REFEDS MFA Profile v1.1

REFEDS Community Chat
October 6, 2022

What is REFEDS MFA Profile?

REFEDS Multi-Factor Authentication (MFA) Profile defines a standard signal to request MFA and to respond to such a request in a federated authentication transaction. It outlines requirements that an authentication event must meet in order to communicate the usage of MFA.

These requirements convey a higher *quality of authentication* than ordinary password authentication, i.e., the authentication is sufficiently secure and trustworthy such that the subject can be strongly associated with the information presented about them.

Charter (and constraints) for this arc of work

- Stay true to the original REFEDS MFA Profile's intent.
- Make Profile clearer:
  - easier to understand and to adopt.
  - reduce ambiguity so that integrating parties (IdP and RP) have consistent understanding and expectations.
- Is backwards-compatible "on the wire" with original Profile - no new identifier.
- Time is of the essence

* REFEDS MFA Subgroup recommendations to update the Profile: MFA Profile Priorities

Contributors to REFEDS MFA Profile v1.1

Fredrik Domeij
SWAMID
(REFEDS MFA Group Chair)

Scott Cantor
The University of Ohio

Albert Wu
Internet2 / InCommon

Alan Buxey
UNiDAYS

Eric Goodman
University of California,
Office of the President

David Bantz
University of Alaska

Dana Watanabe
UC Irvine

Jon Agland
JISC

Chris Phillips
CANARIE

Björn Mattsson
SWAMID

Pavel Brousek
Jeffrey Crawford
Philip Smart
Rafal Lawrukiewicz
Uros Stevanovic
Francisco Jose
Christos Kanellopoulos
Alex Stuart

Sandeep Sathyaprased
Pavel Vyskocil
Sumit Nanda
Miroslav Milinovic
Marina Adomeit
Jule Ziegler
Franscisco Aragó

… and many others who have provided feedback, ideas, and assistance throughout…

Where did this come from? The journey to v1.1

NIH* announces REFEDS MFA support as an access requirement by Fall 2021.

Community questions and feedback indicate need to clarify REFEDS MFA use.

REFEDS Assurange Group convenes MFA Sub-group to develop implementation guidelines to help with REFEDS MFA adoption.

REFEDS Assurance Group directs the Sub-group to further develop a prioritised list of recommended updates and additions to the Profile.

REFEDS Assurance Group directs the Sub-group to update the Profile per recommendations.

MFA Sub-Group publishes updated REFEDS MFA FAQ and recommendations for further improvements.

MFA Sub-Group submits its recommendations: MFA Profile Priorities

REFEDS MFA Profile v1.1 development underway.

Community Chat!

* National Institute of Health - a US federal government agency. NIH is the largest biomedical research agency in the world.

Where are we on the road to publishing v1.1?

Governance convenes working group to update Profile.

Working group develops initial draft; undergoes limited reviews; revises draft.

Working group solicits additional (public) feedback and help with material / direction.

Candidate draft is formally submitted for public comment prior to publication.

Profile is published with governance endorsement.

We are here!

The editors want to know…

- Are we going in the right direction?
- Where do we need to do more?
- Where are we doing too much?

We need help with…

- Writing product-specific deployment guidance
- Identifying implementation implications, particularly when cross-referencing with existing REFEDS MFA deployments and any regional regulatory requirements

Why is this needed

- Some SPs need to ensure that their users are using strong authentication
  - Not just username/password
  - MFA is the most widely-adopted means of achieving this
- Common signalling and standards is better than individually negotiated agreements between SPs and IdPs

The editing process - where we are in the overall process

(and what we are looking for from you)

- The original profile has been updated and clarified
  - Some additional proposed rules/expectations have been added
  - OIDC-specific guidance has been added.

- Needs community review
  - Mostly to confirm the changes meet the expectations of the community
  - Does it satisfy the needs of SPs that would request REFEDS MFA?
  - Are there any undue implementation burdens on IdPs that will support REFEDS MFA?

Highlights 1

Existing profile (V1.0)

- **Introduction**
  - **The profile identifier, for SAML**
- **Syntax**
  - **Profile identifier**
  - **Note of its attribute when used in SAML**

New draft Profile (v1.1)

- **Introduction**
  - **Clarifications on purpose, limitations and included messaging protocols of the profile**
  - **Institution-specific MFA signalling guidance**
  - **Terms and definitions.**
- **Profile Identifier**
  - **Profile identifier for SAML and OIDC**
  - **Requirements for signalling this profile**
  - **Versioning of the identifier**

Highlights 2

Existing profile (V1.0)

- **Criteria**
  - **Short description of multiple factors (ITU-T X.1254)**
  - **independent factors**
  - **mitigation of single-factor only risks**

New draft Profile (v1.1)

- **Authentication Requirements - more in-depth requirements for**
  - **Multiple factors including examples**
  - **Factor Independence**
    - **recover/replace/add factors,**
    - **risk mitigation and guidance**
  - **Validity Lifetime**
    - **all factors challenged w/in 12 hours**
    - **“Remember me” does not satisfy**
  - **Failure Modes**
    - **No IdP exceptions (e.g., no fail open)**
    - **All authentication performed per requirements, including guidance of internal use of the profile**

Highlights 3

Existing profile (V1.0)

SAML-bindings

- **Only mentioned in Syntax section**

New draft Profile (v1.1)

Protocol Specific Bindings

- **SAML**
  - **SAML signalling and syntax (w/examples)**
  - **Signalling Time of Authentication**
  - **Discouraging multiple contexts in requests**
  - **Discouraging inexact context comparison**
  - **Discouraging use of forced authentication**
  - **Error handling recommendations**
  - **Examples (XML)**

Highlights 4

Existing profile (V1.0)

OIDC-bindings

- **Not supported**

New draft Profile (v1.1)

Protocol Specific Bindings

- **OIDC**
  - **OIDC Signalling and syntax (w/examples)**
  - **Discouraging *acr_values* and *amr* claim**
  - **Signalling Time of Authentication**
  - **Discouraging multiple identifiers in requests**
  - **Error handling recommendations**
  - **Examples (JSON)**

Operational implications

- Self-service account reset implementation is not constrained by the profile
  - Other than: *Using a single factor alone to reset the other factor is insufficient*.
  - Applies to resetting password OR other factor
  - Existing reset mechanisms may not meet this expectation.
  - If self-service password reset is used keep in mind that you need to address this.

- If doing MFA, you likely want your own “MFA” AuthenticationContext as a companion to REFEDS MFA
  - Allows best adherence to REFEDS MFA calibre and possible/(very much expected) dilution/alteration for site-specific needs

Things we’re thinking about

- Governance and oversight
  - How do we (the community) keep the profile current?
  - How do new versions (if any) impact existing usage?

- New technology assessments
  - Existing technology diminishing in qualities
    - E.g. How do we convey that X is no longer viable as a factor?

Thank you for attending!

- Review and comment on this updated REFEDS MFA profile
  - Don’t just tell us what’s wrong… tell us what would be right!

- Support/promote REFEDS MFA in your Federation/IdP/SP

- Question and Answer