# Multi-Factor Authentication (MFA) Interoperability Profile Working Group Final Report

Submitted by: Karen Herrington, Chair
June 15, 2016

## ● Contributors

Karen Herrington, Chair
David Walker
Eric Goodman
Jim Jokl
Scott Cantor

## ● Executive Summary

The MFA Interoperability Profile Working Group was formed by the InCommon Assurance Advisory Committee (AAC) and charged with creating an interoperability profile that would enable the community to leverage Multi-Factor Authentication (MFA) provided by an InCommon Identity Provider (IdP) by allowing Service Providers (SPs) to rely on a standard syntax and semantics regarding MFA.

Development of the InCommon MFA profile was guided by a desire to produce a basic multi-factor profile that could be widely adopted with relative ease. Other guiding principles that were communicated to the group included:

1. The profile should be constrained to address the articulated need for distributed MFA.
2. The ability to implement with current MFA and Federation technology should be a core design constraint.
3. Support for this capability should be exposed in the Federation Metadata.

## ● Deliverables

The deliverables produced by the MFA Interoperability Group included the following:

1. Use cases that motivated the work of the group.
2. List of widely deployed MFA technologies in Higher Education that were considered in scope for the profile.
3. The MFA Interoperability Profile.
4. An InCommon Base Level Profile.
5. A Usage Guidance document.
6. A recommended scope and plan for adoption of the profile.
7. A final report from the group.

## Scope

The work of the MFA Interoperability Group focused on the premise that authenticating with only passwords is no longer sufficient in a modern world full of phishing threats. Therefore, the InCommon MFA Profile was defined in terms of mitigating the single-factor-only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor as defined in NIST 800-63-2 Section 6.2.1. Two tables were produced that are intended to aid in the selection of acceptable multi-factor authentication technologies for use with the profile. Table 1 describes commonly used authentication factors and summarizes their resistance to common threats. Table 2 summarizes Authentication Types or Groups of Types which meet the needs of authentication profiles.

The InCommon MFA Profile limits its considerations to the authentication event. Assurance-related practices and processes, such as identity proofing and registration, were determined to be out of scope for this profile. While it is understood that assurance-related issues may be of concern to SPs when authenticating users, these issues must be resolved through other profiles or "out of band" agreements.

Also out of scope for this profile were issues related to accessibility of multi-factor solutions. For accessibility guidance, as well as general guidance about deploying multi-factor authentication, please refer to the work of MFA Cohortium at https://wiki.cohortium.internet2.edu.

## Use Cases

Multiple use cases were considered at the start of this work, including:

- InCommon Certificate Manager
- InCommon Federation Manager
- LIGO
- Federal services
- Enterprise systems, such as WorkDay, that are shared among multiple campuses
- Intra-campus use cases

In all cases, the Service Provider has a requirement for some or all of its users to use MFA. This may be a requirement to use any part of the service, or it may a requirement for certain types of transactions within the service. For the former, the Service Provider will request MFA and only MFA, but for the latter the Service Provider might request MFA but accept anything else. For this reason, the work group has defined two profiles, one to allow specification of MFA, and the other to specify "anything else."

Other lessons learned from the use cases include:

- A Service Provider's request for MFA (and the Identity Provider's response) will typically be made through SAML's authnContext mechanism but can be arranged out of band through special Identity Provider configuration.
- The MFA profile, by itself, is not sufficient for all use cases, most notably the InCommon Federation Manager. Other issues, such as strong identity proofing, may also need to be addressed.

## ● Implementation of Profile

The InCommon MFA Profile specifies the method for communicating multi-factor authentication as a SAML authentication context *http://id.incommon.org/assurance/mfa*. The authentication context may be used by Service Providers (SPs) to request that Identity Providers (IdPs) perform multi-factor authentication and by IdPs to notify SPs that multi-factor authentication has been performed. Criteria that must be met in order to assert the authentication context are identified in the profile.

A Usage Guidance document was created to provide advice on the use of the profile in practice. This document explains in greater detail the risks that must be mitigated in order to assert MFA, provides guidance about what constitutes an acceptable "second factor" and relates SAML-specific guidance for use with the profile.

A second profile, called simply the InCommon Base Level Profile and not specifically related to Multi-Factor Authentication, was also created by the working group. The intent of this profile was to establish a base over which other profiles could be defined. It was also intended to be used by SPs in conjunction with other profiles in SAML requests to indicate that a higher level profile is preferred, but base level is acceptable and to provide a value for systems to affirmatively assert when authentication is done successfully but without MFA (necessarily) being used.

## ● Recommendations

It became evident as the group discussed various use cases that the MFA profile being created would not be strong enough to satisfy some of the use cases. It is therefore the recommendation of the group that future work be done to create a method for asserting MFA that carries a higher level of assurance, likely coupled with corresponding Identity Proofing requirements.

It is likely that future profiles will be defined to address other aspects of assurance, such as identity proofing. We recommend further investigation into how multiple profiles can be composed to allow, for example, a Service Provider to request multifactor authentication and strong identity proofing, and for an Identity Provider to respond to such a request.

**Recommendations for Adoption**

- The group did not reach consensus on whether defining an entity attribute to expose support for (or certification to assert) the MFA Profile through federation metadata has sufficient value to outweigh the cost of implementing such an attribute by all participating federations. Requiring an entity attribute also has the potential to be a barrier to adoption by IdP operators. The group saw the following potential uses for such an attribute:
    - *As a filter for constructing an SP's discovery interface, when the SP will not accept authentication that does not meet the criteria of the InCommon MFA Profile*. This was probably the strongest argument for the entity category that was received during the community comment period. It is not clear, however, that there are SPs that would require federated MFA (and so would not want to be discovered), without providing their own mitigation for authentication risks.
    - *As evidence to increase an SP operator's confidence in MFA authentication performed by the IdP*. This was also mentioned in the community comments. Federations already have policies requiring IdPs to provide accurate information, however, so the actual increase in confidence is questionable. Also, depending on the process established for certifying an IdP, this could be a significant barrier to adoption.
    - *To provide information that can be used by an SP to tailor its authentication flow to the capabilities of the IdP*. The group did not feel that the one-time saving in SP development effort that could be achieved, or the small network overhead that could be avoided, warranted the cost of deploying the entity attribute throughout multiple federations.

  The group has drafted an MFA Support Entity Category, but leaves the decision of whether and how to deploy that entity category to the AAC. The options are:
    1. Do not deploy the entity category.
    2. Deploy the entity category by providing a process (*e.g.*, a check box in an online tool provided by federations) that allows IdP Operators to self-certify their support for the MFA Profile.
    3. Deploy the entity category with a process in which the federation verifies the IdP Operator's compliance with the MFA Profile. (The group does not recommend this option.)
- Independent of the decision of whether to expose support for the MFA Profile in metadata, the group recommends that InCommon implement some method of tracking adoption of the profile.
- Documentation should be developed (or modified) to provide information about the interrelationship among the four profiles supported by InCommon (Bronze, Silver, MFA, and Base Level). That information should be linked at the URLs used to identify the profiles.
- These profiles are likely to have significance internationally. Prior to release, we suggest that InCommon consult with REFEDS to determine if/how the profiles can be made available to all federations participating in eduGAIN.