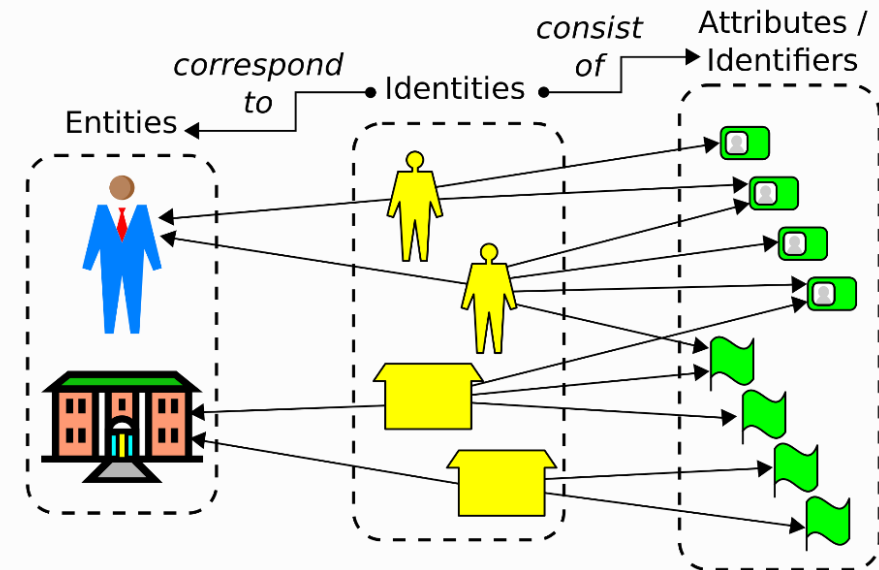

Identity management

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 each 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 each context
 - ◆ Creates / deletes identity profiles
 - ◆ Collects attributes to profiles
 - ◆ Updates attributes in profiles

- ▶ Goal
 - ◆ Identification
 - ◆ Authentication
 - ◆ Authorization / access control
 - ◆ Accounting
 - ◆ Surveillance / tracking

Identity Provider (IdP)

- ▷ A service that provides identity attributes belonging to a subject
 - ◆ As assertions (statements that one strongly believes are true)
- ▷ Assertions possess identity claims
 - ◆ Usually, tuples (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

- ▷ There should be only one
 - ◆ From a logical perspective
 - ◆ The instance could be replicated for redundancy

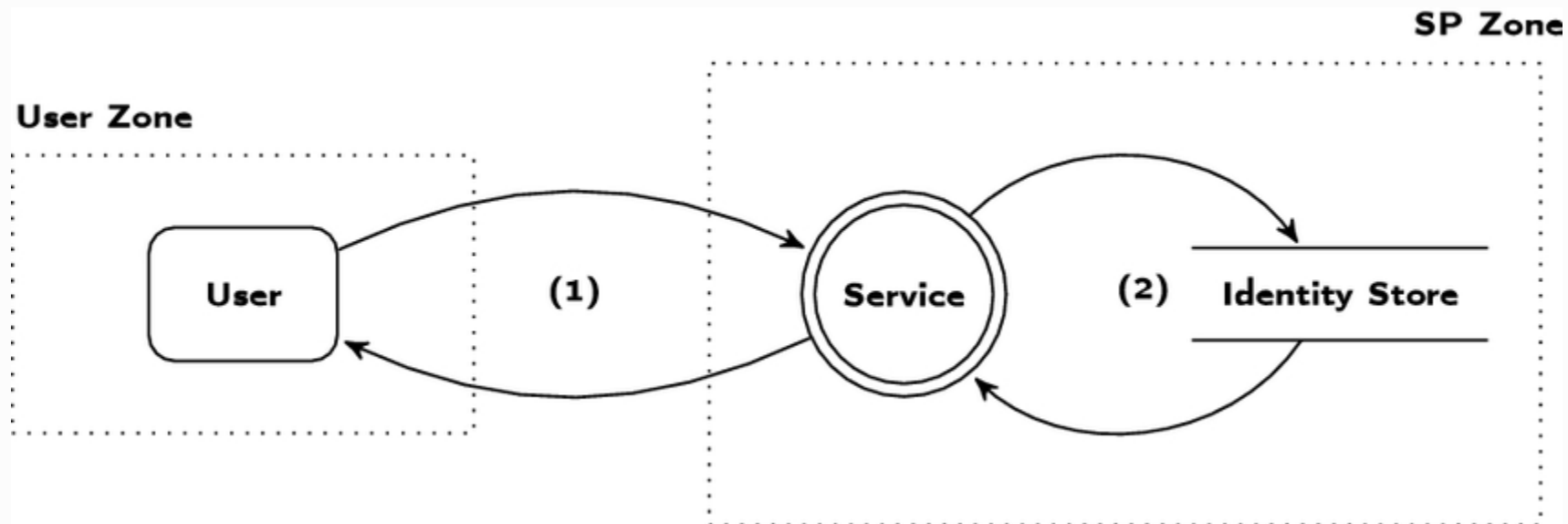
Identity claim

- ▷ Statement that someone makes about the identity of itself or another subject
- ▷ IdMs / IdPs are claim providers
 - ◆ They provide sets of identity claims packed in assertions
- ▷ Assertions are clear statements regarding an identity
 - ◆ Should be trusted: because of their origin or by cryptographic means

Approach 1: Isolated, or Silo-oriented IdM

- ▷ Per-service IdM
 - ◆ No relation between services in the organization (or world)
- ▷ 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 ...
 - ◆ Onboarding and Offboarding issues
 - Need to provision / remove / disable identities across all services

Approach 1: Isolated, or Silo-oriented IdM



Grüner, Andreas & Mühle, Alexander & Lockenvitz, Niko & Meinel, Christoph. (2023). Analyzing and comparing the security of self-sovereign identity management systems through threat modeling. *International Journal of Information Security*. 22. 1-18. 10.1007/s10207-023-00688-w.

Approach 2: 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 management, onboarding and offboarding
 - ◆ Each service uses only the attributes it needs
- ▶ Usually explored with a central IdP
 - ◆ To centralize the authentication of profile owners
 - ◆ To provide assertions with identity claims
- ▶ Services rely on the IdP
 - ◆ Relying Parties (RPs)

Approach 3: Federated identity

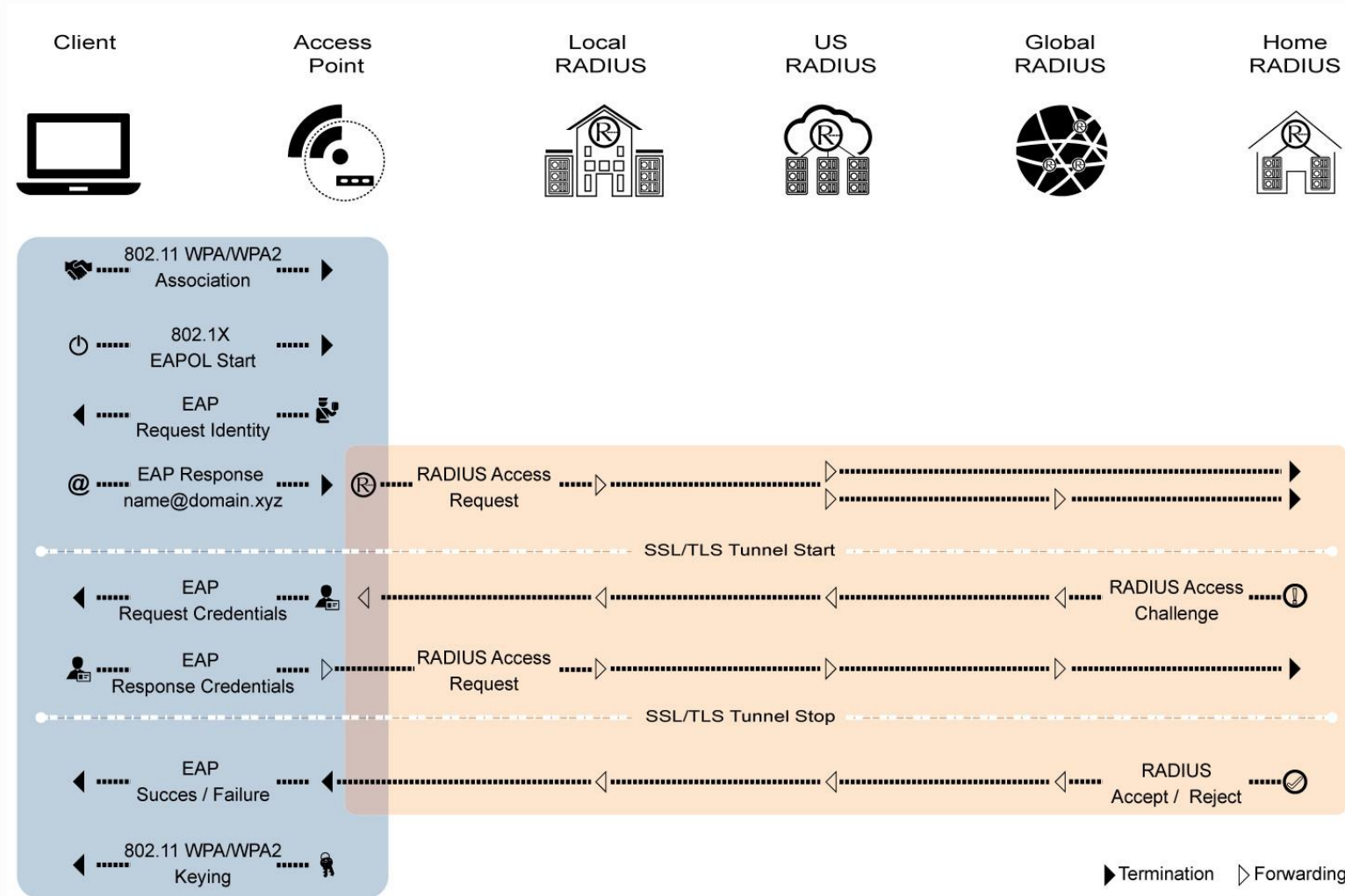
- ▷ Concept that encompasses a common set of policies, practices and protocols to manage identity **across organizations**
- ▷ Goal
 - ◆ Enable an entity to access a service of an organization
 - ◆ with a set of identity claims
 - ◆ provided by one or more trustworthy, third-party IdMs

Approach 3: Federated identity

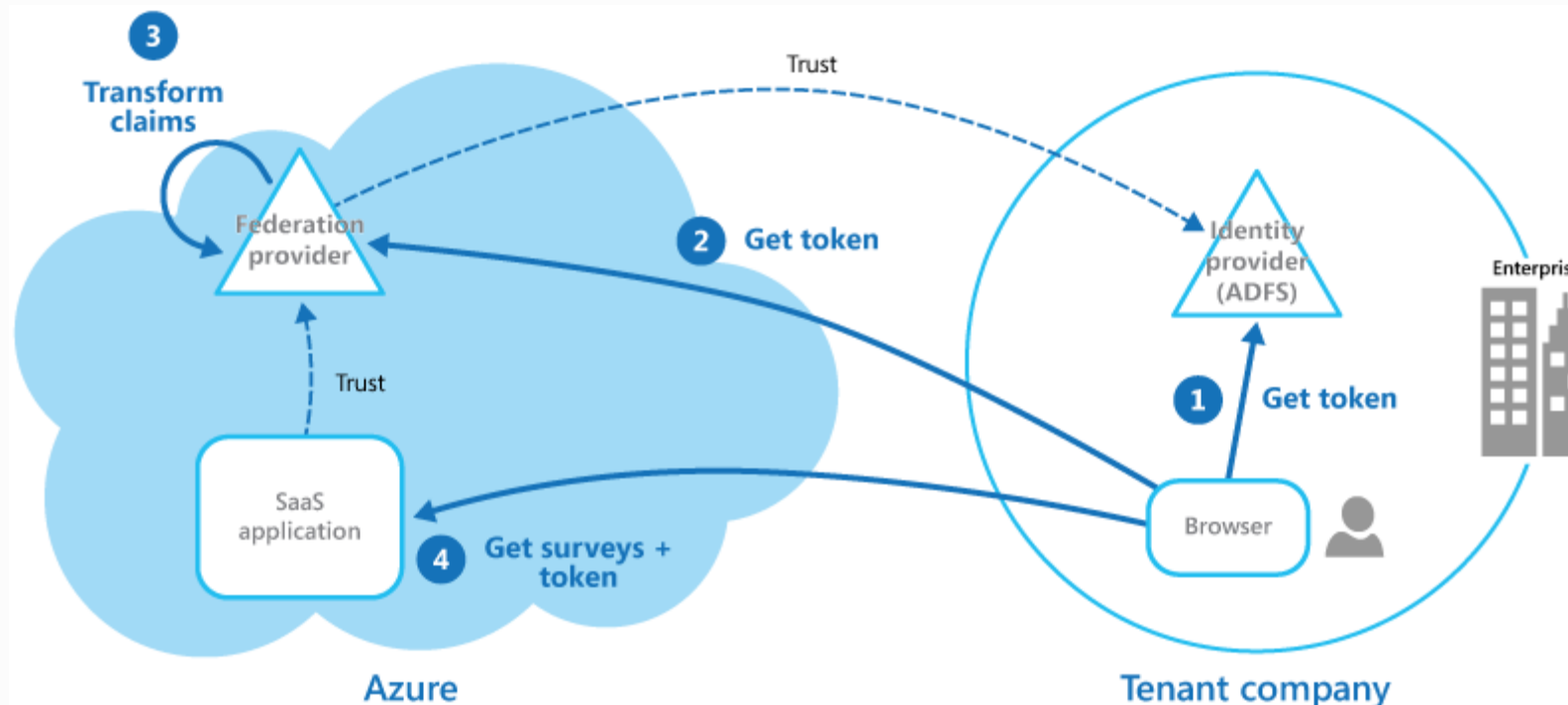
- ▶ Use case: organizations share identity management
 - ◆ Entity@DomainA accesses system@**DomainA**
 - ◆ ...also...
 - ◆ Entity@DomainA accesses system@**DomainB**

- ▶ Organizations agree on using federated identities
 - ◆ Single source of Identities for all Organizations
 - ◆ Can use an independent IdP or accept users from any participant

Approach 3: Federated identity



Approach 3: Federated identity

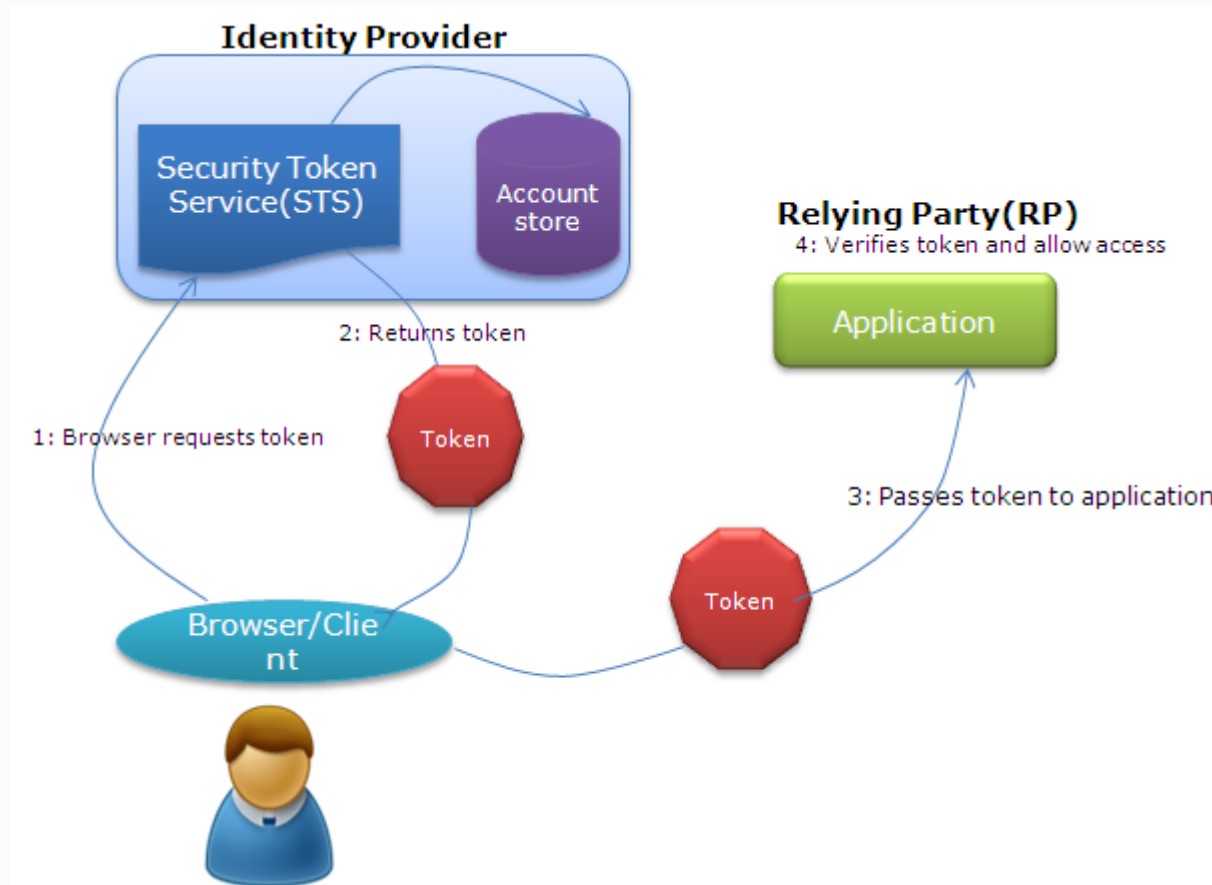


<https://learn.microsoft.com/en-us/azure/architecture/patterns/federated-identity>

Approach 4: Claim-based identity management

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

Approach 4: Claim-based identity management



<https://www.codeproject.com/Articles/268236/Claim-based-Authentication-and-WIF>

Credential

- ▷ Set of a subject's identity claims asserted by an IdM
 - ◆ e.g., identity cards
- ▷ Credentials also have metadata
 - ◆ **Issuing date**
 - ◆ **Validity periods:** automatically limits usage if stolen or lost
 - ◆ **Issuer identity attributes:** identifies origin to establish trust
 - ◆ **Issuing purpose:** subject can have multiple scoped credentials
 - Discloses only the required credential when accessing a service

Privacy issues

▷ Tracking

- ◆ IdMs usually know to which services they provide credentials
- ◆ They know which services each identity profile uses

▷ IdMs should not know the target services that will receive the credentials issued

- ◆ Only the credentials' owners should know that
- ◆ This is what usually happens with physical credentials
- ◆ But... for auditing purposes: they should

▷ 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

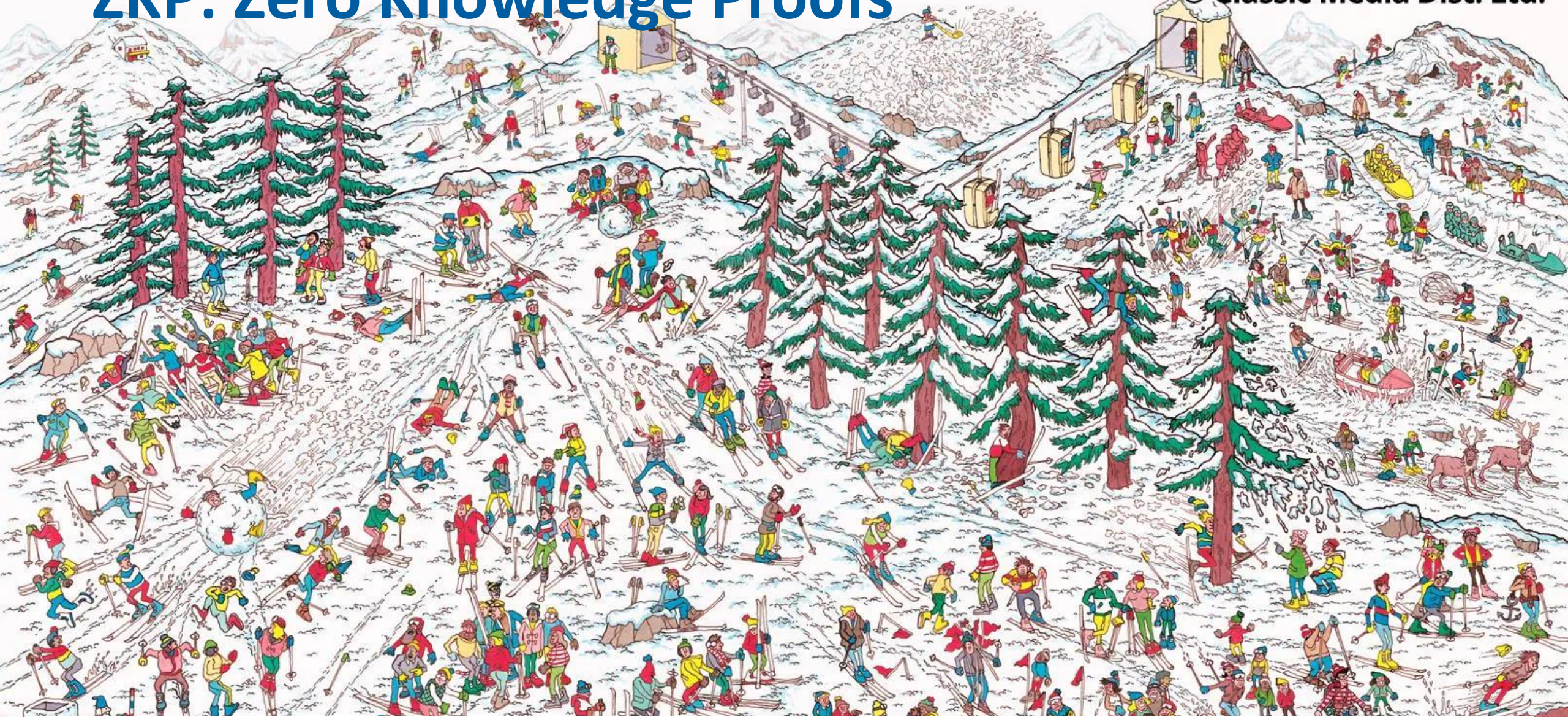
ZKP: Zero Knowledge Proof

ZKP: Zero Knowledge Proofs

- ▷ Method enabling an entity A, to prove and identity of entity B
 - ◆ Without disclosing further information regarding Entity B
- ▷ That is:
 - ◆ Entity A will prove the that entity B knows something
 - ◆ Without entity B disclosing anything about that knowledge, except its result
 - ◆ Also, the world will not gain further information regarding entity B

ZKP: Zero Knowledge Proofs

© Classic Media Dist. Ltd.



Desafio: Mostrar que sabe onde está o Wally sem revelar o segredo

ZKP: Zero Knowledge Proofs



Resposta: Eu sei onde está, mas não digo onde, apenas provo que sei

Self-Sovereign Identity (SSI)

- ▷ Not a very good name ...
 - ◆ Decentralized identity?
- ▷ It requires a digital wallet
 - ◆ For keeping digital credentials
 - ◆ Credentials are Verifiable Credentials 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
 - Usually verified through cryptographic means

▷ Self-attested credentials

- ◆ What I say about myself
 - Opinion, preference, **consent**
- ◆ Still needs credentials issued by TTPs
 - To associate identity attributes recognized by others to your 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
 - ◆ With 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 with each other
 - ◆ Communicate, understand, accept
- ▷ 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

- ▶ Vital for operation of wide scale distributed environments
 - ◆ Across regions, across nations



▷ 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

<https://github.com/eu-digital-identity-wallet>

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:

- Linked to the signer in a unique way and allows their identification
- Created using electronic signature creation data that the signer can use with a high level of trust and under his exclusive control
- 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
- ◆ 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
 - ◆ TSP has government-issued qualifications
- ▷ Essential for non-repudiation
 - ◆ Links a signature to its owner (citizen)
- ▷ Corresponding private key produces signatures with legal value

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)
 - <https://www.gns.gov.pt/pt/trusted-lists/>

- ▷ 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)
 - <https://eidas.ec.europa.eu/efda/tl-browser>

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 to use someone else's eID to access an online service

- ▷ 3 levels: low, substantial, high

- ▷ The LoA considers:
 - ◆ 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

- <https://youtu.be/ojoW5OX2sZQ>

Additional Context

- ▷ eIDAS Regulation for Portugal
 - ◆ <https://www.gns.gov.pt/pt/regulamento-eidas-entidade/>
- ▷ Several Pilots for testing the digital wallet
 - ◆ Potencial: <https://www.digital-identity-wallet.eu/>
 - ◆ EWC: <https://eudiwalletconsortium.org/>
 - ◆ NOBID: <https://www.nobidconsortium.com/>
 - ◆ DC4EU: <https://www.dc4eu.eu/>
- ▷ Open Source Development:
 - ◆ <https://github.com/eu-digital-identity-wallet>