Federal Identity, Credentialing, and Access Management

Privacy Guidance for Trust Framework Assessors and Auditors

Version 1.0

June 29, 2011

Table of Contents

1. INTRODUCTION AND BACKGROUND

The Identity, Credential and Access Management Subcommittee (ICAMSC) of the Federal Chief Information Officer (CIO) Council's Information Security and Identity Management Committee (ISIMC) is charged with developing solutions that leverage identity and access control mechanisms in use by the private sector for the Federal community. The ICAMSC has established the Trust Framework Evaluation Team (TFET) to review and approve Trust Framework Providers (TFPs) at levels of assurance (i.e., trust) 1, 2, and non-PKI 3. A TFP assesses an Identity Provider against the TFP's established set of criteria (i.e., trust framework) to determine Identity Provider conformance to the framework at a particular "level of assurance".

The TFET sets criteria governing the establishment of Federally-recognized trust frameworks, approves TFP applicants as meeting those criteria, and provides oversight on behalf of the Federal government for federated identity trust. It serves the interest of U.S. Government organizations as Relying Parties, and promotes interoperability between Federal and non-Federal entities.

In this role, the TFET is now providing guidance to TFP Assessors and Auditors to assist in their initial and subsequent reviews of Identity Providers compliance with the privacy criteria set forth in *Trust Framework Provider Adoption Process (TFPAP) for levels of Assurance 1, 2, and Non-PKI 3* (TFPAP Privacy Criteria).[1] Assessors and Auditors perform a critical role in ensuring that Identity Providers to be certified by TFPs are adequately implementing TFPAP Privacy Criteria. This guidance document restates the TFPAP Privacy Criteria, and for each, suggests questions that may be useful in the evaluation, and provides detailed explanations to supplement the assessment questions. Identity Providers and Relying Parties both have privacy protection responsibilities, although collaboration on privacy practices between Relying Parties and Identity Providers is anticipated in order to provide a seamless experience for Users and meaningful and effective implementation of the TFPAP Privacy Criteria. Specific agreements between the parties may be relied upon as long as each party ensures that its responsibilities are fulfilled and are in furtherance of such collaboration.
To optimize the assessment process, it is recommended that Assessors and Auditors have accreditation with the International Association of Privacy Practitioners (IAPP) (e.g., CIPP, CIPP/G, CIPP/IT), and strongly recommended that Assessors and Auditors have a working knowledge of privacy concepts including the Fair Information Practice Principles (FIPPs)[2] upon which the TFPAP Privacy Criteria are based.

This document should be used by Assessors and Auditors when determining whether an Applicant Identity Provider should be approved by the TFP, and during re-assessment audits required by TFPs for renewal of an Identity Provider's certification. If Assessors and Auditors find any material deficiencies in the implementation of the TFPAP Privacy Criteria, they should specify them in their written report to the TFP, and should also state what remediation has been implemented to address the deficiency. Assessors and Auditors should revisit the Identify Provider within 6 months to evaluate whether the material deficiency has been fully addressed, and should provide the TFP with a written report describing the manner in which the deficiency has been addressed.

The term "Relying Party" means the federal agency for which the identity assurance solution is being provided. In some cases federal agencies may contract with external contractors or commercial third parties for certain functions. Such non-federal entities are considered agents of the

[1] TFPAP version 1.01.1, August 26, 2009, Section 3.3, Trust Criteria Assessment pp. 12-13.
[2] For more information, see Department of Homeland Security, Privacy Policy Guidance Memorandum 2008-1, "Fair Information Practice Principles; Framework for Privacy Policy at the Department of Homeland Security" December 29, 2010, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

federal government and therefore Identity Providers must interact with them as if they were interacting with a federal agency application.

This guidance document will be reviewed periodically and updated to reflect lessons learned from its users. Please let the TFET know whether additional guidance is needed and whether the Assessors and Auditors have any questions regarding its content.

2. TFPAP PRIVACY CRITERIA AND SUGGESTED ASSESSMENT QUESTIONS

2.1.1 Adequate Notice

Adequate Notice – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.

Suggested Assessment Questions:

1. Is the notice written in plain language so that it is easily understood by the average user?
2. Does the notice convey what information is being transmitted, the user's options, and the outcome of not transmitting the information?
3. Is the user information being transmitted the same information that is described in the notice? Is that the only information being transmitted?
4. Is the notice incorporated into the "opt in" mechanism?
5. If so, is the notice clear, concise, unavoidable, and in real-time?
6. Is the notice merely a linked general privacy policy or terms of service?

Supplemental Explanation: Adequate notice is a practical message that is designed to help the average user understand how to engage in the authentication transaction, including, what information is being transmitted about the user, what options the user has with respect to the transmission of the information, and the consequences of refusing any transmission. For example, if the information to be transmitted is required by the Relying Party for the authentication, the notice should make clear that the transmission is required and refusal will cancel the transaction and return the user to the Relying Party's website for further assistance. If the information to be transmitted is not required for authentication, but, for example, will be collected by the Relying Party in order to provide the service requested by the user more conveniently, the notice should make this distinction clear and indicate that if the user refuses the transmission, the user will be able to provide the information directly on the Relying Party's website. Assessors and Auditors should look for a notice that is generated at the time of the authentication transaction. The notice should be in visual proximity (i.e. unavoidable) to the action being requested, and the page should be designed in such a way that any other elements on the page do not distract the user from the notice. The content of the notice should be tailored to the specific transaction. The notice may be divided into multiple or "layered" notices if such division makes the content more understandable or enables users to make more meaningful decisions. For these reasons, the notice should be incorporated into the "opt in" mechanism as set forth below. In sum, an Adequate Notice is never just a link somewhere on a page that leads to a complex, legalistic privacy policy or general terms and conditions.

2.1.2 Opt-In

Opt In – Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.

Suggested Assessment Questions:

1. Is each attribute, or piece of user information to be transmitted, displayed to the user before each transmission?
2. Is there a mechanism for obtaining explicit user confirmation of the information transmission?
3. Is the mechanism specific to the authentication transaction?
4. Is the mechanism intuitive and easy to use?
5. Does the user have the ability to expressly permit or deny the transmission of specific pieces of user information, to the extent not required by the authentication transaction?

Supplemental Explanation: The goal is for the user is to understand the opt-in process, and to have a meaningful opportunity to agree. There are various ways to implement this goal. Users need to be able to see each piece of information, or attribute that is to be transmitted prior to it being transmitted. The confirmation mechanism must enable the user to make an explicit affirmation to permit the transmission of user information in accordance with the notice as described above. Confirmation mechanisms should be designed so that they are intuitive and easy to use. They need to be specific to the transaction. To the extent the information to be transmitted is not required for authentication (i.e., the Relying Party would like to have the information to pre-populate transaction fields or for other reasons, but the information is not necessary to accomplish the authentication of the user), users should have the ability to expressly permit or deny the transmission of specific pieces of such user information, for example, through radio buttons or similar mechanisms. As described above, the design of the notice and the confirmation mechanism should be considered as an integrated concept. Mechanisms that allow users to affirmatively waive notices and opt-in consents for each transmission such as a “don’t show me this message again” option are acceptable. Mechanisms such as a simple “agree” button on ‘general terms of service’ or pre-checked consents are strongly discouraged because they are unlikely to meet the essential objective of meaningful understanding.

Generally, it is less meaningful to obtain opt-in at the time the credential is issued rather than at the time of the transaction. In certain circumstances, the TFET may approve TFPs that accept this practice. Assessors should be made aware of agreements made between the TFP and TFET that affirmatively accept this practice and any constraints established for this practice.

2.1.3 Minimalism

Minimalism – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile.

Suggested Assessment Questions:

1. Is there written documentation describing the user information requested by the Relying Party?
2. Does the written documentation distinguish between information that the Relying Party needs to conduct the authentication transaction and any other information that the Relying Party would like to collect (e.g. to increase efficiency or convenience in providing the service requested by the user)?
3. Does the Identity Provider actually only transmit those attributes that were explicitly requested by the Relying Party or required by the Federal profile?
4. In the absence of any written documentation, does the Identity Provider only send attributes required by the Federal profile?

Supplemental Explanation: Assessors and Auditors need to ensure that Identity Providers are only sending the information that is explicitly requested by the Relying Party or that is required by the Federal profile. Written documentation is important in ensuring that the Adequate Notice and Opt-in principles are appropriately executed in terms of distinguishing between information that the Relying Party needs to conduct the authentication transaction and information that the Relying Party would like to collect. In the absence of any such written documentation from the Relying Party, only the information required by the Federal profile may be sent.

2.1.4 Activity Tracking

Activity Tracking – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication.

Suggested Assessment Questions:

1. Is there a written policy on how the Identity Provider will comply with this principle?
2. Does the Identity Provider have any technical means for ensuring compliance with its written policy?
3. What other means does the Identity Provider employ to ensure compliance? Employee training?
4. Does the Identity Provider have procedures to measure the effectiveness of its methods?
5. Does the Identity Provider make its compliance with this principle clear to users?

Supplemental Explanation: The purpose of this principle is to ensure that the Identity Provider does not use or disclose any information about the user and his or her interactions with the government, which the Identity Provider learns as a result of providing the authentication service for any purpose other than to provide the authentication service. Assessors and Auditors should check for a written policy that demonstrates how the Identity Provider will comply with this principle. Assessors and Auditors should also evaluate the effectiveness of the means, technical or otherwise, which the Identity Provider uses to

achieve compliance. Finally, Assessors and Auditors should check whether the Identity Provider provides an explanation of this principle to users. This explanation may be located in a general privacy policy about the collection and use of personal information.

2.1.5 Non Compulsory

Non Compulsory – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.

No assessment required because this principle does not apply to Identity Providers.

2.1.6 Termination

Termination – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.

Suggested Assessment Questions:

1. Is there a written policy or plan demonstrating how the Identity Provider will manage sensitive data in the event of a bankruptcy, sale, or voluntary discontinuation of the provision of identity services?
2. What commitments does the policy or plan contain with respect to the destruction or transfer of the data?
3. Does the policy or plan provide for notice to the users in the event of transfer of their sensitive data?

Supplemental Explanation: Assessors and Auditors should evaluate whether the written policy or plan expressly provides for destruction of the data, as appropriate, or a commitment that the Identity Provider, to the best of its abilities, will require that any recipient of the data protect the data in kind. Ideally, Identity Providers also should plan to give users notice when their sensitive data will be transferred to another entity.

2.1.7 Identity Provider Bona Fides

Identity Provider *Bona Fides* - The TFPAP requires that Trust Framework Providers sufficiently review member Identity Provider *bona fides* to ensure that the member Identity Provider has organizational maturity, legitimacy, stability, and reputation. (TFPAP Trust Criteria Assessment 3.3 (3))

Suggested Assessment Questions:

1. In addition to the notice or notices that the Identity Provider has developed under the Adequate Notice principle, does the Identity Provider have a general written privacy or data use policy that covers the personal information it collects from or about users of its services?
2. If so, is such policy posted on its public website? Does it cover how the Identity Provider uses and how long it retains the information collected, and what choices the user may have about the use and retention of such information? Does the content and format for such policy conform to

industry best practices or guidance issued by the Federal Trade Commission or other federal agencies?

3. Does the Identity Provider have a training program for all employees who handle personal information regarding how to comply with the Identity Provider's stated policies? Has the Identity Provider had employee violations of its policies? If so, were the violations handled in accordance with the Identity provider's policies and in a manner reasonably likely to minimize the occurrence of further violations?

4. Does the Identity Provider have a reasonable process for maintaining the accuracy of the personal information that it enters into its systems? Does the Identity Provider have a reasonable process for resolving complaints from users about inaccurate information, mistaken identities, or other problems? Has the Identity Provider received any complaints from users regarding the handling of personal information in its role as an Identity Provider, or in general (if it has multiple lines of business)? If so, how were these complaints resolved?

5. Does the Identity Provider have a data security plan, including a data destruction policy and a data loss response plan? Do such plans conform to any applicable legal requirements and/or industry best practices? Has the Identity Provider experienced any data breaches? If so, were the breaches handled in accordance with the Identity provider's policies and in a manner reasonably likely to minimize the occurrence of further breaches?

6. Does the Identity Provider carry liability insurance that covers potential liability for loss and/or misuse of consumer data?

Supplemental Explanation: In assessing the general organizational maturity, legitimacy, stability, and reputation of the Identity Provider, Assessors and Auditors should look for a general privacy or data use policy that covers how the Identity Provider uses and how long it retains the information collected, and what choices the user may have about the use and retention of such information. Assessors and Auditors should evaluate the Identity Provider's data security practices, with particular attention to the occurrences of data breaches and the Identity Provider's response. Assessors and Auditors also should evaluate whether the identity provider has training for its employees regarding the handling of user information or other means of ensuring compliance with its stated policies. In their overall assessment of the Identity Provider's performance under these principles, Assessors and Auditors should pay particular attention to any complaints from users regarding the Identity Provider's handling of personal information in its role as an Identity Provider, or in general, and how these complaints were resolved. In addition, Assessors and Auditors should evaluate whether the Identity Provider's policies or procedures conform with applicable law, or in the absence of any such law, industry best practices or any guidance issued by the Federal Trade Commission or other federal agencies.

APPENDIX A – ACRONYMS

Acronym	Definition
CIO	Chief Information Officer
CIPP	Certified Information Privacy Professional
CIPP/G	Certified Information Privacy Professional/Government
CIPP/IT	Certified Information Privacy Professional/Information Technology
FIPP	Fair Information Practice Principles
IAPP	International Association of Privacy Practitioners
ICAMSC	Identity, Credential and Access Management Sub Committee
ISIMC	Information Security and Identity Management Committee
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RP	Relying Party
TFET	Trust Framework Evaluation Team
TFP	Trust Framework Provider
TFPAP	Trust Framework Provider Adoption Process