ToIP Glossary

Specification Status: Public Review Draft 01 (PR1)

Latest Draft:

- Github Repository
- Submit/View Issues
- Discussions

Editors:

- Drummond Reed, Gen
- Henk van Cann

Contributors:

- Darrell O'Donnell, Continuum Loop Inc.
- Kevin Griffin, GLEIF
- Kor Dwarshuis
- [Neil Thomson] TODO
- [Nicky Hickman] TODO
- [Rieks Joosten] TODO
- TODO

Participate:

- GitHub repo
- Commit history

---

1. Status

This is the first public review draft of the ToIP Glossary. It is also the first version published using the Spec-Up specification editing utility developed by the Decentralized Identity Foundation.

2. Copyright Notice

This specification is subject to the **OWF Contributor License Agreement 1.0 - Copyright** available at https://www.openwebfoundation.org/the-agreements/the-owf-1-0-agreements-granted-claims/owf-contributor-license-agreement-1-0-copyright.

These terms are inherited from the Technical Stack Working Group at the Trust over IP (ToIP) Foundation. Working Group Charter

3. Terms of Use

These materials are made available under and are subject to the OWF CLA 1.0 - Copyright & Patent license. Any source code is made available under the Apache 2.0 license.

THESE MATERIALS ARE PROVIDED “AS IS.” The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series (“ToIP”), and its members and contributors (each of ToIP, its members and contributors, a “ToIP Party”) expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

4. Introduction

The ToIP Glossary is a deliverable of the ToIP Concepts and Terminology Working Group. Its purpose is to promote shared understanding of terms and concepts across the many different working groups, communities, enterprises, and ecosystems who are collaborating to develop and deploy decentralized digital trust infrastructure.

Contributions and feedback are encouraged from any stakeholder in this area of terminology.

5. Linking to this Glossary

This glossary is designed to be both human and machine readable. All terms are listed alphabetically; acronyms are listed separately and linked to the fully expanded terms. Document authors can link directly to any term using standard web links and anchors following this syntax:

`https://trustoverip.org/ctwg-main-glossary#term:xxxxx`

Where `xxxxx` is the term as it appears in the glossary, with any spaces are replaced by en-dashes (hyphens). For example, a link to the term `self-certifying identifer` would be:

`https://trustoverip.github.io/ctwg-main-glossary#self-certifiying-identifier`

A specification document written using the Decentralized Identity Foundation's open source Spec-Up editor may create special external references to terms in this glossary using the Spec-Up `xref` tag following this syntax:

`[[xref: glossary, xxxxx]]`

Where `glossary` is the text label the document author assigns to the URL of a Web-accessible glossary, and `xxxxx` is the term as it appears in that glossary, with any spaces are replaced by en-dashes (hyphens). For example, a Spec-Up external reference to the term `self-certifying identifer` using the label `toip` for this glossary would look like this:

`[[xref: toip, self-certifying-identifier]]`

6. Referenced Glossaries

The following glossaries were used as sources for some of the definitions in the ToIP Glossary. All source glossaries are cited in the definitions of each term.

Short Name	Source Glossary	URL
Wikipedia	Wikipedia	https://www.wikipedia.org/
eSSIF-Lab	eSSIF-Lab Glossary	https://essif-lab.github.io/framework/docs/essifLab-glossary

Short Name	Source Glossary	URL
NIST-CSRC	NIST Computer Security Resource Center Glossary	https://csrc.nist.gov/glossary/
PEMC IGR	Kantara Privacy Enhancing Mobile Credentials Implementors Guidance Report	https://kantarainitiative.org/download/pemc-implementors-guidance-report/
W3C DID	W3C Decentralized Identifiers (DIDs) 1.0	https://www.w3.org/TR/did-core/#terminology
W3C VC	W3C VC Data Model 1.1	https://www.w3.org/TR/vc-data-model/#terminology
Ethereum	Ethereum.org Glossary	https://ethereum.org/
Merriam-Webster	Merriam-Webster Dictionary	https://www.merriam-webster.com/dictionary/

7. Terms and Definitions

– There are 504 terms –

A B C D E F G H I J K L M N O P Q R S T U V W Z

AAL

See: authenticator assurance level.

ABAC

See: attribute-based access control.

acceptance network

A trust network designed to facilitate acceptance of verifiable data for its members.

acceptance

The action of a party receiving any form of verifiable data and using it to make a trust decision.

See also: acceptance network.

access control

The process of granting or denying specific requests for obtaining and using information and related information processing services.

Source: NIST-CSRC.

Supporting definitions:

Wikipedia: In physical security and information security, access control (AC) is the selective restriction of access to a place or other resource, while access management describes the process. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

accreditation

Formal declaration by an accrediting authority that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Source: NIST-CSRC

ACDC

See: Authentic Chained Data Container.

action

Something that is actually done (a ‘unit of work’ that is executed) by a single actor (on behalf of a given party), as a single operation, in a specific context.

Source: eSSIF-Lab.

actor

An entity that can act (do things/execute actions), e.g. people, machines, but not organizations. A digital agent can serve as an actor acting on behalf of its principal.

Source: eSSIF-Lab.

address

See: network address.

administering authority

See: administering body.

administering body

A legal entity delegated by a governing body to administer the operation of a governance framework and governed infrastructure for a digital trust ecosystem, such as one or more trust registries.

Also known as: administering authority.

agency

In the context of decentralized digital trust infrastructure, the empowering of a party to act independently of its own accord, and in particular to empower the party to employ an agent to act on the party's behalf.

agent

An actor that is executing an action on behalf of a party (called the principal of that actor). In the context of decentralized digital trust infrastructure, the term “agent” is most frequently used to mean a digital agent.

Source: eSSIF-Lab.

See also: wallet.

Note: In a ToIP context, an agent is frequently assumed to have privileged access to the wallet(s) of its principal. In market parlance, a mobile app performing the actions of an agent is often simply called a wallet or a digital wallet.

AID

See autonomic identifier.

anonymous

An adjective describing when the identity of a natural person or other actor is unknown.

See also: pseudonym.

anycast address

A network address (especially an IP address used for anycast routing of network transmissions.

anycast

Anycast is a network addressing and routing methodology in which a single IP-address is shared by devices (generally servers) in multiple locations. Routers direct packets addressed to this destination to the location nearest the sender, using their normal decision-making algorithms, typically the lowest number of BGP network hops. Anycast routing is widely used by content delivery networks such as web and name servers, to bring their content closer to end users.

Source: Wikipedia.

See also: broadcast, multicast, unicast.

appraisability

The ability for a communication endpoint identified with a verifiable identifier (VID) to be appraised for the set of its properties that enable a relying party or a verifier to make a trust decision about communicating with that endpoint.

See also: trust basis, verifiability.

appropriate friction

A user-experience design principle for information systems (such as digital wallets) specifying that the level of attention required of the holder for a particular transaction should provide a reasonable opportunity for an informed choice by the holder.

Source: PEMC IGR.

assurance level

A level of confidence in a claim that may be relied on by others. Different types of assurance levels are defined for different types of trust assurance mechanisms. Examples include authenticator assurance level, federation assurance level, and identity assurance level.

attestation

The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated. In the context of decentralized digital trust infrastructure, an attestation usually has a digital signature so that it is cryptographically verifiable.

Source: NIST-CSRC.

attribute-based access control

An access control approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed. Each object and subject has a set of associated attributes, such as location, time of creation, access rights, etc. Access to an object is authorized or denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and of the requesting subject.

Source: NIST-CSRC.

Supporting definitions:

Wikipedia: Attribute-based access control (ABAC), also known as policy-based access control for IAM, defines an access control paradigm whereby a subject's authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment attributes.

attribute

An identifiable set of data that describes an entity, which is the subject of the attribute.

See also: property.

Supporting definitions:

eSSIF-Lab: Data that represents a characteristic that a party (the owner of the attribute) has attributed to an entity (which is the subject of that attribute).

Note: An identifier is an attribute that uniquely identifies an entity within some context.

audit log

An audit log is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, event, or device.

Source: Wikipedia.

Also known as: audit trail.

See also: key event log.

audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

Source: NIST-CSRC.

auditor

The party responsible for performing an audit. Typically an auditor must be accredited.

See also: human auditable.

Authentic Chained Data Container

A digital data structure designed for both cryptographic verification and chaining of data containers. ACDC may be used for digital credentials.

For more information, see: ToIP ACDC Task Force.

authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source: NIST-CSRC.

See also: authenticator, verifiable message.

Supporting definitions:

Wikipedia: The act of proving an assertion, such as the identity of a computer system user.

authenticator assurance level

A measure of the strength of an authentication mechanism and, therefore, the confidence in it.

Also known as: AAL

Source: NIST-CSRC.

See also: federation assurance level, identity assurance level, identity binding.

Note: In NIST SP 800-63-3, AAL is defined in terms of three levels: AAL1 (Some confidence), AAL2 (High confidence), AAL3 (Very high confidence).

authenticator

Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.

Source: NIST-CSRC.

authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Source: NIST-CSRC.

See also: confidentiality, correlation privacy, cryptographic verifiability.

authoritative source

A source of information that a relying party considers to be authoritative for that information. In ToIP architecture, the trust registry authorized by the governance framework for a trust community is typically considered an authoritative source by the members of that trust community. A system of record is an authoritative source for the data records it holds. A trust anchor is an authoritative source for the beginning of a trust chain.

authoritative

> Information or data that comes from an authority for that information.

authority

A party of which certain decisions, ideas, policies, rules etc. are followed by other parties.

Source: eSSIF-Lab.

authorization graph

A graph of the authorization relationships between different entities in a trust-community. In a digital trust ecosystem, the governing body is typically the trust root of an authorization graph. In some cases, an authorization graph can be traversed by making queries to one or more trust registries.

See also: governance graph, reputation graph, trust graph.

authorization

The process of verifying that a requested action or service is approved for a specific entity.

Source: NIST-CSRC.

See also: permission.

authorized organizational representative

A person who has the authority to make claims, sign documents or otherwise commit resources on behalf of an organization.

Source: Law Insider

autonomic identifier

The specific type of self-certifying identifier defined by the KERI specifications.

Also known as: AID.

biometric

A measurable physical characteristic or personal behavioral trait used to recognize the AID, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Source: NIST

blockchain

A distributed ledger of cryptographically-signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

Source: NIST-CSRC

Supporting definitions:

Wikipedia: A distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). Since each block contains information about the previous block, they effectively form a chain (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

broadcast address

A broadcast address is a network address used to transmit to all devices connected to a multiple-access communications network. A message sent to a broadcast address may be received by all network-attached hosts. In contrast, a multicast address is used to address a specific group of devices, and a unicast address is used to address a single device. For network layer communications, a broadcast address may be a specific IP address.

Source: Wikipedia.

broadcast

In computer networking, telecommunication and information theory, broadcasting is a method of transferring a message to all recipients simultaneously. Broadcast delivers a message to all nodes in the network using a one-to-all association; a single datagram (or packet) from one sender is routed to all of the possibly multiple endpoints associated with the broadcast address. The network automatically replicates datagrams as needed to reach all the recipients within the scope of the broadcast, which is generally an entire network subnet.

Source: Wikipedia.

See also: anycast, multicast, unicast.

Supporting definitions:

NIST-CSRC: Transmission to all devices in a network without any acknowledgment by the receivers.

C2PA

See: Coalition for Content Provenance and Authenticity.

CA

See: certificate authority.

CAI

See: Content Authenticity Initiative.

capability

The ability for an actor or agent to perform a specific action on behalf of party.

certificate authority

The entity in a public key infrastructure (PKI) that is responsible for issuing public key certificates and exacting compliance to a PKI policy.

Source: NIST-CSRC.

Also known as: certification authority.

Supporting definitions:

Wikipedia: In cryptography, a certificate authority or certification authority (CA) is an entity that stores, signs, and issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.[1] The format of these certificates is specified by the X.509 or EMV standard.

certificate

See: public key certificate.

certification authority

See: certificate authority.

certification body

A legal entity that performs certification.

For more information: https://en.wikipedia.org/wiki/Professional_certification

certification

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented

correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Source: NIST-CSRC.

See also: accreditation

chain of trust

See: trust chain.

chained credentials

Two or more credentials linked together to create a trust chain between the credentials that is cryptographically verifiable.

Note: ACDCs are a type of digital credential that explicitly supports chaining.

chaining

See: trust chain.

channel

See: communication channel.

ciphertext

Encrypted (enciphered) data. The confidential form of the plaintext that is the output of the encryption function.

Source: NIST-CSRC.

claim

An assertion about a subject, typically expressed as an attribute or property of the subject. It is called a “claim” because the assertion is always made by

some party, called the issuer of the claim, and the validity of the claim must be judged by the verifier.

Supporting definitions:

W3C VC: An assertion made about a subject.

Wikipedia: A claim is a statement that one subject, such as a person or organization, makes about itself or another subject. For example, the statement can be about a name, group, buying preference, ethnicity, privilege, association or capability.

Note: If the issuer of the claim is also the subject of the claim, the claim is self-asserted.

Coalition for Content Provenance and Authenticity

C2PA is a Joint Development Foundation project of the Linux Foundation that addresses the prevalence of misleading information online through the development of technical standards for certifying the source and history (or provenance) of media content.

Also known as: C2PA.

See also: Content Authenticity Initiative.

communication channel

A communication channel refers either to a physical transmission medium such as a wire, or to a logical connection over a multiplexed medium such as a radio channel in telecommunications and computer networking. A channel is used for information transfer of, for example, a digital bit stream, from one or several senders to one or several receivers.

Source: Wikipedia.

See also: ToIP channel.

Supporting definitions:

eSSIF-Lab: a (digital or non-digital) means by which two actors can exchange messages with one another.

communication endpoint

A type of communication network node. It is an interface exposed by a communicating party or by a communication channel. An example of the latter type of a communication endpoint is a publish-subscribe topic or a group in group communication systems.

Source: Wikipedia.

See also: ToIP endpoint.

communication metadata

Metadata that describes the sender, receiver, routing, handling, or contents of a communication. Communication metadata is often observable even if the contents of the communication are encrypted.

See also: correlation privacy.

communication session

A finite period for which a communication channel is instantiated and maintained, during which certain properties of that channel, such as authentication of the participants, are in effect. A session has a beginning, called the session initiation, and an ending, called the session termination.

Supporting definitions:

NIST-CSRC: A persistent interaction between a subscriber and an end point, either a relying party or a Credential Service Provider. A session begins with an authentication event and ends with a session termination event. A session is bound by use of a session secret that the subscriber's software (a browser, application, or operating system) can present to the relying party or the Credential Service Provider in lieu of the subscriber's authentication credentials.

Wikipedia: In computer science and networking in particular, a session is a time-delimited two-way link, a practical (relatively high) layer in the TCP/IP protocol enabling interactive expression and information exchange between two or more communication devices or ends – be they computers, automated systems, or live active users (see login session). A session is established at a certain point in time, and then 'torn down' - brought to an end - at some later point. An established communication session may involve more than one

message in each direction. A session is typically stateful, meaning that at least one of the communicating parties needs to hold current state information and save information about the session history to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses. An established session is the basic requirement to perform a connection-oriented communication. A session also is the basic step to transmit in connectionless communication modes. However, any unidirectional transmission does not define a session.

communication

The transmission of information.

Source: Wikipedia.

See also: ToIP communication.

complex password

A password that meets certain security requirements, such as minimum length, inclusion of different character types, non-repetition of characters, and so on.

Supporting definitions:

Science Direct: According to Microsoft, complex passwords consist of at least seven characters, including three of the following four character types: uppercase letters, lowercase letters, numeric digits, and non-alphanumeric characters such as & $ * and !

compliance

In the context of decentralized digital trust infrastructure, compliance is the extent to which a system, actor, or party conforms to the requirements of a regulation, governance framework, or trust framework that pertains to that particular entity.

See also: Governance.

Supporting definitions:

eSSIF-Lab: The state of realization of a set of conformance criteria or normative framework of a party.

concept

An abstract idea that enables the classification of entities, i.e., a mental construct that enables an instance of a class of entities to be distinguished from entities that are not an instance of that class. A concept can be identified with a term.

Supporting definitions:

eSSIF-Lab: the ideas/thoughts behind a classification of entities (what makes entities in that class 'the same').

Wikipedia: A concept is defined as an abstract idea. It is understood to be a fundamental building block underlying principles, thoughts and beliefs. Concepts play an important role in all aspects of cognition.

confidential computing

Hardware-enabled features that isolate and process encrypted data in memory so that the data is at less risk of exposure and compromise from concurrent workloads or the underlying system and platform.

Source: NIST-CSRC.

Supporting definitions:

Wikipedia: Confidential computing is a security and privacy-enhancing computational technique focused on protecting data in use. Confidential computing can be used in conjunction with storage and network encryption, which protect data at rest and data in transit respectively. It is designed to address software, protocol, cryptographic, and basic physical and supply-chain attacks, although some critics have demonstrated architectural and side-channel attacks effective against the technology.

confidentiality

In a communications context, a type of privacy protection in which messages use encryption or other privacy-preserving technologies so that only authorized

parties have access.

See also: authenticity, correlation privacy.

Supporting definitions:

NIST-CSRC: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Wikipedia: Confidentiality involves a set of rules or a promise usually executed through confidentiality agreements that limits the access or places restrictions on certain types of information.

connection

A communication channel established between two communication endpoints. A connection may be ephemeral or persistent.

See also: ToIP connection.

consent management

A system, process or set of policies under which a person agrees to share personal data for specific usages. A consent management system will typically create a record of such consent.

Supporting definitions:

Wikipedia: Consent management is a system, process or set of policies for allowing consumers and patients to determine what health information they are willing to permit their various care providers to access. It enables patients and consumers to affirm their participation in e-health initiatives and to establish consent directives to determine who will have access to their protected health information (PHI), for what purpose and under what circumstances. Consent management supports the dynamic creation, management and enforcement of consumer, organizational and jurisdictional privacy policies.

Content Authenticity Initiative

The Content Authenticity Initiative (CAI) is an association founded in November 2019 by Adobe, the New York Times and Twitter. The CAI promotes an industry standard for provenance metadata defined by the C2PA. The CAI cites curbing disinformation as one motivation for its activities.

Source: Wikipedia.

Also known as: CAI.

controlled document

A governance document whose authority is derived from a primary document.

controller

In the context of digital communications, the entity in control of sending and receiving digital communications. In the context of decentralized digital trust infrastructure, the entity in control of the cryptographic keys necessary to perform cryptographically verifiable actions using a digital agent and digital wallet. In a ToIP context, the entity in control of a ToIP endpoint.

See also: device controller, DID controller, ToIP controller.

Supporting definitions:

eSSIF-Lab: the role that an actor performs as it is executing actions on that entity for the purpose of ensuring that the entity will act/behave, or be used, in a particular way.

correlation privacy

In a communications context, a type of privacy protection in which messages use encryption, hashes, or other privacy-preserving technologies to avoid the use of identifiers or other content that unauthorized parties may use to correlate the sender and/or receiver(s).

See also: authenticity, confidentiality.

counterparty

From the perspective of one party, the other party in a transaction, such as a financial transaction.

See also: first party, second party, third party.

Supporting definitions:

Wikipedia: A counterparty (sometimes contraparty) is a legal entity, unincorporated entity, or collection of entities to which an exposure of financial risk may exist.

credential family

A set of related digital credentials defined by a governing body (typically in a governance framework) to empower transitive trust decisions among the participants in a digital trust ecosystem.

credential governance framework

A governance framework for a credential family. A credential governance framework may be included within or referenced by an ecosystem governance framework.

credential offer

A protocol request invoked by an issuer to offer to issue a digital credential to the holder of a digital wallet. If the request is invoked by the holder, it is called an issuance request.

credential request

See: issuance request.

credential schema

A data schema describing the structure of a digital credential. The W3C Verifiable Credentials Data Model Specification defines a set of requirements for credential schemas.

credential

A container of claims describing one or more subjects. A credential is generated by the issuer of the credential and given to the holder of the credential. A credential typically includes a signature or some other means of proving its authenticity. A credential may be either a physical credential or a digital credential.

See also: verifiable credential.

Supporting definitions:

eSSIF-Lab: data, representing a set of assertions (claims, statements), authored and signed by, or on behalf of, a specific party.

W3C VC: A set of one or more claims made by an issuer.

criterion

In the context of terminology, a written description of a concept that anyone can evaluate to determine whether or not an entity is an instance or example of that concept. Evaluation leads to a yes/no result.

cryptographic binding

Associating two or more related elements of information using cryptographic techniques.

Source: NIST-CSRC.

cryptographic key

A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data. Symmetric cryptography refers to the practice of the same key being used for both encryption and decryption. Asymmetric cryptography has separate keys for encrypting and decrypting. These keys are known as the public keys and private keys, respectively.

Source: Wikipedia.

See also: controller.

cryptographic trust

A specialized type of technical trust that is achieved using cryptographic algorithms.

Contrast with: human trust.

cryptographic verifiability

The property of being cryptographically verifiable.

Contrast with: human auditability.

cryptographically bound

A state in which two or more elements of information have a cryptographic binding.

cryptographically verifiable

A property of a data structure that has been digitally signed using a private key such that the digital signature can be verified using the public key. Verifiable data, verifiable messages, verifiable credentials, and verifiable data registries are all cryptographically verifiable. Cryptographic verifiability is a primary goal of the ToIP Technology Stack.

See also: tamper evident, tamper resistant.

Contrast with: human auditable.

cryptography

TODO

custodial wallet

A digital wallet that is directly in the custody of a principal, i.e., under the principal's direct personal or organizational control. A digital wallet that is in the custody of a third party is called a non-custodial wallet.

custodian

A third party that has been assigned rights and duties in a custodianship arrangement for the purpose of hosting and safeguarding a principal's private keys, digital wallet and digital assets on the principal's behalf. Depending on the custodianship arrangement, the custodian may act as an exchange and provide additional services, such as staking, lending, account recovery, or security features.

Contrast with: guardian, zero-knowledge service provider.

See also: custodial wallet.

Supporting definitions:

NIST-CSRC: A third-party entity that holds and safeguards a user's private keys or digital assets on their behalf. Depending on the system, a custodian may act as an exchange and provide additional services, such as staking, lending, account recovery, or security features.

Note: While a custodian technically has the necessary access to in theory impersonate the principal, in most cases a custodian is expressly prohibited from taking any action on the principal's account unless explicitly authorized by the principal. This is what distinguishes custodianship from guardianship.

custodianship arrangement

The informal terms or formal legal agreement under which a custodian agrees to provide service to a principal.

dark pattern

A design pattern, mainly in user interfaces, that has the effect of deceiving individuals into making choices that are advantageous to the designer.

Source: Kantara PEMC Implementors Guidance Report

Also known as: deceptive pattern.

data packet

In telecommunications and computer networking, a network packet is a formatted unit of data carried by a packet-switched network such as the Internet. A packet consists of control information and user data; the latter is also known as the payload. Control information provides data for delivering the payload (e.g., source and destination network addresses, error detection codes, or sequencing information). Typically, control information is found in packet headers and trailers.

Source: Wikipedia.

data schema

A description of the structure of a digital document or object, typically expressed in a machine-readable language in terms of constraints on the structure and content of documents or objects of that type. A credential schema is a particular type of data schema.

Supporting definitions:

Wikipedia: An XML schema is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of documents of that type, above and beyond the basic syntactical constraints imposed by XML itself. These constraints are generally expressed using some combination of grammatical rules governing the order of elements, Boolean predicates that the content must satisfy, data types governing the content of elements and attributes, and more specialized rules such as uniqueness and referential integrity constraints.

data subject

The natural person that is described by personal data. Data subject is the term used by the EU General Data Protection Regulation.

data vault

See: digital vault.

data

In the pursuit of knowledge, data is a collection of discrete values that convey information, describing quantity, quality, fact, statistics, other basic units of meaning, or simply sequences of symbols that may be further interpreted. A datum is an individual value in a collection of data.

Source: Wikipedia.

See also: verifiable data.

Supporting definitions:

eSSIF-Lab: something (tangible) that can be used to communicate a meaning (which is intangible/information).

datagram

See: data packet.

decentralized identifier

A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically. The generic format of a DID is defined in section 3.1 DID Syntax of the W3C Decentralized Identifiers (DIDs) 1.0 specification. A specific DID scheme is defined in a DID method specification.

Source: W3C DID.

Also known as: DID.

See also: DID method, DID URL.

Decentralized Identity Foundation

A non-profit project of the Linux Foundation chartered to develop the foundational components of an open, standards-based, decentralized identity ecosystem for people, organizations, apps, and devices.

See also: OpenWallet Foundation, ToIP Foundation.

For more information, see: http://identity.foundation/

decentralized identity

A digital identity architecture in which a digital identity is established via the control of a set of cryptographic keys in a digital wallet so that the controller is not dependent on any external identity provider or other third party.

See also: federated identity, self-sovereign identity.

Decentralized Web Node

A decentralized personal and application data storage and message relay node, as defined in the DIF Decentralized Web Node specification. Users may have multiple nodes that replicate their data between them.

Source: DIF DWN Specification.

Also known as: DWN.

For more information, see: https://identity.foundation/decentralized-web-node/spec/

deceptive pattern

See: dark pattern.

decryption

The process of changing ciphertext into plaintext using a cryptographic algorithm and key. The opposite of encryption.

Source: NIST-CSRC.

deep link

In the context of the World Wide Web, deep linking is the use of a hyperlink that links to a specific, generally searchable or indexed, piece of web content on a website (e.g. “https://example.com/path/page”), rather than the website’s home page (e.g., “https://example.com”). The URL contains all the information needed to point to a particular item. Deep linking is different from mobile deep linking, which refers to directly linking to in-app content using a non-HTTP URI.

See also: out-of-band introduction.

Source: Wikipedia.

definition

A textual statement defining the meaning of a term by specifying criterion that enable the concept identified by the term to be distinguished from all other concepts within the intended scope.

Supporting definitions:

eSSIF-Lab: a text that helps parties to have the same understanding about the meaning of (and concept behind) a term, ideally in such a way that these parties can determine whether or not they make the same distinction.

Wikipedia: A definition is a statement of the meaning of a term (a word, phrase, or other set of symbols). Definitions can be classified into two large categories: intensional definitions (which try to give the sense of a term), and extensional definitions (which try to list the objects that a term describes). Another important category of definitions is the class of ostensive definitions, which convey the meaning of a term by pointing out examples. A term may have many different senses and multiple meanings, and thus require multiple definitions.

delegatee

The second party receiving a delegation from a first party (the delegator).

delegation credential

A credential used to perform delegation.

delegation

The act of a first party authorizing a second party to perform a set of actions for or on behalf of the first party. Delegation may be performed by the first party (the delegator) issuing a delegation credential that gives a certain set of capabilities to the second party (the delegatee).

delegator

The first party making a delegation to a second party (the delegatee).

Supporting definitions:

eSSIF-Lab: the transferral of ownership of one or more obligation of a party (the delegator), including the associated accountability, to another party (the delegatee), which implies that the delegatee can realize such obligation as it sees fit.

dependent

An entity for the caring for and/or protecting/guarding/defending of which a guardianship arrangement has been established with a guardian.

Source: eSSIF-Lab

See also: custodian.

Mental Model: eSSIF-Lab Guardianship

device controller

The controller of a device capable of digital communications, e.g., a smartphone, tablet, laptop, IoT device, etc.

dictionary

A dictionary is a listing of lexemes (words or terms) from the lexicon of one or more specific languages, often arranged alphabetically, which may include information on definitions, usage, etymologies, pronunciations, translation, etc. It is a lexicographical reference that shows inter-relationships among the data. Unlike a glossary, a dictionary may provide multiple definitions of a term depending on its scope or context.

Source: Wikipedia.

DID controller

An entity that has the capability to make changes to a DID document. A DID might have more than one DID controller. The DID controller(s) can be denoted by the optional `controller` property at the top level of the DID document. Note that a DID controller might be the DID subject.

Source: W3C DID.

See also: controller.

DID document

A set of data describing the DID subject, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID. A DID document might have one or more different representations as defined in section 6 of the W3C Decentralized Identifiers (DIDs) 1.0 specification.

Source: W3C DID.

DID method

A definition of how a specific DID method scheme is implemented. A DID method is defined by a DID method specification, which specifies the precise operations by which DIDs and DID documents are created, resolved, updated, and deactivated.

Source: W3C DID.

For more information: https://www.w3.org/TR/did-core/#methods

DID subject

The entity identified by a DID and described by a DID document. Anything can be a DID subject: person, group, organization, physical thing, digital thing, logical thing, etc.

Source: W3C DID.

See also: subject.

DID URL

A DID plus any additional syntactic component that conforms to the definition in section 3.2 of the W3C Decentralized Identifiers (DIDs) 1.0 specification. This includes an optional DID path (with its leading / character), optional DID query (with its leading ? character), and optional DID fragment (with its leading # character).

Source: W3C DID.

DID

See: decentralized identifier

digital agent

In the context of decentralized digital trust infrastructure, a software agent that operates in conjunction with a digital wallet to take actions on behalf of its controller.

Note: In a ToIP context, a digital agent is frequently assumed to have privileged access to the digital wallets of its principal. In market parlance, a mobile app that performs the actions of a digital agent is often simply called a wallet or a digital wallet.

digital asset

A digital asset is anything that exists only in digital form and comes with a distinct usage right. Data that do not possess that right are not considered

assets.

Source: Wikipedia.

See also: digital credential.

digital certificate

See: public key certificate.

digital credential

A credential in digital form that is signed with a digital signature and held in a digital wallet. A digital credential is issued to a holder by an issuer; a proof of the credential is presented by the holder to a verifier.

See also: issuance request, presentation request, verifiable credential.

Contrast with: physical credential.

Supporting definitions:

Wikipedia: Digital credentials are the digital equivalent of paper-based credentials. Just as a paper-based credential could be a passport, a driver's license, a membership certificate or some kind of ticket to obtain some service, such as a cinema ticket or a public transport ticket, a digital credential is a proof of qualification, competence, or clearance that is attached to a person.

digital ecosystem

A digital ecosystem is a distributed, adaptive, open socio-technical system with properties of self-organization, scalability and sustainability inspired from natural ecosystems. Digital ecosystem models are informed by knowledge of natural ecosystems, especially for aspects related to competition and collaboration among diverse entities.

Source: Wikipedia.

See also: digital trust ecosystem, trust community.

digital identity

An identity expressed in a digital form for the purpose representing the identified entity within a computer system or digital network.

Supporting definitions:

eSSIF-Lab: Digital data that enables a specific entity to be distinguished from all others in a specific context.

Wikipedia: Digital identity refers to the information utilized by computer systems to represent external entities, including a person, organization, application, or device. When used to describe an individual, it encompasses a person's compiled information and plays a crucial role in automating access to computer-based services, verifying identity online, and enabling computers to mediate relationships between entities.

digital rights management

Digital rights management (DRM) is the management of legal access to digital content. Various tools or technological protection measures (TPM) like access control technologies, can restrict the use of proprietary hardware and copyrighted works. DRM technologies govern the use, modification and distribution of copyrighted works (e.g. software, multimedia content) and of systems that enforce these policies within devices.

Source: Wikipedia.

Also known as: DRM.

digital signature

A digital signature is a mathematical scheme that uses cryptography for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authenticity), and that the message was not altered in transit (integrity).

Source: Wikipedia.

Supporting definitions:

NIST-CSRC: The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1. origin authentication, 2. data integrity, and 3. signer non-repudiation.

digital trust ecosystem

A digital ecosystem in which the participants are one or more interoperating trust communities. Governance of the various roles of governed parties within a digital trust ecosystem (e.g., issuers, holders, verifiers, certification bodies, auditors) is typically managed by a governing body using a governance framework as recommended in the ToIP Governance Stack. Many digital trust ecosystems will also maintain one or more trust lists and/or trust registries.

digital trust utility

An information system, network, distributed database, or blockchain designed to provide one or more supporting services to higher level components of decentralized digital trust infrastructure. In the ToIP stack, digital trust utilities are at Layer 1. A verifiable data registry is one type of digital trust utility.

digital vault

A secure container for data whose controller is the principal. A digital vault is most commonly used in conjunction with a digital wallet and a digital agent. A digital vault may be implemented on a local device or in the cloud; multiple digital vaults may be used by the same principal across different devices and/or the cloud; if so they may use some type of synchronization. If the capability is supported, data may flow into or out of the digital vault automatically based on subscriptions approved by the controller.

Also known as: data vault, encrypted data vault.

See also: enterprise data vault, personal data vault, virtual vault.

For more information, see: https://en.wikipedia.org/wiki/Personal_data_service, https://digitalbazaar.github.io/encrypted-data-vaults/

digital wallet

A user agent, optionally including a hardware component, capable of securely storing and processing cryptographic keys, digital credentials, digital assets and other sensitive private data that enables the controller to perform cryptographically verifiable operations. A non-custodial wallet is directly in the custody of a principal. A custodial wallet is in the custody of a third party. Personal wallets are held by individual persons; enterprise wallets are held by organizations or other legal entities.

See also: digital agent, key management system, wallet engine.

Supporting definitions:

eSSIF-Lab: a component that implements the capability to securely store data as requested by colleague agents, and to provide stored data to colleague agents or peer agents, all in compliance with the rules of its principal's wallet policy.

Wikipedia: A digital wallet, also known as an e-wallet, is an electronic device, online service, or software program that allows one party to make electronic transactions with another party bartering digital currency units for goods and services. This can include purchasing items either online or at the point of sale in a brick and mortar store, using either mobile payment (on a smartphone or other mobile device) or (for online buying only) using a laptop or other personal computer. Money can be deposited in the digital wallet prior to any transactions or, in other cases, an individual's bank account can be linked to the digital wallet. Users might also have their driver's license, health card, loyalty card(s) and other ID documents stored within the wallet. The credentials can be passed to a merchant's terminal wirelessly via near field communication (NFC).

Note: In market parlance, a mobile app that performs the actions of a digital agent and has access to a set of cryptographic keys is often simply called a wallet or a digital wallet.

distributed ledger

A distributed ledger (also called a shared ledger or distributed ledger technology or DLT) is the consensus of replicated, shared, and synchronized digital data that is geographically spread (distributed) across many sites, countries, or institutions. In contrast to a centralized database, a distributed ledger does not require a central administrator, and consequently does not have a single (central) point-of-failure. In general, a distributed ledger requires a peer-

to-peer (P2P) computer network and consensus algorithms so that the ledger is reliably replicated across distributed computer nodes (servers, clients, etc.). The most common form of distributed ledger technology is the blockchain, which can either be on a public or private network.

Source: Wikipedia.

domain

See: security domain.

See also: trust domain.

DRM

See: digital rights management.

DWN

See: Decentralized Web Node.

ecosystem governance framework

A governance framework for a digital trust ecosystem. An ecosystem governance framework may incorporate, aggregate, or reference other types of governance frameworks such as a credential governance framework or a utility governance framework.

- Also known as: EGF

ecosystem

See: digital ecosystem.

eIDAS

eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation with the stated purpose of governing “electronic identification and trust services for electronic transactions”. It passed in 2014 and its provisions came into effect between 2016-2018.

Source: Wikipedia.

encrypted data vault

See: digital vault.

encryption

Cryptographic transformation of data (called plaintext) into a form (called ciphertext) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state.

Source: NIST-CSRC.

end-to-end encryption

Encryption that is applied to a communication before it is transmitted from the sender’s communication endpoint and cannot be decrypted until after it is received at the receiver’s communication endpoint. When end-to-end encryption is used, the communication cannot be decrypted in transit no matter how many intermediaries are involved in the routing process.

Supporting definitions:

Wikipedia: End-to-end encryption (E2EE) is a private communication system in which only communicating users can participate. As such, no one, including the communication system provider, telecom providers, Internet providers or malicious actors, can access the cryptographic keys needed to converse. End-to-end encryption is intended to prevent data being read or secretly modified, other than by the true sender and recipient(s). The messages are encrypted by the sender but the third party does not have a means to decrypt them, and stores them encrypted. The recipients retrieve the encrypted data and decrypt it themselves.

End-to-End Principle

The end-to-end principle is a design framework in computer networking. In networks designed according to this principle, guaranteeing certain application-specific features, such as reliability and security, requires that they reside in the communicating end nodes of the network. Intermediary nodes, such as gateways and routers, that exist to establish the network, may implement these to improve efficiency but cannot guarantee end-to-end correctness.

Source: Wikipedia.

For more information, see: https://trustoverip.org/permalink/Design-Principles-for-the-ToIP-Stack-V1.0-2022-11-17.pdf

endpoint system

The system that operates a communications endpoint. In the context of the ToIP stack, an endpoint system is one of three types of systems defined in the ToIP Technology Architecture Specification.

See also: intermediary system, supporting system.

endpoint

See: communication endpoint.

See also: ToIP endpoint.

enterprise data vault

A digital vault whose controller is an organization.

enterprise wallet

A digital wallet whose holder is an organization.

Contrast with: personal wallet.

entity

Someone or something that is known to exist.

Source: eSSIF-Lab.

ephemeral connection

A connection that only exists for the duration of a single communication session or transaction.

Contrast with: persistent connection.

expression language

A language for creating a computer-interpretable (machine-readable) representation of specific knowledge.

Source: Wikipedia.

FAL

See: federation assurance level.

federated identity

A digital identity architecture in which a digital identity established on one computer system, network, or trust domain is linked to other computer systems, networks, or trust domains for the purpose of identifying the same entity across those domains.

See also: decentralized identity, self-sovereign identity.

Supporting definitions:

NIST-CSRC; A process that allows for the conveyance of identity and authentication information across a set of networked systems.

Wikipedia: A **federated identity** in information technology is the means of linking a person's electronic identity and attributes, stored across multiple

distinct identity management systems.

federation assurance level

A category that describes the federation protocol used to communicate an assertion containing authentication) and attribute information (if applicable) to a relying party, as defined in NIST SP 800-63-3 in terms of three levels: FAL 1 (Some confidence), FAL 2 (High confidence), FAL 3 (Very high confidence).

Source: NIST-CSRC.

See also: authenticator assurance level, identity assurance level.

federation

A group of organizations that collaborate to establish a common trust framework or governance framework for the exchange of identity data in a federated identity system.

See also: trust community

Supporting definitions:

NIST-CSRC: A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.

fiduciary

A fiduciary is a person who holds a legal or ethical relationship of trust with one or more other parties (person or group of persons). Typically, a fiduciary prudently takes care of money or other assets for another person. One party, for example, a corporate trust company or the trust department of a bank, acts in a fiduciary capacity to another party, who, for example, has entrusted funds to the fiduciary for safekeeping or investment. In a fiduciary relationship, one person, in a position of vulnerability, justifiably vests confidence, good faith, reliance, and trust in another whose aid, advice, or protection is sought in some matter.

Source: Wikipedia.

first party

The party who initiates a trust relationship, connection, or transaction with a second party.

See also: third party, fourth party.

foundational identity

A set of identity data, such as a credential, issued by an authoritative source for the legal identity of the subject. Birth certificates, passports, driving licenses, and other forms of government ID documents are considered foundational identity documents. Foundational identities are often used to provide identity binding for functional identities.

Contrast with: functional identity.

fourth party

A party that is not directly involved in the trust relationship between a first party and a second party, but provides supporting services exclusively to the first party (in contrast with a third party, who in most cases provides supporting services to the second party). In its strongest form, a fourth party has a fiduciary relationship with the first party.

functional identity

A set of identity data, such as a credential, that is issued not for the purpose of establishing a foundational identity for the subject, but for the purpose of establishing other attributes, qualifications, or capabilities of the subject. Loyalty cards, library cards, and employee IDs are all examples of functional identities. Foundational identities are often used to provide identity binding for functional identities.

gateway

A gateway is a piece of networking hardware or software used in telecommunications networks that allows data to flow from one discrete network to another. Gateways are distinct from routers or switches in that they

communicate using more than one protocol to connect multiple networks[1][2] and can operate at any of the seven layers of the open systems interconnection model (OSI).

See also: intermediary.

Source: Wikipedia.

GDPR

See: General Data Protection Regulation.

General Data Protection Regulation

The General Data Protection Regulation (Regulation (EU) 2016/679, abbreviated GDPR) is a European Union regulation on information privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also governs the transfer of personal data outside the EU and EEA. The GDPR's goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business.

Source: Wikipedia.

Also known as: GDPR.

glossary

A glossary (from Ancient Greek: γλῶσσα, glossa; language, speech, wording), also known as a *vocabulary* or *clavis*, is an alphabetical list of terms in a particular domain of knowledge (scope) together with the definitions for those terms. Unlike a dictionary, a glossary has only one definition for each term.

Source: Wikipedia.

Governance - Risk Management - Compliance

Governance, risk management, and compliance (GRC) are three related facets that aim to assure an organization reliably achieves objectives, addresses

uncertainty and acts with integrity. Governance is the combination of processes established and executed by the directors (or the board of directors) that are reflected in the organization's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organization from reliably achieving its objectives under uncertainty. Compliance refers to adhering with the mandated boundaries (laws and regulations) and voluntary boundaries (company's policies, procedures, etc.)

Source: Wikipedia.

Also known as: GRC.

governance diamond

A term that refers to the addition of a governing body to the standard trust triangle of issuers, holders, and verifiers of credentials. The resulting combination of four parties represents the basic structure of a digital trust ecosystem.

governance document

A document with at least one identifier that specifies governance requirements for a trust community.

Note: A governance document is a component of a governance framework.

governance framework

A collection of one or more governance documents published by the governing body of a trust community.

Also known as: trust framework.

Note: In the digital identity industry specifically, a governance framework is better known as a trust framework. ToIP-conformant governance frameworks conform to the ToIP Governance Architecture Specification and follow the ToIP Governance Metamodel.

governance graph

A graph of the governance relationships between entities with a trust community. A governance graph shows which nodes are the governing bodies and which are the governed parties. In some cases, a governance graph can be traversed by making queries to one or more trust registries.Note: a party can play both roles and also be a participant in multiple governance frameworks.

See also: authorization graph, reputation graph, trust graph.

governance requirement

A requirement such as a policy, rule, or technical specification specified in a governance document.

See also: technical requirement.

governance

The act or process of governing or overseeing the realization of (the results associated with) a set of objectives by the owner of these objectives, in order to ensure they will be fit for the purposes that this owner intends to use them for.

Source: eSSIF-Lab.

See also: governing body, governance framework

governed information

Any information published under the authority of a governing body for the purpose of governing a trust community. This includes its governance framework and any information available via an authorized trust registry.

governed party

A party whose role(s) in a trust community is governed by the governance requirements in a governance framework.

governed use case

A use case specified in a governance document that results in specific governance requirements within that governance framework. Governed use cases may optionally be discovered via a trust registry authorized by the relevant governance framework.

governing authority

See: governing body.

governing body

The party (or set of parties) authoritative for governing a trust community, usually (but not always) by developing, publishing, maintaining, and enforcing a governance framework. A governing body may be a government, a formal legal entity of any kind, an informal group of any kind, or an individual. A governing body may also delegate operational responsibilities to an administering body.

Also known as: governing authority.

GRC

See: Governance - Risk Management - Compliance.

guardian

A party that has been assigned rights and duties in a guardianship arrangement for the purpose of caring for, protecting, guarding, and defending the entity that is the dependent in that guardianship arrangement. In the context of decentralized digital trust infrastructure, a guardian is issued guardianship credentials into their own digital wallet in order to perform such actions on behalf of the dependent as are required by this role.

Source: eSSIF-Lab

See also: custodian, zero-knowledge service provider.

Mental Model: eSSIF-Lab Guardianship

Supporting definitions:

Wikipedia: A legal guardian is a person who has been appointed by a court or otherwise has the legal authority (and the corresponding duty) to make decisions relevant to the personal and property interests of another person who is deemed incompetent, called a ward.

For more information, see: On Guardianship in Self-Sovereign Identity V2.0 (April, 2023).

Note: A guardian is a very different role than a custodian, who does not take any actions on behalf of a principal unless explicitly authorized.

guardianship arrangement

A guardianship arrangement (in a jurisdiction) is the specification of a set of rights and duties between legal entities of the jurisdiction. At a minimum, the entities participating in a guardianship arrangement are the guardian and the dependent.

Source: eSSIF-Lab

See also: custodianship arrangement.

Mental Model: eSSIF-Lab Guardianship

For more information, see: On Guardianship in Self-Sovereign Identity V2.0 (April, 2023).

guardianship credential

A digital credential issued by a governing body to a guardian to empower the guardian to undertake the rights and duties of a guardianship arrangement on behalf of a dependent.

hardware security module

A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing.

Source: NIST-CSRC.

Also known as: HSM.

Supporting definitions:

NIST-CSRC: A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing. FIPS 140-2 specifies requirements for HSMs.

Wikipedia: A physical computing device that safeguards and manages secrets (most importantly digital keys), performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. A hardware security module contains one or more secure cryptoprocessor chips.

hash function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message. Approved hash functions satisfy the following properties: *one-way* (it is computationally infeasible to find any input that maps to any pre-specified output); and *collision resistant* (it is computationally infeasible to find any two distinct inputs that map to the same output).

Source: NIST-CSRC.

hash

The result of applying a hash function to a message.

Source: NIST-CSRC.

Also known as: hash output, hash result, hash value.

holder binding

The process of creating and verifying a relationship between the holder of a digital wallet and the wallet itself. Holder binding is related to but NOT the same as subject binding.

holder

A role an agent performs by serving as the controller of the cryptographic keys and digital credentials in a digital wallet. The holder makes issuance requests for credentials and responds to presentation requests for credentials. A holder is usually, but not always, a subject of the credentials they are holding.

See also: issuer, verifier.

Mental model: W3C Verifiable Credentials Data Model Roles & Information Flows

Supporting definitions:

eSSIF-Lab: a component that implements the capability to handle presentation requests from a peer agent, produce the requested data (a presentation) according to its principal's holder-policy, and send that in response to the request.

W3C VC: A role an entity might perform by possessing one or more verifiable credentials and generating presentations from them. A holder is usually, but not always, a subject of the verifiable credentials they are holding. Holders store their credentials in credential repositories.

host

A host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices.

Source: NIST-CSRC.

Supporting definitions:

Wikipedia: A network host is a computer or other device connected to a computer network. A host may work as a server offering information

resources, services, and applications to users or other hosts on the network. Hosts are assigned at least one network address. A computer participating in networks that use the Internet protocol suite may also be called an IP host. Specifically, computers participating in the Internet are called Internet hosts. Internet hosts and other IP hosts have one or more IP addresses assigned to their network interfaces.

hourglass model

An architectural model for layered systems—and specifically for the protocol layers in a protocol stack—in which a diversity of supporting protocols and services at the lower layers are able to support a great diversity of protocols and applications at the higher layers through the use of a single protocol in the spanning layer in the middle—the "neck" of the hourglass.

See also: trust spanning protocol.

For more information, see: https://trustoverip.org/permalink/Design-Principles-for-the-ToIP-Stack-V1.0-2022-11-17.pdf and https://cacm.acm.org/magazines/2019/7/237714-on-the-hourglass-model/abstract

Note: The Internet's TCP/IP stack follows the hourglass model, and it is the design model for the ToIP stack.

HSM

See: hardware security module.

human auditable

A process or procedure whose compliance with the policies in a trust framework or governance framework can only be verified by a human performing an audit. Human auditability is a primary goal of the ToIP Governance Stack.

Contrast with: cryptographically verifiable.

human experience

The processes, patterns and rituals of acquiring knowledge or skill from doing, seeing, or feeling things as a natural person. In the context of decentralized digital trust infrastructure, the direct experience of a natural person using trust applications to make trust decisions within one or more digital trust ecosystems.

Note: Human experience includes social experiences (e.g., rituals, behaviors, ceremonies and rites of passage), as well as customer experience, worker or employee experience, and user experience.

human-readable

Information that can be processed by a human but that is not intended to be machine-readable.

human trust

A level of assurance in a trust relationship or a trust decision that can be achieved only via human evaluation of applicable trust factors.

Contrast with: technical trust.

IAL

See: identity assurance level.

identification

The action of a party obtaining the set of identity data necessary to serve as that party's identity for a specific entity.

Note: The act of identification of a specific entity is relational to each party that needs to perform that action. Therefore each party may end up with their own set of identity data that meets their specific requirements for their specific scope.

identifier

A single attribute—typically a character string—that uniquely identifies an entity within a specific context (which may be a global context). Examples include the name of a party, the URL of an organization, or a serial number for a man-made thing.

Supporting definitions:

eSSIF-Lab: a character string that is being used for the identification of some entity (yet may refer to 0, 1, or more entities, depending on the context within which it is being used).

identity assurance level

A category that conveys the degree of confidence that a person's claimed identity is their real identity, for example as defined in NIST SP 800-63-3 in terms of three levels: IAL 1 (Some confidence), IAL 2 (High confidence), IAL 3 (Very high confidence).

Source: NIST-CSRC.

See also: authenticator assurance level, federation assurance level.

identity binding

The process of associating a set of identity data, such as a credential, with its subject, such as a natural person. The strength of an identity binding is one factor in determining an authenticator assurance level.

See also: identity assurance level, identity proofing.

identity controller

The controller (e.g., a natural person or organization) of an identity, especially a digital identity.

identity data

The set of data held by a party in order to provide an identity for a specific entity.

identity document

A physical or digital document containing identity data. A credential is a specialized form of identity document. Birth certificates, bank statements, and utility bills can all be considered identity documents.

identity proofing

The process of a party gathering sufficient identity data to establish an identity for a particular subject at a particular identity assurance level.

See also: identity binding.

Supporting definitions:

NIST-CSRC: The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity.

identity provider

An identity provider (abbreviated IdP or IDP) is a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network.

Source: Wikipedia.

Note: The term “identity provider” is used in federated identity systems because it is a required component of their architecture. By contrast, decentralized identity and self-sovereign identity systems do not use the term because they are architected to enable entities to create and control their own digital identities without the need to depend on an external provider.

identity

A collection of attributes or other identity data that describe an entity and enable it to be distinguished from all other entities within a specific scope of identification. Identity attributes may include one or more identifiers for an entity, however it is possible to establish an identity without using identifiers.

Supporting definitions:

eSSIF-Lab: the combined knowledge about that entity of all parties, i.e. the union of all partial identities of which that entity is the subject.

Note: Identity is relational to the party performing the identification. For example, if 100 different parties have an identity for the same entity, each of them may hold a different set of identity data enabling identification of that entity.

IDP

See: identity provider.

impersonation

In the context of cybersecurity, impersonation is when an attacker pretends to be another person in order to commit fraud or some other digital crime.

Supporting definitions:

Wikipedia: An impersonator is someone who imitates or copies the behavior or actions of another. As part of a criminal act such as identity theft, the criminal is trying to assume the identity of another, in order to commit fraud, such as accessing confidential information, or to gain property not belonging to them. Also known as social engineering and impostors.

integrity

In IT security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.

Source: Wikipedia.

intermediary system

An intermediary system routes messages between endpoint systems but is not otherwise involved in the processing of those messages. In the context of end-

to-end encryption, intermediary systems cannot decrypt the messages sent between the endpoint systems. In the ToIP stack, intermediary systems operate at ToIP Layer 2, the trust spanning layer. An intermediary system is one of three types of systems defined in the ToIP Technology Architecture Specification; the other two are endpoint systems and supporting systems.

See also: endpoint system, supporting system.

Internet protocol suite

The Internet protocol suite, commonly known as TCP/IP, is a framework for organizing the set of communication protocols used in the Internet and similar computer networks according to functional criteria. The foundational protocols in the suite are the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), and the Internet Protocol (IP).

Source: Wikipedia

Also known as: TCP/IP.

See also: protocol stack.

Internet Protocol

The Internet Protocol (IP) is the network layer communications protocol in the Internet protocol suite (also known as the TCP/IP suite) for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Source: Wikipedia.

Also known as: IP.

See also: Transmission Control Protocol, User Datagram Protocol.

IP address

An Internet Protocol address (IP address) is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: network interface identification, and location addressing.

Source: Wikipedia.

IP

See: Internet Protocol.

issuance request

A protocol request invoked by the holder of a digital wallet to obtain a digital credential from an issuer.

See also: presentation request.

issuance

The action of an issuer producing and transmitting a digital credential to a holder. A holder may request issuance by submitting an issuance request.

See also: presentation, revocation.

issuer

A role an agent performs to package and digitally sign a set of claims, typically in the form of a digital credential, and transmit them to a holder.

See also: verifier, holder.

Mental model: W3C Verifiable Credentials Data Model Roles & Information Flows

Supporting definitions:

eSSIF-Lab: a component that implements the capability to construct credentials from data objects, according to the content of its principal's issuer-Policy (specifically regarding the way in which the credential is to be

digitally signed), and pass it to the wallet-component of its principal allowing it to be issued.

W3C VC: A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.

jurisdiction

The composition of: a) a legal system (legislation, enforcement thereof, and conflict resolution), b) a party that governs that legal system, c) a scope within which that legal system is operational, and d) one or more objectives for the purpose of which the legal system is operated.

Source: eSSIF-Lab

Mental model: eSSIF-Lab Jurisdictions

KATE

See: keys-at-the-edge.

KERI

See: Key Event Receipt Infrastructure.

key establishment

A process that results in the sharing of a key between two or more entities, either by transporting a key from one entity to another (key transport) or generating a key from information shared by the entities (key agreement).

Source: NIST-CSRC.

key event log

An ordered sequence of records of key events.

Note: Key event logs are a fundamental data structure in KERI.

Key Event Receipt Infrastructure

A decentralized permissionless key management architecture.

Also known as: KERI.

For more information, see: https://keri.one/, ToIP ACDC Task Force

key event

An event in the history of the usage of a cryptographic key pair. There are multiple types of key events. The inception event is when the key pair is first generated. A rotation event is when the key pair is changed to a new key pair. In some key management systems (such as KERI), key events are tracked in a key event log.

key management system

A system for the management of cryptographic keys and their metadata (e.g., generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction). An automated key management system may be used to oversee, automate, and secure the key management process. A key management is often protected by implementing it within the trusted execution environment (TEE) of a device. An example is the Secure Enclave on Apple iOS devices.

Also known as: KMS.

Source: NIST-CRSC.

key

See: cryptographic key.

keys-at-the-edge

A key management architecture in which keys are stored on a user's local edge devices, such as a smartphone, tablet, or laptop, and then used in conjunction with a secure protocol to unlock a key management system (KMS) and/or a digital vault in the cloud. This approach can enable the storage and sharing of

large data structures that are not feasible on edge devices. This architecture can also be used in conjunction with confidential computing to enable cloud-based digital agents to safely carry out “user not present” operations.

Also known as: KATE.

KMS

See: key management system.

knowledge

The (intangible) sum of what is known by a specific party, as well as the familiarity, awareness or understanding of someone or something by that party.

Source: eSSIF-Lab.

Laws of Identity

A set of seven “laws” written by Kim Cameron, former Chief Identity Architect of Microsoft (1941-2021), to describe the dynamics that cause digital identity systems to succeed or fail in various contexts. His goal was to define the requirements for a unifying identity metasystem that can offer the Internet the identity layer it needs.

For more information, see: https://www.identityblog.com/?p=352.

Layer 1

See: ToIP Layer 1.

Layer 2

See: ToIP Layer 2.

Layer 3

See: ToIP Layer 3.

Layer 4

See: ToIP Layer 4.

Legal Entity Identifier

The Legal Entity Identifier (LEI) is a unique global identifier for legal entities participating in financial transactions. Also known as an LEI code or LEI number, its purpose is to help identify legal entities on a globally accessible database. Legal entities are organisations such as companies or government entities that participate in financial transactions.

Source: Wikipedia.

Note: LEIs are administered by the Global Legal Entity Identifier Foundation (GLEIF).

legal entity

An entity that is not a natural person but is recognized as having legal rights and responsibilities. Examples include corporations, partnerships, sole proprietorships, non-profit organizations, associations, and governments. (In some cases even natural systems such as rivers are treated as legal entities.)

See also: Legal Entity Identifier, legal person, organization.

legal identity

A set of identity data considered authoritative to identify a party for purposes of legal accountability under one or more jurisdictions.

See also: foundational identity, functional identity.

legal person

In law, a legal person is any person or 'thing' that can do the things a human person is usually able to do in law – such as enter into contracts, sue and be sued, own property, and so on.[3][4][5] The reason for the term "legal person" is that some legal persons are not people: companies and corporations are "persons" legally speaking (they can legally do most of the things an ordinary person can do), but they are not people in a literal sense (human beings).

Source: Wikipedia.

Contrast with: natural person.

See also: legal entity, organization.

legal system

A system in which policies and rules are defined, and mechanisms for their enforcement and conflict resolution are (implicitly or explicitly) specified. Legal systems are not just defined by governments; they can also be defined by a governance framework.

Source: eSSIF-Lab

LEI

See: Legal Entity Identifier.

level of assurance

See: assurance level.

liveness detection

Any technique used to detect a presentation attack by determining whether the source of a biometric sample is a live human being or a fake representation. This is typically accomplished using algorithms that analyze biometric sensor data to detect whether the source is live or reproduced.

Also known as: proof of presence.

locus of control

The set of computing systems under a party's direct control, where messages and data do not cross trust boundaries.

machine-readable

Information written in a computer language or expression language so that it can be read and processed by a computing device.

Contrast with: human-readable.

man-made thing

A thing generated by human activity of some kind. Man-made things include both active things, such as cars or drones, and passive things, such as chairs or trousers.

Source: Sovrin Foundation Glossary V3

Contrast with: natural thing.

Note: Active things are the equivalent of non-human actorsin the eSSIF-Lab mental model Parties, Actors, Actions. Also see Appendix B and Appendix C of the Sovrin Glossary.

mandatory

A requirement that must be implemented in order for an implementer to be in compliance. In ToIP governance frameworks, a mandatory requirement is expressed using a MUST or REQUIRED keyword as defined in IETF RFC 2119.

See also: recommended, optional.

For more information, see: https://www.rfc-editor.org/rfc/rfc2119.

message

A discrete unit of communication intended by the source for consumption by some recipient or group of recipients.

Source: Wikipedia.

See also: ToIP message, verifiable message.

metadata

Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

Source: NIST-CSRC.

See also: communication metadata.

Supporting definitions:

Wikipedia: Metadata (or metainformation) is "data that provides information about other data", but not the content of the data itself, such as the text of a message or the image itself.

mobile deep link

In the context of mobile apps, deep linking consists of using a uniform resource identifier (URI) that links to a specific location within a mobile app rather than simply launching the app. Deferred deep linking allows users to deep link to content even if the app is not already installed. Depending on the mobile device platform, the URI required to trigger the app may be different.

Source: Wikipedia.

MPC

See: multi-party computation.

multi-party computation

Secure multi-party computation (also known as secure computation, multi-party computation (MPC) or privacy-preserving computation) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a

function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

Source: Wikipedia.

Also known as: MPC, secure multi-party computation.

multi-party control

A variant of multi-party computation where multiple parties must act in concert to meet a control requirement without revealing each other's data. All parties are privy to the output of the control, but no party learns anything about the others.

multi-signature

A cryptographic signature scheme where the process of signing information (e.g., a transaction) is distributed among multiple private keys.

Source: NIST-CSRC.

multicast address

A multicast address is a logical identifier for a group of hosts in a computer network that are available to process datagrams or frames intended to be multicast for a designated network service.

Source: Wikipedia.

See also: broadcast address, unicast address.

multicast

In computer networking, multicast is group communication where data transmission is addressed (using a multicast address) to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many

distribution. Multicast should not be confused with physical layer point-to-multipoint communication.

Source: Wikipedia.

See also: anycast, broadcast, unicast.

natural person

A person (in legal meaning, one who has its own legal personality) that is an individual human being, as distinguished from the broader category of a legal person, which may refer to either a natural person or an organization of any kind.

Source: Wikipedia.

See also: legal entity, party.

Contrast with: legal person

natural thing

A thing that exists in the natural world independently of humans. Although natural things may form part of a man-made thing, natural things are mutually exclusive with man-made things.

Source: Sovrin Foundation Glossary V3.

Contrast with: man-made thing.

For more information see: Appendix B and Appendix C of the Sovrin Glossary

Note: Natural things (those recognized to have legal rights) can be parties but never actors in the eSSIF-Lab mental model Parties, Actors, Actions.

network address

A network address is an identifier for a node or host on a telecommunications network. Network addresses are designed to be unique identifiers across the network, although some networks allow for local, private addresses, or locally administered addresses that may not be unique. Special network addresses are

allocated as broadcast or multicast addresses. A network address designed to address a single device is called a unicast address.

Source: Wikipedia.

NIST-CSRC

Abbreviation for the NIST Computer Security Resource Center Glossary.

node

In telecommunications networks, a node (Latin: nodus, 'knot') is either a redistribution point or a communication endpoint. The definition of a node depends on the network and protocol layer referred to. A physical network node is an electronic device that is attached to a network, and is capable of creating, receiving, or transmitting information over a communication channel.

Source: Wikipedia.

non-custodial wallet

A digital wallet that is directly in the control of the holder, usually because the holder is the device controller of the device hosting the digital wallet (smartcard, smartphone, tablet, laptop, desktop, car, etc.) A digital wallet that is in the custody of a third party is called a custodial wallet.

objective

Something toward which a party (its owner) directs effort (an aim, goal, or end of action).

Source: eSSIF-Lab.

OOBI

See: out-of-band introduction.

OpenWallet Foundation

A non-profit project of the Linux Foundation chartered to build a world-class open source wallet engine.

See also: Decentralized Identity Foundation, ToIP Foundation.

For more information, see: https://openwallet.foundation/

operational circumstances

In the context of privacy protection, this term denotes the context in which privacy trade-off decisions are made. It includes the regulatory environment and other non-technical factors that bear on what reasonable privacy expectations might be.

Source: PEMC IGR

optional

A requirement that is not mandatory or recommended to implement in order for an implementer to be in compliance, but which is left to the implementer's choice. In ToIP governance frameworks, an optional requirement is expressed using a MAY or OPTIONAL keyword as defined in IETF RFC 2119.

See also: mandatory, recommended.

For more information, see: https://www.rfc-editor.org/rfc/rfc2119.

organization

A party that consists of a group of parties who agree to be organized into a specific form in order to better achieve a common set of objectives. Examples include corporations, partnerships, sole proprietorships, non-profit organizations, associations, and governments.

See also: legal entity, legal person.

Supporting definitions:

eSSIF-Lab: a party that is capable of setting objectives and making sure these are realized by actors that it has onboarded and/or by (vetted) parties that are committed to contribute to these objectives.

organizational authority

A type of authority where the party asserting its right is an organization.

out-of-band introduction

A process by which two or more entities exchange VIDs in order to form a cryptographically verifiable connection (e.g., a ToIP connection), such as by scanning a QR code (in person or remotely) or clicking a deep link.

Also known as: OOBI.

owner

The role that a party performs when it is exercising its legal, rightful or natural title to control a specific entity.

Source: eSSIF-Lab.

See also: controller.

P2P

See: peer-to-peer.

packet

The logical unit of network communications produced by the transport layer.

Source: NIST-CRSC.

party

An entity that sets its objectives, maintains its knowledge, and uses that knowledge to pursue its objectives in an autonomous (sovereign) manner. Natural persons and organizations are the typical examples.

Source: eSSIF-Lab.

See also: first party, second party, third party

password

A string of characters (letters, numbers and other symbols) that are used to authenticate an identity, verify access authorization or derive cryptographic keys.

Source: NIST-CSRC.

See also: complex password.

peer-to-peer

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the network. This forms a peer-to-peer network of nodes.

Source: Wikipedia.

peer

In the context of digital networks, an actor on the network that has the same status, privileges, and communications options as the other actors on the network.

See also: peer-to-peer.

Supporting definitions:

eSSIF-Lab: the actor with whom/which this other actor is communicating in that communication session.

permission

Authorization to perform some action on a system.

Source: NIST-CSRC.

persistent connection

A connection that is able to persist across multiple communication sessions. In a ToIP context, a persistent connection is established when two ToIP endpoints exchange verifiable identifiers (VIDs) that they can use to re-establish the connection with each other whenever it is needed.

Contrast with: ephemeral connection.

person

See natural person.

personal data store

See: personal data vault.

Note: In the market, the term “personal data store” has also been used to generally mean a combination of the functions of a personal digital agent, personal wallet, and personal data vault.

personal data vault

A digital vault whose controller is a natural person.

personal data

Any information relating to an identified or identifiable natural person (called a data subject under GDPR).

Source: NIST-CSRC.

personal wallet

A digital wallet whose holder is a natural person.

Contrast with: enterprise wallet.

personally identifiable information

Information (any form of data) that can be used to directly or indirectly identify or re-identify an individual person either singly or in combination within a single record or in correlation with other records. This information can be one or more attributes/fields/properties in a record (e.g., date-of-birth) or one or more records (e.g., medical records).

Source: NIST-CSRC

Also known as: PII.

See also: personal data, sensitive data.

physical credential

A credential in a physical form such as paper, plastic, or metal.

Contrast with: digital credential.

PII

See: personally identifiable information.

PKI

See: public key infrastructure.

plaintext

Unencrypted information that may be input to an encryption operation. Once encrypted, it becomes ciphertext.

Source: NIST-CSRC.

policy

Statements,rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component. Policies may be human-readable or machine-readable or both.

Example: An authorization policy might specify the correct access control rules for a software component.

Source: NIST-CSRC

See also: governance framework, governance requirement, rule.

PoP

See: proof of personhood.

presentation attack

A type of cybersecurity attack in which the attacker attempts to defeat a biometric liveness detection system by providing false inputs.

Supporting definitions:

NIST-CSRC: Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.

presentation request

A protocol request sent by the verifier to the holder of a digital wallet to request a presentation.

See also: issuance request.

presentation

A verifiable message that a holder may send to a verifier containing proofs of one or more claims derived from one or more digital credentials from one or more issuers as a response to a specific presentation request from a verifier.

Supporting definitions:

eSSIF-Lab: A (signed) digital message that a holder component may send to a verifier component that contains data derived from one or more verifiable credentials (that (a colleague component of) the holder component has received from issuer components of one or more parties), as a response to a specific presentation request of a verifiercomponent.

primary document

The governance document at the root of a governance framework. The primary document specifies the other controlled documents in the governance framework.

principal

The party for whom, or on behalf of whom, an actor is executing an action (this actor is then called an agent of that party).

Source: eSSIF-Lab

Principles of SSI

A set of principles for self-sovereign identity systems originally defined by the Sovrin Foundation and republished by the ToIP Foundation.

For more information, see: https://sovrin.org/principles-of-ssi/ and https://trustoverip.org/wp-content/uploads/2021/10/ToIP-Principles-of-SSI.pdf

privacy policy

A statement or legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data.

Source: Wikipedia

See also: security policy.

private key

In public key cryptography, the cryptographic key which must be kept secret by the controller in order to maintain security.

Supporting definitions:

NIST-CSRC: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

proof of control

See: proof of possession.

proof of personhood

Proof of personhood (PoP) is a means of resisting malicious attacks on peer-to-peer networks, particularly, attacks that utilize multiple fake identities, otherwise known as a Sybil attack. Decentralized online platforms are particularly vulnerable to such attacks by their very nature, as notionally democratic and responsive to large voting blocks. In PoP, each unique human participant obtains one equal unit of voting power, and any associated rewards.

Source: Wikipedia.

Also known as: PoP.

proof of possession

A verification process whereby a level of assurance is obtained that the owner of a key pair actually controls the private key associated with the public key.

Source: NIST-CSRC.

proof of presence

See: liveness detection.

proof

A digital object that enables cryptographic verification of either: a) the claims from one or more digital credentials, or b) facts about claims that do not reveal the data itself (e.g., proof of the subject being over/under a specific age without revealing a birthdate).

See also: zero-knowledge proof.

property

In the context of digital communication, an attribute of a digital object or data structure, such as a DID document or a schema.

See also: attribute, claim.

protected data

Data that is not publicly available but requires some type of access control to gain access.

protocol layer

In modern protocol design, protocols are layered to form a protocol stack. Layering is a design principle that divides the protocol design task into smaller steps, each of which accomplishes a specific part, interacting with the other parts of the protocol only in a small number of well-defined ways. Layering allows the parts of a protocol to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple.

Source: Wikipedia.

See also: hourglass model, ToIP stack.

protocol stack

The protocol stack or network stack is an implementation of a computer networking protocol suite or protocol family. Some of these terms are used interchangeably but strictly speaking, the *suite* is the definition of the communication protocols, and the *stack* is the software implementation of them.

Source: Wikipedia

See also: protocol layer.

pseudonym

A pseudonym is a fictitious name that a person assumes for a particular purpose, which differs from their original or true name (orthonym). This also differs from a new name that entirely or legally replaces an individual's own. Many pseudonym holders use pseudonyms because they wish to remain anonymous, but anonymity is difficult to achieve and often fraught with legal issues.

Source: Wikipedia.

public key certificate

A set of data that uniquely identifies a public key (which has a corresponding private key) and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information and is digitally signed by a certification authority (i.e., a trusted party), thereby binding the public key to the owner.

Source: NIST-CSRC.

See also: public key infrastructure.

Supporting definitions:

Wikipedia : In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the validity of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the

certificate's subject. In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization. However, in Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices.

public key cryptography

Public key cryptography, or asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key. Key pairs are generated with cryptographic algorithms based on mathematical problems termed one-way functions. Security of public key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security.

Source: Wikipedia.

See also: public key infrastructure.

public key infrastructure

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. The PKI includes the hierarchy of certificate authorities that allow for the deployment of digital certificates that support encryption, digital signature and authentication to meet business and security requirements.

Source: NIST-CSRC.

Supporting definitions:

Wikipedia: A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

public key

In public key cryptography, the cryptographic key that can be freely shared with anyone by the controller without compromising security. A party's public key must be verified as authoritative in order to verify their digital signature.

Supporting definitions:

NIST-CSRC: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

QR code

A QR code (short for “quick-response code”) is a type of two-dimensional matrix barcode—a machine-readable optical image that contains information specific to the identified item. In practice, QR codes contain data for a locator, an identifier, and web tracking.

Source: Wikipedia.

See also: out-of-band introduction.

RBAC

See: role-based access control.

real world identity

A term used to describe the opposite of digital identity, i.e., an identity (typically for a person) in the physical instead of the digital world.

Also known as: RWI.

See also: legal identity.

recommended

A requirement that is not mandatory to implement in order for an implementer to be in compliance, but which should be implemented unless the implementer has a good reason. In ToIP governance frameworks, a recommendation is

expressed using a SHOULD or RECOMMENDED keyword as defined in IETF RFC 2119.

See also: mandatory, optional.

For more information, see: https://www.rfc-editor.org/rfc/rfc2119.

record

A uniquely identifiable entry or listing in a database or registry.

registrant

The party submitting a registration record to a registry.

registrar

The party who performs registration on behalf of a registrant.

registration agent

A party responsible for accepting registration requests and authenticating the registrant. The term may also apply to a party accepting issuance requests for digital credentials.

registration

The process by which a registrant submits a record to a registry.

registry

A specialized database of records that serves as an authoritative source of information about entities.

See also: trust registry.

relationship context

A context established within the boundary of a trust relationship.

relationship

See ToIP relationship.

See also: trust relationship.

relying party

A party who accepts claims, credentials, trust graphs, or any other form of verifiable data from other parties (such as issuers, holders, trust registries, or other authoritative sources) in order to make a trust decision.

See also: verifier.

Note: The term “relying party” is more commonly used in federated identity architecture; the term “verifier” is more commonly used with decentralized identity architecture and verifiable credentials.

reputation graph

A graph of the reputation relationships between different entities in a trust community. In a digital trust ecosystem, the governing body may be one trust anchor of a reputation graph. In some cases, a reputation graph can be traversed by making queries to one or more trust registries.

See also: authorization graph, governance graph, trust graph.

reputation system

Reputation systems are programs or algorithms that allow users to rate each other in online communities in order to build trust through reputation. Some common uses of these systems can be found on e-commerce websites such as eBay, Amazon.com, and Etsy as well as online advice communities such as Stack Exchange.

Source: Wikipedia.

reputation

The beliefs or opinions that are generally held about an entity, typically developed as a result of social evaluation on a set of criteria, such as behavior, performance, or trustworthiness.

requirement

A specified condition or behavior to which a system needs to comply. Technical requirements are defined in technical specifications and implemented in computer systems to be executed by software actors. Governance requirements are defined in governance documents that specify policies and procedures to be executed by human actors. In ToIP specifications, requirements are expressed using the keywords defined in Internet RFC 2119.

See also: mandatory, recommended, optional.

For more information, see: https://www.rfc-editor.org/rfc/rfc2119.

revocation

In the context of digital credentials, revocation is an event signifying that the issuer no longer attests to the validity of a credential they have issued. In the context of cryptographic keys, revocation is an event signifying that the controller no longer attests to the validity of a public/private key pair for which the controller is authoritative.

See also: issuance, presentation.

Supporting definitions:

eSSIF-Lab: the act, by or on behalf of the party that has issued the credential, of no longer vouching for the correctness or any other qualification of (arbitrary parts of) that credential.

NIST-CSRC: **For digital certificates**: The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward. **For cryptographic keys**: A process whereby a notice is

made available to affected entities that keys should be removed from operational use prior to the end of the established cryptoperiod of those keys.

risk assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the overall ecosystem, resulting from the operation of an information system. Risk assessment is part of risk management, incorporates threat and vulnerability analyses, and considers risk mitigations provided by security controls planned or in place.

Source: NIST-CSRC.

Also known as: risk analysis.

Supporting definitions:

Wikipedia: Risk assessment determines possible mishaps, their likelihood and consequences, and the tolerances for such events.[1] The results of this process may be expressed in a quantitative or qualitative fashion. Risk assessment is an inherent part of a broader risk management strategy to help reduce any potential risk-related consequences. More precisely, risk assessment identifies and analyses potential (future) events that may negatively impact individuals, assets, and/or the environment (i.e. hazard analysis). It also makes judgments "on the tolerability of the risk on the basis of a risk analysis" while considering influencing factors (i.e. risk evaluation).

risk decision

See: trust decision.

risk management

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii)

employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Source: NIST-CSRC.

Supporting definitions:

eSSIF-Lab: a process that is run by (or on behalf of) a specific party for the purpose of managing the risks that it owns (thereby realizing specific risk objectives).

Wikipedia: Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

risk mitigation

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Source: NIST-CSRC.

risk

The effects that uncertainty (i.e. a lack of information, understanding or knowledge of events, their consequences or likelihoods) can have on the intended realization of an objectiveof a party.

Source: eSSIF-Lab

Supporting definitions:

NIST-CSRC: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

role-based access control

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Source: NIST-CSRC.

Supporting definitions:

Wikipedia: In computer systems security, role-based access control (RBAC) or role-based security is an approach to restricting system access to authorized users, and to implementing mandatory access control (MAC) or discretionary access control (DAC).

role credential

A credential claiming that the subject has a specific role.

role

A defined set of characteristics that an entity has in some context, such as responsibilities it may have, actions (behaviors) it may execute, or pieces of knowledge that it is expected to have in that context, which are referenced by a specific role name.

Source: eSSIF-Lab.

See also: role credential.

router

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions between networks and on the global Internet. Data sent through a network, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node. This process is called routing.

> Source: Wikipedia.

routing

> Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet. A router is a computing device that specializes in performing routing.
>
> Source: Wikipedia.

rule

> A prescribed guide for conduct, process or action to achieve a defined result or objective. Rules may be human-readable or machine-readable or both.
>
> See also: governance framework, policy.

RWI

> See: real world identity.

schema

> A framework, pattern, or set of rules for enforcing a specific structure on a digital object or a set of digital data. There are many types of schemas, e.g., data schema, credential verification schema, database schema.
>
> For more information, see: W3C Data Schemas.
>
> Note: `credentialSchema` is a Property Definition in the W3C VC Data Model, see 3.2.1

SCID

> See: self-certifying identifier.

scope

In the context of terminology, scope refers to the set of possible concepts within which: a) a specific term is intended to uniquely identify a concept, or b) a specific glossary is intended to identify a set of concepts. In the context of identification, scope refers to the set of possible entities within which a specific entity must be uniquely identified. In the context of specifications, scope refers to the set of problems (the problem space) within which the specification is intended to specify solutions.

Supporting definitions:

eSSIF-Lab: the extent of the area or subject matter (which we use, e.g., to define pattern, concept, term and glossaries in, but it serves other purposes as well).

second party

The party with whom a first party engages to form a trust relationship, establish a connection, make a delegation, or execute a transaction.

See also: third party.

Secure Enclave

A coprocessor on Apple iOS devices that serves as a trusted execution environment.

secure multi-party computation

See: multi-party computation.

Secure Sockets Layer

The original transport layer security protocol developed by Netscape and partners. Now deprecated in favor of Transport Layer Security (TLS).

Also known as: SSL.

security domain

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Source: NIST-CSRC

See also: trust domain.

security policy

A set of policies and rules that governs all aspects of security-relevant system and system element behavior.

Source: NIST-CSRC

See also: privacy policy.

self-asserted

A term used to describe a claim or a credential whose subject is also the issuer.

self-certified

When a party provides its own certification that it is compliant with a set of requirements, such as a governance framework. The term is also applied to data structures that are cryptographically verifiable such as self-certifying identifiers.

self-certifying identifier

A subclass of verifiable identifier (VID) that is cryptographically verifiable without the need to rely on any third party for verification because the identifier is cryptographically bound to the cryptographic keys from which it was generated.

See also: autonomic identifier.

Also known as: SCID.

self-sovereign identity

Self-sovereign identity is a decentralized identity architecture that implements the Principles of SSI — principally that it puts the identity controller (e.g., a natural person or organization) directly in control of the identifiers and credentials they use to assert their digital identity.

See also: federated identity.

Also known as: SSI.

Supporting definitions:

eSSIF-Lab: SSI (Self-Sovereign Identity) is a term that has many different interpretations, and that we use to refer to concepts/ideas, architectures, processes and technologies that aim to support (autonomous) parties as they negotiate and execute electronic transactions with one another.

Wikipedia: Self-sovereign identity (SSI) is an approach to digital identity that gives individuals control over the information they use to prove who they are to websites, services, and applications across the web. Without SSI, individuals with persistent accounts (identities) across the internet must rely on a number of large identity providers, such as Facebook (Facebook Connect) and Google (Google Sign-In), that have control of the information associated with their identity.

sensitive data

Personal data that a reasonable person would view from a privacy protection standpoint as requiring special care above and beyond other personal data.

Supporting definitions:

PEMC IGR: While all Personal Information may be regarded as sensitive in that an unauthorized processing of an individual's data may be offensive to that person, we use the term here to denote information that a reasonable person would view as requiring special care above and beyond other personal data. For reference see GDPR Recital #51 or Sensitive Personal Data in the W3C Data Privacy Vocabulary.

session

See: communication session.

sociotechnical system

An approach to complex organizational work design that recognizes the interaction between people and technology in workplaces. The term also refers to coherent systems of human relations, technical objects, and cybernetic processes that inhere to large, complex infrastructures. Social society, and its constituent substructures, qualify as complex sociotechnical systems.

Source: Wikipedia

software agent

In computer science, a software agent is a computer program that acts for a user or other program in a relationship of agency, which derives from the Latin *agere* (to do): an agreement to act on one's behalf. A user agent is a specific type of software agent that is used directly by an end-user as the principal.

Source: Wikipedia.

See also: digital agent.

Sovrin Foundation

A 501 ©(4) nonprofit organization established to administer the governance framework governing the Sovrin Network, a public service utility enabling self-sovereign identity on the internet. The Sovrin Foundation is an independent organization that is responsible for ensuring the Sovrin identity system is public and globally accessible.

For more information, see: https://sovrin.org/

spanning layer

A specific layer within a protocol stack that consists of a single protocol explicitly designed to provide interoperability between the protocol layers above

it and below it.

See also: hourglass model, trust spanning layer.

For more information, see: https://www.isi.edu/newarch/iDOCS/final.finalreport.pdf, National Academies of Sciences, Engineering, and Medicine. 1997. The Unpredictable Certainty: White Papers. Washington, DC: The National Academies Press. https://doi.org/10.17226/6062.

specification

See: technical specification.

SSI

See: self-sovereign identity.

Note: In some contexts, such as academic papers or industry conferences, this acronym has started to replace the term it represents.

SSL

See: Secure Sockets Layer.

stream

In the context of digital communications, and in particular streaming media, a flow of data delivered in a continuous manner from a server to a client rather than in discrete messages.

streaming media

Streaming media is multimedia for playback using an offline or online media player. Technically, the stream is delivered and consumed in a continuous manner from a client, with little or no intermediate storage in network elements. Streaming refers to the delivery method of content, rather than the content itself.

> Source: Wikipedia.

subject

The entity described by one or more claims, particularly in the context of credentials.

Supporting definitions:

W3C VC: A thing about which claims are made.

eSSIF-Lab: the (single) entity to which a given set of coherent data relates/pertains. Examples of such sets include attributes, Claims/Assertions, files/dossiers, verifiable credentials, (partial) identities, employment contracts, etc.

subscription

In the context of decentralized digital trust infrastructure, a subscription is an agreement between a first digital agent—the *publisher*—to automatically send a second digital agent—the *subscriber*—a message when a specific type of event happens in the wallet or vault managed by the first digital agent.

supporting system

A system that operates at ToIP Layer 1, the trust support layer of the ToIP stack. A supporting system is one of three types of systems defined in the ToIP Technology Architecture Specification.

See also: endpoint system, intermediary system.

Sybil attack

A Sybil attack is a type of attack on a computer network service in which an attacker subverts the service's reputation system by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence. It is named after the subject of the book *Sybil*, a case study of a woman diagnosed with dissociative identity disorder.

> Source: Wikipedia.

system of record

A system of record (SOR) or source system of record (SSoR) is a data management term for an information storage system (commonly implemented on a computer system running a database management system) that is the authoritative source for a given data element or piece of information.

Source: Wikipedia

See also: authoritative source, trust registry, verifiable data registry.

tamper evident

A process which makes alterations to the data easily detectable. Form digital data objects, this is typically achieved via cryptographic verification.

Source: NIST-CSRC.

tamper resistant

A process which makes alterations to data difficult (hard to perform), costly (expensive to perform), or both. For digital data objects, this is typically achieved via cryptographic verification.

Source: NIST-CSRC.

TCP/IP stack

The protocol stack implementing the TCP/IP suite.

TCP/IP

See: Internet Protocol Suite.

TCP

See: Transmission Control Protocol.

technical requirement

A requirement for a hardware or software component or system. In the context of decentralized digital trust infrastructure, technical requirements are a subset of governance requirements. Technical requirements are often specified in a technical specification.

For more information, see: https://datatracker.ietf.org/doc/html/rfc2119

Note: In ToIP architecture, both technical requirements and governance requirements are expressed using the keywords defined in IETF RFC 2119.

technical specification

A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component and often the procedures for determining whether these provisions have been satisfied.

Source: NIST-CSRC

See also: governance framework, governance requirement, policy, rule.

technical trust

A level of assurance in a trust relationship that can be achieved only via technical means such as hardware, software, network protocols, and cryptography.Cryptographic trust is a specialized type of technical trust.

Contrast with: human trust.

TEE

See: trusted execution environment.

term

A unit of text (i.e., a word or phrase) that is used in a particular context or scope to refer to a concept (or a relation between concepts, or a property of a concept).

Supporting definitions:

eSSIF-Lab: a word or phrase (i.e.: text) that is used in at least one scope /context to represent a specific concept.

Merriam Webster: a word or expression that has a precise meaning in some uses or is peculiar to a science, art, profession, or subject.

Note: A term MUST NOT be confused with the concept it refers to (which is an extremely common mistake).

terminology

Terminology is a group of specialized words and respective meanings in a particular field, and also the study of such terms and their use; the latter meaning is also known as *terminology science*. A term is a word, compound word, or multi-word expressions that in specific contexts is given specific meanings—meaning which may deviate from the meanings the same words have in other contexts and in everyday language. Terminology is a discipline that studies, among other things, the development of such terms and their interrelationships within a specialized domain. Terminology differs from *lexicography*, as the former involves the study of concepts, conceptual systems and their labels (terms), whereas lexicography studies words and their meanings.

Source: Wikipedia.

terms community

A group of parties who share the need for a common terminology.

See also: trust community.

terms wiki

A wiki website used by a terms community to input, maintain, and publish its terminology. The Concepts and Terminology Working Group at the ToIP

Foundation has created a simple template for GitHub-based terms wikis.

thing

An entity that is neither a natural person nor an organization and thus cannot be a party. A thing may be a natural thing or a man-made thing.

third party

A party that is not directly involved in the trust relationship between a first party and a second party, but provides supporting services to either or both of them.

three party model

The issuer—holder—verifier model used by all types of physical credentials and digital credentials to enable transitive trust decisions.

Also known as: trust triangle.

timestamp

A token or packet of information that is used to provide assurance of timeliness; the timestamp contains timestamped data, including a time, and a signature generated by a trusted timestamp authority (TTA).

Source: NIST-CSRC.

Supporting definitions:

TechTarget: A timestamp is the current time of an event that a computer records. Through mechanisms, such as the Network Time Protocol, a computer maintains accurate current time, calibrated to minute fractions of a second. Such precision makes it possible for networked computers and applications to communicate effectively.

TLS

See: Transport Layer Security.

ToIP application

A trust application that runs at ToIP Layer 4, the trust application layer.

ToIP channel

See: ToiP relationship.

ToIP communication

Communication that uses the ToIP stack to deliver ToIP messages between ToIP endpoints, optionally using ToIP intermediaries to provide authenticity, confidentiality, and correlation privacy.

ToIP connection

See: ToIP relationship.

ToIP controller

The controller of a verifiable identifier (VID) used with the ToIP stack.

ToIP endpoint

An endpoint that communicates via the ToIP Trust Spanning Protocol (TSP) as described in the ToIP Technology Architecture Specification.

ToIP Foundation

A non-profit project of the Linux Foundation chartered to define an overall architecture for decentralized digital trust infrastructure known as the ToIP stack.

See also: Decentralized Identity Foundation, OpenWallet Foundation.

For more information, see: https://trustoverip.org/.

ToIP Governance Architecture Specification

The specification defining the requirements for the ToIP Governance Stack published by the ToIP Foundation.

For more information, see: https://trustoverip.org/our-work/deliverables/.

ToIP governance framework

A governance framework that conforms to the requirements of the ToIP Governance Architecture Specification.

ToIP Governance Metamodel

A structural model for governance frameworks that specifies the recommended governance documents that should be included depending on the objectives of the trust community.

ToIP Governance Stack

The governance half of the four layer ToIP stack as defined by the ToIP Governance Architecture Specification.

See also: ToIP Technology Stack.

ToIP identifier

A verifiable identifier (VID) for an entity that is addressable using the ToIP stack.

See also: autonomic identifier, decentralized identifier, self-certifying identifier.

For more information, see: Section 6.4 of the ToIP Technology Architecture Specification.

ToIP intermediary

See: intermediary system.

ToIP Layer 1

The trust support layer of the ToIP stack, responsible for supporting the trust spanning protocol at ToIP Layer 2.

ToIP Layer 2

The trust spanning layer of the ToIP stack, responsible for enabling trust task protocols at ToIP Layer 3.

ToIP Layer 3

The trust task layer of the ToIP stack, responsible for enabling trust applications at ToIP Layer 4.

ToIP Layer 4

The trust application layer of the ToIP stack, where end-users have the direct human experience of using applications that call trust task protocols to engage in trust relationships and make trust decisions using ToIP decentralized digital trust infrastructure.

ToIP layer

One of four protocol layers in the ToIP stack. The four layers are ToIP Layer 1, ToIP Layer 2, ToIP Layer 3, and ToIP Layer 4.

For more information, see: ToIP Technology Architecture Specification, ToIP Governance Architecture Specification.

ToIP message

A message communicated between ToIP endpoints using the ToIP stack. ToIP messages are transmitted over the ToIP Trust Spanning Protocol (TSP) at Layer 2 of the ToIP stack.

ToIP relationship

A VID-to-VID relationship formed between two entities over the ToIP Trust Spanning Protocol.

ToIP specification

A specification published by the ToIP Foundation. ToIP specifications may be in one of three states: *Draft Deliverable*, *Working Group Approved Deliverable*, or *ToIP Approved Deliverable*.

ToIP stack

The layered architecture for decentralized digital trust infrastructure defined by the ToIP Foundation. The ToIP stack is a dual stack consisting of two halves: the ToIP Technology Stack and the ToIP Governance Stack. The four layers in the ToIP stack are ToIP Layer 1, ToIP Layer 2, ToIP Layer 3, and ToIP Layer 4.

For more information, see: ToIP Technology Architecture Specification, ToIP Governance Architecture Specification.

ToIP system

A computing system that participates in the ToIP Technology Stack. There are three types of ToIP systems: endpoint systems, intermediary systems, and supporting systems.

For more information, see: Section 6.3 of the ToIP Technology Architecture Specification.

ToIP Technology Architecture Specification

The technical specification defining the requirements for the ToIP Technology Stack published by the ToIP Foundation.

For more information: ToIP Technology Architecture Specification.

ToIP Technology Stack

The technology half of the four layer ToIP stack as defined by the ToIP Technology Architecture Specification.

See also: ToIP Governance Stack, ToIP layer.

ToIP trust community

A trust community governed by a ToIP governance framework.

ToIP trust network

A trust network implemented using the ToIP stack.

ToIP Trust Registry Protocol

The open standard trust task protocol defined by the ToIP Foundation to perform the trust task of querying a trust registry. The ToIP Trust Registry Protocol operates at Layer 3 of the ToIP stack.

ToIP Trust Spanning Protocol

The ToIP Trust Spanning Protocol (TSP) is the ToIP Layer 2 protocol for verifiable messaging that implements the trust spanning layer of the ToIP stack. The TSP enables actors in different digital trust domains to interact in a similar way to how the Internet Protocol (IP) enables devices on different local area networks to exchange data.

Mental model: hourglass model see the Design Principles for the ToIP Stack.

For more information, see: Section 7.3 of the ToIP Technology Architecture Specification and the Trust Spanning Protocol Task Force.

ToIP

See: Trust Over IP

transaction

A discrete event between a user and a system that supports a business or programmatic purpose. A digital system may have multiple categories or types of transactions, which may require separate analysis within the overall digital identity risk assessment.

Source: NIST-CSRC.

See also: connection.

Supporting definitions:

eSSIF-Lab: the exchange of goods, services, funds, or data between some parties (called participants of the transaction).

transitive trust decision

A trust decision made by a first party about a second party or another entity based on information about the second party or the other entity that is obtained from one or more third parties.

Note: A primary purpose of digital credentials, chained credentials, trust registries, and the ToIP stack is to facilitate transitive trust decisions.

For more information, see: Design Principles for the ToIP Stack.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.

Source: Wikipedia.

Also known as: TCP.

See also: User Datagram Protocol.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and Voice over IP, but its use in securing HTTPS remains the most publicly visible. The TLS protocol aims primarily to provide security, including privacy (confidentiality), integrity, and authenticity through the use of cryptography, such as the use of certificates, between two or more communicating computer applications.

Source: Wikipedia.

Also known as: TLS.

Note: TLS replaced the deprecated Secure Sockets Layer (SSL) protocol.

transport layer

Layer of the TCP/IP protocol stack that is responsible for reliable connection-oriented or connectionless end-to-end communications.

Source: NIST-CRSC.

tribal knowledge

Knowledge that is known within an “in-group” of people but unknown outside of it. A tribe, in this sense, is a group of people that share such a common knowledge.

Source: Wikipedia

trust anchor

The authoritative source that serves as the origin of a trust chain.

Also known as: trust root.

For more information, see: Design Principles for the ToIP Stack.

Note: The term “trust anchor” is most commonly used in cryptography and public key infrastructure.

trust application layer

In the context of the ToIP stack, the trust application layer is ToIP Layer 4. Applications running at this layer call trust task protocols at ToIP Layer 3.

trust application

An application that runs at ToIP Layer 4 in order to perform trust tasks or engage in other verifiable messaging using the ToIP stack.

trust assurance

A process that provides a level of assurance sufficient to make a particular trust decision.

trust basis

The properties of a verifiable identifier (VID) or a ToIP system that enable a party to appraise it to determine a trust limit.

See also: appraisability.

trust boundary

The border of a trust domain.

trust chain

A set of cryptographically verifiable links between digital credentials or other data containers that enable transitive trust decisions.

See also: chained credentials, trust graph.

For more information, see: Design Principles for the ToIP Stack.

trust community

A set of parties who collaborate to achieve a mutual set of trust objectives.

See also: digital trust ecosystem, ToIP trust community.

Note: A trust community may be large or small, formal or informal. In a formal trust community, the set of policies and rules governing behavior of members are usually published in a governance framework or trust framework. In an informal trust community, the policies or rules governing the behavior of members may be tribal knowledge.

trust context

The context in which a specific party makes a specific trust decision. Many different factors may be involved in establishing a trust context, such as: the relevant interaction or transaction; the presence or absence of existing trust relationships; the applicability of one or more governance frameworks; and the location, time, network, and/or devices involved. A trust context may be implicit or explicit; if explicit, it may be identified using an identifier. A ToIP governance framework is an example of an explicit trust context identified by a verifiable identifier (VID).

See also: trust domain.

For more information, see: Design Principles for the ToIP Stack.

trust decision

A decision that a party needs to make about whether to engage in a specific interaction or transaction with another entity that involves real or perceived risks.

See also: transitive trust decision.

For more information, see: Design Principles for the ToIP Stack.

trust domain

A security domain defined by a computer hardware or software architecture, a security policy, or a trust community, typically via a trust framework or

governance framework.

See also: trust context, digital trust ecosystem.

trust ecosystem

See digital trust ecosystem.

trust establishment

The process two or more parties go through to establish a trust relationship. In the context of decentralized digital trust infrastructure, trust establishment takes place at two levels. At the technical trust level, it includes some form of key establishment. At the human trust level, it may be accomplished via an out-of-band introduction, the exchange of digital credentials, queries to one or more trust registries, or evaluation of some combination of human-readable and machine-readable governance frameworks.

trust factor

A property, relationship, or other signal that can contribute to a party making a trust decision.

trust framework

A term (most frequently used in the digital identity industry) to describe a governance framework for a digital identity system, especially a federation.

trust graph

A data structure describing the trust relationship between two or more entities. A simple trust graph may be expressed as a trust list. More complex trust graphs can be recorded or registered in and queried from a trust registry. Trust graphs can also be expressed using trust chains and chained credentials. Trust graphs can enable verifiers and relying parties to make transitive trust decisions.

See also: authorization graph, governance graph, reputation graph.

trust limit

A limit to the degree a party is willing to trust an entity in a specific trust relationship within a specific trust context.

For more information, see: Design Principles for the ToIP Stack.

trust list

A one-dimensional trust graph in which an authoritative source publishes a list of entities that are trusted in a specific trust context. A trust list can be considered a simplified form of a trust registry.

trust network

A network of parties who are connected via trust relationships (such as via a membership agreement) conforming to requirements defined in a legal regulation, trust framework or governance framework. A trust network is more formal than a digital trust ecosystem; the latter may connect parties more loosely via transitive trust relationships and/or across multiple trust networks.

See also: ToIP trust network.

trust objective

An objective shared by the parties in a trust community to establish and maintain trust relationships.

Trust over IP

A term coined by John Jordan to describe the decentralized digital trust infrastructure made possible by the ToIP stack. A play on the term *Voice over IP* (abbreviated *VoIP*). The term was adopted as the name for the Trust over IP Foundation aka ToIP Foundation.

Also known as: ToIP.

trust registry protocol

See: ToIP Trust Registry Protocol.

trust registry

A registry that serves as an authoritative source for trust graphs or other governed information describing one or more trust communities. A trust registry is typically authorized by a governance framework.

See also: trust list, verifiable data registry.

trust relationship

A relationship between a party and an entity in which the party has decided to trust the entity in one or more trust contexts up to a trust limit.

Supporting definitions:

NIST: An agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.

For more information, see: Design Principles for the ToIP Stack.

trust root

See: trust anchor

trust service provider

In the context of specific digital trust ecosystems, such as the European Union's eIDAS regulations, a trust service provider is a legal entity that provides specific trust support services as required by legal regulations, trust frameworks, or governance frameworks. In the larger context of ToIP infrastructure, a trust service provider is a provider of services based on the ToIP stack. Most generally, a trust service provider is to the trust layer for the Internet what an Internet service provider (ISP) is to the Internet layer.

Supporting definitions:

Wikipedia: A trust service provider (TSP) is a person or legal entity providing and preserving digital certificates to create and validate electronic signatures and to authenticate their signatories as well as websites in general. Trust service providers are qualified certificate authorities required in the European Union and in Switzerland in the context of regulated electronic signing procedures.

Note: In the industry, the acronym "TSP" is used for both trust service provider and the ToIP Trust Spanning Protocol. In the ToIP Glossary, the acronmym "TSP" will only be used for the latter.

trust spanning layer

A spanning layer designed to span between different digital trust domains. In the ToIP stack, the trust spanning layer is ToIP Layer 2.

Mental model: hourglass model see ToIP Technology Architecture Specification

For more information, see: Section 7.3 of the ToIP Technology Architecture Specification.

trust spanning protocol

See: ToIP Trust Spanning Protocol.

trust support layer

In the context of the ToIP stack, the trust support layer is ToIP Layer 1. It supports the operations of the ToIP Trust Spanning Protocol at ToIP Layer 2.

trust support

A system, protocol, or other infrastructure whose function is to facilitate the establishment and maintenance of trust relationships at higher protocol layers. In the ToIP stack, the trust support layer is Layer 1.

trust task layer

In the context of the ToIP stack, the trust task layer is ToIP Layer 3. It supports trust applications operating at ToIP Layer 4.

trust task protocol

A ToIP Layer 3 protocol that implements a specific trust task on behalf of a trust application operating at ToIP Layer 4.

trust task

A specific task that involves establishing, verifying, or maintaining trust relationships or exchanging verifiable messages or verifiable data that can be performed on behalf of a trust application by a trust task protocol at Layer 3 of the ToIP stack.

For more information, see Section 7.4 of the ToIP Technology Architecture Specification.

trust triangle

See: three-party model.

trust

A belief that an entity will behave in a predictable manner in specified circumstances. The entity may be a person, process, object or any combination of such components. The entity can be of any size from a single hardware component or software module, to a piece of equipment identified by make and model, to a site or location, to an organization, to a nation-state. Trust, while inherently a subjective determination, can be based on objective evidence and subjective elements. The objective grounds for trust can include for example, the results of information technology product testing and evaluation. Subjective belief, level of comfort, and experience may supplement (or even replace) objective evidence, or substitute for such evidence when it is unavailable. Trust is usually relative to a specific circumstance or situation (e.g., the amount of money involved in a transaction, the sensitivity or criticality of information, or

whether safety is an issue with human lives at stake). Trust is generally not transitive (e.g., you trust a friend but not necessarily a friend of a friend). Finally, trust is generally earned, based on experience or measurement.

Source: NIST Special Publication 800-39 p.24

See also: trust decision, transitive trust decision.

For more information, see: Design Principles for the ToIP Stack.

trusted execution environment

A trusted execution environment (TEE) is a secure area of a main processor. It helps code and data loaded inside it to be protected with respect to confidentiality and integrity. Data integrity prevents unauthorized entities from outside the TEE from altering data, while code integrity prevents code in the TEE from being replaced or modified by unauthorized entities, which may also be the computer owner itself as in certain DRM schemes.

Source: Wikipedia.

Also known as: TEE.

See also: Secure Enclave.

trusted role

A role that performs restricted activities for an organization after meeting competence, security and background verification requirements for that role.

trusted third party

In cryptography, a trusted third party (TTP) is an entity which facilitates interactions between two parties who both trust the third party; the third party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions as well as cryptographic protocols, for example, a certificate authority (CA) would issue a digital certificate to one of two parties. The CA then becomes the TTP

to that certificate's issuance. Likewise transactions that need a third party recordation would also need a third-party repository service of some kind.

Source: Wikipedia.

Also known as: TTP.

Supporting definitions:

NIST-CSRC: A third party, such as a CA, that is trusted by its clients to perform certain services. (By contrast, the two participants in a key-establishment transaction are considered to be the first and second parties.)

trusted timestamp authority

An authority that is trusted to provide accurate time information in the form of a timestamp.

Source: NIST-CSRC.

Also known as: TTA.

trustworthiness

An attribute of an entity, such as a person or organization, that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. Trustworthiness is also a characteristic of information technology products and systems. The attribute of trustworthiness, whether applied to people, processes, or technologies, can be measured, at least in relative terms if not quantitatively. The determination of trustworthiness plays a key role in establishing trust relationships among persons and organizations. The trust relationships are key factors in risk decisions made by senior leaders/executives.

Source: NIST Special Publication 800-39 p.24

trustworthy

A property of an entity that has the attribute of trustworthiness.

TSP

See: ToIP Trust Spanning Protocol.

TTA

See: trusted timestamp authority.

TTP

See: trusted third party.

UDP

See: User Datagram Protocol.

unicast address

A network address used for a unicast.

unicast

In computer networking, unicast is a one-to-one transmission from one point in the network to another point; that is, one sender and one receiver, each identified by a network address (a unicast address). Unicast is in contrast to multicast and broadcast which are one-to-many transmissions. Internet Protocol unicast delivery methods such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are typically used.

Source: Wikipedia.

See also: anycast.

Uniform Resource Identifier

A Uniform Resource Identifier (URI) is the generic standard for all types of identifiers used to link resources in the World Wide Web. The most common

type of a URI is a URL (Uniform Resource Locator). The URI standard is defined by IETF RFC 3986. URNs (Uniform Resource Names) are another type of URIs intended for persistent identifiers.

Uniform Resource Locator

A Uniform Resource Locator (URL) is the standard form of a Web address used to link resources in browsers and other Internet applications. Technically, it is a specific type of Uniform Resource Identifier (URI).

Contrast with: Uniform Resource Name.

Uniform Resource Name

A Uniform Resource Name (URN) is a type of URI (Uniform Resource Identifier) designed for persistent identifiers that are intended to be assigned once to a resource and never changed to identify a different resource. In some cases a URN is also intended to serve as a persistent way to locate the identified resource over time even as it moves locations on the network. The URN standard is defined by IETF RFC 8141.

Contrast with: Uniform Resource Locator.

URI

See: Uniform Resource Identifier.

URL

See: Uniform Resource Locator.

URN

See: Uniform Resource Name.

user agent

A software agent that is used directly by the end-user as the principal. Browsers, email clients, and digital wallets are all examples of user agents.

Supporting definitions:

Wikipedia: On the Web, a user agent is a software agent capable of and responsible for retrieving and facilitating end user interaction with Web content.[1] This includes all common web browsers, such as Google Chrome, Mozilla Firefox, and Safari, some email clients, standalone download managers like youtube-dl, other command-line utilities like cURL, and arguably headless services that power part of a larger application, such as a web crawler.

The user agent plays the role of the client in a client–server system. The HTTP User-Agent header is intended to clearly identify the agent to the server. However, this header can be omitted or spoofed, so some websites use other agent detection methods.

User Datagram Protocol

In computer networking, the User Datagram Protocol (UDP) is one of the core communication protocols of the Internet protocol suite used to send messages (transported as datagrams in packets) to other hosts on an Internet Protocol (IP) network. Within an IP network, UDP does not require prior communication to set up communication channels or data paths.

Source: Wikipedia.

Also known as: UDP.

utility governance framework

A governance framework for a digital trust utility. A utility governance framework may be a component of or referenced by an ecosystem governance framework or a credential governance framework.

validation

An action an agent (of a principal) performs to determine whether a digital object or set of data meets the requirements of a specific party.

See also: verification.

Supporting definitions:

eSSIF-Lab: The act, by or on behalf of a party, of determining whether or not that data is valid to be used for some specific purpose(s) of that party.

NISTConfirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

vault

See: digital vault.

VC

See: verifiable credential.

verifiable credential

A standard data model and representation format for cryptographically-verifiable digital credentials as defined by the W3C Verifiable Credentials Data Model Specification.

Source: W3C DID

Also known as: VC.

See also: digital credential.

Mental model: W3C Verifiable Credentials Data Model Roles & Information Flows

Supporting definitions:

W3C VC: A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects.

verifiable data registry

A registry that facilitates the creation, verification, updating, and/or deactivation of decentralized identifiers and DID documents. A verifiable data registry may also be used for other cryptographically-verifiable data structures such as verifiable credentials.

Source: W3C DID

Also known as: VDR.

See also: authoritative source, trust registry, system of record.

Mental model: W3C Verifiable Credentials Data Model Roles & Information Flows

For more information, see: W3C Verifiable Credentials Data Model Specification.

Note: There is an earlier definition in the W3C VC 1.1. glossary that is not as mature as this one (it is not clear about the use of cryptographically verifiable data structures). We do not recommend that definition.

verifiable data

Any digital data or object that is digitally signed in such a manner that it can be cryptographically verified.

Note: In the context of ToIP architecture, verifiable data is signed with the cryptographic keys associated with the verifiable identifier (VID) of the data controller.

verifiable identifier

An identifier over which the controller can provide cryptographic proof of control. Each type of VID defines a specific means for discovering the public key, network endpoints, or other metadata necessary to prove control. Decentralized identifiers (DIDs) are a W3C standard for VIDs. VIDs are the cryptographically verifiable identifiers used in the ToIP stack.

See also: decentralized identifier, autonomic identifier.

- Also known as: VID

- Also known as: VID

verifiable message

A message communicated as verifiable data by virtue of being digitally signed.

See also: ToIP messages

verifiable

In the context of digital communications infrastructure, the ability to determine the authenticity of a communication (e.g., sender, contents, claims, metadata, provenance), or the underlying sociotechnical infrastructure (e.g., governance, roles, policies, authorizations, certifications).

See also:appraisable, digital signature.

verification

An action an agent (of a principal) performs to determine the authenticity of a claim or other data object. Cryptographic verification uses cryptographic keys.

See also: validation.

Mental model: W3C Verifiable Credentials Data Model Roles & Information Flows

Supporting definitions:

eSSIF-Lab: The act, by or on behalf of a party, of determining whether that data is authentic (i.e. originates from the party that authored it), timely (i.e. has not expired), and conforms to other specifications that apply to its structure.

verifier

A role an agent performs to perform verification of one or more proofs of the claims in a digital credential or other verifiable data.

See also: relying party; issuer, holder.

Mental model: W3C Verifiable Credentials Data Model Roles & Information Flows

Supporting definitions:

W3C VC: A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing. Other specifications might refer to this concept as a relying party.

eSSIF-Lab: a component that implements the capability to request peer agents to present (provide) data from credentials (of a specified kind, issued by specified parties), and to verify such responses (check structure, signatures, dates), according to its principal's verifier policy.

NIST The entity that verifies the authenticity of a digital signature using the public key.

VID relationship

The communications relationship formed between two VIDs using the ToIP Trust Spanning Protocol. A particular feature of this protocol is its ability to establish as many VID relationships as needed to establish different relationship contexts between the communicating entities.

VID-to-VID

The specialized type of peer-to-peer communications enabled by the ToIP Trust Spanning Protocol. Each pair of VIDs creates a unique VID relationship.

VID

See verifiable identifier.

virtual vault

A digital vault enclosed inside another digital vault by virtue of having its own verifiable identifier (VID) and its own set of encryption keys that are separate

from those used to unlock the enclosing vault.

Voice over IP

Voice over Internet Protocol (VoIP), also called IP telephony, is a method and group of technologies for voice calls for the delivery of voice communication sessions over Internet Protocol (IP) networks, such as the Internet.

Also known as: VoIP.

VoIP

See: Voice over IP.

W3C Verifiable Credentials Data Model Specification

A W3C Recommendation defining a standard data model and representation format for cryptographically-verifiable digital credentials. Version 1.1 was published on 03 March 2022.

For more information, see: https://www.w3.org/TR/vc-data-model/

wallet engine

The set of software components that form the core of a digital wallet, but which by themselves are not sufficient to deliver a fully functional wallet for use by a digital agent (of a principal). A wallet engine is to a digital wallet what a browser engine is to a web browser.

For more information: The charter of the OpenWallet Foundation is to produce an open source digital wallet engine.

wallet

See: digital wallet.

witness

A computer system that receives, verifies, and stores proofs of key events for a verifiable identifier (especially an autonomic identifier). Each witness controls its own verifiable identifier used to sign key event messages stored by the witness. A witness may use any suitable computer system or database architecture, including a file, centralized database, distributed database, distributed ledger, or blockchain.

Note: KERI is an example of a key management system that uses witnesses.

zero-knowledge proof

A specific kind of cryptographic proof that proves facts about data to a verifier without revealing the underlying data itself. A common example is proving that a person is over or under a specific age without revealing the person's exact birthdate.

Also known as: zero-knowledge protocol, ZKP.

Supporting definitions:

Ethereum: A zero-knowledge proof is a way of proving the validity of a statement without revealing the statement itself.

Wikipedia: a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while avoiding conveying to the verifier any information beyond the mere fact of the statement's truth.

zero-knowledge service provider

The provider of a zero-knowledge service that hosts encrypted data on behalf of the principal but does not have access to the private keys in order to be able to decrypt it.

zero-knowledge service

In cloud computing, the term "zero-knowledge" refers to an online service that stores, transfers or manipulates data in a way that maintains a high level of confidentiality, where the data is only accessible to the data's owner (the client), and not to the service provider. This is achieved by encrypting the raw data at the client's side or end-to-end (in case there is more than one client), without

disclosing the password to the service provider. This means that neither the service provider, nor any third party that might intercept the data, can decrypt and access the data without prior permission, allowing the client a higher degree of privacy than would otherwise be possible. In addition, zero-knowledge services often strive to hold as little metadata as possible, holding only that data that is functionally needed by the service.

Source: Wikipedia.

Also known as: no knowledge, zero access.

zero-trust architecture

A network security architecture based on the core design principle “never trust, always verify”, so that all actors are denied access to resources pending verification.

Also known as: perimeterless security, zero-trust security, ZTA.

Contrast with: attribute-based access control, role-based access control.

Supporting definitions:

NIST-CSRC: A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

Wikipedia: The zero trust security model, also known as zero trust architecture (ZTA), and sometimes known as perimeterless security, describes an approach to the strategy, design and implementation of IT systems. The main concept behind the zero trust security model is “never trust, always verify,” which means that users and devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.

ZKP

See: zero-knowledge proof.