

DRAFT IDESG SELF ASSESSMENT MATRIX

Name of Service Provider:

Contact Person Name:

Contact Person Title:

Date of this document:

Note: this is only a rough sample.
The actual form for self-assessments and submission to IDESG may change, and must be downloaded from IDEFregistry.org.

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-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						

		<div>FULLY IMPLEMENTED</div> <div>IMPLEMENTATION UNDERWAY</div> <div>UNDER CONSIDERATION</div> <div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div>						
Number	Baseline Requirement	Applies to:	Status (choose one)					Comments:
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						
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						

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.

DRAFT: EXAMPLE ONLY
 Form may change; do not submit data on this form

				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-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						

		<div> <div>FULLY IMPLEMENTED</div> <div>IMPLEMENTATION UNDERWAY</div> <div>UNDER CONSIDERATION</div> <div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div> </div>					<p>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.</p>	
Number	Baseline Requirement	Applies to:	Status (choose one)					Comments:
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						<div> <div> DRAFT: EXAMPLE ONLY </div> <div> Form may change; do not submit data on this form </div> </div>
		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						

Number	Baseline Requirement	Applies to:	<div> <div>FULLY IMPLEMENTED</div> <div>IMPLEMENTATION UNDERWAY</div> <div>UNDER CONSIDERATION</div> <div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div> </div>					Comments:
			Status (choose one)					
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						

			<div> <div>FULLY IMPLEMENTED</div> <div>IMPLEMENTATION UNDERWAY</div> <div>UNDER CONSIDERATION</div> <div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div> </div>					
Number	Baseline Requirement	Applies to:	Status (choose one)					Comments:
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						
		Intermediation						
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						

		<div><div>FULLY IMPLEMENTED</div><div>IMPLEMENTATION UNDERWAY</div><div>UNDER CONSIDERATION</div><div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div></div>					
Number	Baseline Requirement	Applies to:	Status (choose one)				Comments:
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					
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					

Number	Baseline Requirement	Applies to:	Status (choose one)	Comments:
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	<div> <div>FULLY IMPLEMENTED</div> <div>IMPLEMENTATION UNDERWAY</div> <div>UNDER CONSIDERATION</div> <div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div> </div>	
		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		

		<div> <div>FULLY IMPLEMENTED</div> <div>IMPLEMENTATION UNDERWAY</div> <div>UNDER CONSIDERATION</div> <div>NOT APPLICABLE OR NOT UNDER CONSIDERATION</div> </div>					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	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	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-3	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.	Registration						
		Credentialing						
		Authentication						
		Authorization						
		Intermediation						

Number	Baseline Requirement	Applies to:	Status (choose one)					Comments:
			FULLY IMPLEMENTED	IMPLEMENTATION UNDERWAY	UNDER CONSIDERATION	NOT APPLICABLE OR NOT UNDER CONSIDERATION		
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						

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.

DRAFT: EXAMPLE ONLY
 Form may change; do not submit data on this form