IDESG

TO THE IDENTITY ECOSYSTEM STEERING GROUP PLENARY

Version 1 of the Identity Ecosystem Framework (IDEF) is comprised of a Scoping Statement, Baseline Functional Requirements v1.0 (Requirements) as developed and approved by IDESG's committees, and the previously approved Functional Model v1.0. The Management Council has approved the Baseline Functional Requirements v1.0 and asks that the Plenary confirm these Requirements as ready for publication and sharing with our broader identity community, as guidance and a first set of tools towards concrete, widely-reliable voluntary networks for safe, constructive and productive digital identity transactions.

DRAFT IDEF Baseline Functional Requirements v1.0: as reviewed by IDESG Management Council 9 June 2015

File name: FMO-Combined-Reqts-Baseline-v4.1-20150609
File location: https://www.idecosystem.org/filedepot/folder/185 (eventual)

NOTE: (A) The text presented below is as finally approved by each committee. (B) Short titles for each item are included here, for ease of reading, but are not considered part of the normative text. (C) Certain words are CAPITALIZED below for ease of review, and identifying specific roles. That capitalization is not part of the normative text, and may be styled differently (for example, by hyperlinks to short glossary entries) in the presentation to self-assessors. (D) Please bear in mind that the order (ordinality) of these items may vary, based on how they are presented to self-assessors. We recommend that each one be viewed as a potentially independent statement, as if presented on single index cards or web screens.

Scope of the IDEF Baseline Functional Requirements v.1.0

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.

IDESG

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. *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.

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-8. *THIRD-PARTY COMPLIANCE*
Entities that act as 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.

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.

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*
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.

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.

IDESG

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.

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 factors 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.

IDESG

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

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.

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.

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.

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.

INTEROP-BP-E. *RECOMMENDED MODULARITY*
Entities SHOULD implement modular identity components in their digital identity management functions.

INTEROP-BP-F. *RECOMMENDED ACCOUNTABILITY*
Entities SHOULD be accountable for conformance to the IDESG Baseline Requirements, by providing mechanisms for auditing, validation, and verification.

INTEROP-BP-G. *RECOMMENDED USER REDRESS*
Entities SHOULD provide effective redress mechanisms for, and facilitation on behalf of, USERS who believe they have been harmed by the entity's failure to comply with the IDESG Baseline Requirements.

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.

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.

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.

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.