

Identity management

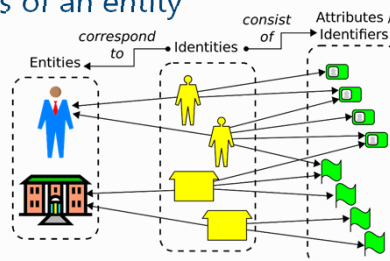


Digital identity

David W. Chadwick. "Federated Identity Management". Springer. 2009.

▷ An arbitrary set of attributes of an entity

- ♦ Which can be segregated in different contexts



▷ Only a subset of those attributes is used to unequivocally recognize the entity in a given context

- ♦ Those attributes are called (contextual) identifiers

https://en.wikipedia.org/wiki/Identity_management#/media/File:Identity-concept.svg



Identity Manager (IdM)

- ▷ An entity (service) that manages identity profiles in a given context
 - ♦ Creates / deletes identity profiles
 - ♦ Collects attributes to profiles
 - ♦ Updates attributes in profiles
- ▷ Goal
 - ♦ Identification
 - ♦ Authentication
 - ♦ Authorization / access control
 - ♦ Accounting



Identity Provider (IdP)

- ▷ A service that provides identity attributes belonging to a subject
 - ♦ As assertions
- ▷ Assertions possess identity claims
 - ♦ Usually pairs attribute name + attribute value
- ▷ An IdP can provide different sets of attributes to different requesters
 - ♦ Need-to-know principle
 - ♦ Privacy issues
 - ♦ Protection rules



Authoritative source

- ▷ Top-most IdM responsible for providing a given identity attribute of a subject
 - ♦ Aka Attribute Authority



Identity claim

- ▷ Statement that someone makes about the identity of itself or another subject
- ▷ IdMs / IdPs are claim providers
 - ♦ They provide sets of identity claims packet in assertions



Silo-oriented IdM

- ▷ Per-service IdM
 - ♦ No relation with other services
- ▷ Identity attributes are not shared among services
 - ♦ Duplication
 - Each person would have an identity profile on each service
 - Each service must ensure proper protection mechanisms
 - ♦ Not scalable for users, nor user-friendly
 - Unless you use the same identifiers and authentication credentials
 - ♦ But possibly better against identity theft!
 - Unless you use the same identifiers and authentication credentials ...



Aggregated IdM

- ▷ One IdM for several services
 - ♦ A single profile for each entity
 - Each profile contains the union of all attributes required by all services
 - More efficient
 - ♦ Each service uses only the attributes it needs
- ▷ Usually explored with a central IdP
 - ♦ To concentrate the authentication of profile owners
 - ♦ To provide assertions with identity claims
- ▷ Services rely on the IdP
 - ♦ Relying parties



Federated identity

- ▷ Concept that encompasses a common set of policies, practices and protocols to manage identity across organizations
- ▷ Goal
 - ♦ Enable an entity to access a service of organization with a set of identity claims provided by one or more trustworthy, third-party IdMs



Claim-based identity management

- ▷ Multi-IdP identity claims' provisioning
- ▷ A service provider asks for several identity attributes
 - ♦ As identity claims
 - ♦ And proposes alternative IdMs
- ▷ The service client uses one or more IdMs to get all the necessary identity claims
 - ♦ Usually no more than one



Credential

- ▷ Set of a subject's identity claims asserted by an IdM
 - ♦ e.g. identity cards
- ▷ Credentials also have metadata
 - ♦ Issuing date
 - ♦ Validity periods
 - ♦ Issuer identity attributes



Privacy issues

- ▷ Tracking
 - ♦ IdMs usually know to which service they provide credentials
 - ♦ They know which services each identity profile uses
- ▷ For privacy sake, IdMs should not know the target services that will receive the credentials they issue
 - ♦ Only the credentials' owners should know that
 - ♦ This is what usually happens with physical credentials
- ▷ Requirements
 - ♦ The credential owner must prove the credential's ownership
 - ♦ The credential owner controls the presentation of its credentials



Verifiable credential (VC)

- ▷ Cryptographically-sealed credential provided to a holder
 - ♦ The holder is someone that will be able to make use of it
 - ♦ A verifier can check the identity of its issuer
- ▷ It may contain identity attributes of more than one entity
 - ♦ e.g. marriage agreement
- ▷ It may contain only attributes of another entity
 - ♦ e.g. a dog's vaccination record
- ▷ It can be revoked by issuers at any time
 - ♦ Some public, shared repository would be required (blockchain)



Verifiable presentation of VCs

- ▷ Trustworthy validation of a set of provided VCs
 - ♦ **Authenticity**
 - Valid issuer signature, trust on issuer
 - ♦ **Validity**
 - In the validity period, not revoked
- ▷ **Selective or ZKP presentation of credentials' information**
 - ♦ Show only part of the identity attributes
 - ♦ Prove the possession of an attribute without disclosing the related identity claim



Self-Sovereign Identity (SSI)

- ▷ Not a very good name ...
 - ♦ Decentralized identity?
- ▷ It requires a digital wallet
 - ♦ For keeping digital credentials
 - ♦ Credentials are VCs that can prove to a verifier:
 - Who is the issuer
 - To whom they were issued
 - Whether it has been altered since it was issued
 - Whether it has been revoked by the issuer



SSI: Types of credentials

- ▷ Third-party attested credentials
 - ♦ The credentials a person shows to others to prove their identity attributes
 - ♦ They imply the trust of the credential receiver in the credentials' issuers
- ▷ Self-attested credentials
 - ♦ What I say about myself
 - Opinion, preference, consent
 - ♦ Still needs credentials issued by TTPs
 - To associate identity attributes recognized by other to you opinion, preference or consent



SSI:

Credential issuers

- ▷ They act in response to requests of credentials owners
 - ♦ And not the services they access
- ▷ They can change / revoke issued credentials at any time
 - ♦ But credential owners can still use them
 - ♦ Revocation verification should not require a contact with the credential issuer
 - Some public repository must exist (blockchain)



SSI:

P2P sessions

- ▷ Each entity possesses a wallet
 - ♦ Which contains an asymmetric key pair
- ▷ Thus, each pair of entities can establish a secure, P2P "connection", or "session"
 - ♦ With which they can securely exchange credentials



Interoperability

- ▷ Capacity of different systems to cooperate (communicate, understand, accept) with each other
- ▷ Syntactic interoperability
 - ♦ They can communicate
 - ♦ They can parse the communication items
- ▷ Semantic interoperability
 - ♦ They can understand each other
 - ♦ What is sent is what is understood



Interoperability in identity management

- ▷ Interoperability between a large group of stakeholders involved in identity management
 - ♦ Identity owners
 - ♦ Identity providers
 - ♦ Identity consumers



eIDAS

▷ Electronic identification, Authentication and trust Systems

- ♦ EU regulation
 - On electronic identification and trust services for electronic transactions in the internal market
- ♦ Sets the standards and criteria for
 - Simple electronic signature
 - Advanced electronic signature
 - Qualified electronic signature
 - Qualified certificates
 - Online trust services
- ♦ Rules electronic transactions and their management



eIDAS:

Types of electronic signature (1/3)

▷ Electronic signature

- ♦ Data in an electronic format attached (or logically associated) to other electronic data that the signer uses to accept the contents of a document



eIDAS:

Types of electronic signature (2/3)

▷ Advanced electronic signature

♦ An electronic signature that:

- It is linked to the signer in a unique way and allows their identification
- It has been created using electronic signature creation data that the signer can use with a high level of trust and under his exclusive control
- It is linked and sealed with the signed data so that any subsequent modification of it is noticeable



eIDAS:

Types of electronic signature (3/3)

▷ Qualified electronic signature

- ♦ Advanced electronic signature created by a qualified electronic signature creation device and based on a qualified electronic signature certificate



eIDAS:

Qualified trust services (1/2)



▷ Services electronically provided that

- ♦ Meet eIDAS requirements
 - To operate at a high level of confidence and technical security
- ♦ A natural or a legal person who provides one or more trust services
 - Either as a qualified or non-qualified trust service provider
- ♦ Hold authenticity presumption



eIDAS:

Qualified trust services (2/2)



▷ Services, normally provided for remuneration, of:

- ♦ Creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services
- ♦ Creation, verification and validation of certificates for website authentication
- ♦ Preservation of electronic signatures, seals or certificates related to those services



eIDAS:

Qualified (digital) certificate

- ▷ Public key certificate issued by a qualified trust service provider



eIDAS:

Trusted lists (TSL)

- ▷ Each Member State shall establish, maintain and publish trusted lists
 - ♦ Relation (Trusted-Service Status List) of certifying entities that are registered or accredited by the accrediting authority
 - ♦ Information about qualified trust service providers for which it is responsible
 - ♦ A TSL may include information on non-qualified trust service providers
 - It shall be clearly indicated that they are not qualified according to EU Regulation
- ▷ Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists in a form suitable for automated processing
 - ♦ Usually XML



eIDAS: Trusted lists

- ▷ Member States shall notify to the Commission information on the body responsible for establishing, maintaining and publishing their national TSL
 - And details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto
 - In Portugal: GNS (Gabinete Nacional de Segurança)
- ▷ The Commission publishes, through a secure channel, the information about member States' TSL
 - In electronically signed or sealed form suitable for automated processing
 - LOTL (List of Trust Lists)



eIDAS: eID Levels of Assurance (LoA)

- ▷ Confidence in the identity claimed by a person
 - How certain a service provider can be that it is you the one using your eID to authenticate to the service
 - And not someone else pretending to be you
 - The difficulty one would have trying to use someone else's eID to access an online service
- ▷ 3 levels: low, substantial, high
- ▷ The LoA takes into account:
 - The process of obtaining the eID scheme (enrolment)
 - How the eID means is managed, how it is designed
 - How authentication is performed



eIDAS:

CEF (connecting Europe Facility) eID

- ▷ Citizens from an MS can prove and verify their identification when accessing on-line services in other MS
 - ♦ Using their national eIDs and connecting with their country IdP
- ▷ Steps:
 - ♦ A citizen requests an on-line service in another MS
 - ♦ The citizen is requested to authenticate themselves by the on-line service
 - ♦ The citizen chooses to authenticate with an eIDAS eID
 - ♦ The authentication request is delegated to the citizen's country
 - Through the eIDAS network, to the citizen's IdP
 - ♦ The authentication result is returned to the service provider
 - ♦ Authentication is complete
 - And the citizen can proceed with accessing the service



eIDAS:

CEF (Connecting Europe Facility) eID

- ▷ September 29, 2018
 - ♦ All online public services requiring electronic identification assurance with substantial or high LoA must be able to accept the notified eID schemes of other EU countries
- ▷ Extending the use of online services across Borders video

