A-SIT

Secure Information Technology Center – Austria

Service Provider Accreditation with Attribute Constraints

A-SIT

Service Provider Accreditation with Attribute Constraints

Author: Stefan More
Mail: smore@tugraz.at
Date: April 2024

Abstract:
In credential-based authentication systems, users transmit personally identifiable and potentially sensitive data to Service Providers (SP; also called Relying Parties, RP). In doing so, users often must rely on the assumption that they are communicating with a legitimate Service Provider and trust that the SP has a legitimate reason for requesting all the attributes about the user. In the event of data misuse, it can be difficult to identify and hold the SP accountable. One solution to this is to implement mutual authentication before transferring sensitive data. To fully authenticate a SP and establish trust in it, the SP gets accredited by a party trusted by all users. To ensure that the SP can only access data based on a legal basis, these accreditations are combined with a set of access constraints, i.e., a policy that restricts the queryable data. The motivations for this work are privacy demands as well as legal requirements (e.g., GDPR: Article 5 "Personal data shall be collected for specified, explicit and legitimate purposes", Article 6 "Processing shall be lawful only if [...] processing is necessary").

This project aims to analyze the accreditation of service providers, focusing on limiting the attributes that an SP can request from a user based on provided evidence of the reason for the request. This report also discusses enforcement of pseudonym-support by SPs. Further, the report incorporates privacy-enhancing measures into the constraints, such as limiting executable zero-knowledge predicates.

Contents

1. Introduction

In credential-based authentication systems, the exchange of personal data between users and Service Providers (SPs) is the basis for the SP's authentication decision. However, this practice raises significant concerns regarding privacy, data security, and user trust. Users often find themselves in a position where they must entrust sensitive information to SPs, relying solely on the assumption of the SP's legitimacy and the necessity of the data requested.

The potential misuse of this data poses a considerable challenge, as identifying and holding SPs accountable for such breaches can be complex. As a response to these challenges, the concept of mutual authentication has emerged as a promising solution. By implementing mutual authentication protocols, both users and SPs can verify each other's identities before engaging in data exchange, thereby establishing a foundation of trust.

However, mutual authentication alone is not sufficient to address the broader issues of data privacy and security. To establish trust in the SP's identity, it is essential to go beyond authentication and include the accreditation of SPs. Accreditation involves the validation of SPs by a trusted party, ensuring their legitimacy and adherence to specific standards and regulations (e.g., GDPR). This accreditation process, coupled with access constraints, serves as a mechanism to limit the data that SPs can request from users, thereby safeguarding sensitive information. In contrast to merely displaying the accreditation information to the user and relying on their judgement, constraints are machine-enforceable and thus enable automated checking of a request's legitimacy.

The motivations driving this report are multifaceted, stemming from both privacy demands and legal considerations. With regulations such as the General Data Protection Regulation (GDPR) mandating the collection and processing of personal data for explicit and legitimate purposes, there is a pressing need to develop robust mechanisms that uphold these principles. Moreover, advancements in privacy-enhancing technologies enable even better privacy measures into authentication systems to mitigate privacy risks effectively.

To demonstrate the significance of this project, let us consider a few examples. Imagine a scenario where a user accesses an online healthcare portal to schedule an appointment. In this context, the SP requires access to specific health-related attributes to fulfill its service. However, without proper accreditation and access constraints, there is a risk of unauthorized access to sensitive medical information, potentially violating the user's privacy rights.

Similarly, in the context of financial services, users often provide personal and financial data to SPs for transactions and account management purposes. Without effective accreditation measures and access constraints, SPs may overreach in their data requests, exposing users to financial risks and privacy breaches.

These examples underscore the critical importance of analyzing the accreditation of SPs and implementing effective access constraints to safeguard user privacy and data security. Furthermore, by incorporating privacy-enhancing measures such as pseudonym-support and zero-knowledge predicates, this report also considers new ways of data protection in credential-based authentication systems.

1.1. Bird's-eye view: Concept

In this section we provide a bird's eye view from the user's perspective of how an accreditation check unfolds. The concept is discussed in more detail in the rest of this report.

1. Service Access: The user wants to access some service or resource. Since the service is protected by some access control system, the Service Provider (SP) asks the user to provide (*present*) some credentials so that it can authenticate the user and grant (or deny) access.
2. Presentation Request: The user receives a request from the SP to present their credentials for authentication. In this request, the SP tells the user what credentials (or attributes) it requires. For example, since the SP needs to perform an age verification, the SP asks the user for a government-issued credential containing the user's date of birth.
3. Authenticate SP: The user verifies the identity of the SP, checking that the provided SP accreditation represents the entity that sent the presentation request.
4. Check SP Trustworthiness: The user validates the SP's certificate for trustworthiness. This includes verifying if the accreditation document was issued by a trusted accreditation body. Further, the user checks for any revocation status, and consults an accreditation registry with Certificate Transparency (CT) logs to ensure the SP's accreditation status. The last step is needed to ensure that competent entities (like data protection authorities and NGOs) can audit the list of accredited entities.
5. Check Constraints: The user evaluates the access constraints imposed on the SP by the accreditation body, ensuring that the requested attributes align with regulations and that the SP has a legally justifiable purpose to process these data. For example, if the SP asks the user for a date of birth, the user checks if this specific SP is authorized to ask for that date.
6. Ask User for Consent: The user is prompted to consent to the sharing of their credentials and attributes based on the SP's request. This ensures that the requested attributes align with the user's expectations and privacy preferences.
7. Build Presentation: Upon receiving user consent, a presentation containing the requested credentials and attributes is constructed by the user.
8. Log Request & Response in Wallet: The details of the request and the user's response, along with any relevant metadata, are logged in the user's digital wallet for future reference. This can be used as evidence in case any misbehavior of the SP is discovered later, e.g., if the SP processed the data in a different way than specified in the accreditation or communicated to the user.
9. Sign & Send: The user digitally signs the presentation and sends it securely to the SP.

2. Background and Definitions

2.1. Architecture and Entities

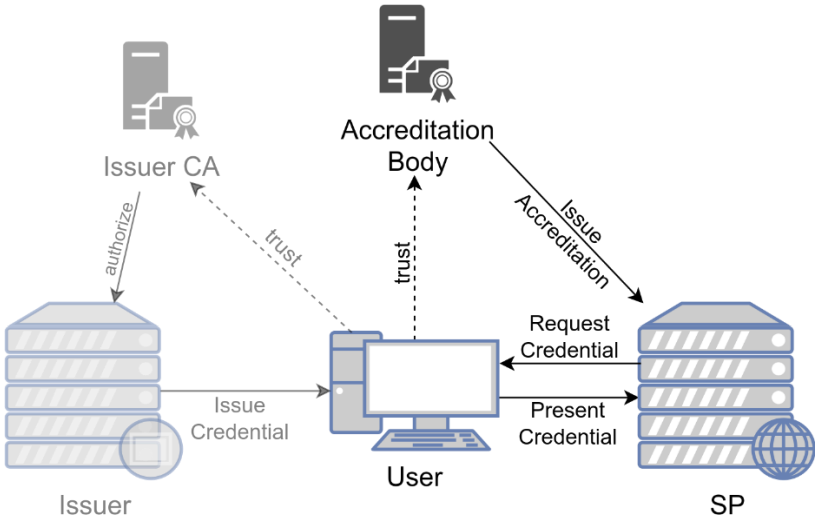

Figure 1: Overview of the Entities, with a focus on the Credential Presentation process

- Issuer CA/Trust Root: The Issuer Certificate Authority (CA) or Trust Root is the entity responsible for issuing digital certificates to Issuers, authorizing them to issue certain credentials.

- Issuer/IDP: The Issuer or Identity Provider (IDP) is responsible for issuing credentials to users. These credentials contain digital representations of the user's identity attributes, such as name, email address, or other pertinent information. Those credentials are signed using the issuer's certificate.

- Holder/User/Wallet: The User or Holder is the entity that possesses and presents credentials to Service Providers (SPs) for authentication. The Wallet is the user's software (typically on the user's phone) serves as a secure repository for storing and managing digital credentials.

- SP/RP/Verifier: The Service Provider (SP) or Relying Party (RP) is the entity that operates a service and requests authentication from users. The Verifier refers to the tools or software operated by the SP to verify the authenticity and validity of the credentials presented by the user (sometimes also called *SP Instance*).

- Accreditation Body: The Accreditation Body (AB) is an authoritative entity responsible for accrediting Service Providers based on predefined standards and regulations. It issues accreditations to SPs, validating their legitimacy and adherence to established protocols. Additionally, it assesses the data processing purpose provided by the SP and issues constraints as part of the accreditation. The AB is in turn commonly accredited by a legal authority that enables some liability as part of a governance framework.

- Credential: A credential is a digital representation of a user's identity attributes, typically issued by an Issuer. It contains information such as the user's name, email address, role, affiliations, or other relevant details. Credentials are encoded in machine-readable form and serve as proof of identity when presented to Service Providers for authentication purposes. Cryptographic signatures are used to both ensure the authenticity of the credentials (signature by the SP) and to link a credential to a specific user (public key of the user in the credential).

2.2. Pseudonyms

Pseudonyms serve as a privacy-enhancing mechanism by allowing users to interact with Service Providers without revealing their true identities or a persistent identifier.

One common approach to pseudonymity is Pairwise Pseudonymous Identifiers.[1] Pairwise Pseudonymous Identifiers involve the creation of unique identifiers for each pairwise relationship between a user and a Service Provider. This means that each user generates a new pseudonym for each Service Provider it interacts with, and does not re-use the pseudonym from one SP with another SP. These identifiers are used as temporary or one-time pseudonyms during interactions, preventing SPs from tracking users across different services or sessions (*Linkability*).

Another special form of pseudonyms (e.g., ABC4Trust Pseudonyms [4]) provide anonymous/pseudonymous and unlinkable usage of a service but enables a trusted entity (*Inspector*) or set of entities to later reveal the identity of a pseudonym.

2.3. Privacy-enhancing Technologies

2.3.1. Selective Disclosure

Selective disclosure refers to the ability of users to control and limit the information they reveal to Service Providers during authentication processes. By employing privacy-enhancing technologies such as attribute-based credentials or SD-JWTs,[2] users can selectively disclose specific attributes from a credential, without revealing the other attributes. For example, a user can use a passport-credential and only reveal their date of birth, hiding all the other attributes of the passport. This ensures that only relevant and necessary information is shared, minimizing the risk of privacy breaches and unauthorized access to sensitive data. At the same time, selective disclosure mechanisms empower users to maintain control over their personal information while still participating in authentication procedures, thereby fostering trust and confidence in the authentication system.

2.3.2. Zero-knowledge Proofs

Zero-knowledge proofs (ZKPs) represent a cryptographic technique utilized to demonstrate the validity of a statement without revealing any sensitive information. In the context of authentication systems, zero-knowledge proofs enable users to authenticate themselves to Service Providers without disclosing their underlying credentials or personal data. By leveraging zero-knowledge protocols, users can prove possession of certain attributes or credentials without actually revealing the attributes themselves, thus safeguarding their privacy. This enhances user control over their data while ensuring the integrity and security of the authentication process. Incorporating zero-knowledge proofs into authentication systems reinforces privacy protection measures and strengthens user trust in the system's security.

In the context of this report, zero-knowledge proofs and protocols can be used to take selective disclosure a step further and authorize a SP to only request *predicates* on user attributes. For example, while a user is in possession of a passport-credential containing the full date of birth, the SP can be authorized to only ask for the user's age, calculated from the date of birth. In that example, neither the date of birth itself nor any other attributes are revealed to the SP, but an age-verification is still possible.

[1] https://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg
[2] https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/

3. Goals and Motivation

3.1. Privacy Expectations

To increase user acceptance in a credential system, and to fulfill users' privacy expectations, we use some basic privacy goals [1] as the basis for this report's scope. We model these expectations after everyday life interactions in the offline world. We discuss further aspects of those goals in the sections below.

- Confidentiality: When presenting a credential to some Service Provider, the user has the expectation that their credential is only accessible by that specific service provider.[3] To fulfill that expectation, a system must be able to authenticate the service provider, present that information to the user, and ensure that the data is directly transmitted (and, i.e., encrypted) to that provider.
- Data Minimization: Users expect that a service provider only receives the data that it needs to provide a service, and data that the SP needs to collect or process by law (e.g., due to KYC requirements). Users can consent to the sharing of more data for further *lawful* processing, e.g., personalization or marketing.
- Anonymity and Pseudonymity: Many interactions in daily life are anonymous. Users expect that they can use services without revealing their identity. For example, the US Supreme Court even argues that there is a constitutional Right to Anonymity,[4] stating that the "decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." In some cases, full anonymity is not desirable, for example when a recurring user wants to use an online forum. In that case users expect pseudonymity, i.e., the use of a pseudonym that is not linked to their legal identity.
- Unlinkability: Users expect that they can use a credential or a set of credentials with different service providers without reducing their privacy. Specifically, the involved service providers should not be able to link the interactions with each other, which would allow for user profiling. In the case of anonymous/pseudonymous interactions, users would like to use the same credential twice (i.e., for age verification) in two interactions. The expectation is that the service cannot link the two interactions with each other, i.e., does not know that the same user interacted with it twice (*multi-show unlinkability*).
- Unobservability: In the same way, users expect that no party except those directly involved in an interaction (i.e., the user and the service provider) learn that the interaction takes place. Specifically, users expect that the issuer or some other authority (e.g., the government) does not learn at what SP the user is using their wallet, or even *that* the user is using their wallet.

3.2. Usability and Lawfulness

This report acknowledges the complexities users face in evaluating every authentication request. Particularly, issues arise concerning users' ability to discern the legitimacy of Service Provider and the purpose of data disclosure. Drawing parallels to challenges encountered with Extended Validation (EV) certificates in the Web PKI (HTTPS), where users often struggle to differentiate between legitimate and

[3] This does not necessarily mean that there are no lawful ways to share the data with further parties, as for example GDPR allows that service providers delegate the processing of data to third parties (under certain conditions). However, they stay accountable in case of breaches or misuse.

[4] https://epic.org/issues/democracy-free-speech/anonymity/

malicious entities,[5] the system recognizes the necessity for automated enforcement mechanisms. This entails automatic checks to ensure that requests for data align with legal requirements. While users may retain the option to override automated decisions, such actions could lead to unintentional over-sharing, e.g., in case of authentication under stress or when the consequences are not easy to assess. Additionally, while this report also considers scenarios involving optional data disclosure, there is still the need for a legitimate purpose even for non-mandatory information.

3.3. Enable Liability of SPs

To enable liability of misbehaving SPs, the system implements measures to collect signed presentation requests, effectively serving as evidence of the accreditation and purpose invoked during authentication. By gathering this evidence, the system establishes evidence for holding SPs accountable for their actions. In cases where legal recourse becomes necessary, the availability of verifiable traces and evidence empowers credential holders to justify claims of overreach or misconduct by SPs. This ensures that SPs can be held liable for any breaches of trust, thereby fostering accountability within the authentication ecosystem.

3.4. GDPR Compliance

Ensuring compliance with data protection regulations like the GDPR [8] is paramount for any SP's authentication system. For example, GDPR Articles 5 and 6 emphasize the purpose and lawfulness of processing personal data. It is imperative to scrutinize the purpose for processing data, ensuring alignment with GDPR principles. Additionally, the framework must assess whether the purpose justifies accessing qualified data or if accessing unqualified data is sufficient. In many cases, merely obtaining a user's name suffices without the need for a government-issued credential. More generally, this underscores the importance of adhering to the principle of "privacy by design", "need to know", and implementing the principle of least privilege. By assessing the purpose, and strictly limiting data access to what is essential for the intended purpose, an accreditation system can enhance GDPR compliance, mitigate privacy risks, and uphold user rights to data protection.

3.5. eIDAS Identity Wallets (April 2024)

The European eIDAS 2 regulation amends the original eIDAS regulation from 2016, introducing a framework for European digital identity wallets [9]. The new eIDAS regulation introduces further privacy rules, in addition to the existing privacy rules of the GDPR [5; 8]. Those rules are tailored to the wallet context. For this report, the most relevant articles are Article 5a—introducing the identity wallet—and Article 5b—covering service providers. Furthermore, Article 5 establishes a right to the use of pseudonyms.

- SP Registration: A SP shall register in the Member State where it is established. SPs shall identify themselves to the user (Article 5b).
- Purpose Registration: During registration, a SP shall provide indication of the data to be requested from users, and shall not request any other data than indicated (Article 5b).
- Purpose Information: Wallets shall inform the user whether the SP has the permission to access a credential (Article 5a).

[5] https://arstechnica.com/information-technology/2017/12/nope-this-isnt-the-https-validated-stripe-website-you-think-it-is/

- Auditability: The list of registered SPs and their indicated data processsing shall be public in a form suitable for automated processing (Article 5b).
- Unlinkability: The technical framework shall ensure unlinkability (Article 5a).
- Selective Disclosure: The technical framework shall ensure that selective disclosure of data is possible (Article 5a).
- Unobservability: The technical framewark shall not allow Issuers or any other party to track, link or correlate user behavior (Article 5a).
- Pseudonyms: The use of pseudonyms that are chosen and managed by the user shall not be prohibited (Article 5). Wallets shall enable the user to generate pseudonyms and store them encrypted and locally (Article 5a). SPs shall not refuse the use of pseudonyms, except where the identification of the user is required by law (Article 5b).
- Control: Users shall have full control of the use of the wallet and of the data in their wallet (Article 5a).

3.6. Prevent Profiling by SPs

To address the threat of profiling by Service Providers, accreditations should also consider the mitigation of linkability, enabling unlinkability. Nonconsensual profiling is a key concern tied to privacy-loss, surveillance capitalism, advertising, and surveillance. To counteract linkability, accreditation systems could allow or mandate the use of pseudonyms, ensuring that user identities remain neither uniquely identifiable nor persistent over time to prevent tracking and profiling. A stronger privacy goal is multi-show-unlinkability, allowing users to freely generate pseudonyms without compromising their privacy.

An open discussion point is about whether to allow an infinite number of pseudonyms or limiting that number per service provider. On the one hand, limiting the number of pseudonyms aids SPs in verifying sybil resistance, eliminating the need for intrusive measures like phone number verification. This represents an important incentive for SPs to use a credential system and results in better privacy for users. On the other hand, limiting users in how many pseudonyms (and thus accounts) they can create limits their freedom of using the service. Additionally, it is not clear how to limit the number of pseudonyms to a specific number that is not one.

3.7. Prevent Profiling by Authorities and Infrastructure

To prevent surveillance and profiling by authorities and infrastructure operators, we emphasize unobservability as a fundamental principle. The goal is to ensure that authentication processes remain unobservable to external entities. Crucially, the accreditation body is not directly involved in the accreditation check process by the user.

3.8. Prevent Over-asking and Over-identification

Accreditation systems can provide measures to address both excessive identification and the transfer of unnecessary personal information [5; 6; 7, Section 7.6].

Over-identification is the excessive identification in previously anonymously conducted interactions. It could be mitigated by limiting the disclosure of personally identifiable information to use cases where trustworthy information is really needed (e.g., required by law), and only share what is essential for authentication purposes.

Similarly, over-asking occurs when Service Providers request more attributes from users than necessary for their use case. By enforcing strict access constraints and adherence to the principle of data minimization, a system could ensure that SPs only collect the minimum required attributes for authentication. Through these measures, the system strives to strike a balance between fulfilling SPs' *legitimate* needs and safeguarding users' privacy rights.

Both over-identification and over-asking present an additional challenge, given that qualified data in the hand of a SP has more value than unsigned data. This represents a very attractive target for attacks, hence the need to limit the entities with access to the data.

4. Limitations

While accreditations play a crucial role in ensuring the trustworthiness of Service Providers, it is essential to recognize their limitations.

Accreditations, while valuable, cannot resolve all issues, particularly those rooted in legal or governance frameworks. For instance, certain jurisdictions may mandate the disclosure of real names or identifiers. If this is enforced by law, a government-controlled system could not prevent SPs from executing this regulation. Specifically, accreditation bodies would then accredit all SPs to retrieve names or other identifiable data. However, users can still refuse to share credentials – with the possible effect of no access to services. Additionally, accreditations are susceptible to exploitation. For example, accreditation bodies may issue accreditations with overly permissive constraints. Consequently, trust in the accreditation body is paramount, necessitating transparency measures such as public logs of accreditations and constraints. These logs enable competent entities to monitor accreditation activities and ensure compliance with established standards. While this cannot prevent intrusive accreditation constraints, it at least allows for their detection by the public, potentially holding the authority accountable.

Another limitation lies in the nature of digital data. Once data is *lawfully* shared, enforcing usage and storage limitations becomes challenging: The user has no control about what the SP *really* does with the data, and with whom it shares the data. While liability mechanisms exist, such as presentation/access logs stored by the user, they do not inherently prevent misuse or unauthorized access. However, they serve as evidence of data sharing and can be instrumental in holding parties accountable for breaches. Additionally, accreditation primarily covers the showing process and does not extend to protecting against unauthorized access to the wallet itself. For instance, in scenarios where a border authority confiscates a user's phone, accreditation mechanisms may not offer direct protection against data exposure.[6]

5. Accreditation and Constraints

5.1. Baseline

As the baseline for our report, we consider a credential system where the user has no information about the Service Provider (SP) it is interacting with. Even in scenarios where some form of mutual authentication is performed without accreditation, i.e., the SP provides information about their identity, the user has no way to trust the provided identity information. In the absence of trustworthy accreditation information,

[6] While mechanisms like app attestation could make direct access to the data harder, it cannot fully prevent unauthorized access by entities with physical access to the user's device.

the authentication process lacks a layer of accountability and trustworthiness. Without accreditation, users have no assurance regarding the legitimacy or reliability of SPs, leaving them vulnerable to potential risks and abuses.

5.2. SP Accreditation

To introduce a verifiable – and trustworthy – identity of the Service Provider (SP), accreditations are used. Accreditations are created by Accreditation Bodies (AB) – entities which are trusted by the user. By introducing ABs into the system, the challenge of establishing trust on every single SP gets reduced to a single trust relationship. Based on this trust relationship with the AB, trust is delegated to individual SPs. Hence, by directly trusting a single AB directly, users can (indirectly) trust the identity information provided by all accredited SPs in the system. Additionally, ABs can also check whether SPs comply with data protection regulations and other laws before issuing accreditations to them. For example, they can check if the SP has a legitimate purpose for processing the user's personal data.

In a system where accreditation offers a mechanism for establishing the legitimacy and trustworthiness of Service Providers, users are empowered with the ability to verify and make informed decisions. Accreditation provides users with a means to assess the credibility of SPs, thereby enhancing trust and confidence in the authentication process. Additionally, accreditation introduces a layer of liability, holding SPs accountable for their actions and decisions in case of misbehavior.

However, using the accreditations to make informed decisions can be challenging for users. The complexity of the accreditation processes and the assessment of accreditation criteria may pose obstacles to users. While a wallet system can assist the user by only sharing credentials with accredited SPs, the user still must judge on their own what credentials and attributes they share with the SP. This can lead to over-asking and thus over-sharing of private data.

5.3. Accreditation Constraints

To further assist the user and prevent too much data from being shared with an SP, we couple accreditations with constraints. Accreditation constraints introduce a critical layer of control and protection within the authentication system. By imposing specific constraints on SPs, such as limiting the type of data they can request from users, the system enhances user privacy and security. Such constraints can limit what credentials a SP can request, or be more flexible policies, such as limiting access to certain attributes or even zero-knowledge predicates. We discuss possible types of accreditation constraints in Section 7 below.

By granting access only to the data that the SP can lawfully process, Accreditation Bodies (ABs) help users with preventing their data from being misused.

The user's wallet plays a pivotal role in enforcing these constraints, ensuring that only authorized data is shared with SPs during the authentication processes. While the wallet can automatically control that no data is shared for which the SP has no permission, it depends on the system's design whether the user can override this decision.

This proactive approach not only safeguards against over-asking and unnecessary data disclosure but also empowers users with greater control over their personal information. Constraints serve as a safeguard, aligning authentication processes with privacy principles and legal requirements, ultimately fostering trust and confidence in the authentication system.

6. Accreditation Forms

To allow for automated verification and checking by wallet software, accreditations and Accreditation Constraints need to be created in a machine-readable form. This can take many forms. The main requirement is that in the end the information is available to the wallet in a trustworthy manner during the interaction with the SP. For example, the publication of accreditation information can take the following forms:

- Accreditation Certificate issued to the SP: After describing their service, stating the purpose for data processing, and passing the accreditation check, SPs receive some form of Accreditation Certificate from the Accreditation Body (AB). This certificate is digitally signed by the AB and contains accreditation information and the constraints. During the authentication, the SP presents this certificate to the user. The user then uses their local trust store to check the certificate, and then uses the certificate to authenticate the SP. The user also utilizes standard revocation checks (OCSP or OCSP-stapling) to ensure the accreditation is still valid.
- Accreditation Registry: In this more centralized approach, the result of the accreditation process is not a certificate, but an entry into some public registry. While this entry is linked to the SP by means of a (self-signed) certificate, the accreditation information itself is directly stored in the registry. The advantage of this approach is that competent entities can monitor and audit the list of accredited SPs, and that the information can more easily be updated. When naively implemented, a disadvantage of this approach is that the registry potentially learns when a wallet interacts with a specific SP, resulting in observability. This could be mitigated by continuously downloading a snapshot of the registry, or other more privacy-preserving architectures.
- Combination: A combination of both Accreditation Certificate and Registry could potentially enable both privacy during the authentication process, and auditability of the system. In that approach, the trust in the SP is established by verifying the certificate (like in the first option), and then checking whether the certificate is linked to the registry (e.g., using mechanisms like the Web PKI's Certificate Transparency [2]). By doing so, the burden of verifying whether an AB issued a accreditation that is too permissive is transferred from the user to competent entities.

7. Types of Accreditation Constraints

7.1. Boolean Constraint

Boolean accreditation constraints represent the baseline case described above: a Service Provider (SP) is either accredited or not. For an accredited SP, the wallet grants access to all credentials stored in the wallet. In that case, the user must decide whether to grant access to the requested data or not.

7.2. Ordinal Constraint

Ordinal accreditation constraints represent the accreditation in the form of a numeric level. In that case, ether each level is mapped to a set of more advanced constraints inside the wallet. Or each credential or attribute is connected to a specific level. The second approach is similar to the secrecy classification approach often applied to classified information, i.e., there needs to be a math between the SP's accreditation level and the level of the information. For example, an accreditation for personal-but-not-

sensitive information could grant a SP permission to query for the user's name, address, and date of birth, but more sensitive information like health-related data is not accessible.

7.3. Advanced Constraints

The following advanced types of accreditations enable more flexible access control. Instead of granting all-or-nothing access or relying on pre-defined levels, Accreditation Bodies (ABs) explicitly authorize access to specific credentials, attributes, or predicates.

7.3.1. Credentials

Accreditation certificates contain a list of all the types of credentials the SP can access. Credential types can be for example identified using Uniformed Resource Names (URNs), Digital Object Identifiers (DOIs), and Credential Schemas.

7.3.2. Attributes

To enable more flexible control, accreditation certificates can also contain a list of attributes as constraints. In the same way than for credentials, attributes can be identified using various schemes, e.g., URNs[7] or other identification schemas.[8]

7.3.3. Predicates

To support privacy-preserving and -enhancing technologies like attribute-based credentials and zero-knowledge proofs, accreditation certificates can restrict the access to date to specific predicates on that data. For example, if the only legitimate purpose stated by a SP is an age-check of its users, the AB could accredit this SP only to age-check or date-difference predicates. By doing so, the SP has no access to other data, not even the user's date of birth [3].

7.3.4. Pseudonyms

Another type of accreditation constraint is concerned with the handling of the user's identifiable information, i.e., identity identifier or pseudonyms. For example, a social network might be accredited to use the wallet system merely to (re-)authenticate users (e.g., as a more convenient or secure replacement for a password manager or second factor system). In that case, the social network acting as SP has no business in learning any other information about the user. While the access to the user's credentials and attributes is easily restricted using the constraint types discussed above, the SP still has access to the user's identifier. Thus, the SP can link multiple visits by the same user and apply other profiling techniques.

To support users in their choice of identities, ABs can restrict SPs to only access user's pseudonyms, and to prevent that only a single pseudonym is possible for each SP. This is the wallet counterpart to a user that creates multiple accounts with an SP, without creating any link between those accounts.

For example, OIDC's pairwise pairwise pseudonymous identifiers prevent system-wide profiling by colluding SPs, but don't stop a SP from profiling multiple visits by the user. In contrast, pseudonyms that are freely generated by the users (somehow linked to their wallet identity or not) preserve the user's privacy and freedom of choice. While in general it's up to the users how many pseudonyms they use for each service, there might be a limit to sybil restrictions (see discussion in Section 3.6 above).

[7] https://eid.egiz.gv.at/anbindung/uebersicht-der-personenmerkmale-attribute/
[8] https://schema.org

8. Conclusion

Accreditations and accreditation constraints represent foundational pillars in the architecture of credential-based authentication systems. Those techniques play an important role in establishing trust, ensuring accountability, and safeguarding user privacy. By subjecting Service Providers (SPs) to accreditation processes, users are enabled to assess the SPs' legitimacy and trustworthiness. Moreover, accreditation constraints add a layer of protection, preventing over-asking and unnecessary data disclosure while empowering users with greater control over their personal information. The effectiveness of accreditations and constraints depends on Accreditation Bodies' rigor to check SPs and their processing needs. Striking a balance between facilitating seamless authentication experiences, enabling innovation, and upholding privacy principles remains the goal. As authentication technologies continue to evolve, ongoing efforts to refine accreditation processes and integrate constraint mechanisms will be crucial in ensuring the integrity, security, and user-centricity of authentication systems in the digital age.

References

[*] OpenAI. ChatGPT (3.5) [Large language model] was used to edit parts of the text.
[1] A. Pfitzmann, M. Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version 0.28), 2006.
[2] D. Kales, O. Omolola and S. Ramacher, Revisiting User Privacy for Certificate Transparency, IEEE EuroS&P, 2019.
[3] S. More, S. Ramacher, L. Alber and M. Herzl, Extending Expressive Access Policies with Privacy Features, IEEE TrustCom, 2022.
[4] K. Rannenberg, J. Camenisch, A. Sabouri, Attribute-based credentials for trust. 2015.
[5] Epicenter Works, Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures, 2024.
[6] Germany: eIDAS 2.0 Architecture Concept (Version 2), 2024.
[7] EUDI Wallet: Architecture and Reference Framework (Version 1.3), 2024.
[8] European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 2016.
[9] European Parliament and Council of the European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2), 2024.
[10] S. More, J. Heher, E. Fasllija, M. Mathie, Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems, ARES EDId, 2024.