IDENTITY ECOSYSTEM STEERING GROUP
IDEF Baseline Functional Requirements v1.0 with Supplemental Guidance

26 September FMO version v0.92 for Plenary ballot

File name: FMO-IDESG-Baseline-Reqts-ForBallot-v0.92-20150926

*NOTES: (A) The Requirements language is presented in **bold face text** in this document and is the normative form of the requirements as approved by the IDESG Plenary. IDESG may update it with newer versions from time to time, based on member, expert and stakeholder feedback, and welcomes your comments. (B) The IDESG also has approved a set of Best Practice statements, at the end of this set, which indicate additional advisable steps, and note matters that may become the subject of future Requirements. (C) These Requirements primarily are directed at identity service providers; the classes of service provider activity listed for each Requirement (see: "APPLIES TO ACTIVITIES") are based on the IDESG Functional Model v1.0 (https://www.idecosystem.org/filedepot_download/943/1423) are its specification of a provider's functional Core Operations Activities on pages 6-9, particularly Table 1. (D) The Supplemental Guidance materials and related references are provided by IDESG's committees and experts as additional assistive but nonnormative information. Short titles and keywords for each item also are included here, for ease of use, but also are not considered part of the normative text. (E) APPENDIX A presents a set of commonly-recurring words and concepts, along with some limited additional non-normative information and references to other external guidance. Appendix A likely will be replaced in the future by a normative IDESG Glossary. In this document, certain words are CAPITALIZED in the text below for ease of review and identifying recurring concepts; however, that **capitalization is not part of the normative text**; the words may be styled differently (for example, by hyperlinks) in other presentations of this material; and in later versions, may be changed or superseded by the eventual normative Glossary.*

TEMPORARY EDITING NOTES (26 SEPTEMBER 2015):

*This material (26 September FMO balloting version) reflects all changes made to the Requirements and Supplemental Guidance during the Tampa Plenary week. This v0.92 version is marked **only** to show changes from the prior 25 June 2015 Plenary-approved Requirements. No Supplemental Guidance is marked, because all of that final committee content is coming to the Plenary for the first time, on this ballot. Therefore, this is the official compilation of the Requirements amendments and Supplemental Guidance for the Plenary to consider in its October ballot.*

A different version, v0.91, has the same content, but with markup cumulating all prior annotations, showing changes going back to the 11 September special markup. It is an unofficial diagnostic version, for purposes of tracking recent edits.

*Please note also that (a) the Requirements have been **renumbered** due to the recent edits; (b) **capitalization** of words in the text is not normative, and may change, as noted above; and (c) **hyperlinks** are not normative and may change, as the document is prepared for production.*

IDESG

Table of Contents

SCOPE

The National Strategy for Trusted Identities in Cyberspace (NSTIC) envisions widespread, trusted identity exchanges using federated methods that are secure, interoperable, privacy-enhancing and easy to use. Realization of that vision will require companies, agencies and individuals to perform at a new level. The Requirements are our first step towards that goal, by describing a set of functions that parties must be able to fulfill, and a set of criteria for assessing those capabilities.

The Requirements are an informed step forward in privacy, security, interoperability and usability based on the work of the IDESG's diverse membership of practitioners expert in their respective fields.

Identity Ecosystem stakeholders can use the Requirements to identify and measure capabilities and services today and identify others to implement. The IDESG Framework includes guidance, listing and self-reporting facilities as part of the IDESG's Self-Assessment Listing Service (SALS). The SALS will support both informal and formal self-assessment. IDESG plans include an option to expand the program to third-party certification based on execution of the initial listing and IDESG's outreach, activities and stakeholder input.

BASELINE REQUIREMENTS

INTEROP-1. THIRD PARTY AUTHENTICATION

Entities MUST be capable of accepting external USERS authenticated by THIRD-PARTIES.

SUPPLEMENTAL GUIDANCE

This Requirement applies to RELYING-PARTY consumers (i.e., entities making access control decisions) of a THIRD-PARTY authentication and requires such entities to be capable of accepting identities authenticated by multiple (i.e., more than one THIRD-PARTY), but does not require that all authenticated identities be accepted if their policies/business rules do not permit. RELYING-PARTIES that use portals, service providers, or transaction intermediaries would meet this Requirement if they can accept identities authenticated by THIRD-PARTIES, even if those RELYING-PARTIES do not consume tokens directly. (For example, RELYING-PARTIES satisfy this Requirement either by accepting and consuming identity assertions in nonproprietary published formats directly (such as SAML or another protocol to convey the authentication status), or by receiving them via an intermediate who accepts and consumes those assertions for them.)

Regarding "nonproprietary published formats", see Appendix A.

REFERENCES

National Strategy for Trusted Identities in Cyberspace (2012), *https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*

APPLIES TO ACTIVITIES

AUTHORIZATION

KEYWORDS

INTERMEDIARIES, INTEROPERABILITY, THIRD-PARTIES

INTEROP-2. THIRD-PARTY CREDENTIALS

Entities who issue credentials or assertions MUST issue them using content and methods that are capable of being consumed for multiple purposes and multiple recipients.

SUPPLEMENTAL GUIDANCE

This Requirement applies to entities that issue identity credentials and/or assertions and requires that the credentials/assertions issued by such entities may be accepted by multiple THIRD-PARTIES (such as RELYING-PARTIES). This does not require that such credentials/assertions must be accepted by all THIRD-PARTIES; rather, the Requirement is that credentials/assertions may be accepted by multiple (more than one) THIRD-PARTIES. Single-purpose Identity credentials/assertions that are used exclusively for access to a single enterprise/online resource that are not permitted for authentication by any external THIRD-PARTY would not conform to this Requirement.

This Requirement addresses the format or expression of the credential or assertion data itself and policies for its use, and not its method of exchange, which is addressed in INTEROP-04 (STANDARDIZED DATA EXCHANGES).

REFERENCES

IDESG Functional Model: *https://www.idecosystem.org/filedepot_download/943/1423*

APPLIES TO ACTIVITIES

CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSERTION, CREDENTIAL, INTEROPERABILITY, THIRD-PARTIES

INTEROP-3. STANDARDIZED CREDENTIALS

Entities that issue credentials or assertions MUST issue them in a format that conforms to public open STANDARDS listed in the IDESG Standards Registry, or if that Registry does not include feasible options, then to non-proprietary specifications listed in the IDESG Standards Inventory.

SUPPLEMENTAL GUIDANCE

This Requirement applies to entities that issue identity credentials or assertions and requires that the formats conform to IDESG approved standards and/or open standards listed in the IDESG Standards Inventory. The intent of this Requirement is to ensure that credentials or assertions are capable of being accepted by interoperable solutions. This Requirement recognizes that sufficient options exist today that entities should not need to use proprietary credential structures, but the developing IDESG Registry may not yet include references to all appropriate, useful standards or specifications pertaining to credential issuance.

Regarding "nonproprietary specifications", see Appendix A.

REFERENCES

Reference for open standards: OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, *https://www.whitehouse.gov/omb/circulars_a119*

Reference for roles, functions, and operations, IDESG Functional Model, *https://www.idecosystem.org/filedepot_download/943/1423*

Reference examples of published credential or assertion formats: SAML 2.0 Attribute Assertions with XACML 3.0, *http://docs.oasis-open.org/xacml/xacml-saml*-profile/v2.0/xacml-saml-profile-v2.0.html; Open ID Connect with Java Web Tokens (JWT), *http://openid.net/developers/libraries/*

APPLIES TO ACTIVITIES

CREDENTIALING, AUTHENTICATION, INTERMEDIATION

KEYWORDS

ASSERTION, CREDENTIAL, INTEROPERABILITY, OPEN-STANDARDS

INTEROP-4. STANDARDIZED DATA EXCHANGES

Entities that conduct digital identity management functions MUST use systems and processes to communicate and exchange identity-related data that conform to public open STANDARDS.

SUPPLEMENTAL GUIDANCE

This Requirement is that entities must use public open STANDARDS when conducting data interface and exchange transactions with THIRD-PARTIES. It does not require that entities must be capable to use all interface STANDARDS, but must be capable of using at least one. Sufficient options exist among nonproprietary published methods today.

This Requirement addresses transmission and exchange data protocols, reliable messaging, and database/repository/registry transactions, within which entities may offer, seek and obtain identity data. Please note, however, that this Requirement does not address formats or expressions for the identity data itself (which are addressed by INTEROP-2 (THIRD-PARTY CREDENTIALS) and INTEROP-3 (STANDARDIZED CREDENTIALS)), nor transport or protective methods and protocols (which are addressed separately in the Security requirements (SECURE-1 through SECURE-15)).

Regarding "digital identity management functions", see Appendix A.

REFERENCES

Reference for open standards: OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, *https://www.whitehouse.gov/omb/circulars_a119*

Reference for roles, functions, and operations, IDESG Functional Model, *https://www.idecosystem.org/filedepot_download/943/1423*

Reference examples for interface and exchange protocols: SAML 2.0, *http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf;* XACML 3.0, *http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html;* OAuth 2.0, *http://tools.ietf.org/html/rfc6749*.

APPLIES TO ACTIVITIES

CREDENTIALING, AUTHENTICATION, INTERMEDIATION

KEYWORDS

DATA-INTERFACE, EXCHANGE,INTEROPERABILITY OPEN-STANDARDS, TRANSACTION

INTEROP-5. DOCUMENTED PROCESSES

Entities MUST employ documented business policies and processes in conducting their digital identity management functions, including internally and in transactions between entities.

SUPPLEMENTAL GUIDANCE

This Requirement is that entities shall document business policies and procedures that are employed for identity management functions related to the transmission, receipt, and acceptance of data between systems. Having documented procedures is a necessary prerequisite for transparency and accountability, quality control, auditability, and ease of interoperability among federated communities.

However, this Requirement does not mandate adoption of any specific policies and procedures, or any specific systematic approaches to procedures. Rather, the entity making this assertion should simply affirm that it does maintain such documents in writing, and can make them available as described. The obligation for policies to be transparent to USERS in this context includes prospective users such as eligible applicants.

Regarding "digital identity management functions", see Appendix A.

REFERENCES

Reference examples for requirements that entities maintain written policies and procedures generally: HIPAA Security and Privacy Regulations regarding development and maintenance of policies and procedures: 45 CFR Part 164, § 164.316(a), § 164.530(a), § 164.530(a)(1)(i), § 164.530(i) and § 164.530(j): *http://www.ecfr.gov/cgi-bin/text-idx?node=pt45.1.164&rgn=div5;* Sarbanes-Oxley Sec. 404, Assessment of Internal Controls, *https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act#Sarbanes.E2.80.93Oxley_Section_404:_Assessment_of_internal_control*

Reference example of a federation's published policies, see: *https://www.incommon.org/policies.html*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

NOTICE, INTEROPERABILITY, POLICIES, PROCESS, TRANSACTION

Note: Committee has recommended that INTEROP-6 become the Best Practice tentatively designated INTEROP-BP-F.

~~***INTEROP-6. FEDERATION COMPLIANCE***~~

~~***When conducting digital identity management functions within an identity FEDERATION, entities MUST comply in all substantial respects with the published policies and system rules that explicitly are required by that FEDERATION, according to the minimum criteria set by that FEDERATION.***~~

Note: Committee has recommended that INTEROP-7 become the Best Practice tentatively designated INTEROP-BP-G.

~~***INTEROP-7. LEGAL COMPLIANCE***~~

~~**When conducting digital identity management functions, entities MUST comply in all substantial respects with all laws and regulations applicable to those relevant functions.**~~

INTEROP-6[8]. THIRD-PARTY COMPLIANCE

Entities that act as THIRD-PARTY~~intermediaries or~~ service providers for another entity, in conducting digital identity management functions, must comply with each of the applicable IDESG Baseline Requirements that apply to that other entity and those relevant functions.

SUPPLEMENTAL GUIDANCE

This Requirement applies to outsourcing or delegation of digital identity management functions or transactions to THIRD-PARTIES. An entity assessing its compliance with the applicable IDESG Baseline Requirements must also apply them to the functions or transactions carried out on its behalf by a service provider. For purposes of this Requirement, the term "THIRD-PARTY service provider" refers to THIRD-PARTIES that an assessed entity outsources or delegates to perform digital identity management functions on behalf of the assessed entity.

In some FEDERATIONS, the federation itself may also act as a service provider for participant entities in some identity management functions, and thereby be subject to this Requirement.

Cloud computing service providers providing data storage or other services for an entity may also be within the scope of this Requirement, depending on the functions performed on behalf of the assessed entity, and the provider's access to the data handled on behalf of the assessed entity. See comments about "data storage companies" in the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act (2013), Final Rule comments on HITECH Act Section 13408: *http://federalregister.gov/a/2013-01073*

Regarding "digital identity management functions", see Appendix A.

REFERENCES

Reference for cloud computing processors of personal information: ISO/IEC 27018 (2014): Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. *http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498*, and *https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en*

Reference example of intermediaries and similar subcontractors or service agencies who fulfill data transactions for others, and take responsibility for their compliance with various requirements: see "Business Associate" regulations in the HIPAA Privacy Regulations: 45 CFR Parts 160 and 164, §§ 160.103, 164.502(a)(3), (a)(4) and (e); and the treatment of "Clearinghouse" functions in § 164.500(b): *http://www.ecfr.gov/cgi-bin/text-idx?node=pt45.1.164&rgn=div5*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

COMPLIANCE, INTEROPERABILITY, INTERMEDIARIES, TRANSACTION, THIRD-PARTIES

INTEROP-~~7[9]~~7. USER REDRESS

Entities MUST provide effective ~~redress~~ mechanisms for redress of complaints or problems arising from identity transactions or the~~, and facilitation on behalf of, USERS who believe they have been harmed by the entity's~~ failure of the entity to comply with the IDESG Baseline Requirements. These mechanisms MUST be easy for USERS to find and access.

SUPPLEMENTAL GUIDANCE

"Effective" in this Requirement means that use of the redress mechanism will result in a timely correction of errors, resolution of the dispute or complaint, and the process shall not be overly burdensome or complex.

Resolution of disputes shall be conducted in a fair and consistent manner. Where feasible, further mechanisms for USERS to seek redress can be instituted through the use of internal or independent THIRD-PARTY services (i.e. ombudsmen, etc.)

Entities must provide to USERS the source of any verification or information that leads to an eligibility, authentication or authorization decision. If USERS seek redress, they must be provided with a mechanism to dispute or change erroneous information at the source of the information.

If credentialing is denied or a credential is revoked from a USER, justification for that decision should be presented along with the source of any information that contributed to that decision.

Note: Intermediaries may not have a direct relationship with USERS who move through their systems, but should facilitate endpoints' ability to conform to this requirement. See the IDESG Functional Model for definition of "Transaction Intermediation,", which describes it as "Processes and procedures that limit linkages transactions and facilitate credential portability. " This includes functions defined as "Blinding", "Pseudonymization/Anonymization," and "Exchange".

Entities should provide a mechanism for redress and include the ability to correct or otherwise address any issues USERS may have.

Pathways for redress should be clear and available to the user throughout the process.

A redress mechanism should be considered must-see-this-first information in a first encounter and then provided as appropriate to the USER in a consistent manner thereafter.

Please note that INTEROP-5 (DOCUMENTED PROCESSES) applies to this Requirement. Regarding "redress", see also Appendix A.

REFERENCES

Consult USABLE-4 (NAVIGATION) supplemental guidance for additional considerations that apply to redress.

Consult the UXC Resources page located here for examples:
https://www.idecosystem.org/wiki/UXC_resources

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING

KEYWORDS

ACCOUNTABILITY, COMPLIANCE, INTEROPERABILITY, POLICIES, REDRESS, RISK

INTEROP-~~8~~10. ACCOUNTABILITY

Entities MUST be accountable for conformance to the IDESG Baseline Requirements, by providing mechanisms for auditing, validation, and verification.

SUPPLEMENTAL GUIDANCE

By the term ”mechanism” it is intended there is a means to support a determination of compliance with these Requirements. This means may be through documented policy, audit, direct observation, or other means to support a determination of compliance. This Requirement does not intend that the means is provided publicly, just that it is available to the service provider for the determination of compliance and may be examined independently when appropriate.

REFERENCES

Reference for “accountability” requirements: ISO/IEC 29100 (2011) Privacy Framework, Section 5.10 Accountability, *http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

AUDIT, COMPLIANCE, INTEROPERABILITY, POLICIES, VALIDATION

PRIVACY-1. DATA MINIMIZATION

Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

SUPPLEMENTAL GUIDANCE

Regarding "personal information," see Appendix A.

This Requirement is intended to apply to each transaction or data exchange in which personal information is collected, generated, used, transmitted or stored. Groups of related transactions may share a common purpose and legal requirements; but each data exchange is subject to the minimization mandate. [Entities are encouraged to address this issue by design, before run time, by limiting or applying controls or filters to classes of data.]

The boundaries of a TRANSACTION between a service provider and a user are defined by the purpose of the collection, generation, use, transmission, or storage of their personal information. SEE PRIVACY-2 (PURPOSE LIMITATION).

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

LIMITATION, MINIMIZATION, PRIVACY, PURPOSE

PRIVACY-2. PURPOSE LIMITATION

Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.

SUPPLEMENTAL GUIDANCE

Regarding "personal information", see Appendix A. Entities should also assure that their data controls reliably apply these limitations to their future actions.

See also Requirement PRIVACY-1 (DATA MINIMIZATION) on the application of limitations to, and scope of, individual transactions and data exchanges.

Please note the applicability of best practice INTEROP-BP-G (RECOMMENDED LEGAL COMPLIANCE) regarding limitations imposed by laws. Please note the applicability of best practice [INTEROP-BP-F (RECOMMENDED FEDERATION COMPLIANCE) and Requirement INTEROP-6 (THIRD-PARTY COMPLIANCE) regarding limitations arising from the involvement of THIRD-PARTIES such as intermediaries, similar service providers, or FEDERATIONS.

See the IDESG Functional Model for definition of Transaction Intermediation for the scope of "intermediaries." The functional model describes Transaction Intermediation as "Processes and procedures that limit linkages between transactions and facilitate credential portability. This includes functions defined as "Blinding," "Psuedonymization/Anonymization," and "Exchange."

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

LIMITATION, PRIVACY, PURPOSE

PRIVACY-3. ATTRIBUTE MINIMIZATION

Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

SUPPLEMENTAL GUIDANCE

Where feasible, Identity Providers (and any other entities releasing attributes) should provide the opportunity for attributes to be released as claims as well as detailed attributes; see also PRIVACY-1 (DATA MINIMIZATION) on granularity of requests to support data minimization by requesters, generally.

Attribute providers may be required by their own business processes to collect and store, although not necessarily transmit, attributes in their attribute form, in which case significant alteration or filtering may be required when that data is re-used or transmitted to others.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ATTRIBUTE, IDENTIFIER, LIMITATION, MINIMIZATION, PRIVACY

PRIVACY-4. CREDENTIAL LIMITATION

Entities MUST NOT request USERS' credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

SUPPLEMENTAL GUIDANCE

Intermediaries may not have a direct relationship with individuals who move through their systems, but should facilitate endpoints' ability to conform to this Requirement.

See the IDESG Functional Model for definition of Transaction Intermediation for the scope of "intermediaries." The functional model describes Transaction Intermediation as "Processes and procedures that limit linkages between transactions and facilitate credential portability. This includes functions defined as "Blinding," "Psuedonymization/Anonymization," and "Exchange."

See Requirements PRIVACY-1 (DATA MINIMIZATION) and PRIVACY-2 (PURPOSE LIMITATION) on the application of limitations to, and scope of, individual transactions and data exchanges.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CREDENTIAL, IDENTIFIER, LIMITATION, PRIVACY, PURPOSE, RISK

PRIVACY-5. DATA AGGREGATION RISK

Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.

SUPPLEMENTAL GUIDANCE

Regarding "personal information", see Appendix A, and PRIVACY-1 (DATA MINIMIZATION).

Collection of personal information from repeated data transactions, which can be associated to form a larger body of knowledge about individuals, may increase their privacy risk. For example: An Identity Provider's ability to facilitate transactions between a user and multiple relying parties may give the Identity Provider privileged insights into the users' behavior. Such information is the result of the Identity Provider's ability to link user interactions across transactions.

"Users' explicit consent" alone should not be used to mitigate privacy risks created by technical architecture or design, such as to mitigate risks that individuals could not be reasonably expected to be able to assess.

See also Requirements PRIVACY-1 (DATA MINIMIZATION) and PRIVACY-2 (PURPOSE LIMITATION) on the application of limitations to, and scope of, individual transactions and data exchanges.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

AGGREGATION, CONSENT, DESIGN, LIMITATION, PRIVACY, RISK

PRIVACY-6. USAGE NOTICE

Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

SUPPLEMENTAL GUIDANCE

Regarding "personal information", see Appendix A, and see PRIVACY-1 (DATA MINIMIZATION).

The goal of notice is to work toward informed consent from USERS: functional requirements should work toward strategies for improving USERS' understanding of their choices when engaging with services. Strategies include layered approaches, just-in-time notice, and other examples that can illustrate effective types of notice mechanism alternatives to privacy policies. In the case of material changes to the service, entities shall provide clear and conspicuous descriptions of the changes and their impacts on USERS in advance of the change.

"Consent" alone should not be used to mitigate privacy risks created by technical architecture or design, such as to mitigate risks that individuals could not be reasonably expected to be able to assess; see PRIVACY-5 (DATA AGGREGATION RISK).

See also Requirements PRIVACY-1 (DATA MINIMIZATION) and PRIVACY-2 (PURPOSE LIMITATION) on the application of limitations to, and scope of, individual transactions and data exchanges.

See also the IDESG Usability Requirements (USABLE-1 through USABLE-7) regarding the clarity of notices given to USERS and others.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

NOTICE, POLICIES, PRIVACY

PRIVACY-7. USER DATA CONTROL

Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

SUPPLEMENTAL GUIDANCE

Regarding "personal information," see Appendix A, and PRIVACY-1 (DATA MINIMIZATION) and INTEROP-7 (USER REDRESS).

"Appropriate" broadly means mechanisms for management of personal information should be effective, easy to use, and accessible. (See USABLE-1 (USABILITY PRACTICES), USABLE-3 (PLAIN LANGUAGE), and USABLE-5 (ACCESSIBILITY) for guidance on the usability of such mechanisms.)

"Deletion" generally refers to removal of the data from availability. Data disposal, its complete removal from the complying entity's own systems and control, may depend on the legal and contractual requirements applicable to the data; see PRIVACY-14 (DATA RETENTION AND DISPOSAL).

Note: Intermediaries may not have direct control over the information that flows through their systems, but should deploy mechanisms that support endpoints' ability to conform to this Requirement. See INTEROP-6 (THIRD-PARTY COMPLIANCE).

See the IDESG Functional Model for definition of Transaction Intermediation for the scope of "intermediaries." The functional model describes Transaction Intermediation as "Processes and procedures that limit linkages between transactions and facilitate credential portability. This includes functions defined as "Blinding," "Psuedonymization/Anonymization," and "Exchange."

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHANGES, CHOICE, CONTROL, CORRECTION, PRIVACY, RETENTION

IDESG

PRIVACY-8. THIRD-PARTY LIMITATIONS

Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

SUPPLEMENTAL GUIDANCE

Regarding "personal information, " seer Appendix A and PRIVACY-1 (DATA MINIMIZATION).

One example of a USER's choice that creates a use limitation would be their election to restrict the use of their personal information to specific purposes only. This Requirement broadly means that entities convey all such restrictions to the "downstream" recipients of personal information, when they share that information. However, this Requirement does not dictate what elective choices a USER should be prompted to make; and it does not require an entity to convey (or enforce) a USER's choices or instructions if those choices contradict law, regulation or legal process.

Please note, Requirement INTEROP-6] (THIRD-PARTY COMPLIANCE) also includes certain specific duties in connection with THIRD-PARTIES receiving personal information from an entity.

Responsibilities for liability should be spelled out in agreements between organizations exchanging personal information in the identity ecosystem, as well as the format and style of the communication of user-stated privacy preferences and information.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHOICE, LIMITATION, NOTICE, PORTABILITY, PRIVACY, THIRD-PARTIES

PRIVACY-9. USER NOTICE OF CHANGES

Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

SUPPLEMENTAL GUIDANCE

Once USERS have been notified of the planned uses and processing of their personal information (see PRIVACY 6 (USAGE NOTICE)), and exercised whatever consent, limitation or withdrawal rights they have (see PRIVACY-7 (USER DATA CONTROL)), material changes to those uses or processing may render their choices obsolete, so entities should refresh the USER's opportunity to exercise those controls in light of the new information. (See USABLE-4 (NAVIGATION), USABLE-5 (ACCESSIBILITY) and USABLE-6 (USABILITY FEEDBACK).)

Regarding "personal information," see Appendix A and PRIVACY-1 (DATA MINIMIZATION).

"Express affirmative consent" should not be used to mitigate privacy risks created by technical architecture or design, or to mitigate risks that individuals could not be reasonably expected to be able to assess; see PRIVACY-5 (DATA AGGREGATION RISK).

"Compensating controls" are controls or mechanisms, which may operate either by policy or (preferably) technology, designed to mitigate privacy risks that may arise when a material change is made to the system. Examples might include an opportunity to assent or withdraw, or risk-shifting rules occurring upon a change. Those controls can be under user administration, but only if the user can be reasonably expected to understand how to use those mechanisms to effectively mitigate their risk.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHANGES, CONSENT, NOTICE, PRIVACY, PURPOSE

PRIVACY-10. USER OPTION TO DECLINE

USERS MUST have the opportunity to decline registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

SUPPLEMENTAL GUIDANCE

Regarding "personal information," see Appendix A and PRIVACY-1 (DATA MINIMIZATION).

Although an entity's digital identity management functions and transactions should provide an opportunity to the USER to decline to provide personal information or consent to its use, that decision may appropriately result in the partial or complete failure of the entity's intended transaction. (See USABLE-4 (NAVIGATION), USABLE-5 (ACCESSIBILITY) and USABLE-6 (USABILITY FEEDBACK).)

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION

KEYWORDS

CHOICE, CONSENT, PRIVACY

PRIVACY-11. OPTIONAL INFORMATION

Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

SUPPLEMENTAL GUIDANCE

Regarding "personal information," see Appendix A, and PRIVACY-1 (DATA MINIMIZATION).

See also the IDESG Usability Requirements (USABLE-1 through USABLE-7) regarding the clarity of notices given to USERS and others.

Additional best practices for indicating optionality are provided in PRIVACY-BP-C (RECOMMENDED CONSEQUENCES OF DECLINING) below.

It may be appropriate to have a "don't ask me again" check box for a series of transactions of the same type.

For example: If personal information is requested from USERS during registration that is beyond the minimum necessary to complete an eligibility decision, that personal information should be clearly marked as optional.

Regarding "mandatory" and "optional", in this Requirement, if personal information is requested from USERS during registration that is beyond the minimum necessary to complete an eligibility decision, that personal information should be clearly marked as optional. That optional designation should include a short and clear description justifying the request of that data.

If an organization requests to release attributes values during a transaction that are the beyond the minimum necessary to complete that transaction, that release should be clearly presented as optional/a choice. That optional designation should include a short and clear description justifying the release of that data.

If information or attribute value release is designated as mandatory, that designation should include a short and clear description of the consequences of declining to provide that information or allowing that release. See PRIVACY-10 (USER OPTION TO DECLINE).

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, AUTHORIZATION

KEYWORDS

CHOICE, LIMITATION, NOTICE, PRIVACY

PRIVACY-12. ANONYMITY

Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

SUPPLEMENTAL GUIDANCE

In support of legal, policy or personal requirements for anonymous or pseudonymous USER participation, digital identity management functions and systems should permit anonymous and (persistent across sessions) pseudonymous registration and participation, where required by law or otherwise feasible. To further facilitate that goal, identifiers and personal data (including attributes) should be kept separate wherever feasible: see PRIVACY-4 (CREDENTIAL LIMITATION) and PRIVACY-15 (ATTRIBUTE SEGREGATION).

See INTEROP-6 (THIRD-PARTY COMPLIANCE) on the mitigation of risks associated with third-party service providers or data users.

See PRIVACY-5 (DATA AGGREGATION RISK) regarding the risk of collecting additional information.

See PRIVACY-13 (CONTROLS PROPORTIONATE TO RISK) regarding the implementation of controls to mitigate identified privacy risk.

See PRIVACY-11 (OPTIONAL INFORMATION) regarding availability of user choices regarding optional disclosure of personal information.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ACCOUNT, ANONYMITY, CHOICE, IDENTIFIER, PRIVACY

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

SUPPLEMENTAL GUIDANCE

Regarding "personal information," See Appendix A and PRIVACY-1 (DATA MINIMIZATION).

Regarding "digital identity management functions" see Appendix A.

Many risk analysis models include examples or guidance about the implementation of controls that are appropriate to either specific risks or levels of existing risk. Entities may satisfy this Requirement by confirming that they have conducted that risk assessment and, based on that assessment, made appropriate adjustments to their practices.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSESSMENT, CONTROLS, LIMITATION, POLICIES, PRIVACY, RISK

PRIVACY-14. DATA RETENTION AND DISPOSAL

Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

SUPPLEMENTAL GUIDANCE

Retention requirements arising from "law, regulation or legal process" may include litigation-related legal holds, and requirements arising from mandatory audits.

Regarding "personal information," see Appendix A and PRIVACY-1 (DATA MINIMIZATION).

"Functions" refer to the functions listed in the IDESG Functional Model; see supplemental guidance in PRIVACY-13 (CONTROLS PROPORTIONATE TO RISK).

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

LIMITATION, PRIVACY, PURPOSE, RETENTION

PRIVACY-15. ATTRIBUTE SEGREGATION

Wherever feasible, identifier data MUST be segregated from attribute data.

SUPPLEMENTAL GUIDANCE

This recommendation is intended to apply to identity data while used and stored internally by an entity, as well as when collected from or transmitted to another. These goals may be most easily accomplished when identity management systems are being designed or renovated.

Regarding "identifiers," see Appendix A.

REFERENCES

Further reference materials and to aid organizations interested in conforming to these Requirements can be found at *https://www.idecosystem.org/wiki/Supplemental_Privacy_Guidance*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHORIZATION

KEYWORDS

ARCHITECTURE, ATTRIBUTE, IDENTIFIER, PRIVACY, PROCESS

IDESG

SECURE-1. SECURITY PRACTICES

Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.

SUPPLEMENTAL GUIDANCE

Entities may satisfy this Requirement by confirming that they (a) have considered existing information security standards, guidelines and practices relevant to their environment; (b) have identified the specific sources of guidance that are appropriate for their operations, in light of the information security risks they face; and (c) have implemented the portions of that guidance they deemed appropriate.

This Requirement does not mandate which information security policies, procedures or technologies an entity should or must use. However, some specific policies and technologies are the subject of other, more specific items elsewhere in this Requirements set.

Entities must have risk-based countermeasures and safeguards in place to resist common threats to identity solutions and identity data, including, for example, Session hijacking; Eavesdropping; Theft; Man-in-the-middle; Online Guessing; Replay; Unauthorized copying or duplication; and Insider Threats.

The security standards, guidelines, and practices employed in digital identity management services, to govern the security of their networks, devices, solutions, and systems, must be both operational and well documented. Please note the applicability of Requirement INTEROP-5 (DOCUMENTED PROCESSES) regarding documentation and best practice INTEROP-BP-G (RECOMMENDED LEGAL COMPLIANCE) regarding limitations imposed by laws. Please note the applicability of best practice INTEROP-BP-F (RECOMMENDED FEDERATION COMPLIANCE) and Requirement INTEROP-6 (THIRD-PARTY COMPLIANCE) regarding limitations arising from the involvement of THIRD-PARTIES such as intermediaries, similar service providers, or FEDERATIONS.

REFERENCES

Potential candidates for adoption include: ISO/IEC 27000 series, PCI-DSS, NIST SP 800-53-4, CSA CCM, COBIT v5, FFIEC (multiple documents), PCI-DSS, NISTIR 7621 R1 (draft)

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

POLICIES, RISK, SECURITY, OPEN-STANDARDS

SECURE-2. DATA INTEGRITY

Entities MUST implement industry-accepted practices to protect the confidentiality and integrity of identity data - including authentication data and attribute values - during the execution of all digital identity management functions, and across the entire data lifecycle (collection through destruction).

SUPPLEMENTAL GUIDANCE

The execution of all identity transactions and functions must make use of transport that offers confidentiality and integrity protection (e.g., properly configured TLS).

Where operations and functions are executed by separate organizations, secure transport mechanisms and business processes must be used to preserve the confidentiality and integrity of identity data being transmitted to and stored by service providers.

Authentication data (e.g., passwords and passphrases) must be properly protected through industry accepted cryptographic techniques (e.g., salted and hashed).

Sensitive data collected during identity transactions must be protected at all times using industry accepted practices for encryption and data protection.

Appropriate access control measures must be in place to ensure access to identity data is restricted to only authorized users with a need to know. Appropriate access control measures including multifactor authentication must be in place to ensure that access to identity data by data custodians is restricted to users responsible for administering and maintaining the data. See SECURE-8 (MULTIFACTOR AUTHENTICATION). All access to identity data must be securely logged and separation of duties should be considered as a means to further limit access. See SECURE-14 (SECURITY LOGS).

Please note, the IDESG Privacy Requirements (PRIVACY-1 through PRIVACY-15) also impose separate requirements on the handling and storage of identifiers attributes and credentials.

REFERENCES

FICAM TFPAP Trust Criteria, LOA 1-3, Multiple Sections, PCI-DSS (actually Requirement 7 & 8 – pages 61-72), ISO 27002 (2005) Sec. 11, FFIEC, Wholesale Payment System Booklet (*http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_WholesalePaymentSystems.pdf*)

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ATTRIBUTE, DATA-INTEGRITY, SECURITY

SECURE-3. CREDENTIAL REPRODUCTION

Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.

SUPPLEMENTAL GUIDANCE

Potential controls that can be put in place to prevent unauthorized disclosure and reproduction include: The use of secure transport for credential and token data (see SECURE-2 (DATA INTEGRITY)); Implementation of industry accepted cryptographic techniques for the storage of credential and token data (see SECURE-2 (DATA INTEGRITY)); Implementation of industry accepted key management and protection techniques (see SECURE-11 (KEY MANAGEMENT)); Out-of-band distribution of credentials or tokens; In-person issuance of credentials or tokens; and Anti-tampering and/or counterfeiting mechanism for tokens with a physical instantiation

REFERENCES

FICAM TFPAP Trust Criteria, Registration and Issuance, LOA 2-3, #3 (p.21, 37)

APPLIES TO ACTIVITIES

CREDENTIALING

KEYWORDS

CREDENTIAL, DUPLICATION, DATA-INTEGRITY, PROCESS, SECURITY, TOKEN

SECURE-4. CREDENTIAL PROTECTION

Entities that issue or manage credentials and tokens MUST implement industry-accepted data integrity practices to enable individuals and other entities to verify the source of credential and token data.

SUPPLEMENTAL GUIDANCE

When providing token and credential information to users, steps must be taken to allow users to authenticate the source of the information. This can include digital signing of credential information, providing secure transport mechanisms for the information (e.g., properly configured TLS), or delivering the information out of band (e.g., traditional mail or SMS).

REFERENCES

FICAM TFPAP Trust Criteria, Registration and Issuance, LOA 2-3, #4 (p.21, 37)

APPLIES TO ACTIVITIES

CREDENTIALING

KEYWORDS

CREDENTIAL, DATA-INTEGRITY, SECURITY, TOKEN

SECURE-5. CREDENTIAL ISSUANCE

Entities that issue or manage credentials and tokens MUST do so in a manner designed to assure that they are granted to the appropriate and intended USER(s) only. Where registration and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of registration and issuance information that are commensurate with the stated assurance level MUST be included in business agreements and operating policies.

SUPPLEMENTAL GUIDANCE

Procedures exist to ensure the user(s) who receives the credential and associated tokens is the same user(s) who participated in registration. These can include: The use of secure transport for credential and token data (see SECURE-2 (DATA INTEGRITY)); Out-of-band distribution of credentials or tokens; In-person issuance of credentials or tokens.

Attribute verification (i.e., identity proofing) done during registration must be robust enough to provide sufficient confidence in the identity to support the intended use(s) of the credential. Subsequent attribute verification (i.e., proofing) must be executed in a manner consistent with intended use of the attributes.

REFERENCES

FICAM TFPAP Trust Criteria, Registration and Issuance, LOA 2-3, #4 (p.21, 37)

APPLIES TO ACTIVITIES

CREDENTIALING

KEYWORDS

CREDENTIAL, DATA-INTEGRITY, PROCESS, PROVISIONING, SECURITY, TOKEN

SECURE-6. CREDENTIAL UNIQUENESS

Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.

SUPPLEMENTAL GUIDANCE

A unique identifier must be assigned to each pairing of associated account and credential. This is to be used for the purposes of binding registration information with credentials in order to facilitate authentication and to avoid collisions of identifiers in the namespace.

REFERENCES

FICAM TFPAP Trust Criteria, Security, LOA 1-3, #1 (p.19), ISO 27002 (2005) Section 11 (Access Control), FFIEC, PCI-DSS 8.1, *http://pcidsscompliance.net/pci-dss-requirements/how-to-comply-to-requirement-8-of-pci-dss/*

APPLIES TO ACTIVITIES

CREDENTIALING, AUTHENTICATION

KEYWORDS

CREDENTIAL, IDENTIFIER, PROVISIONING, SECURITY

SECURE-7. TOKEN CONTROL

Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.

SUPPLEMENTAL GUIDANCE

Successful authentication requires that the user prove, through a secure authentication protocol, that he or she controls the appropriate token(s). Control is best demonstrated by a user providing token value through the authentication protocol (e.g., password, PIN, or biometric).

REFERENCES

FICAM TFPAP Trust Criteria, Authentication Process, LOA 2, #6 (p.21)

APPLIES TO ACTIVITIES

AUTHENTICATION

KEYWORDS

CONTROLS, IDENTIFIER, PROVISIONING, SECURITY, TOKEN

SECURE-8. MULTIFACTOR AUTHENTICATION

Entities that authenticate a USER MUST offer authentication mechanisms which augment or are alternatives to a password.

SUPPLEMENTAL GUIDANCE

Entities must offer users an authentication mechanism other than single-factor authentication based on a password as a shared secret. Examples include (but are not limited to): "something-you-have" (e.g., computing device, USB token, mobile phone, key fob, etc.) or "something-you-are" (e.g., biometric), or a combination of these. The additional or alternative mechanism(s) must ensure the binding and integration necessary for use as an authentication mechanism. See SECURE-9 (AUTHENTICATION RISK ASSESSMENT) and its Supplemental Guidance for more information about choosing risk appropriate authentication mechanisms.

REFERENCES

NIST SP 800-63-2

APPLIES TO ACTIVITIES

AUTHENTICATION

KEYWORDS

AUTHENTICATION, MULTIFACTOR, SECURITY, TOKEN

SECURE-9. AUTHENTICATION RISK ASSESSMENT

Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.

SUPPLEMENTAL GUIDANCE

Entities relying on authentication mechanisms must have a process in place for assessing the risks associated with providing access to their systems, applications, and/or network(s) and must leverage this to inform decisions on the selection of authentication mechanisms and supporting identity services.

Additional controls (e.g., geolocation or device identification) may be used. The party granting access may also request additional verified attributes to support authorization decisions where required by risk or business needs.

REFERENCES

NIST SP 800-63

APPLIES TO ACTIVITIES

AUTHORIZATION

KEYWORDS

ASSESSMENT, AUTHENTICATION, RISK, SECURITY

SECURE-10. UPTIME

Entities that provide and conduct digital identity management functions MUST have established policies and processes in place to maintain their stated assurances for availability of their services.

SUPPLEMENTAL GUIDANCE

At a minimum, service providers should have documented policies and processes to address disaster recovery, continuity of business, and denial of service prevention/recovery. See INTEROP-5 (DOCUMENTED PROCESSES).

REFERENCES

FFIEC-Business Continuity Planning, Retail Payment System Handbook, and Wholesale Payment System Handbook, E-Banking Handbook, *https://www.ffiec.gov/*; "IT Handbooks", at *http://ithandbook.ffiec.gov/it-booklets.aspx*; ISO 20000-1 (2011) (Part 1: Service management system requirements) and -2 (2012) (Part 2: Guidance on the application of service management systems) 1.6.3.1 & 1.6.3.2, ISO 27002 (2005)- Section 14.1; CSA CCM, *https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/* , NIST 800-53-4, Continuity Planning, Incident Response; COBIT V5 DSS04 "Manage Continuity"

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

PROCESS, SECURITY, UPTIME

SECURE-11. KEY MANAGEMENT

Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with industry-accepted practices.

SUPPLEMENTAL GUIDANCE

To support the security and interoperability of cryptographic solutions, organizations must follow best practices and standards for cryptographic algorithms and key management including the generation, protection, distribution, and recovery of keys.

REFERENCES

NIST 800-57 (3-parts – Key Management- *http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1*, *http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf*, *http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1;* , ISO/IEC 27002 - 12.3.1; PCI-DSS- 3.6.1-3.6.8 ; (see table of requirements at page 18+); FFIEC - Information Security *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf*, see 5.1.2.3(a), 5.3, 5.3.2, 2.1.2, 2.11; Wholesale Payment Systems Booklet, *http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_WholesalePaymentSystems.pdf*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

PKI, POLICIES, SECURITY

SECURE-12. RECOVERY AND REISSUANCE

Entities that issue credentials and tokens MUST implement methods for reissuance, updating, and recovery of credentials and tokens that preserve the security and assurance of the original registration and credentialing operations.

SUPPLEMENTAL GUIDANCE

Procedures must be in place to reasonably prevent hijacking of an account through recovery and reset options: a common vector for identity thieves and other attackers. At a minimum, service providers must provide reset, recovery, and reissuance procedures that afford a commensurate level of security to the processes used during the initial registration and credentialing operations. These procedures may include out-of-band verification, device identification, or any combination of similar techniques used to increase the security of reset, reissuance, and recovery options while also meeting IDESG Usability Requirements (USABLE-1 through USABLE-7).

REFERENCES

FICAM TFPAP Trust Criteria "Token & Credential Management"), LOA 2-3, #1, #2, #4, TFPAP Trust Criteria, Management and Trust Criteria, LOA 2-3, #3,#4, #6 (p.35); PCI-DSS v 2.0- 8.5.2 (p. 48) (corresponds to 8.2.2 in PCI-DSS v3. – p.67); NIST SP 800-63, Token and Credential Management Activities 7.1.2 (p. 58)

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING

KEYWORDS

ACCOUNT, CREDENTIAL, EXPIRY, LOSS, PROCESS, PROVISIONING, RECOVERY, SECURITY, TOKEN

SECURE-13. REVOCATION

Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.

SUPPLEMENTAL GUIDANCE

Service Providers must be capable of revoking, deactivating, or otherwise invalidating credentials or tokens. Invalidated credentials include those that have expired, have been determined to be compromised, or have been canceled by either the issuing entity or user.

Timeliness of revocation and deactivation may be dictated by regulation, environment, or trust frameworks.

REFERENCES

FICAM TFPAP Trust Criteria, Token & Credential Management, LOA 2-3, #4 (p.32)

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING

KEYWORDS

CREDENTIAL, EXPIRY, LOSS, PROCESS, REVOCATION, SECURITY, TOKEN

SECURE-14. SECURITY LOGS

Entities conducting digital identity management functions MUST log their transactions and security events, in a manner that supports system audits and, where necessary, security investigations and regulatory requirements. Timestamp synchronization and detail of logs MUST be appropriate to the level of risk associated with the environment and transactions.

SUPPLEMENTAL GUIDANCE

Transactions and events associated with systems that support identity management functions must be time-stamped and logged. Where necessary additional information related to the events also must be logged (such as the source of an authentication assertion) with the data needed to support audits.

Selection of logging and timestamping standards, processes, and procedures should be consistent with the processes outlined in SECURE-1 (SECURITY PRACTICES).

Audit records and logs must be protected consistent with SECURE-2 (DATA INTEGRITY).

REFERENCES

As an example: HIPAA Security Regulations regarding development and maintenance of logging procedures and records: 45 CFR Part 164, § 164.308(a)(1)(ii)(D), § 164.408(c): *http://www.ecfr.gov/cgi-bin/text-idx?node=pt45.1.164&rgn=div5*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

AUDIT, LOGS, PROCESS, SECURITY

SECURE-15. SECURITY AUDITS

Entities MUST conduct regular audits of their compliance with their own information security policies and procedures, and any additional requirements of law, including a review of their logs, incident reports and credential loss occurrences, and MUST periodically review the effectiveness of their policies and procedures in light of that data.

SUPPLEMENTAL GUIDANCE

Both internal and third-party audits are considered acceptable for conformance to this Requirement. This Requirement does not dictate frequency of audits. However, the processes, policies, procedures for conducting audits, and audit findings, as well as those for defining the frequency of audits, must be documented. Additionally, a process for remediating and correcting deficiencies identified during audits must also be documented.

REFERENCES

As an example: HIPAA Security Regulations regarding auditable controls and periodic review of logs: 45 CFR Part 164, § 164.308(a)(1)(ii)(D), § 164.312(b): *http://www.ecfr.gov/cgi-bin/text-idx?node=pt45.1.164&rgn=div5*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

AUDIT, LOGS, POLICIES, PROCESS, SECURITY

USABLE-1. USABILITY PRACTICES

Entities conducting digital identity management functions MUST apply user-centric design, and industry-accepted appropriate usability guidelines and practices, to the communications, interfaces, policies, data transactions, and end-to-end processes they offer, and remediate significant defects identified by their usability assessment.

SUPPLEMENTAL GUIDANCE

The term "user-centric" design is a key tenet and requirement of the IDESG founding document: the National Strategy for Trusted Identities in Cyberspace (NSTIC) dated April 15, 2011. This term is further described in Appendix A and is a common term in the User Experience domain.

REFERENCES

Consult the UXC Resources page located here for examples of non-normative UX practices: *https://www.idecosystem.org/wiki/UXC_resources*.

Consult the UXC Dictionary page located here for examples of UXC definitions of terms in these requirements and supplemental guidelines, in addition to those provided in Appendix A to this document: *https://www.idecosystem.org/wiki/UXC_Dictionary*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSESSMENT, DESIGN, REMEDIATION, USABILITY

USABLE-2. USABILITY ASSESSMENT

Entities MUST assess the usability of the communications, interfaces, policies, data transactions, and end-to-end processes they conduct in digital identity management functions.

SUPPLEMENTAL GUIDANCE

Entities may satisfy this Requirement by confirming that they have conducted a usability assessment of their digital identity management functions. Other Requirements and best practices in this set address their duty to mitigate issues identified in that assessment.

REFERENCES

Consult the UXC Guidelines and Metrics page:
https://www.idecosystem.org/wiki/User_Experience_Guidelines_Metrics

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSESSMENT, USABILITY

USABLE-3. PLAIN LANGUAGE

Information presented to USERS in digital identity management functions MUST be in plain language that is clear and easy for a general audience or the transaction's identified target audience to understand.

SUPPLEMENTAL GUIDANCE

Instructions for use of the system should be visible or easily retrievable whenever appropriate.

Help and documentation information should be easy to search, focused on the users' task, listing concrete steps to be carried out, and be concise.

Platform conventions for words, actions, and situations are consistent across the platform. Example: users should not have to wonder whether different words, situations, or actions mean the same thing across the platform.

The system should speak the users' language, following real-world conventions and making information appear in a natural and logical order. Example: Systems should use words or phrases and graphics or icons familiar to the user rather than system-oriented terms. Example: although the phrase "privacy enhancing technology" is widely in use in industry, research suggests that "privacy protection" is more readily understood and used by real users.

Error messages should be expressed in plain language, without codes, clearly indicating the problem and constructively suggesting a solution.

The user's identity status on a system should be clear to the user. Example: It should be clear to the user whether their identity is anonymous, pseudonymous or verified.

Any change in identity status should be presented in clear language to the user. Example: If a process requires a user to switch to a verified identity from a more anonymous state, the user should be clearly prompted to change their identity status.

Descriptions of states of identity (verified, anonymous, pseudonymous) should be linked to clear, easy to read, understandable and concise definitions.

If standard definitions are available, they should be used.

The design of the website should eliminate information that is irrelevant or rarely needed.

Layout and look/feel/branding, in addition to language, should also eliminate information that is rarely needed.

REFERENCES

None.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHOICE, CLARITY, LANGUAGE, OPTIONS, USABILITY

USABLE-4. NAVIGATION

All choices, pathways, interfaces, and offerings provided to USERS in digital identity management functions MUST be clearly identifiable by the USER.

SUPPLEMENTAL GUIDANCE

Systems should provide clear and easy to use pathways to help users recognize, diagnose, and recover from user-made errors.

The information needed by the user to understand any choice should be clearly visible in a single, visible window. Dialogues should not contain information that is irrelevant or rarely needed.

To mitigate the risk of errors, systems should allow the user the option to cancel, skip or decline, before they commit to a pathway action as well as provide a confirmation notice after they commit.

If an entity decides an action is required, and a user chooses to skip or decline this action, the entity's system should state clearly to the user if the transaction will not be completed and present a pathway for redress.

If a user accepts, skips or declines an option, the entity's system should state clearly to the user the transaction was or was not completed.

An entity's systems should allow users the choice to proceed anonymously, pseudonymously or with any chosen / assigned identity where appropriate.

An entity's systems should allow the user choice and clear options for changing the status of their identity. For example: switching to anonymous browsing.

Information users need to make decisions should be readily available and transparent to the user.

The identity of the entity and entity's systems with which the user is interacting should be clearly visible and understandable to users at all times. This includes third parties and changes between entities and users during sessions.

When a new user chooses an identity provider, the available options should be clearly presented so that a user can make an informed decision. When a new user visits a relying party site, the user should be presented with information about the request for identity proofing, verification or attributes and the types of identity providers or frameworks that are acceptable.

Clear pathways should exist for users to procure desired services.

The user should be presented with pathways to the identity services they desire, such as: privacy options, identity caching, etc.

Organizations should operate in a manner that allows individuals to easily switch service providers if the organization fails to meet user expectations, becomes insolvent, is incapable of adhering to policies, or revises their terms of service. See also INTEROP-BP-A (RECOMMENDED PORTABILITY).

REFERENCES

None.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHOICE, CLARITY, CONTROLS, CORRECTION, DESIGN, OPTIONS, USABILITY

USABLE-5. ACCESSIBILITY

All digital identity management functions MUST make reasonable accommodations to be accessible to as many USERS as is feasible, and MUST comply with all applicable laws and regulations on accessibility.

SUPPLEMENTAL GUIDANCE

Entities should review all accessibility standards and apply what they deem feasible to their sites based upon their legal and regulatory environment.

All entities, when feasible, should provide equivalent access to and use of information and systems to users with disabilities that is comparable to the use and access by those who are users without disabilities.

All sites should provide all feasible functionality to any user with a compatible internet connected device as those available to individuals without disabilities.

User with disabilities should have access to documentation tailored to their needs, as is feasible.

User-Centered Design that accounts for accessibility issues should be used whenever possible.

The specific requirements applicable to particular vertical industries (health, finance, etc.) should also be reviewed and applied when relevant.

REFERENCES

Some existing relevant standards and regulations include:

Section 508 contains information about accessibility: *https://www.section508.gov/*

For example, see ISO 9241 (2010) "Human-centred design processes for interactive systems" and ISO/IEC 40500 (2012) Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.0

Consult the UXC Resources page located here for examples of non-normative UX practices: *https://www.idecosystem.org/wiki/User_Experience_Guidelines_Metrics*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ACCESSIBLE, ACCOMMODATION, DESIGN, USABILITY

USABLE-6. USABILITY FEEDBACK

All communications, interfaces, policies, data transactions, and end-to-end processes provided in digital identity management functions MUST offer a mechanism to easily collect USERS' feedback on usability.

SUPPLEMENTAL GUIDANCE

All websites should provide a mechanism to gather feedback from users on site usability, adjusting the site design in response when appropriate.

Users should be provided equitable choices where possible around the mechanisms they can use to express their feedback to entities. Parameters, risks and benefits for those choices should be clear to the user.

REFERENCES

Additional information on collecting USER feedback can be found in our UXC Guidelines and Metrics page: *https://www.idecosystem.org/wiki/User_Experience_Guidelines_Metrics*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSESSMENT, DESIGN, FEEDBACK, USABILITY

USABLE-7. USER REQUIREMENTS

Wherever public open STANDARDS or legal requirements exist for collecting user requests~~requirements~~, entities conducting digital identity management functions MUST offer structured opportunities for USERS to document and express these requests~~their interface and accessibility requirements~~, early in their interactions with those functions. Entities MUST provide a response to those user requests~~requirement communications~~ on a reasonably timely basis.

SUPPLEMENTAL GUIDANCE

Any entity "collecting personal data," whether they are first or third parties, would mean that the entity is interacting with USERS directly and therefore should provide a response to user requests early on in the interaction or collection. Website USER do-not-track requests are an example of a USER request. An example of a site that handles responses to Do Not Track (DNT) requests in this manner is *Medium.com* which sends a single popup to new users, whether or not they are registered, about how they will handle the DNT request.

As a general principle, consent choices or other similar must-see-this-first information should be exchanged in a first encounter, and then honored in and presented in a consistent manner thereafter.

Suggested ways for User Experience mitigation includes using pop-up boxes or email responses to user requests. Links to information regarding additional use should provide adequate time for users to read the information presented to them.

The entity gathering requests should state whether identity information is being used, and the user must be notified.

Please note that the IDESG Privacy Requirements apply to these interactions and the data they generate.

REFERENCES

More information about Do Not Track can be found at these links:

FTC website on Do Not Track: *https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track*

Do Not Track standard work at the W3C: *http://www.w3.org/2011/tracking-protection/*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ACCESSIBLE, ACCOMMODATION, ACCOUNT, CHOICE, CONSENT, FEEDBACK, OPEN-STANDARDS, USABILITY

BEST PRACTICES AND POTENTIAL FUTURE REQUIREMENTS

INTEROP-BP-A. RECOMMENDED PORTABILITY

Entities SHOULD utilize services and systems that allow for identity account portability; specifically:
(a) IDENTITY-PROVIDERS SHOULD provide an easy to use method to allow to switch to a new provider(s).
(b) IDENTITY-PROVIDERS SHOULD provide departing USERS a mechanism to link their RELYING-PARTY accounts with their new provider(s).
(c) RELYING-PARTIES SHOULD provide USERS with a mechanism to associate multiple credentials to a single account.
(d) RELYING-PARTIES SHOULD provide USERS with a mechanism to have a single account per credential.
(e) IDENTITY-PROVIDERS SHOULD utilize services and systems that allow for affordable identity account portability.
(f) Wherever feasible, IDENTITY-PROVIDERS SHOULD provide USERS with a mechanism for portability of their privacy and other USER preferences.

SUPPLEMENTAL GUIDANCE

The term "account portability" means the ability for a USER to move to a different service provider to provide registration, credentialing and authentication services, and authorize the transfer of account information from an original service provider to the chosen provider. Portable identity data should include the following types of information: registration information, credentials, preferences, and associated accounts.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION

KEYWORDS

ACCOUNT, CHOICE, INTEROPERABILITY, PORTABILITY, USABILITY

INTEROP-BP-B. RECOMMENDED EXCHANGE STANDARDS

Entities that conduct digital identity management functions SHOULD utilize systems and processes to communicate and exchange identity-related data that conform to public open STANDARDS listed in the IDESG Standards Registry, or if that Registry does not include feasible options, then to nonproprietary specifications listed in the IDESG Standards Inventory.

SUPPLEMENTAL GUIDANCE

This best practice adds, to the requirement of INTEROP-4, the recommendation that the public open STANDARDS used for these data interface and exchange functions be selected from the IDESG Standards Registry or IDESG Standards Inventory. Please note the additional recommendations for use of formal models, at a higher level of abstraction, in INTEROP-BP-D.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ATTRIBUTE, INTEROPERABILITY, OPEN-STANDARDS, PROCESS, TRANSACTION

INTEROP-BP-C. RECOMMENDED TAXONOMY STANDARDS

Entities SHOULD utilize stable, published common taxonomies to enable semantic interoperability of attributes, and SHOULD use public open STANDARDS for those taxonomies when operating within communities where such STANDARDS have been established.

SUPPLEMENTAL GUIDANCE

Most taxonomies are used within a specific community of interest, such as the InCommon community for federated higher education identity transactions. See, for example, the published set at: *http://www.incommon.org/federation/attributesummary.html* That example provides detailed definitions and usage notes for the attributes most commonly shared within that community, and a more formal definition model at: *https://www.internet2.edu/media/medialibrary/2013/09/04/internet2-mace-dir-eduperson-201203.html*.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSERTION, ATTRIBUTE, INTEROPERABILITY, OPEN-STANDARDS

INTEROP-BP-D. RECOMMENDED PROCESS MODELS

Entities SHOULD employ stable, published common formal models and business processes for digital identity management functions, and SHOULD use public open STANDARDS for those models and processes where such STANDARDS have been established and are appropriate for those functions.

SUPPLEMENTAL GUIDANCE

This best practice recommends the adoption of standardized, modeled processes for digital identity management functions, so that participants in an identity ecosystem (including USERS, IDENTITY-PROVIDERS, AND RELYING-PARTIES) can have reasonable and common understanding of identity exchanges being conducted among communities of interest and identity federations. This best practice and potential future requirement anticipates the standardization of these functions and processes, eventually through standard development organizations and adoption by the IDESG.

Please note, this recommendation INTEROP-BP-D seeks adoption of formal models and formally defined business processes, in contrast to the use of on-the-wire data exchange standards recommended in INTEROP-BP-B. For more on the distinctions among business process layers, data structure layers (in the "business operational view") and data exchange methods and formats (in the "functional service view"), see ISO/IEC 14661 (2010).

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ARCHITECTURE, INTEROPERABILITY, OPEN-STANDARDS, PROCESS, TRANSACTION

INTEROP-BP-E. RECOMMENDED MODULARITY

Entities SHOULD implement modular identity components in their digital identity management functions.

SUPPLEMENTAL GUIDANCE

This best practice is for IDENTITY-PROVIDERS to offer modular identity solutions for the services and functions they perform relating to digital identity management. "Modular identity solutions" are services that can be used by USERS, RELYING-PARTIES and other participants either individually, or in combination with other modular services from the same or different providers, in order to provide choices and efficiencies in meeting their needs. Often such services are designed and offered around single function, and with STANDARDS-based interfaces that allow them to be composed with other purchased services or the purchaser's own systems.

On the concept of service modularity and composition generally, see: A Practical Guide to Federal Service Oriented Architecture (Federal CIO Council, 2008), at page 16: *https://cio.gov/wp-content/uploads/downloads/2013/03/PGFSOA_v1-1.pdf*, and OASIS SOA Reference Model (2006): *http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.html*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ARCHITECTURE, DESIGN, INTEROPERABILITY, OPEN-STANDARDS

INTEROP-BP-F. RECOMMENDED FEDERATION COMPLIANCE

When conducting digital identity management functions within an identity FEDERATION, entities SHOULD comply in all substantial respects with the published policies and system rules that explicitly required by that FEDERATION, according to the minimum criteria set by that FEDERATION.

SUPPLEMENTAL GUIDANCE

This best practice applies to entities that participate in a structured identity federation with published policies and system rules that apply to all participants in the federation. Entities are responsible for assessing and monitoring their own compliance with federation or system rules, except in cases where those rules provide for additional measures. This best practice only recommends that an entity confirm that they are in substantial compliance in all respects with the rules of the federation when operating within that federation.

Regarding "digital identity management functions", see Appendix A.

REFERENCES

References for Federation policies and rules: InCommon Bronze/Silver Identity Assurance profile, *https://www.incommon.org/docs/assurance/IAP.pdf;* Kantara Identity Assurance Framework, *https://kantarainitiative.org/confluence/display/certification/Identity+Assurance+Accreditation+and+Approval+Program;* FICAM Trust Framework Provider Adoption Process, *http://www.idmanagement.gov/documents/trust-framework-provider-adoption-process-tfpap-all-levels-assurance*

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

COMPLIANCE, FEDERATION, INTEROPERABILITY, POLICIES

INTEROP-BP-G. RECOMMENDED LEGAL COMPLIANCE

When conducting digital identity management functions, entities SHOULD comply in all substantial respects with all laws and regulations applicable to those relevant functions.

SUPPLEMENTAL GUIDANCE

This best practice applies to digital identity management functions for entities that operate in a regulated industry or perform online transactions subject to specific statutory/regulatory requirements such as HIPAA and COPPA. Such regulated entities are responsible for determining themselves the laws and regulations that apply to their activities, but this best practice applies only to those laws and regulations that address identity management functions. This best practice only recommends that entities have assessed and confirm that they have made that determination, and are in compliance. Entities who conduct identity transactions with them simply ought to be able to rely on the assumption that their counterparty is operating in accordance with applicable laws. Absence of findings from examiners or other reviewers are an indication of compliance.

REFERENCES

Some entities, and different classes of digital identity management transactions, may be subject to specialized or additional obligations by operation of law or regulation. Reference examples include: Know Your Customer Requirements, USA Patriot Act sec. 326; Health Insurance Portability and Accountability Act (HIPAA) regulations for certain healthcare personal and payment information; and Children's Online Privacy Protection Act (COPPA) for entities whose transactions are governed by its requirements.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

COMPLIANCE, INTEROPERABILITY, REGULATION

PRIVACY-BP-A. RECOMMENDED QUALITY CONTROLS

Entities SHOULD determine the necessary quality of personal information used in their digital identity management functions based on the risk of those functions and the information, including risk to the USERS involved.

SUPPLEMENTAL GUIDANCE

Entities obtaining personal information about a USER may have multiple ways to obtain the necessary data, or to assure its quality (generally, its accuracy, detail, timeliness or authoritative source). Some of those choices may be less invasive, or create less risk of USER privacy loss, than others. Additionally, some may result in higher- or lower-quality accuracy of the data. Entities SHOULD consider the effects of these choices on the USER whose personal information is being collected and used.

In the absence of formal data quality standards, entities SHOULD consider the timeliness, completeness, accuracy, and sources of data when evaluating the quality of personal information. These goals may be most easily implemented in system design, when identity management systems are being designed or renovated.

Regarding "personal information," see Appendix A and PRIVACY-1 (DATA MINIMIZATION).

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ARCHITECTURE, DATA-INTEGRITY, LIMITATION, RISK

PRIVACY-BP-B. RECOMMENDED TECHNOLOGY ENFORCEMENT

Wherever feasible, privacy requirements and policies SHOULD be implemented through technical mechanisms. Those technical privacy controls SHOULD be situated as low in the technology stack as possible.

SUPPLEMENTAL GUIDANCE

Privacy controls are mechanisms that mitigate privacy risk. These may overlap with security controls.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ARCHITECTURE, POLICIES, PROCESS

PRIVACY-BP-C. RECOMMENDED CONSEQUENCES OF DECLINING

Entities SHOULD provide short, clear notice to USERS of the consequences of declining to provide mandatory and optional personal information.

SUPPLEMENTAL GUIDANCE

This recommendation builds on and improves the mandate in Requirement PRIVACY-11 (OPTIONAL INFORMATION).

Regarding "personal information," see Appendix A and PRIVACY-1 (DATA MINIMIZATION). See also the IDESG Usability Requirements (USABLE-1 through USABLE-7) regarding the clarity of notices given to USERS and others.

If personal information is requested from USERS during registration that is optional, that designation should include a short and clear description justifying the request of that data.

If information collection or attribute value release is designated as mandatory, that designation should include a short and clear description of the consequences of declining to provide that information or allowing that release.

If an entity requests to release attributes values during a transaction that are the beyond the minimum necessary to complete that transaction, that release should be clearly presented as optional/a choice. That optional designation should include a short and clear description justifying the release of that data.

APPLIES TO ACTIVITIES

REGISTRATION, AUTHORIZATION

KEYWORDS

CHOICE, LIMITATION, NOTICE, USABILITY

USABLE-BP-A. RECOMMENDED ATTRIBUTE REQUIREMENTS QUERY

Entities conducting digital identity management functions SHOULD offer persistent opportunities for USERS to document and communicate their unique requirements about their attributes and how they are used. Entities SHOULD provide good-faith responses to those communications about requirements, before the USER is asked to agree to share their attributes.

SUPPLEMENTAL GUIDANCE

As a general principle, consent choices or other similar must-see-this-first information should be exchanged in a first encounter, and then honored in and presented in a consistent manner thereafter.

Suggested ways for User Experience mitigation include pop-up boxes or email responses to requests. Links to information for additional use and adequate time to read should be included in the process for [~~end~~] users.

Entities should state clearly in an easy to find manner to users whether identity information is being used.

Special attention should be paid to the unique dynamics and vulnerabilities for users around attribute exchanges, particularly toward transparency of communications.

See the related user-requirements-gathering processes described in USABLE-7 (USER REQUIREMENTS).

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION,

KEYWORDS

ACCOMMODATION, ATTRIBUTE, CHOICE, CONSENT, MINIMIZATION, USABILITY

IDESG

APPENDIX A: Defined Terms

The material below is a partial set of defined terms, a work-in-progress gathered from the IDESG Glossary, the User Experience Committee's "UXC Dictionary wiki", and the Requirements descriptions developed by various IDESG committees.
These definitions will be harmonized as a single normative glossary in a future edition of the Requirements. In this document, they are informative but not normative, and may be considered part of the Supplemental Guidance to this Requirements set. Some meanings may vary from Requirement to Requirement based on context.

* * *

ANONYMOUS: An interaction designed such that the data collected is not sufficient to infer the identity of the USER involved nor is such data sufficient to permit an entity to associate multiple interactions with a USER or to determine patterns of behavior with a USER.

DIGITAL IDENTITY MANAGEMENT FUNCTIONS: includes each of the functions described in the IDESG Functional Model (registration, credentialing, authentication, authorization, and intermediation), which also encompass enrollment, identity proofing, identity vetting, access control, attribute management, transaction processing, and identity data maintenance.

ENTITY / ENTITIES: Any organization providing identity services.

IDENTIFIERS: numbers or other non-attribute designations designed to specify individuals or sets of individuals in a system.

NONPROPRIETARY PUBLISHED FORMAT/SPECIFICATION: a known and consistent format that is published and transparent to all RELYING-PARTIES and IDENTITY-PROVIDERS in the relevant network, and is not controlled by a commercial interest.

PERSONAL INFORMATION: broadly means any information about or linked to a USER that is collected, used, transmitted, or stored in or by digital identity management functions. <

PSEUDONYMOUS: An interaction designed such that the data collected is not sufficient to allow the entity to infer the USER involved but which does permit an entity to associate multiple interactions with the USER's claimed identity.

REDRESS: When (a) an entity offers an opportunity for a party who is transacting with it to complain or ask for adjustment, if the transaction is unsatisfactory to that other party; and (b) the entity responds clearly to each request of that kind; and (c) if the request relates to the entity's failure to

comply with the IDESG Baseline Requirements, the entity cures the failure to comply, or provides a remedy for the failure.

USER: In USABILITY statements, refers to an individual human being. This does not include machines, algorithms, or other non-human agents or actors. Equivalents and related terms may include: user, user centric, user centered, human centered, end user, individual user, user-friendly.
In SECURITY statements, may refer either to an individual natural person, or to an entity such as a company or agency: Various security requirements may confer opportunities, rights or remedies on a party or account which is served by a cybersecurity function, whether that account relates to a single human or to an organization.
For definitions of user, user-centric and others, see the NSTIC Strategy (page 8 and throughout) :
https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

USER-CENTRIC: Systems, design and/or program processes that put the individual human being at the center of the activity. Equivalents and related terms may include: user centric, user centered, human centered, end user, individual user, user-friendly. For definitions of user, user-centric and others, see the NSTIC Strategy (at pages 8, 12, 15, 19, 21, 35 and 36):
https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

IDESG

INDEX OF KEYWORDS by page number

(non-normative, auto-generated)