one of which must be a current primary government photo ID that contains the applicant's picture, and either address of record or nationality (e.g. driver's license or passport). A new recording of a biometric of the applicant at the time of application is also required to ensure the applicant cannot repudiate the application.

Level 4 – Authentication assurance
Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.

My organisation can only meet requirements for Level 1 at this time. Does that mean we’re not compliant with the Rules for Participants?

No. The purpose of the framework is to allow your organisation to describe the processes you have used to identify and authenticate users, using a standard vocabulary. Service providers can then use this information to determine whether to allow the user access to their service. If you only meet the requirements for Level 1, that is fine. However, it does mean that your users will not be able to access services that require higher levels.

If some of our users need to access a service that requires Level 2, do we have to meet Level 2 requirements for all of our users?

No. If only a small number of your users need to access Level 2 services – some research staff members, for example – you can meet the Level 2 requirements for those users only and continue to assert a Level 1 for the rest of your users.

Where can I find more information?

NIST SP 800-63-2 is available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf. This document is the basis of Tuakiri’s levels of assurance framework.

The specification for the eduPersonAssurance and AuthenticationMethod attributes is described in the auEduPerson Definition and Attribute Vocabulary.