IDEF Baseline Functional Requirements
v1.0

Approved 10/15/2015

IDENTITY ECOSYSTEM STEERING GROUP

IDEF Baseline Functional Requirements v1.0

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, include in the expanded version of this document, *IDEF Baseline Functional Requirements v1.0 with Supplemental Guidance*, 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 IDEF Functional Model v1.0 (*https://workspace.idesg.org/kws/public/download.php/81/IDEF-Functional-Model-v1.0.pdf*) are its specification of a provider's functional Core Operations Activities on pages 4-7, particularly Table 1.

(D) The Supplemental Guidance materials and related references are provided by IDESG's committees and experts as additional assistive but non-normative 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(for example, by hyperlinks) in other presentations of this material; and in later versions, may be changed or superseded by the eventual normative Glossary.

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.

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.

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.

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.

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.

INTEROP-6. THIRD-PARTY COMPLIANCE

Entities that act as THIRD-PARTY 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.

INTEROP-7. USER REDRESS

Entities MUST provide effective mechanisms for redress of complaints or problems arising from identity transactions or the, failure of the entity to comply with the IDESG Baseline Requirements. These mechanisms MUST be easy for USERS to find and access.

INTEROP-8. ACCOUNTABILITY

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

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.

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.

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.

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.

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.

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.

PRIVACY-7. USER DATA CONTROL

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

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.

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.

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.

PRIVACY-11. OPTIONAL INFORMATION

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

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.

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.

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.

PRIVACY-15. ATTRIBUTE SEGREGATION

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

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.

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).

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.

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.

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.

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.

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.

SECURE-8. MULTIFACTOR AUTHENTICATION

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

SECURE-9. AUTHENTICATION RISK ASSESSMENT

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

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.

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.

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.

SECURE-13. REVOCATION

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

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.

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.

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.

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.

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.

USABLE-4. NAVIGATION

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

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.

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.

USABLE-7. USER REQUESTS

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

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-centric, user-centered, human-entered, 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, 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