Web Authorization Protocol
Internet-Draft
Intended status: Standards Track
Expires: 11 November 2025

L. Sbriz
Cybersecurity, Risk & Privacy Senior Consultant

10 May 2025

Identity Trust System
draft-sbriz-identity-trust-system-03

Abstract

This document defines an *identity trust system*, which is a digital identity authentication system based on a symmetric exchange of authentication messages that does not require federation of authentication domains. The main components are:

1. *Symmetric authentication protocol* - A protocol for the mutual recognition of entities based on a collaboration scheme between Identity Providers (IdPs) and a symmetric exchange of authentication messages. It builds on and extends the OAuth Authorization Framework RFC6749.

2. *Trustees network* - Network infrastructure that provides a secure environment for the exchange of authentication messages between IdPs.

3. *Custodian concept* - This is a special type of IdP to protect personal data and the relationship between digital and physical identity. The generic IdP is called a "*_trustee_*" and is only responsible for digital authentication, while the special IdP, called a "*_custodian_*", has the legal right to process the individual’s real data and maintain the relationship with the digital identity. It acts under the control of the authorities of the individual’s country.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction 3
  1.1. Use cases of both authentication schemes 4
2. Conventions and Definitions 6
3. Symmetric authentication protocol 7
4. Identity Provider - Trustee Concept 10
  4.1. Importance of this role 11
  4.2. Infrastructure 11
5. Identity Provider - Custodian Concept 12
  5.1. General schema 12
    5.1.1. Issuing of a New Digital Identity 14
6. Sustainable Digital Identity Trust Schema 17
7. Security Considerations 19
  7.1. User registration 19
    7.1.1. Registration with an identity custodian (IdC). . . . 20
    7.1.2. Registration with an identity provider (IdP). 20
    7.1.3. Registration with a service provider (SP). 20
8. Conclusions 20
9. IANA Considerations 21
10. References 21
  10.1. Normative References 21
  10.2. Informative References 21
Acknowledgments 22
Author's Address 23

1. Introduction

The typical model of access to Internet protected resources requires that the identity of the user, i.e. the *_resource owner_*, be authenticated by the resource manager, i.e. the *_service provider_*. The authentication process is not the primary task of the service provider and therefore can be entrusted to a third party shared between the user and the service provider, known as an *_identity provider_*. A popular authentication mechanism is defined by [RFC6749].

This mechanism is asymmetric, only the resource owner must be recognized but not vice versa. Furthermore, the digital identity has value only within the digital ecosystem of the identity provider, i.e. its authentication domain or in a set of domains in a relationship of trust between them. It follows that when the digital ecosystem changes, the resource owner needs a new user to be recognized in the new digital environment. Instead, with a symmetric authentication scheme, the new user is no longer necessary. Moreover, it is not even necessary to create a trust relationship between domains. Trust is assigned only to the entity that guarantees identity authentication process, i.e. the identity provider that guarantees the inviolability and truthfulness of the authentication messages exchanged.

The concept used to build symmetric authentication is the request for equal dignity in recognition, i.e. each entity must be recognized by the other. To achieve this equal relationship, an identity recognition process based on a mirrored sequence of messages exchanged is necessary. Consequently, basing this symmetric process on the trust assigned to the identity provider has a great advantage, it is no longer necessary to define a specific trust between domains or create new users to be able to operate in an ecosystem different from that of belonging.

To implement this solution it is necessary to modify the authentication protocol to support the symmetric exchange of identification messages, and also implement a similar message exchange mechanism between identity providers. For security reasons, an infrastructure dedicated to identity providers is required. Furthermore, dividing IdPs into two categories reduces the amount of personal data used in registrations. The first category will be made up of those who are only authorized to recognize digital identity. The second category consists of those with the legal authority to also manage the real identity. The second category will act as a guarantor of the authenticity of the identity used in registration on the providers of the first category.

1.1. Use cases of both authentication schemes

Figure 1 depicts the use case of the classic identity recognition method with asymmetry in the process of exchanging authentication messages [RFC6749]. A SVG image is available here (https://raw.githubusercontent.com/Luigi-Sbriz/identity/main/images/1_Asymmetric-depiction.svg). The scenario depicted represents a resource owner who needs to retrieve a resource from the service provider. The identity provider MUST verify the identity of the resource owner before accessing the resource server. The relying party who manages the resource does not provide any information about its identity, it provides the resource only to authorized requests.

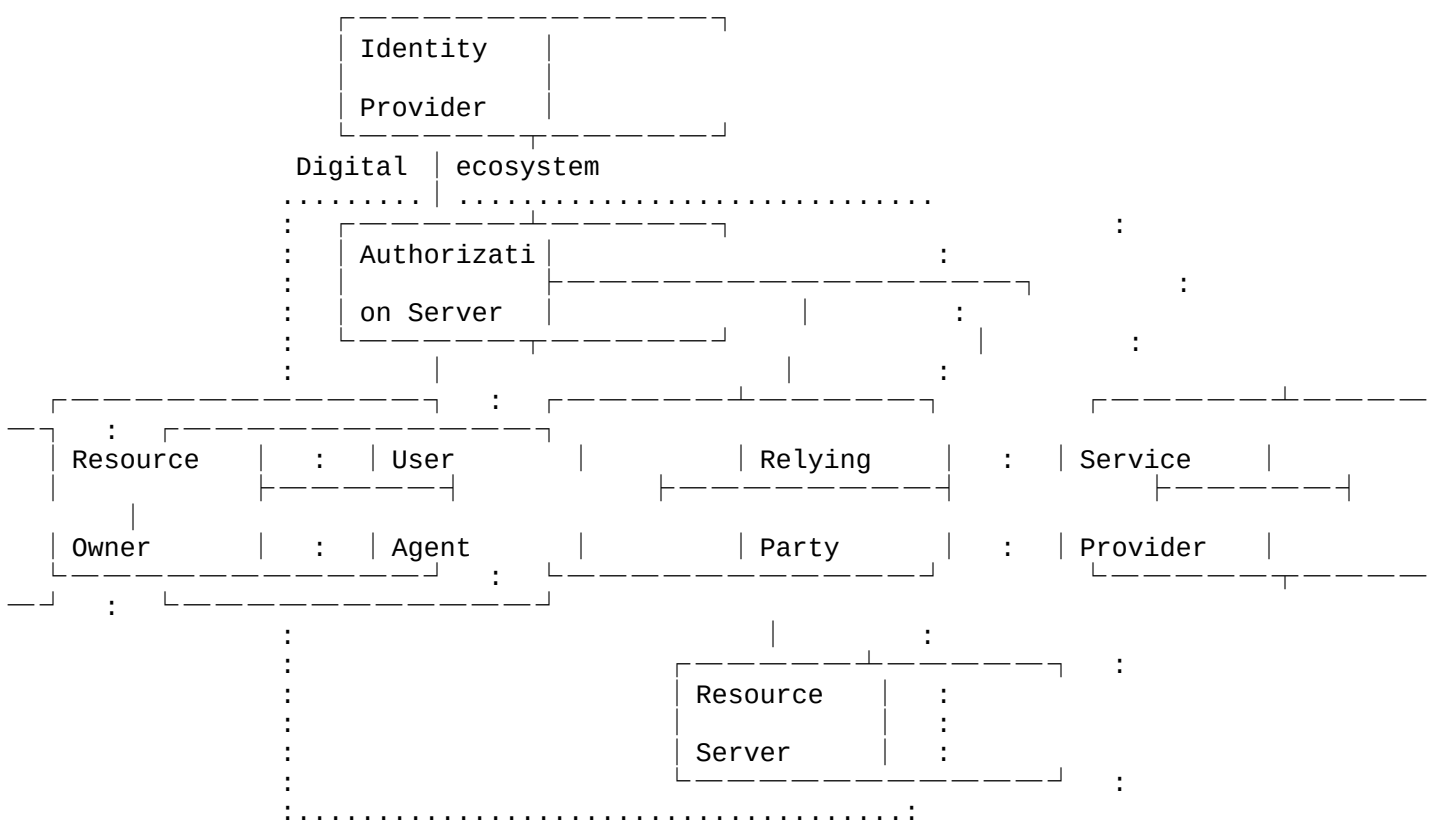


Figure 1: Use case of the authorization flow - Asymmetrical case

Figure 2 depicts the use case with the components needed to enable the identity authentication process in a symmetric manner capable of operating in different digital ecosystems. A SVG image is available here (https://raw.githubusercontent.com/Luigi-Sbriz/identity/main/images/2_Symmetric-depiction.svg). The new scenario depicts two different ecosystems, one for the resource owner (client accessing the resource) and the other for the service provider (server managing

the resource). This means that any entity involved in the authentication process will have its own identity provider, and they will interact with each other to ensure the completion of the symmetric authentication process.

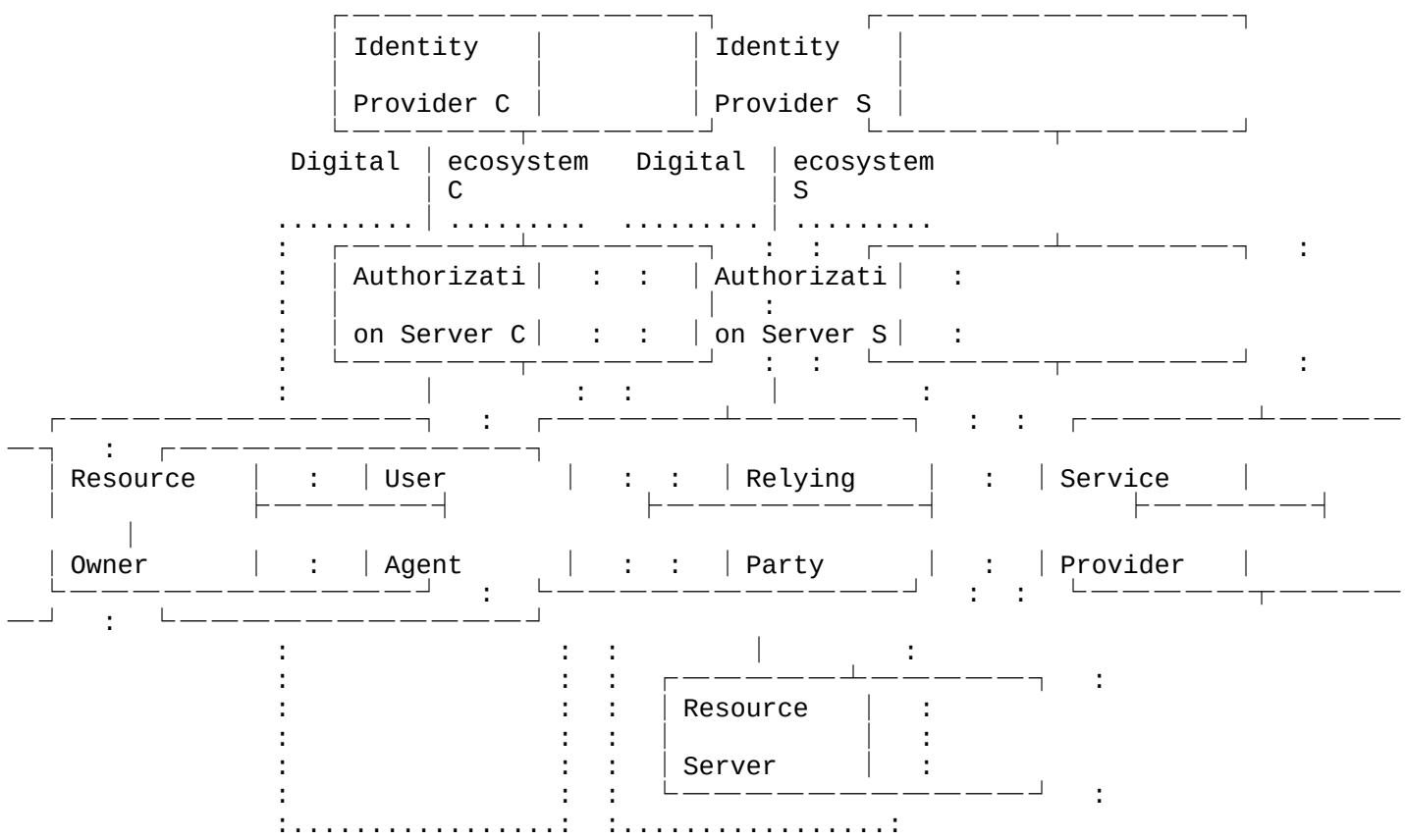


Figure 2: Use case of the authorization flow - Symmetrical case

The two representations are very similar to each other but note that the symmetric protocol requires direct communication between the identity providers' authentication servers to allow the circular transit of authentication messages. Therefore, no trust between domains or new users is necessary. This idea was first exposed in some articles published on ISACA Journal (see [LS1], [LS2], [LS3], [LS4], [LS5]) with some specific use cases and examples of potential implementations.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Some terms are used with a precise meaning.

* "*_resource owner_*": An entity capable of granting access to a protected resource. When the resource owner is a person, it is also referred to as "*_end user_*", "*_consumer_*" or "*_individual_*". This is sometimes abbreviated as "*_RO_*".

* "*_service provider_*": An entity capable of managing access to a protected resource. It is generally a legal person. This is sometimes abbreviated as "*_SP_*".

* "*_identity provider_*": An entity capable of managing and recognizing the identity of registered entities. The set of all entities registered by the identity provider is also known as the IdP’s digital ecosystem. This is sometimes abbreviated as "*_IdP_*".

* "*_resource server_*": The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens. The resource server is often accessible via an API. This is sometimes abbreviated as "*_RS_*".

* "*_client_*", for software is also referred to as "*_user agent_*": An application making protected resource requests on behalf of the resource owner and with its authorization. The term "client" does not imply any particular implementation characteristics (e.g., whether the application executes on a server, a desktop, or other devices).

* "*_relying party_*": An application making protected resource authorization on behalf of the service provider and also managing its identity. The "relying party" acts as the "client" but on service provider side. This is sometimes abbreviated as "*_RP_*".

* "*_authorization server_*": The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization. This is sometimes abbreviated as "*_AS_*".

* "*_access token_*": The concept is the same of the [RFC6749], a tiny piece of code that contains the necessary authentication data, issued by the authorization server.

* "*_identity token_*" or "*_ID token_*": The structure is similar to access token but it is used as proof that the user has been authenticated. The ID token may have additional information about the user and, it is signed by the issuer with its private key. To verify the token, the issuer’s public key is used.

* "*_digital ecosystem_*": Internet environment composed of all entities based on the same identity provider.

The detail of the information exchanged or protocols in the interactions between the authorization server and the requesting client, or between relying party and resource server, or the composition of tokens, is beyond the scope of this specification.

3. Symmetric authentication protocol

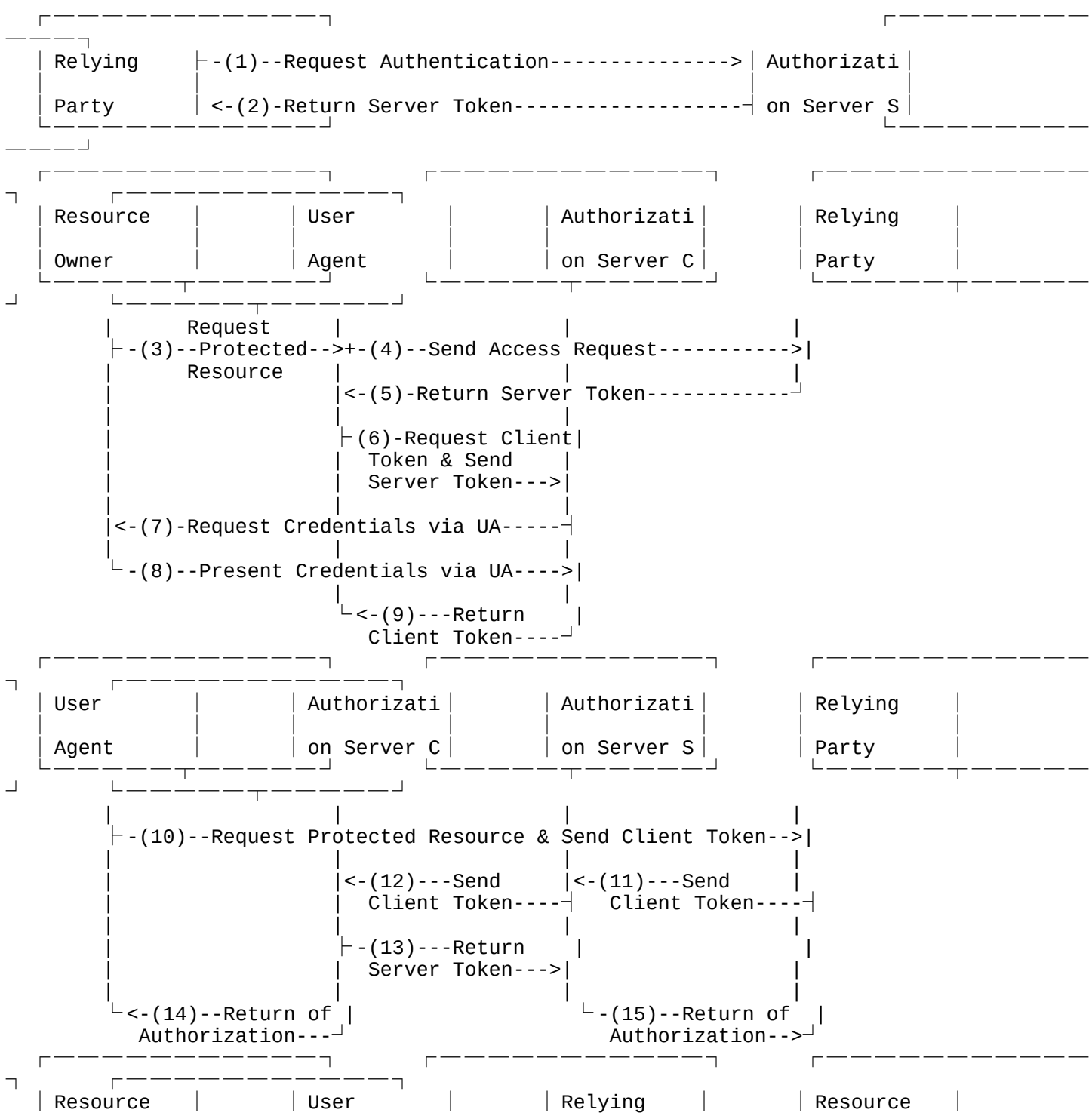
The symmetric authentication flow is conceptually not too dissimilar from the classic one referring to the single ecosystem [RFC5234], except that the authentication is dual because the two flows reflect the same operations symmetrically. Both the *client* (_resource owner_) and the *server* (_service provider_) MUST authenticate their identity through their IdP. The details of each basic operation in the symmetric process are the same as the corresponding single ecosystem specification [RFC6749] and MUST maintain alignment with it over time.

The authentication sequence between a consumer and a resource provider operating in different environments will be:

_1._ Entities exchange the access tokens received from their authentication server with each other.
_2._ Entities send the received token to their authentication server.
_3._ Authentication servers exchange access tokens with each other.
_4._ Authentication servers verify tokens with their original.
_5._ Authentication servers send the result to their own entity.
_6._ Entities are authenticated and can now exchange information.

Conceptually, in a client-server schema, the authentication process begins with the resource owner requesting access to the protected resource to the service provider. Both respond with their access tokens and request their IdP to validate the received token. The IdPs exchange tokens for validation and send the result to their entity. On success, access to the resource is allowed.

Figure 3 shows the abstract depiction of the symmetric authentication sequence. A SVG image is available here (https://raw.githubusercontent.com/Luigi-Sbriz/identity/main/images/3_Symmetric-sequence-diagram.svg).



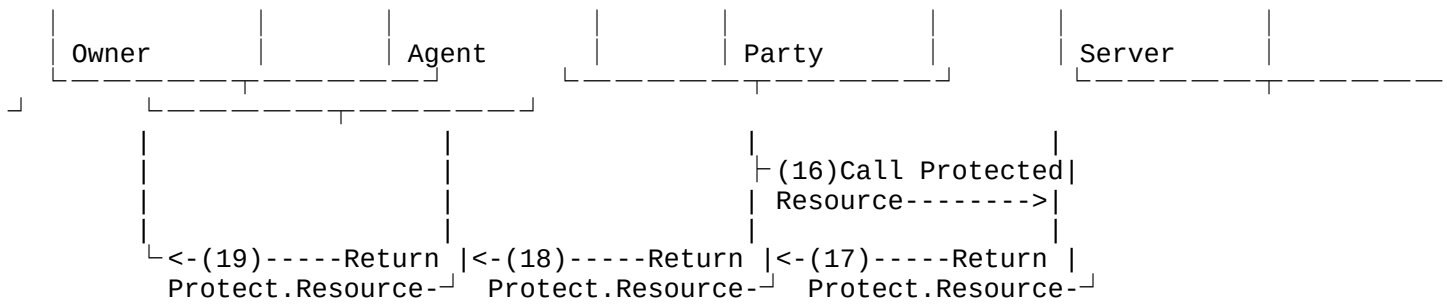


Figure 3: Symmetric Authentication Protocol - Sequence diagram

(1) - (2) The *_RP_* requests authentication to its *_AS_* (marked "S" as server) and receives the server token (access token from the service provider’s AS). The relying party must be provided with its own access token to resolve multiple requests.
(3) - (5) The *_RO_* requests access to the protected resource via the user agent. The *_UA_* activates the authentication process by requesting access to the *_RP_*, which responds by providing the server token. The response may also include the server ID token.
(6) - (9) The *_UA_* requests the client token (access token from the client’s AS) to its *_AS_* (marked "C" as client), sending also the server token received from *_RP_*. The client’s *_AS_* requests credentials from the *_RO_* and returns the client token to the *_UA_*.
(10) - (11) The *_UA_* requests the protected resource from the *_RP_* by sending the client token. Then, relying party requests to service provider’s AS to verify the client token.
(12) - (15) Both authentication servers must verify that the tokens received match the originals. Then, client’s AS informs the *_UA_* of the outcome and the same is done by the service provider’s AS to the *_RP_*. The outcome sent to the relying party may also include the client ID token.
(16) - (17) The *_RP_* notifies the *_RS_* of the legitimate request of ’*_UA_*. The *_RS_* returns the protected resource to *_RP_*.
(18) - (19) The *_RP_* sends the protected resource to *_UA_*, which then presents it to the requester *_RO_*.

Notes regarding some steps:
(4) If the server token is not available at this time, sequence (1) - (2) will be executed between steps (4) and (5) to provide the server token. Additionally, this change may also be necessary for a periodic refresh of the server token or if the entities are both clients.
(6) The client's authorization could be performed in advance and the client token stored securely by the user agent for handling multiple authentication requests. This means performing only the server token communication here, avoiding the following steps (7) - (9) because already done.

The verification of the authenticity of the tokens is carried out by the IdPs who exchange messages on a dedicated network to reduce the risk of intrusion. Security is strengthened by the presence of two interfaces for the exchange of tokens, one is for the party in trust and the other is for the opposing party. If one is compromised, the other interrupts the flow avoiding authorization. The trust placed in the mutual validation of messages avoids having to merge authentication domains, leaving great flexibility to the system as a whole.

Identity recognition information resides only with a trusted identity provider. This reduces the need to store too much personal information in Internet registrations. Furthermore, to easily identify which IdP holds the entity's authentication credentials, it can be easily extracted from the username structure if this is defined following the same technique used to compose an email address [RFC5322], that means an username, an @ sign, and a domain name.

4. Identity Provider - Trustee Concept

The symmetric authentication protocol bases its functioning on the existence of trusted entities, called *_identity providers (IdPs)_*. The identity provider is the owner of a digital ecosystem and, in addition to the authentication service in its own domain, also guarantees the secure transmission of authentication messages on other domains according to the symmetric authentication scheme already mentioned. Before being able to use the authentication service, it is necessary to register the natural or legal persons who need the digital identity. The integrity and confidentiality of this information must be guaranteed both in the registration process and in the authentication phases. The need for a high degree of confidentiality of the link between the digital identity and the real one requires the creation of a special category of IdPs with constraints linked to the laws of the real world.

In the specific network between IdPs, authentication messages are exchanged to ensure digital identity. Each IdP acts as a point of reference for the identity authentication service in its digital ecosystem, and must be able to communicate with every other IdP to recognize identities belonging to other ecosystems, securely from intrusions or tampering. The effectiveness of the entire authentication system depends on the trust placed in these identity providers but it must be deserved. This requires a robust organisation, subject to systematic oversight by independent certification body, to ensure transparent operational management by the IdPs.

4.1. Importance of this role

The identity provider is the guarantor of the authenticity of the relationship between digital credentials and the identity of natural or legal persons in digital communication. For this role it can also be called an *ID trustee* and the greatest criticality it must face is the inviolability of the messages exchanged. Furthermore, when processing personal data, the laws of the country to which the data subject belongs must be considered. It may also provide additional services (e.g. anonymous email, answering machine, anonymous accounts,...), but always in full compliance with the applicable law and only if they do not present risk for the data subject. Anonymization services are intended exclusively for the intended recipient but not for the authority exercising the applicable law (e.g. for a whistleblowing).

An IdP MUST be a legal entity subject to both the laws of the country to which it belongs and to international certification bodies, to guarantee compliance with this standard, the security of the information processed, the expected level of quality of service and the lawful processing of data.

4.2. Infrastructure

The infrastructure underlying symmetric communication is the IdP Network, dedicated to the exchange of authentication messages between IdPs. Ideally, each IdP always has two connectors, one to communicate with its trusted entity and the other to exchange messages with another IdP. With its own entity the mechanism is exactly the one defined by [RFC6749]. With other IdPs, a reserved channel is required for the exchange of tokens, which provides guarantees on the integrity of the messages and their origin. This channel SHOULD have low latency because it represents an additional step compared to the single ecosystem authentication scheme. The intended mechanism for sharing messages is that of a mail server [RFC5321]. The process for adding a new node (IdP) in the IdP

Network MUST require the identification of the legal entity that owns the node, but also the registration of identification data of the installed network devices, for security controls on the reliability of the node itself. Any variation must be promptly updated or the node will be disabled.

The dedicated network for the identity providers is not technically necessary for the authentication protocol but is essential for security, to reduce the risk of fraud or identity theft and, to ensure trust in lawful behavior. There MUST also be an international control body over IdPs and the management of the IdP Network. This authority will be responsible for governing the overall system, i.e. defining technical standards, or carrying out audits to ensure compliance with the rules, or acting to exclude nodes in case of violation of the rules.

5. Identity Provider - Custodian Concept

The relationship between digital and physical identity should be managed only by a particular identity provider, called *_identity custodian (IdC)_*, who has the legal authority to manage the personal data of the natural person. Only in this way it will be the perfect candidate to guarantee the identity provider the validity of the request for the release of a new digital identity, without having to disclose the physical identity to the IdP. Guaranteeing the digital identity of a user corresponding to a legal entity will not be the task of the identity custodian but of an authority or a process compliant with the law of the country to which the legal entity belongs. The identity token contains the indication between users of a natural person or a legal entity. The identity token makes it possible to distinguish the user of a natural or legal person and to know who has guaranteed the physical identity. An identity custodian can also act as an identity trustee, keeping roles distinct in communication protocols.

5.1. General schema

The identity custodian certifies that it is a real identity that requires the digital identity but can also provide personal data to identity trustee with the consent of the data subject. The identity trustee provides the authentication service for its digital ecosystem. A use case describing the relationship between identity custodian, identity trustee, and digital identity is provided in figure 4. A SVG image is available here (https://raw.githubusercontent.com/Luigi-Sbriz/identity/main/images/4_Identity-custodian-concept.svg).

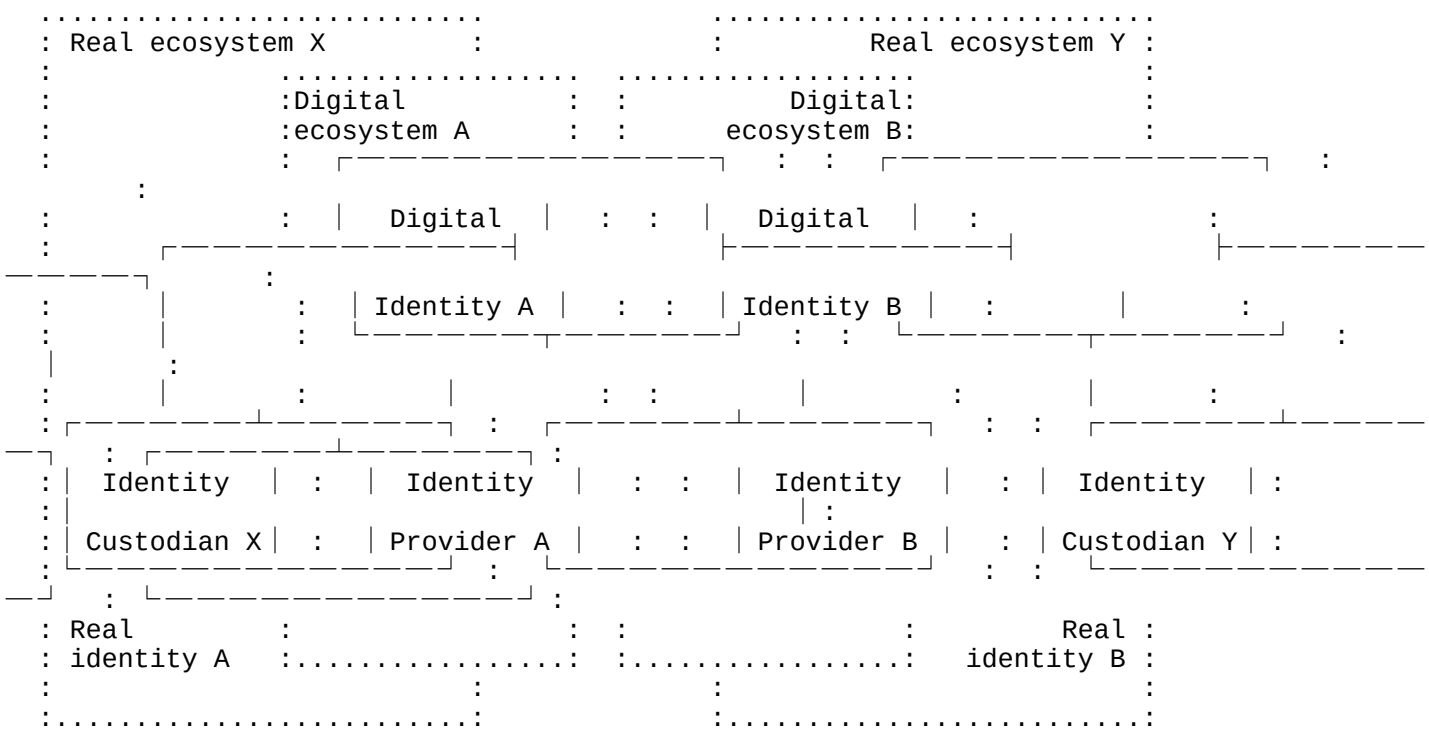


Figure 4: The Identity Custodian Use Case

Generally, identity provider must carry out the recognition and registration of the user's personal data before being able to guarantee its identity. The collection of the data of the natural person must be carried out in accordance with the protection provided for by the regulations in force. To ensure that the processing of personal data is restricted and controlled, it is useful to divide the set of IdPs into two categories. In the first, there will be IdPs (also called trustees) that only manage digital identity operations, and in the second, IdCs (identity custodians) that guarantee trustees that the applicant's identity is real. The IdC's category should operate under the responsibility of the legal authority that manages the real identity of the individual (i.e. who issues the identity card).

Through the identity custodian, each individual can request the issuing of a new digital identity to their trusted IdP. It will be the trusted IdP who will ask for confirmation of the applicant's authenticity directly from the IdC. The applicant must send an ID token with their IdC contact information to initiate the request. The request will be managed entirely online and will not require any personal data from the data subject but, subject to consent, everything will be sent by the IdC. The new identity will be useful to meet the typical needs of transactions on the Internet, with the right confidentiality for the holder and an added value for the authority, being able to identify the real person. The digital legal identity to sign contracts should be managed directly by IdC.

In short the roles involved in the trust-based authentication system.
- The *_identity custodian_* is the guarantor of the existence of the natural person and has the ability to uniquely identify it but only following a formal request from the legitimate authority.
- The *_identity provider_* receives the identification data that the data subject has decided to provide and will match these to the digital identity.
- The *_service provider_* will have the guarantee that the user is linked to a real person for security, contractual or legal reasons.
- The *_data subject_* can provide personal information according to their need, also maintaining anonymity.
- The *_public authority_* that manages the real data will be able to identify the individual with certainty in case of violations of the law (i.e. to protect the service provider).

5.1.1. Issuing of a New Digital Identity

The request for a new digital identity is activated by the natural person towards the chosen trustee. The trustee will request confirmation from the identity custodian if the request lawfully came from a real person. In case of confirmation, it will record the personal data that the data subject has authorized IdC to transfer. A use case describing the request of a new digital identity is provided in figure 5. A SVG image is available here (https://raw.githubusercontent.com/Luigi-Sbriz/identity/main/images/5_New-identity-use-case.svg).

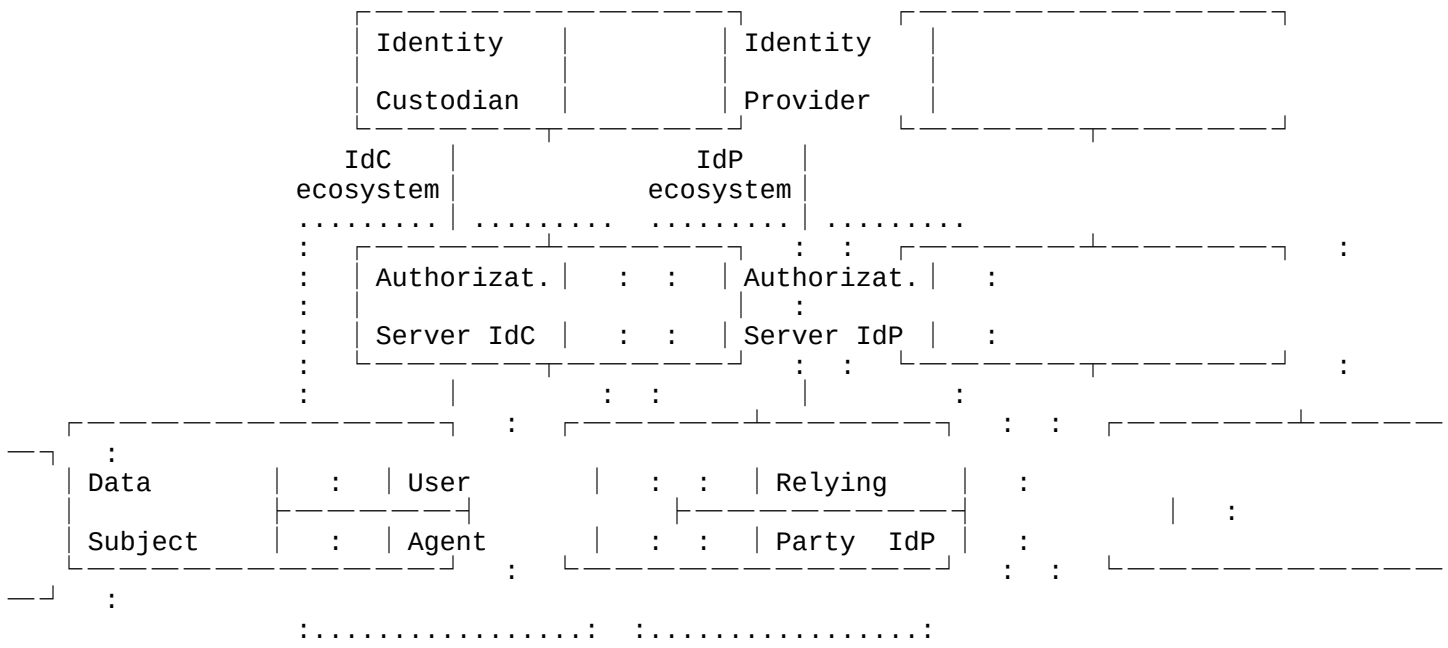


Figure 5: Abstract of New Digital Identity Request

Figure 6 shows the abstract representation of the message exchange sequence to request a new digital identity. A SVG image is available here (https://raw.githubusercontent.com/Luigi-Sbriz/identity/main/images/6_New-identity-sequence-diagram.svg).

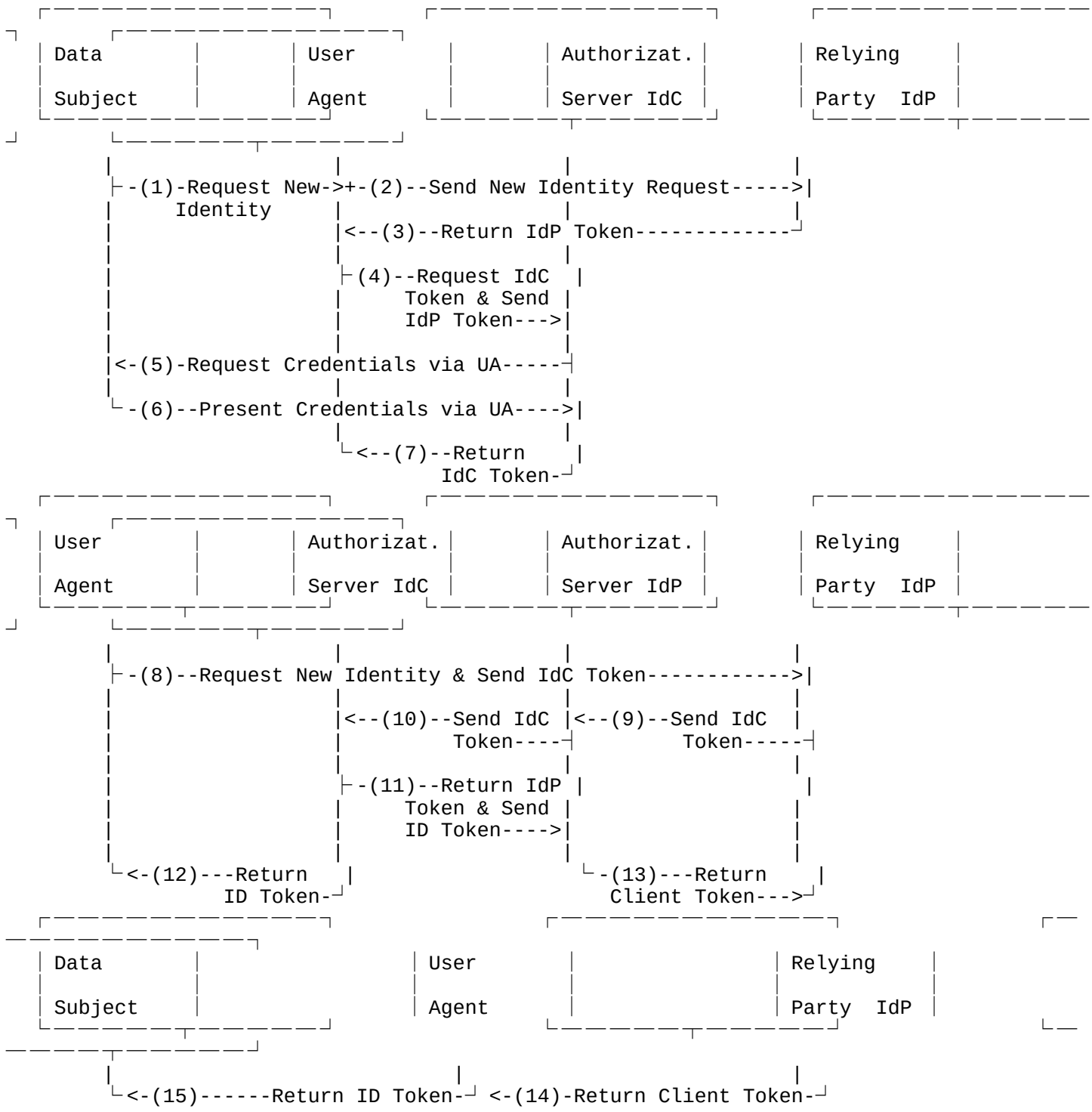


Figure 6: New Digital Identity Request - Sequence diagram

(1) - (3) The *_data subject_* requests the new digital identity via the user agent to the identity provider. The *_UA_* activates the authentication process by requesting the new identity to the *_RP_*, which responds by providing the IdP token (access token from IdP's AS).
(4) - (7) The *_UA_* requests the IdC token (access token from the custodian's AS) to its *_AS_*, sending also the IdP token received from *_RP_*. The custodian's *_AS_* requests credentials from the *_data subject_* and returns the IdC token to the *_UA_*.
(8) - (9) The *_UA_* requests the new digital identity from the *_RP_* by sending the IdC token. Then, relying party requests to identity provider's AS to verify the IdC token.
(10) - (11) Both authentication servers must verify that the tokens received match the originals. If required by data subject, the custodian's AS will send an additional ID token with personal data.
(12) - (13) Custodian's AS informs the *_UA_* of the outcome and, if required, sends also a copy of the ID token. The identity provider's AS sends to the *_RP_* the client token (related the new identity provided by IdP).
(14) - (15) The *_RP_* sends the client token to *_UA_*, which then informs the *_data subject_* of the outcome and, if required, sends a readable copy of the ID token to check the personal information shared.

Notes regarding some steps:
(3) If the relying party does not have the IdP token available, this will be requested from the authentication server after step (2).
(4) IdC token does not contains any real identity information as default. If requested, an ID token with a standard set of real information can be included during this step.

Any new digital identity with legal value is issued according to the rules defined by the relevant authority. It is presumable that there is also physical recognition of the data subject before the provision of credentials but no reference model is defined in this document.

6. Sustainable Digital Identity Trust Schema

For the effectiveness of the identity trust system based on the paradigm of trust towards a third party recognizable as reliable, it is necessary to guarantee a transparent and verifiable mechanism. The objective is to achieve universal participation and it is only possible if trust in the system as a whole is demonstrable. For this reason it is necessary to establish founding principles that guide the rules to guarantee equal dignity and balance in all components of the system. The following nine principles are established:

1. The digital identity can be cancelled or deleted without impacting the physical identity.

2. The digital identity must be linkable to the physical identity in a verifiable manner.

3. Only the authority that legally manages the individual’s physical identity can verify this link.

4. The authentication system must be flexible (i.e., able to adapt to technological evolutions or emerging needs).

5. The authentication system must be accessible to all potential users (i.e., without discriminatory costs).

6. The authentication system must be secure (i.e., continuously aligned with security best practices).

7. The authentication system must be privacy-friendly (i.e., not requiring any personal information unless strictly necessary).

8. The authentication system must be resilient (i.e., with availability appropriate for needs and the ability to cope with adversity).

9. The authentication system technology must be open (i.e., able to evolve based on transparent shared standards and verifiable developments).

To guarantee the principles set out, the requirements of the authentication system MUST include the protection of personal data and the guarantee of anonymity for lawful purposes, that is:

1. Ensure mutual recognition to guarantee the identity of the provider to the consumer.

2. Ensure the capability to authenticate the digital identities of consumers and providers against their real-world identity, without unnecessarily exposing real data.

The capability to validate the authenticity of the relationship between digital identity and physical identity lies only with the public authority responsible for managing the citizen’s identity. Operationally, it is implemented through a digital identity recognition service (i.e. IdC), technologically compliant with the operational protocols of an identity provider but under the supervision of the public authority.

7. Security Considerations

There are some cautionary points regarding security that need to be considered. - Integrity and resilience are the most critical parameters. The integrity of the messages is fundamental to guarantee the authenticity of the identity, while the availability of the authentication service is the basis for ensuring the feasibility of the entire process. - Symmetric authentication contrast the risk of man-in-the-middle attack because it should successfully attack both message flows at the same time. - The trustee is a critical component of the identity system and must be subjected to rigorous checks on compliance with the standards. - The relying party and the resourse server should be on different servers using a dedicated communication channel.

Referring to the term identification, we mean at least three different types, the device, the digital user and the individual.

* The *_device_* is identified with technical methods suited to the various needs. For example, geolocalization using International Mobile Equipment Identity (IMEI) [ITU1] and Integrated Circuit Card ID (ICCID) [ITU2].

* The *_digital user_* is well managed by [RFC6749] but inside the digital ecosystem. To manage users of multiple domains, either the user registrations are duplicated for each domain involved, or the domains involved are joined in a trust relationship.

* The *_individual_*, or natural person, is well managed with classic physical methods (e.g. photo ID) but the link with the digital identity needs to be improved because the quality is not satisfactory. This topic is beyond the scope of this specification and it was explored for example in [LS3].

An in-depth defense system SHOULD consider all the components involved and in this case not just the pure digital authentication of the user. In this document only the digital user is treated but extensions applicable to mixed situations with multiple types are certainly welcome to improve the overall security profile.

7.1. User registration

It is important to control the amount of data exchanged during the authentication process but also that the data required to issue a new digital identity are the only ones strictly necessary. To assign access credentials to a protected resource to a user, a process of recording the user’s identification and contact data is necessary, as they are necessary for the authentication of the digital identity and

for the attribution of access rights to the resource. Data provided or exchanged with IdPs MUST comply with the need-to-know principle. Three ways of recording are required.

7.1.1. Registration with an identity custodian (IdC).

The IdC has the legal authority to retain all personal data essential to complete the process of recognizing the real individual. Consequently it also has full authority over digital identity data and registration is subject to the law of the individual’s country of origin.

7.1.2. Registration with an identity provider (IdP).

The IdP has to guarantee the authenticity of the digital identity and the collection of personal data SHOULD be limited to the sole purpose of this operation. For the registration of a natural person, the IdP requests confirmation from the IdC of the real identity of the applicant before issuing the digital identity. The process is completely online and does not require any physical recognition. For legal entities, the data is provided by the owner or a delegate.

7.1.3. Registration with a service provider (SP).

The service provider SHOULD know only the data necessary to build the authorization roles to govern access to resources and nothing more. These are provided directly by the user or by an ID token, in addition to those received automatically from their IdP relating to digital identity.

8. Conclusions

To operate effectively between the different digital ecosystems, the identity management system MUST be based on a common authentication protocol that symmetrically carries out the same operations in complete transparency, entrusting the decision on recognition to a trusted third party. Confidence in the reliability of recognition carried out by the identity guarantor (IdP or IdC) cannot be based on the technological component alone. It is therefore necessary to involve an independent supervisory authority for technological aspects and the local competent public authority responsible for data protection.

To improve trust in the digital operations between the consumer and the service provider three guarantees must be provided.

1. The mutual recognition between consumer and service provider.

2. The control and minimization of the personal information processed.

3. In case of legal need, the ability to match the digital identities of consumer and provider against their real-world identity.

Due to the strong synergy that can be achieved, it is advisable to maintain constant technical alignment with the standard [RFC6749] and the related specifications to implement point-to-point authentication, within the broader symmetric authentication framework.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. Normative References

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/rfc/rfc5322>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/rfc/rfc5321>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/rfc/rfc5234>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

10.2. Informative References

[ITU1] International Telecommunications Union, "QTR-RLB-IMEI - Reliability of International Mobile Station Equipment Identity (IMEI), Technical Report", July 2020, <https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-CCICT-2020-PDF-E.pdf>.

[ITU2] International Telecommunications Union, "E.118: The International Telecommunication Charge Card", May 2006, <https://www.itu.int/rec/T-REC-E.118>.

[LS1] Sbriz, L., "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 1: Identity Trust Abstract Model, ISACA Journal, vol.2", April 2022, <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/a-symmetrical-framework-for-the-exchange-of-identity-credentials-based-on-the-trust-paradigm-part-1>.

[LS2] Sbriz, L., "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 2: Identity Trust Service Implementation, ISACA Journal, vol.2", April 2022, <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/a-symmetrical-framework-for-the-exchange-of-identity-credentials-based-on-the-trust-paradigm-part-2>.

[LS3] Sbriz, L., "How to Digitally Verify Human Identity: The Case of Voting, ISACA Journal, vol.1", January 2023, <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/how-to-digitally-verify-human-identity>.

[LS4] Sbriz, L., "Modeling an Identity Trust System, ISACA Journal, vol.6", November 2023, <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/modeling-an-identity-trust-system>.

[LS5] Sbriz, L., "The Role of the Identity Provider, ISACA Journal, vol.2", February 2025, <https://www.isaca.org/resources/isaca-journal/issues/2025/volume-2/the-role-of-the-identity-provider>.

Acknowledgments

This document was prepared using a text editor with Markdown syntax (kramdown-rfc dialect).

Author’s Address

Luigi Sbriz
Cybersecurity, Risk & Privacy Senior Consultant
Italy
Email: luigi@sbriz.eu