Dealing with Institution MFA Policies

- How should “Exceptions” to MFA Policy be handled?
- Is the Profile suitable for local enterprise use?
- Is SMS acceptable as a second factor?
- Is IP network-restriction based access valid “MFA”?

How should “Exceptions” to MFA Policy be handled?

The REFEDS MFA Profile is designed for inter-institution federated authentication. External organizations will not have agreed to any internal policy decisions regarding exceptions and MFA grace periods. Therefore you MUST NOT apply those policies (such as fail-open, special exemptions, unsuitable remember-me values, etc) when using REFEDS MFA Profile to signal that MFA has occurred. If you need to support local enterprise use cases, we recommend defining an alternate local AuthnContextClassRef value for use in local SSO use cases instead.

Is the Profile suitable for local enterprise use?

No. The REFEDS MFA Profile is designed for inter-institution federated authentication. Many institutions grant exceptions in its local MFA policies for reasons particular to that institution’s internal needs. External organizations will not have agreed to any internal policy decisions regarding exceptions and MFA grace periods. Therefore you MUST NOT apply those policies (such as fail-open, special exemptions, unsuitable remember-me values, etc) when using REFEDS MFA Profile to signal that MFA has occurred. If you need to support local enterprise use cases, we recommend defining an alternate local AuthnContextClassRef value for use in local SSO use cases instead.

Is SMS acceptable as a second factor?

The REFEDS MFA Profile does not prohibit SMS as an authentication factor. However, SMS as an authentication method has multiple known weaknesses. Many security experts consider it a weaker factor than other second factor methods.

Consult the InCommon MFA Interoperability Profile Working Group Analysis: MFA Technologies, Threats, and Usage

Is IP network-restriction based access valid “MFA”?

No. IP network-restriction based access is not considered a “MFA” factor in REFEDS MFA Profile.