DRAFT IDESG SELF ASSESSMENT MATRIX

December 2015

FMO DRAFT v3.8 20151229

Name of Service Provider:	
Contact Person Name:	
Contact Person Title:	
Date of this Document:	

This document is part of the IDESG Self-Assessment Listing Service program. Before completing this, please review the Application Instructions: http://j.mp/SALS-instruc

Number	Baseline Requirement	Applies to:	FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	Comments: (This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.)
INTEROP-1	Entities MUST be capable of accepting external USERS authenticated by THIRD-PARTIES.	Authentication					
INTEROP-2	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.	Credentialing					
		Authentication					
		Authorization					
		Intermediation					
INTEROP-3	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.	Credentialing					
INTEROP-4	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.	Registration					
		Credentialing					
		Authentication					
		Authorization					
		Intermediation					
INTEROP-5	Entities MUST employ documented business policies and processes in conducting their digital identity management functions, including internally and in transactions between entities.	Registration					
		Credentialing					
		Authentication					
		Authorization					
		Intermediation					
INTEROP-6	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.	Registration					
		Credentialing					
		Authentication					
		Authorization					
		Intermediation					
INTEROP-7	When conducting digital identity management functions, entities MUST comply in all substantial respects with all laws and regulations applicable to those relevant functions.	Registration					
		Credentialing					
		Authentication					
		Authorization					
		Intermediation					

Number	Baseline Requirement		Applies to:	FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	Comments: (This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.)
INTEROP-8	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-1	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-2	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-3	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-4	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-5	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					

				FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.
Number	**Baseline Requirement**		**Applies to:**	**Status (choose one)**				**Comments:**
PRIVACY-6	Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-7	Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-8	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-9	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-10	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
PRIVACY-11	Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.		Registration					
			Authorization					
PRIVACY-12	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					

				FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.
Number	**Baseline Requirement**		**Applies to:**	**Status (choose one)**				**Comments:**
PRIVACY-13	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-14	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-15	Wherever feasible, identifier data MUST be segregated from attribute data.		Registration					
			Credentialing					
			Authorization					
SECURE-1	Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
SECURE-2	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).		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
SECURE-3	Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.		Credentialing					
SECURE-4	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.		Credentialing					
SECURE-5	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.		Credentialing					
SECURE-6	Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.		Credentialing					
			Authentication					

				FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.
Number	**Baseline Requirement**		**Applies to:**	**Status (choose one)**				**Comments:**
SECURE-7	Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.		Authentication					
SECURE-8	Entities that authenticate a USER MUST offer authentication factors which augment or are alternatives to a password.		Authentication					
SECURE-9	Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.		Authorization					
SECURE-10	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
SECURE-11	Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with industry-accepted practices.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
SECURE-12	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.		Registration					
			Credentialing					
SECURE-13	Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.		Registration					
			Credentialing					
SECURE-14	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					

				FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.
Number	**Baseline Requirement**		**Applies to:**	**Status (choose one)**				**Comments:**
SECURE-15	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
USABLE-1	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
USABLE-2	Entities MUST assess the usability of the communications, interfaces, policies, data transactions, and end-to-end processes they conduct in digital identity management functions.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
USABLE-4	All choices, pathways, interfaces, and offerings provided to USERS in digital identity management functions MUST be clearly identifiable by the USER.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
USABLE-5	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
USABLE-6	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
USABLE-7	Wherever public open STANDARDS or legal requirements exist for collecting user requirements, Entities MUST provide a response to those user requirement communications on a reasonably timely basis.Entities MUST provide a response to those user requirement communications on a reasonably timely basis.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					

				FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.
Number	**Baseline Requirement**		**Applies to:**	**Status (choose one)**				**Comments:**
	Recommended Best Practices:							
INTEROP-BP-A	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.		Registration					
			Credentialing					
			Authorization					
INTEROP-BP-B	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
INTEROP-BP-C	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
INTEROP-BP-D	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
INTEROP-BP-E	Entities SHOULD implement modular identity components in their digital identity management functions.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					

				FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION	This column is for additional information on the self-assessment status, support for the determination of compliance, status of actions underway to fulfill the requirement, plans for action to comply, or why the requirement is not under consideration or not applicable.
Number	**Baseline Requirement**		**Applies to:**	**Status (choose one)**				**Comments:**
INTEROP-BP-F	Entities SHOULD be accountable for conformance to the IDESG Baseline Requirements, by providing mechanisms for auditing, validation, and verification.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
INTEROP-BP-G	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-BP-A	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-BP-B	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					
PRIVACY-BP-C	Entities SHOULD provide short, clear notice to USERS of the consequences of declining to provide mandatory and optional personal information.		Registration					
			Authorization					
USABLE-BP-A	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.		Registration					
			Credentialing					
			Authentication					
			Authorization					
			Intermediation					