IDESG Glossary

Final Draft

April 29, 2016

Prepared by

IDEF Functional Model & Glossary Working Group

Chair

Andrew Hughes

# Introduction

In March the Plenary Chair asked each standing IDESG Committee to designate a representative for an inter-committee work group to develop a glossary of terms from the IDEF for use by applicants in the IDESG SALS program.

Background. The WG started with the Key Words that were identified by the FMO and all committees and included with the Baseline Requirements – there were 64 of these undefined key terms. The WG used the following processes to develop the draft definitions for IDEF terms.

1. Review the use/context of all terms in the IDEF to determine whether the terms were used consistently in the IDEF -- the terms were used consistently.
2. Exclude any terms that were used with standard dictionary usage/definition. Include terms that have special meaning in the context of the IDEF.
3. Present definitions of terms from standards that have been adopted by the IDESG through the standards adoption process.
4. Present definitions for terms still undefined from standards that have been nominated and are currently in the standards adoption process.
5. Present definitions for terms still undefined from open standards in IDESG Inventory.
6. Determine best definition(s) for the intent/use of the term in the IDEF.

This document presents the proposed definitions from the WG for IDEF terms to be included in the glossary. The proposed definitions are intended to best represent the intended use for all uses of the term. They are derived from definitions found in the indicated standard sources, with minor modifications in some cases for clarity in the context of the Identity Ecosystem Framework (IDEF.) The source references can be used to find the original definitions.

The glossary terms are used in the following three IDESG documents, and some of the definitions are taken from these documents, particularly the Functional Model:

* IDEF Baseline Functional Requirements v1.0 with Supplemental Guidance [REQTS]
https://workspace.idesg.org/kws/public/download/85/IDEF-Baseline-Requirement-v1.0-with-Supplemental-Guidance.pdf
* Functional Model Representation of the Identity Ecosystem [FM]
https://workspace.idesg.org/kws/public/download/81/IDEF-Functional-Model-v1.0.pdf
* Standards Adoption Policy Version 2.0 (final draft) [SAPv2]
https://workspace.idesg.org/kws/public/document?document\_id=2642

# Glossary

|  |  |
| --- | --- |
| **Glossary term** | Definition and source or reference (see References) |
| ACCESSIBLE | A product, service, environment or facility which is usable by USERs with the widest range of capabilities. [ISO 9241-210] |
| ACCOUNTABILITY | The property of a system or system resource that ensures that the actions of a USER or AGENT may be traced uniquely to that USER or AGENT, which can then be held responsible for its actions. [RFC4949] |
| AGENT | A non-human application or service acting in the digital environment on behalf of a human USER. Synonymous with "non-person entity" (NPE).See USER. |
| 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 of a USER. [IDESG IDEF] [UXC-Dict]See PSEUDONYMOUS |
| ASSERTION | A statement from an ATTRIBUTE provider to a RELYING PARTY. [NIST SP 800-63-2]NOTE: ASSERTIONs may be used to communicate CLAIMs, ATTRIBUTEs, IDENTIFIERs, or DIGITAL IDENTITIES. See CLAIM |
| ATTRIBUTE | A named quality or characteristic that is claimed to be inherent in or ascribed to someone or something. [IDESG Taxonomy] |
| AUTHENTICATION[FM] | "AUTHENTICATION" is defined in the IDEF Functional Model in part as a "Process of determining the validity of one or more CREDENTIALs used to claim a DIGITAL IDENTITY." [FM]CREDENTIAL AUTHENTICATION: Process of determining the validity of one or more CREDENTIALs used to claim a DIGITAL IDENTITY. [IDESG Taxonomy]DIGITAL IDENTITY AUTHENTICATION: Process used to achieve sufficient confidence in the binding between the USER or AGENT and the presented DIGITAL IDENTITY. [OpenID Connect] |
| AUTHORIZATION[FM] | "AUTHORIZATION" is defined in the IDEF Functional Model in part as a "Process of granting or denying requests for specific access to resources." [FM] |
| CLAIM | A statement about the USER or AGENT asserting a property of the USER or AGENT without necessarily containing identity information.NOTE: CLAIMs refer to the content of an ASSERTION rather than the specific source and destination.See ASSERTION |
| CONTROL | SECURITY CONTROL: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [SP 800-37]PRIVACY CONTROL: The administrative, technical, and physical safeguards employed within an entity to ensure compliance with applicable privacy requirements and manage privacy risks. |
| CREDENTIAL | A set of data presented as evidence of a claimed DIGITAL IDENTITY. [IDESG Taxonomy] |
| CREDENTIALING[FM] | "CREDENTIALING" is defined in the IDEF Functional Model in part as a "Process to bind an established DIGITAL IDENTITY with a CREDENTIAL." [FM] |
| DATA INTEGRITY | The property that data has not been inappropriately altered.  |
| DIGITAL IDENTITY | An ATTRIBUTE set that can be uniquely distinguished in a given context and can be used for a digital interaction. [IDESG Taxonomy] |
| DIGITAL IDENTITY MANAGEMENT FUNCTIONS[FM] | 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 | Any organization providing or using identity services. [IDESG IDEF][UXC-Dict]NOTE: The correct usage of ENTITY is “Organization providing or using identity services”; synonymous with Service Provider in the ID Ecosystem. USER should be used for persons. AGENT should be used for non-persons. NOTE: The word “actor” has been employed in this Glossary to replace the term “entity” previously used in some definitions, where ENTITY (as an organization) is not exclusively intended. |
| FEDERATION | An association comprising any number of service providers and IDENTITY PROVIDERS. [SAML v2.0] NOTE: This definition concerns IDENTITY and CREDENTIAL FEDERATIONs. |
| IDENTIFIER | ATTRIBUTE or value that can be used to distinguish a DIGITAL IDENTITY. [IDESG Taxonomy] |
| IDENTITY | see DIGITAL IDENTITY |
| IDENTITY PROVIDER | An ENTITY that creates, maintains, and manages trusted identity information. [NSTAC] |
| INTERACTION | An event involving two or more actors.See TRANSACTION |
| INTERACTION DESIGN | A term given to a set of design areas that focuses on the INTERACTION value of content, as opposed to its presentation or information value. The INTERACTION topics include USER interface controls, error handling, and feedback systems. The term “INTERACTION DESIGN” is intended to differentiate these topics from other topics for purposes of evaluation and development. [Human Factors] |
| INTERMEDIATION[FM] | "INTERMEDIATION" (or "Transaction Intermediation") is defined in the IDEF Functional Model in part as "Processes and procedures that limit linkages between TRANSACTIONs and facilitate CREDENTIAL portability." [FM] |
| INTEROPERABILITY | The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together to mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate. [NSTAC] |
| MINIMIZATION | See the IDESG Baseline Requirement “PRIVACY-1. DATA MINIMIZATION” [Reqts] |
| MULTIFACTOR | MULTIFACTOR AUTHENTICATION: AUTHENTICATION using two or more different factors to achieve AUTHENTICATION. Factors include something one knows (e.g., password/PIN), something one has (e.g., cryptographic identification device, token), or something one is (e.g., biometric). [SP 800-53] |
| 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. [IDESG IDEF] |
| PATHWAY | A route or routes of events, actions or INTERACTIONs leading to a defined result. [UXC-Dict] |
| PERSONAL INFORMATION | Any information about or linked to a USER that is collected, used, transmitted, or stored in or by DIGITAL IDENTITY MANAGEMENT FUNCTIONS. [IDESG IDEF] |
| PROVISIONING | Creating USER access accounts and assigning privileges or entitlements within the scope of a defined process or INTERACTION; providing USERs with access rights to applications and other resources that may be available in an environment; may include the creation, modification, deletion, suspension or restoration of a defined set of privileges. [ABAC] |
| 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. [IDESG IDEF] [UXC-Dict] |
| REGISTRATION[FM] | "REGISTRATION" is defined in the IDEF Functional Model in part as a "process that establishes a DIGITAL IDENTITY for the purpose of issuing or associating a CREDENTIAL." [FM] |
| RELYING PARTY | Actor that relies on an identity ASSERTION or CLAIM. [ISO/IEC 29115] |
| STANDARD | OPEN STANDARDS are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. OPEN STANDARDS facilitate INTEROPERABILITY and data exchange among different products or services and are intended for widespread adoption. (ITU-T)See also: IDESG Standards Adoption Policy v2.0 [SAPv2] |
| TOKEN | Something that the claimant possesses and controls that is used to authenticate the claimant’s DIGITAL IDENTITY. [IDESG Taxonomy] |
| TRANSACTION | A specialized form of INTERACTION that involves an exchange of some kind.See INTERACTION |
| USABILITY | Extent to which a system, product or service can be used by USERs to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. [ISO/IEC 9241-210] |
| USER | An individual human being.See AGENT |
| 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. [IDESG IDEF] [UXC-Dict] |
| USER EXPERIENCE | A USER’s perceptions and responses resulting from the use of an ENTITY’s services as rendered by expected USER AGENTs. |

# References

| **Glossary source** | public URI | label (as cited in definition) |
| --- | --- | --- |
| **IDESG-approved Standards:** |  |  |
| NIST SP 800-37 | https://www.idesg.org/portals/0/documents/registry/sp800-37-rev1-final.pdf | [SP 800-37] |
| NIST SP 800-53 | https://www.idesg.org/portals/0/documents/registry/NIST.SP.800-53r4.pdf | [SP 800-53] |
| SAML v2.0 | https://www.oasis-open.org/standards#samlv2.0 | [SAML v2.0] |
| ISO/IEC 27001 & 27002 | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/ | [ISO/IEC 27000] |
| ISO/IEC 29115 Entity authentication assurance framework | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/ | [ISO/IEC 29115] |
| OpenID Connect Core 1.0  | http://openid.net/specs/openid-connect-core-1\_0.html#Terminology | [OpenID Connect] |
| **Other IDESG-created glossary sources:** |  |  |
| Taxonomy AHG and Management Council approved terms | https://wiki.idesg.org/wiki/index.php?title=Taxonomy\_AHG\_Glossary | [IDESG Taxonomy] |
| Appendix A of Baseline Functional Reqts v1.0 | https://workspace.idesg.org/kws/public/download/83/IDEF-Baseline-Requirements-v1.0-FINAL-10152015.pdf&wg\_abbrev=idesg\_document | [IDESG IDEF] |
| UXC Dictionary | https://wiki.idesg.org/wiki/index.php?title=UXC\_Dictionary(note that several terms in [IDESG IDEF] originated from this source) | [UXC-Dict] |
| Functional Model Representation of the Identity Ecosystem | https://workspace.idesg.org/kws/public/download/81/IDEF-Functional-Model-v1.0.pdf | [FM] |
| **Other glossary sources:** |  |  |
| NIST/NCCOE Attribute Based Access Control Building Block | https://nccoe.nist.gov/sites/default/files/documents/NCCoE\_ABAC\_Building\_Block\_v2\_final.pdf | [ABAC] |
| RFC 4949 - Internet Security Glossary v2 | https://tools.ietf.org/html/rfc4949 | [RFC4949] |
| Human Factors International | http://www.humanfactors.com/downloads/Glossary\_of\_Usability\_Terms.pdf | [Human Factors] |
| NSTAC Report to the President on the Internet of Things | https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf | [NSTAC] |
| ForeSee Results’ E-Government Transparency Index | http://www.nrc.gov/public-involve/open/evaluating-progress/foresee-transparency-index.pdf | [ForeSee] |
| **Standards under review by IDESG:** |  |  |
| NIST SP 800-63-2 | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf | [NIST SP 800-63-2] |
| ISO/IEC 9241-210 Human-centred design for interactive systems | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/ | [ISO/IEC 9241-210] |
| ISO/IEC 40500:2012 W3C Web Content Accessibility Guidelines 2.0 | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=58625 | [ISO/IEC 40500:2012] |
| **Sources consulted but not cited** |  |  |
| NICCS Cyber Glossary | https://niccs.us-cert.gov/glossary |  |
| NISTIR 7298 | http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf |  |
| OAUTH 2.0 | http://tools.ietf.org/html/rfc6749, etc. |  |
| InCommon Glossary | http://www.incommon.org/glossary.html |  |
| ISO/IEC Guide 98-1 Uncertainty of Measurement | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?c snumber=4633  |  |
| ISO/IEC 9241-11 | http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/ |  |
| Wikipedia | https://en.wikipedia.org/ |  |