DRAFT
InCommon MFA Profile

(DRAFT - 4/14/2016)

Identifier: `http://id.incommon.org/assurance/mfa`
Date Approved: TBD

Purpose

This InCommon Multifactor Authentication Profile specifies requirements that an authentication event must meet in order to communicate that multi-factor authentication was used. It also defines a SAML authentication context for expressing this in SAML.

The “InCommon MFA” Authentication Context can be used by Service Providers (SPs) to request that Identity Providers (IdPs) perform multi-factor authentication, as defined below, and by IdPs to notify SPs that multi-factor authentication has been performed.

Use in SAML

In a SAML assertion, compliance can be communicated by asserting the InCommon Multifactor Authentication AuthnContextClassRef: `http://id.incommon.org/assurance/mfa`

[ToDo: Define the formal AuthnContextClassRef]

Scope

It should be noted that there are other assurance-related issues, such as identity proofing and registration, that may be of concern to SPs when authenticating users. This profile, however, does not establish any requirements for those other issues; they must be resolved through other profiles or “out of band” agreements.

Criteria

Compliance with this profile may be asserted only when the following criteria are met:

- The authentication of the user's current session used a combination of at least two of the three distinct types of factors defined in NIST Special Publication 800-63-2: Electronic Authentication Guideline, section 3, *Definitions and Abbreviations* (something you *know*, something you *have*, something you *are*).
- The factors must be independent, in that access to one factor must not by itself grant access to other factors.
- The combination of the factors mitigates single-factor-only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.