National Identity Exchange Federation

Privacy Policy

Version 2.0

August 27, 2021

Table of Contents

1. Target Audience and Purpose

This document specifies technical privacy requirements for participants in the National Identity Exchange Federation (NIEF). The target audience includes technical representatives of organizations that intend to participate in NIEF. This document focuses only on issues of End User privacy for Federated Identity, Credential, and Access Management (Federated ICAM) transactions such as Single Sign-On (SSO).

2. References

Table 1 contains a list of references used within this document.

References	
Document ID	**Document Name and URL if Applicable**
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels

Table 1: References

3. Notation for Normative Content

This document contains both normative and non-normative content. Sections containing normative content are marked appropriately. In those sections, the key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are to be interpreted as described in [RFC 2119].

4. NIEF Privacy Policy Rules

NIEF participants are subject to the following rules regarding the protection of end-users' privacy during ICAM transactions.

1. **Run-Time Opt-In for Federated ICAM Transactions** – When participating in a Federated ICAM transaction, an organization MUST obtain positive confirmation from the End User before any End User information is transmitted to any partner organizations' systems. Confirmation MUST be obtained at "run-time" (just before the information is transmitted) and MUST enable the End-User to see each attribute that is to be transmitted to the partner system(s) as part of the opt-in process. Also, the organization SHOULD allow the End User to opt out of the transmission of individual attributes for each transaction.

2. **Minimal ICAM Attribute Release** – When transmitting ICAM attributes about local End Users, an organization MUST transmit only those attributes that were explicitly requested by a partner organization's system(s).

3. **Limited Use and Disclosure of End User ICAM Activities** – An organization MUST NOT disclose information on its End Users' activities to any party, or use the

information for any purpose other than federated authentication, audit, and privilege management, unless required by law.

4. **Adequate Notice of Federated Authentication** – An organization MUST provide local End Users with adequate notice regarding federated authentication. "Adequate Notice" includes a general description of the authentication event, any transaction(s) with the relying party system(s), the purpose of the transaction(s), and a description of any disclosure or transmission of personally identifiable information (PII) to any party. Adequate Notice SHOULD be incorporated into the organization's Opt-In process for local End Users.

5. **Termination of ICAM Services** – In the event that an organization ceases to provide its services to, or on behalf of, an End User, the organization MUST continue to protect any sensitive data, including PII, about the End User.

6. **Appropriate ICAM Attribute Request and Usage** – An organization MUST request only those ICAM attributes that it requires for the purposes of making authorization decisions, dynamically provisioning accounts, or performing audit logging. In addition, an organization MUST use requested ICAM attributes only for the purposes of making authorization decisions, dynamically provisioning accounts, or performing audit logging.