CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Attribute Based Credentials for Subscription-based Services

Master's thesis in Computer science and Engineering

Souptik Paul

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2024

Master's thesis 2024

Attribute Based Credentials for Subscription-based Services

Souptik Paul

UNIVERSITY OF
GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2024

Attribute Based Credentials for Subscription-based Services
Proposed Integration of Attribute Based Credentials in Subscription-Based Services
Souptik Paul

Supervisor: Victor Morel, Data and Information technology
Examiner: Alejandro Russo, Data and Information technology

Master's Thesis 2024
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Gothenburg, Sweden 2024

Attribute Based Credentials for Subscription-based Services
Souptik Paul
Department of Computer Science and Engineering
Chalmers University of Technology

Abstract

In the digital era, where data privacy concerns are paramount, traditional authentication methods often fall short in safeguarding user information. To address this issue, this thesis examines the application of Attribute-Based Credentials (ABCs) within subscription-based services, focusing on their potential to enhance data privacy while ensuring the retention of essential service functionalities. ABCs offer a viable alternative by facilitating authentication through the verification of necessary user attributes without disclosing underlying personal information, addressing critical privacy issues inherent in digital interactions.

The research delineates the theoretical framework of ABCs and their operational capabilities, particularly their integration into existing digital infrastructures. It assesses compatibility across various operating systems and devices, crucial for widespread adoption. The trustworthiness of ABCs on smartphones is also evaluated, considering their potential to accurately represent user identities in a secure and privacy-preserving manner.

Empirical evidence from a structured proof of concept within a media streaming service context demonstrates that ABCs can maintain all the functionalities of traditional authentication systems while providing additional privacy benefits. This includes selective information disclosure, minimal data storage, and the capability to manage user attributes directly.

The findings suggest that ABCs are not only a secure and privacy-enhancing technology but also fully capable of supporting the dynamic requirements of modern digital services without compromising on functionality. This thesis contributes to digital identity management literature, proposing ABCs as a substantial enhancement over traditional methods in the context of subscription-based digital services.

Keywords: Attribute Based Credentials, Data Privacy, Subscription Based Services, Digital Identity Management, Privacy-Enhancing Technologies.

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Victor Morel, for his invaluable guidance, support, and encouragement throughout the duration of my research. His insights and expertise were instrumental in the successful completion of this thesis.

I am also deeply thankful to my friends, whose companionship and encouragement have been a constant source of motivation. Their support helped me stay focused and positive during challenging times.

Lastly, I extend my heartfelt thanks to my family for their unwavering love, patience, and understanding. Their continuous support has been my foundation and driving force throughout my academic journey.

Souptik Paul, Gothenburg, 2024-06-13

Contents

List of Figures

List of Tables

1

Introduction

In recent years, the digital realm has become essential for numerous activities, such as entertainment, socializing, banking, and shopping. Consequently, individuals frequently engage with various online service providers, necessitating authentication for access. Similar to presenting an employee ID to gain entry to an office building, users authenticate themselves using credentials like usernames and passwords to establish trust with service providers.

Authentication requirements vary depending on the context, reflecting the concept of contextual identity [1], where individuals reveal different facets of themselves based on the situation. For instance, an employer may require confirmation of an employee's status, while a video streaming service may need to verify subscriber activity, and a tax assessment service might request a social security number. It is crucial for user privacy that only the essential information relevant to the context is disclosed to service providers. This aligns with the data minimization [2] principle of the General Data Protection Regulation (GDPR), which emphasizes collecting and processing only the minimum amount of personal data necessary for a specific purpose. By adhering to this principle, organizations can reduce the risk of data breaches and ensure that individuals' privacy rights are respected. In this thesis, we propose a solution using Attribute Based Credentials(ABCs) that enables service providers to maintain all functionalities of a particular service while minimizing the amount of data collected and processed, thereby enhancing data privacy. Before delving into the proposed solution, we first examine the underlying problem.

1.1 Problem

In today's digital landscape, many service providers collect personal data during registration, such as email addresses and date of birth, and predominantly rely on username-password mechanisms for authentication. This association of personal information with user accounts allows service providers to uniquely identify users and log their activities, potentially compromising privacy.

A significant risk associated with sharing personal information with service providers is the potential for data breaches where customer information might be exposed, shared, or sold to third parties. A notable example of this occurred in 2017 during the Equifax data breach. In this incident, sensitive personal information of approximately 147 million people was compromised. The exposed data included Social Security numbers,

birth dates, addresses, and, in some cases, driver's license numbers. Additionally, for some consumers, credit card numbers and dispute documents containing personal identifying information were also jeopardized [3].

Another example more specify to subscription based services occurred in December 2020 incident involving Spotify. Spotify discovered a significant security vulnerability that exposed user registration information to some of its business partners. This vulnerability, present from April 9, 2020, to November 12, 2020, potentially revealed users' email addresses, display names, passwords, gender, and dates of birth. Although Spotify contained and remediated the breach upon discovery, the incident underscores the risks associated with personal data collection. Affected users were advised to change their passwords and monitor their accounts for suspicious activity, highlighting the potential privacy implications and the need for robust data protection measures [4].

By addressing these challenges through the implementation of Attribute-Based Credentials (ABCs), we aim to propose a solution that enhances data privacy while maintaining essential service functionalities.

1.2 Approach

The escalating concerns about security and privacy in the digital domain are driving an increased public demand for stringent data protection measures. This research investigates the utility of Privacy-Enhancing Technologies (PETs), specifically ABCs, within the framework of subscription-based services. Such services, which range from streaming platforms to software subscriptions and online publications, typically require user authentication for access. Traditional methods, however, often necessitate the collection of extensive personal information, thereby elevating privacy risks.

Attribute-Based Credentials represent a strategic solution to these challenges by allowing users to authenticate via specific, necessary attributes without disclosing additional personal details. For instance, ABCs enable the verification of attributes such as "Age $>$ 18" – certified by national agencies – without requiring the full date of birth. This method minimizes the amount of personal information service providers need to handle and store, aligning with privacy preservation goals. Furthermore, ABCs facilitate selective attribute disclosure, empowering users to control what information they share based on the context. For example, a streaming service might only request verification of age when a user accesses adult content, with no need to disclose their name.

By integrating ABCs, subscription-based services can significantly bolster privacy protections, enhance security measures, and build stronger trust with users. This approach not only adheres to stringent privacy regulations, such as the GDPR, but also preserves the comprehensive functionality of these services.

This thesis provides a thorough exploration of the ABCs framework and its implementation in a subscription-based context through a detailed proof of concept. The demonstration aims to show that services like video and music streaming can

maintain their full operational capabilities while improving the management of user privacy. By incorporating PETs such as ABCs, this study addresses critical concerns about data privacy in digital interactions, proposing a viable framework that mitigates risks associated with traditional data handling practices by service providers. Additionally, the thesis discusses an adversarial model for the PoC, identifying and addressing potential threats to this implementation.

1.3 Research Questions

This thesis explores the application of ABCs within subscription-based services, aiming to critically assess their potential in enhancing privacy and reducing the exposure of personal data. The investigation pivots around a primary research question supplemented by a series of secondary questions that delve into both the practical deployment and theoretical implications of ABCs.

Primary Research Question

- Can ABCs be effectively implemented in subscription-based services to minimize personal data exposure while maintaining service functionality?

Secondary Questions

1. Can ABCs maintain the functionalities currently provided by subscription-based services using traditional authentication methods?
2. What are the intrinsic advantages of ABCs when compared to traditional authentication methods?
3. Can ABCs reduce the exposure of personal data within subscription-based services?
4. Are ABCs compatible with different operating systems (hosting platforms) and end-user devices (Android, iOS)?
5. Are ABCs on users' smartphones reliable enough for service providers (verifiers) to trust them as accurate representations of users' true identities?

1.4 Outline

The thesis is organized into several distinct chapters: Chapter 1 sets the stage by discussing data privacy issues in digital interactions, especially within subscription-based services, and introduces ABCs as a viable alternative to traditional authentication methods. Chapter 2 provides a theoretical foundation for understanding ABCs, focusing on cryptographic primitives necessary for their implementation. Chapter 3 examines existing literature and technologies related to ABCs, comparing them with other privacy-enhancing technologies, and includes a review of Netflix's authentication mechanisms and the conceptual integration of ABCs into Netflix's architecture.

Chapter 4 details the methodology used in the thesis, including the ABCs framework, the setup of the proof of concept, and an adversarial model for evaluating the PoC. Chapter 5 discusses the implementation and results of the proof of concept within a media streaming service and evaluates its performance. Finally, Chapter 6 summarizes the findings and explores potential future research directions. Additional supporting materials and technical details are provided in the Appendices.

2

Theory

2.1 Background

This section of the thesis provides a detailed overview of data privacy and its significance in data protection. It discusses various methods for achieving data privacy, including legal frameworks like the General Data Protection Regulation (GDPR) and technological solutions such as Privacy-Enhancing Technologies (PETs), with a focus on Attribute-Based Credentials (ABCs). The section introduces the fundamental concepts and properties of ABCs, explaining their role in privacy-preserving user authentication. It also covers the IRMA project and the Privacy by Design Foundation's development of the Yivi app, which facilitates secure attribute-based authentication.

Additionally, the section delves into the cryptographic principles underlying ABCs, such as the Discrete Logarithm Problem (DLP), Zero Knowledge Proofs, Pedersen Commitments, and Camenisch-Lysyanskaya Signatures. It describes the Idemix credential issuance and verification processes, highlighting secure authentication and selective disclosure of attributes. The section also describes what subscription-based services are and the different types of subscription-based services. Finally, it explores the application of ABCs in various subscription-based services, demonstrating their potential to enhance privacy and security in these contexts.

2.1.1 Data Privacy - The Concept

Data privacy, also known as information privacy, is a critical aspect of data protection that encompasses the secure storage, access, retention, immutability, and security of sensitive data. It primarily focuses on safeguarding personal data or personally identifiable information (PII) such as names, addresses, Social Security numbers, and credit card numbers. However, data privacy extends beyond personal information to include financial data, intellectual property, and personal health information. Various vertical industry guidelines and regulatory requirements govern data privacy practices to ensure compliance with governing bodies and jurisdictions.

Ensuring data privacy involves implementing robust measures to prevent unauthorized access, theft, or loss of data. It is essential to maintain the confidentiality and security of data through sound data management practices and by preventing unauthorized alterations or theft. Data breaches, where sensitive information is exposed, can have

severe consequences for individuals leading to identity theft or privacy intrusion and for businesses resulting in the compromise of intellectual property or confidential communications.

2.1.2 Methods of achieving Data Privacy - Laws and Technology

Privacy can be ensured through a combination of legal and technological measures. Governments worldwide have acknowledged the importance of preserving individuals' privacy and safeguarding personal data in the digital era [5]. As a response, they have enacted data protection regulations on a global scale, with the General Data Protection Regulation (GDPR) [6] being a prominent example. GDPR is designed to protect the privacy rights of data subjects by stipulating that their data must be processed lawfully, fairly, and transparently. It mandates that data should only be used for its intended purpose, stored for an appropriate duration, and collected in the least intrusive manner possible. Furthermore, the GDPR imposes severe fines and penalties on entities found to be unlawfully collecting or processing personal data, with non-compliance resulting in substantial financial repercussions [7]. While these legal measures represent a significant step forward in regulating data collection and protection, they are accompanied by technological solutions that play a crucial role in ensuring privacy in the digital age.

One of the technical methods for ensuring data privacy is through the use of Privacy-Enhancing Technologies (PETs) [8]. PETs refer to a coherent system of technologies specifically engineered to safeguard privacy by minimizing or eliminating personal data or by preventing unnecessary and/or undesired processing of such data, all while maintaining the functionality of the information system. With PETs, security and privacy are not mutually exclusive but can be achieved concurrently. In this thesis, we consider Attribute-Based Credentials (ABCs) as a prime example of a privacy-enhancing technology. ABCs enable users to selectively disclose only relevant attributes, while keeping the rest of their personal information confidential, thereby preserving privacy without sacrificing the functionality of the credentialing system. By leveraging PETs like ABCs, organizations and individuals can ensure robust privacy protections without compromising the usability and effectiveness of the underlying systems. A detailed description of ABCs is provided in the upcoming sections.

2.1.3 Attribute Based Credentials (ABCs)

Attribute based credentials (ABCs)[9] are a prime example of a PETs, particularly in the realm of privacy-preserving user authentication. In the context of this thesis, ABCs are strategically employed to maintain the secrecy of identity attributes within subscription-based services. This section serves to offer an overview of ABCs, highlighting their fundamental concepts and key properties at a high level. By elucidating the underlying principles of ABCs, readers will gain a foundational understanding of how these credentials operate and their significance in safeguarding privacy within subscription-based service environments. Through this exploration,

the thesis aims to lay the groundwork for further examination and implementation of ABCs in practical settings, with a focus on enhancing privacy protections for users in subscription-based services.

User authentication can be achieved based on individual characteristics, rather than strictly relying on personal identity. These characteristics, known as personal attributes, encapsulate various pieces of information pertaining to a user, such as age, student status, or name. While some attributes directly identify a user, such as their name or bank account number, others, like age or gender, are more generalized and apply to multiple users. ABCs serve as cryptographic containers for sets of attributes. These credentials enable users to access online resources or log in to websites by selectively disclosing relevant attributes. The disclosure of attributes determines whether the user is identified or remains anonymous to the service provider conducting the authentication. For instance, a user can anonymously access an adult chatroom by disclosing only their 'age $>$ 18' attribute. However, if the user chooses to disclose their name along with the 'age $>$ 18' attribute, they will be identified by the chat service provider and other chatroom users.

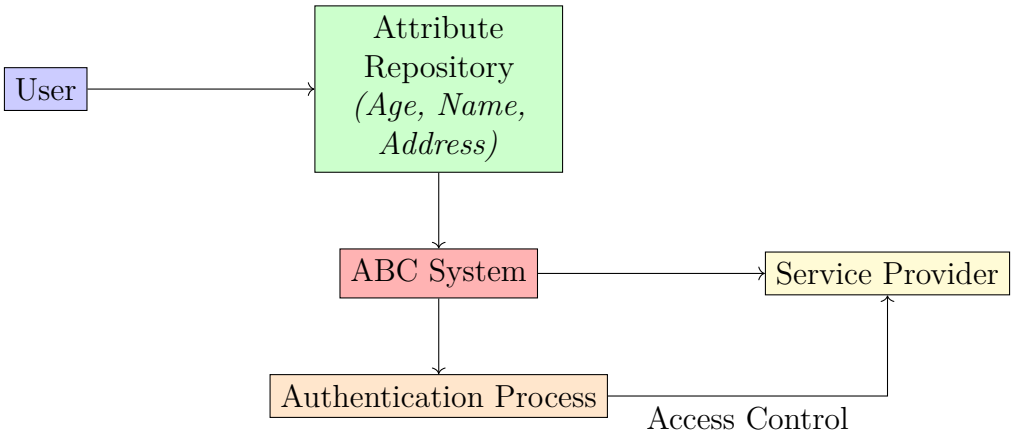

Figure 2.1: Diagram showing the relationship between User, Attribute Repository, ABC System, Service Provider, and Authentication Process.

Attribute-based credential systems are designed to instill trust, akin to conventional cryptographic certificates, while simultaneously preserving the privacy of the credential holder. Users obtain credentials from a trusted issuer, who authenticates the validity of the attributes contained within the credential for that specific user. Each credential has a defined duration, is associated with a unique cryptographic key belonging to the user, and is digitally signed by the issuing authority. During authentication at a service provider (SP), the user selectively discloses some or all attributes from the issued credential and provides proof of their authenticity. The SP then validates these attributes based on its trust in the issuer and verifies the user's proof before granting access to the requested service. A high level representation of the relation between these components can be seen in Figure 2.1 It is crucial to note that the credential issuer does not participate in the authentication session between the user and the SP, ensuring a separation of roles and maintaining privacy during the authentication process. Subsequently, we take a look at the implementation of

ABCs using the IRMA framework.

2.1.4 I Reveal My Attributes - IRMA

Cryptographic methods facilitating secure and privacy-conscious attribute-based authentication have been in existence for over a decade [9]. Despite their cryptographic soundness and privacy benefits, the widespread integration of ABCs into mainstream applications remains limited. This could be attributed to the insufficient focus on simplifying the ABC system, which comprises intricate concepts, cryptographic mechanisms, numerous protocols, and features, to make it easily understandable and usable by individuals without specialized knowledge. Additionally, there has been a lack of effort in developing ABC systems that seamlessly integrate with contemporary user workflows, often revolving around mobile devices like smartphones and tablets.

Recognizing the untapped potential of ABCs in real-world applications, the IRMA (I Reveal My Attributes) project was initiated in 2012 within the Digital Security group in Nijmegen, Netherlands. This project aimed to explore the practical feasibility of attribute-based authentication, aiming to bridge the gap between complex cryptographic concepts and user-friendly implementation.

Initially, a thorough examination was conducted on three attribute based credential systems: U-prove [10], self-blindable attributes [11], and Idemix (Identity Mixer) [12], to analyze their respective weaknesses, strengths, and potential opportunities. Among these, Idemix emerged as the most adaptable, offering advanced privacy features such as multi-show unlinkability. Figure 2.2 showcases the Idemix and U-prove, attribute based credential systems. Consequently, in this thesis, whenever we refer to ABCs, we specifically mean the Idemix Attribute-Based Credential system, as it is the one implemented in IRMA.

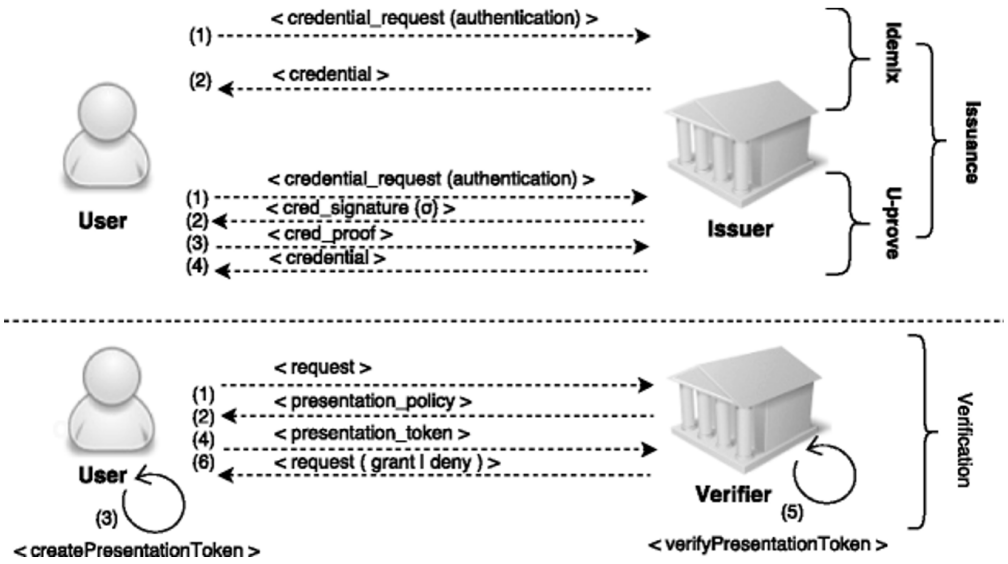

Figure 2.2: Idemix and U-prove ABC systems

2.1.5 Privacy by Design Foundation

This section discusses the Privacy by Design Foundation, which is responsible for creating and maintaining the Yivi app, a critical component in the Proof of Concept implementation. In 2016, stemming from the IRMA project, an independent non-profit venture emerged known as the Privacy by Design (PbD) Foundation. The foundation's primary mission is to develop and maintain free open-source software with a paramount focus on user privacy, with the IRMA system being its flagship project. Moreover, PbD Foundation actively engages in forging formal partnerships with various societal organizations to facilitate the advancement and widespread adoption of IRMA technology.

On the technical front, the PbD Foundation has spearheaded the creation of an open-source smartphone application known as the Yivi app (previously known as IRMA app)[13][14]. This application builds upon IRMA's smartcard-based implementation of Idemix ABCs[15], integrating an intuitive user interface. Acting as an ABC-wallet, the IRMA app enables users to collect attribute based credentials from multiple issuers and utilize them for context-based authentication. Available on both Android and iOS platforms, the IRMA app facilitates seamless access to ABCs.

The central mission of the IRMA project is to validate the practical utility and reliability of ABCs through a dual approach of academic exploration and real-world implementation. This thesis can form a crucial segment of the academic research efforts within the IRMA project, which focuses specifically on two key objectives: identifying digital domains where ABC technology can offer advantages to all stakeholders, including credential issuers, service providers, and end users, and addressing the trust and security challenges inherent in implementing ABCs on smartphone platforms while proposing technical solutions to mitigate these challenges.

2.1.6 Privacy and security assurances provided by ABCs

In the realm of attribute-based identity management, the integrity and security of ABCs are paramount. To ensure the trustworthiness of ABCs, several fundamental properties and protocols have been established. These properties and protocols serve as foundational pillars, safeguarding the authenticity, integrity, and privacy of ABC systems. Authored by Gergely Alpar [16], the following excerpt elucidates these principles succinctly.

1. **(S1) Authenticity** The content of an ABC signed by the issuer cannot be modified, and the verifier can verify the signature using this issuer's public key.
2. **(S2) Unforgeability** prevents a malicious third party from forging a valid ABC.
3. **(S3) Non-repudiation** Non-repudiation prevents the issuer from denying that the credential's signature was produced by him.
4. **(S4) Non-transferability** prevents the user from transferring her ABC to another user of the system.

5. **(P1) Offline issuer.** The issuer of a credential is not involved in the verification protocol.
6. **(P2) Issuer unlinkability** prevents an issuer from tracing his credentials. More precisely, an adversary (e.g., a colluding set of issuers and verifiers) cannot decide if an issuing protocol and a verification protocol belong to the same credential.
7. **(P3) Multi-show unlinkability.** Verifiers cannot trace the activities of a user. More precisely, seeing two verification protocols, no adversary (e.g., a colluding set of verifiers and issuers) can distinguish whether those protocols were performed using the same credential or not.
8. **(P4) Selective disclosure.** Any subset of attributes from a credential can be revealed and proven independently.
9. **(P5) Minimal information.** During verification protocols, no other information is revealed to the verifier beyond the disclosed attributes, the credential names and the corresponding issuers.

2.2 Preliminaries

This section introduces crucial cryptographic primitives and concepts foundational to the operation of ABCs, discussed in detail in Chapter 4. It covers essential topics such as the Discrete Logarithm Problem (DLP), Zero Knowledge Proofs, Pedersen Commitments, and Camenisch-Lysyanskaya Signatures, which are pivotal for implementing secure and private digital systems. While detailed for comprehensive understanding, readers familiar with cryptography may opt to skim or skip these explanations. However, those new to these concepts should consider reviewing this section thoroughly to fully grasp the mechanisms supporting ABCs' functionality and security.

2.2.1 Discrete Logarithm Problem (DLP)

The Discrete Logarithm Problem (DLP) serves as a cornerstone in modern cryptography, forming the basis of various cryptographic primitives and protocols. Informally, the DLP involves finding an exponent x in a group G given a generator g and an element $h = g^x$ in the group. This problem is defined as follows:

$$\text{Given } g \in G \text{ and } h = g^x, \text{ find } x \in \mathbb{Z}_q. \tag{2.1}$$

Here, G represents a group in which efficient group operations can be performed, and $\mathbb{Z}_q$ denotes the integers modulo q. The order of the subgroup generated by g, denoted as q, is typically a prime number.

The security of many cryptographic systems relies on the assumption that solving the DLP in a given group is computationally infeasible. If an adversary could efficiently

solve the DLP, it would compromise the security of various cryptographic protocols, including those based on public-key cryptography.

Examples of prime groups in which the DLP assumption holds include:

- Prime Order Groups:
  - Let $G = \mathbb{Z}_p^*$, where p is a prime number, and $g \in G$ generates a cyclic subgroup $\langle g \rangle$ of order q, also prime. The bit lengths of p and q are typically chosen to be sufficiently large for cryptographic security.
- Elliptic Curve Groups:
  - Groups of points with a special point addition operation defined over an elliptic curve in a finite field. The order of the cyclic subgroup generated by a point on the curve is assumed to be known.

In these examples, the parameters describing the cryptographic systems include the group G, the generator g, and the order q of the subgroup generated by g (i.e., (G, g, q)).

It is worth noting that while the DLP is hard in groups where the order of the subgroup is prime, it becomes more challenging in groups where the order is not prime and is hidden. In such cases, the difficulty of solving the DLP is further compounded by the hidden order, adding an extra layer of security to the cryptographic system. [17]

Cryptographic Rationale:

To prove the computational complexity of the DLP, consider an adversary attempting to derive x from g and h. Without knowledge of x, the adversary must exhaustively search through all possible values of x until finding the correct one. With sufficiently large groups and exponents, this exhaustive search becomes computationally infeasible, providing evidence for the security of cryptographic systems based on the DLP.

2.2.2 Zero Knowledge Proofs

In the realm of ABCs, a commonly employed cryptographic concept is the proof of knowledge. This type of proof serves the purpose of a user, or prover, convincing a verifier of a particular statement. For instance, in a challenge-response scenario, a user demonstrates knowledge of her private key by effectively responding to a challenge issued by the verifier through signing or decrypting operations.

To articulate such proofs of knowledge, we adopt the notation introduced by Camenisch and Stadler [18]. For example, the expression

$$PK(\alpha) : h \equiv g^{\alpha} \mod p \tag{2.2}$$

signifies a proof of knowledge regarding a value α, such that $h = g^{\alpha} \mod p$, effectively demonstrating knowledge of the exponent (α) in a discrete logarithm problem.

Furthermore, a zero-knowledge protocol serves as a method to convince the verifier that the user indeed possesses knowledge of a specific secret, all the while disclosing no additional information to the verifier beyond what is already known. Specifically, the term zero-knowledge denotes that any information gleaned by the verifier from the user could theoretically have been independently generated by the verifier alone, without the involvement of the user. Nevertheless, a verifier who has executed the protocol would be confidently convinced that the user does indeed possess the specified knowledge, such as the private key.

An honest-verifier zero-knowledge proof must adhere to three primary properties:

- **Completeness**: A prover who possesses knowledge of x can successfully convince the verifier. In other words, the verification equation

$$u \equiv g^r h^c \mod p \tag{2.3}$$

  holds true for such a prover.

- **Soundness**: If the prover lacks knowledge of x, then she cannot persuade the verifier. This property assures the verifier that the user indeed possesses the secret.

- **Zero-knowledge**: The verifier gains no additional information beyond the prover's knowledge of x. This is because the verifier could have independently computed such a triple (u,c,r) by selecting c and r randomly and calculating

$$u \equiv g^r h^c \mod p \tag{2.4}$$

2.2.2.1 Schnorr's Protocol

A widely recognized instance of a zero-knowledge protocol is Schnorr's protocol [19], utilized to validate knowledge of a discrete logarithm. Schnorr's protocol operates within a cyclic group G, where the public description (p, q, g) is accessible. Here, p and q denote primes, with q dividing $(p-1)$; q represents the order, and g serves as the generator of group G. The user's private key is the discrete logarithm x, and her public key is represented by

$$h = g^x \mod p \tag{2.5}$$

To prove the user's knowledge of the private key x, she initiates by committing to a random value r, conveying the commitment

$$\rho = g^r \mod p \tag{2.6}$$

to the verifier. Subsequently, the verifier generates a random challenge e and transmits it to the user, who computes the response d based on the challenge. Finally, the verifier verifies whether

$$u = g^d h^e \mod p \tag{2.7}$$

This protocol is illustrated in Figure 2.3. The tuple (u, e, t) derived from Schnorr's protocol forms a transcript corroborating the user's knowledge of the private key x.

Protocol Π_{dlog}

Common Input: the description of a prime-order group $\mathbb{G}$ of (exponentially large) order p with a generator g, and a group element h.

Prover Witness: A value $x \in \mathbb{Z}_p$ such that $g^x = h$.

Protocol:

1. $\mathcal{P}$: pick $r \xleftarrow{\$} \mathbb{Z}_p$, send $\rho \leftarrow g^r$.
2. $\mathcal{V}$: pick $e \xleftarrow{\$} \mathbb{Z}_p$, send e.
3. $\mathcal{P}$: send $d \leftarrow e \cdot x + r \bmod p$

Verification: $\mathcal{V}$ accepts iff $g^d = h^e \rho$.

Figure 2.3: Schnorr's Protocol[20]

Schnorr's zero-knowledge protocol operates effectively for groups with known order. In this context, the modular reduction (mod q) is used during the response computation to ensure the uniform distribution of the response and concealment of the private key x. However, a similar protocol can be devised for groups where the order of the subgroup is not universally known. An example is the RSA setting, where the group's order is only known by the party possessing the primes p and q. Consequently, the user cannot perform modular reduction using the group's order when computing the response. Consequently, the response no longer effectively conceals the secret x as it lacks uniform distribution. Thus, the user must select a significantly larger random value e to ensure that r is statistically close to uniform over the subgroup generated by the generator g, with the secret x statistically hidden in the response d.

2.2.2.2 Fiat-Shamir Heuristic

The Schnorr's protocol illustrated in Figure 2.1 involves active interaction between the user and the verifier. This interaction entails communication during which the response is computed based on the challenge transmitted by the verifier. However, practical implementations of zero-knowledge protocols often opt for non-interactive variants. The Fiat-Shamir heuristic [21] offers a means to transform an interactive zero-knowledge protocol into a non-interactive proof. This transformation is particularly useful for converting zero-knowledge protocols into signature schemes or reducing the communication overhead associated with interactive protocols. To render a zero-knowledge protocol non-interactive, the challenge c is computed as,

$$c = \text{Hash}(u) \tag{2.8}$$

where Hash represents a cryptographic hash function and u denotes the commitment computed by the user in the previous step. This non-interactive proof of knowledge can serve as a signature when the challenge is computed as,

$$c = \text{Hash}(\text{msg}; u) \tag{2.9}$$

where msg is the message to be signed. Both the commitment u and the response r are calculated as in the interactive Schnorr's proof. The resulting transcript (u, c, r) serves as a signature on msg. Verification involves checking whether the following equation holds:

$$c = \text{Hash}(\text{msg}; \hat{u}), \tag{2.10}$$

where $\hat{u} = g^r h^{-c}$. If the proof (c, r) is valid, this equation holds true since:

$$\hat{u} = g^r h^{-c} = g^{t+cx} h^{-c} = g^t = u \mod p. \tag{2.11}$$

This type of non-interactive zero-knowledge proof is often referred to as a signature proof of knowledge, owing to the inclusion of the message in the proof.

2.2.3 Pedersen Commitments

Pedersen commitments provide a robust mechanism for securely associating entities with values while maintaining confidentiality. These commitments are significant across a spectrum of cryptographic protocols, spanning from zero-knowledge proofs [22] to Attribute-Based Credential systems. The commitment process unfolds through two critical phases: commitment and revelation [23].

2.2.3.1 Commitment Phase

During the commitment phase, an entity selects a value a and transmits $C(a)$ to a receiver, where

$$C(a) = g^a \tag{2.12}$$

based on a Discrete Logarithm (DL) framework (G, g, q). This process ensures the concealment of a while uniquely binding the entity to the committed value.

2.2.3.2 The Pedersen Commitment Scheme

The Pedersen commitment scheme, rooted in the challenges posed by the Discrete Logarithm problem, is formulated as

$$C(a) = g^r \cdot h^a \tag{2.13}$$

Here, r is uniformly drawn from Z_q, and h serves as an auxiliary generator. This commitment effectively conceals a, making it computationally infeasible to alter a without knowledge of r. The security of Pedersen commitments lies in the difficulty of finding distinct pairs of exponents that yield identical commitments, a challenge due to the complexity of the representation assumption [24].

2.2.3.3 Cryptographic Properties

1. **Hiding Property Rationale**

   The hiding property of Pedersen commitments asserts that for any value a, the commitment

   $$C(a) = g^r \cdot h^a \tag{2.14}$$

   conceals a. This property is formally proven by demonstrating that given $C(a)$, it is computationally infeasible to determine the original value a without knowledge of r and h. This proof relies on the hardness of the Discrete Logarithm problem in the group (G, g, q) [24].

2. **Binding Property Rationale**

   The binding property of Pedersen commitments ensures that an entity cannot change the committed value without revealing the opening information. Formally, this property is proven by showing that for any two distinct pairs of exponents (a, r) and (a', r'), the commitments

   $$C(a) = g^r \cdot h^a \quad \text{and} \quad C(a') = g^{r'} \cdot h^{a'} \tag{2.15}$$

   are computationally independent [25].

2.2.3.4 Pedersen Commitments in ABCs

Pedersen commitments play a pivotal role in constructing ABCs, offering a sophisticated cryptographic solution that ensures secure entity-value associations while safeguarding against manipulation and unauthorized disclosure. In the context of ABCs, Pedersen commitments provide a robust mechanism for securely associating attributes with entities without revealing sensitive information [26], [27]. Some of the properties provided by Pedersen commitments to ABCs are mentioned below.

1. **Confidentiality**

   Pedersen commitments enable the storage of cryptographic commitments of attribute values in certificates instead of storing the values directly. This approach ensures that the certificates do not leak any information about the sensitive attributes, maintaining confidentiality.

   Cryptographic Rationale: To prove the confidentiality provided by Pedersen commitments, consider an adversary attempting to extract information about the sensitive attributes from the certificates. Given a Pedersen commitment

   $$C(a) = g^r \cdot h^a \tag{2.16}$$

   representing an attribute value a, the adversary aims to derive a from $C(a)$ without knowledge of r. However, due to the hiding property of Pedersen commitments, extracting a from $C(a)$ without knowing r is computationally infeasible. This cryptographic proof guarantees that Pedersen commitments preserve the confidentiality of attribute values in ABCs.

2. **Selective Attribute Disclosure**

   With Pedersen commitments, users can selectively choose which attributes to reveal and how to use them. This selective attribute disclosure mechanism empowers users to control the information they share, enhancing privacy and security.

   Cryptographic Rationale: In the context of selective attribute disclosure, consider a user possessing Pedersen commitments for multiple attributes. To disclose a specific attribute, the user reveals the corresponding commitment along with the blinding factor r. By providing $C(a)$ and r, the user proves knowledge of a without revealing the actual value. The security of this selective disclosure mechanism relies on the binding property of Pedersen commitments, ensuring that the user cannot change the committed attribute value without revealing r. This cryptographic proof demonstrates the security and privacy guarantees offered by Pedersen commitments in selective attribute disclosure scenarios.

3. **Provable Security**

   Pedersen commitments offer provably secure and efficient protocols for attribute-based credential systems. By leveraging the Pedersen commitment scheme, users can prove the validity of attribute values without revealing unnecessary information, ensuring the integrity and authenticity of the credentialing process.

   Cryptographic Rationale: In a provably secure attribute-based credential system utilizing Pedersen commitments, users can provide cryptographic proofs of possession and knowledge of attribute values during credential issuance and verification processes. These proofs are based on the binding property of Pedersen commitments, which ensures that users cannot alter committed attribute values without revealing the corresponding blinding factors. By presenting commitments and their associated blinding factors, users can cryptographically demonstrate ownership and knowledge of attributes without disclosing sensitive information. This cryptographic proof guarantees the security and integrity of attribute-based credential protocols employing Pedersen commitments.

4. **Enhanced Security**

   The use of Pedersen commitments in ABCs addresses the challenge of limited attribute concealment. By employing a generalized Pedersen commitment scheme, the system enhances security against brute-force extraction techniques, making it more resilient to adversarial attacks.

   Cryptographic Rationale: The enhanced security provided by Pedersen commitments against brute-force extraction techniques can be formally proven by analyzing the computational complexity of reversing the commitment scheme. In a generalized Pedersen commitment scheme, altering committed attribute values without knowledge of the blinding factors requires solving the discrete logarithm problem, which is computationally infeasible. This cryptographic proof demonstrates that the security of Pedersen commitments in ABCs remains

robust even against sophisticated adversaries attempting to extract sensitive attribute information through brute-force methods.

2.2.4 Camenisch-Lysyanskaya Signatures

ABCs serve as containers for attributes, with each attribute bearing the signature of the credential issuer. In the realm of Idemix/IRMA, the Camenisch-Lysyanskaya (CL) signature scheme is utilized to construct ABCs. Our explanation of the CL signature scheme and its accompanying notation is embedded in the specifications described within the Identity Mixer cryptographic library.

2.2.4.1 Key Usage in CL signature scheme

In the Camenisch-Lysyanskaya (CL) signature scheme, the keys are structured to operate within the quadratic residue subgroup (QR_n) of $\mathbb{Z}_n$, where the strong RSA assumption holds. The public key of the issuer comprises the RSA modulus n and several random generators from the quadratic residue group: $S, Z, \{R_i\}_{i=1}^{M}$, where M denotes the maximum number of attributes supported by this public key. The modulus n is formed by the product of two safe primes, namely p and q, such that $p_0 = (p-1)/2$ and $q_0 = (q-1)/2$ are also primes. The private key of the signer consists of p and q. The order of the QR_n group is represented by $|QR_n| = p_0 q_0$, which is exclusively known to the signer, who also acts as the issuer in the attribute-based credential (ABC) scenario.

2.2.4.2 CL Signature Generation

To sign a collection of attributes $\{a_i\}_{i \in M}$, these a_i first need to be aggregated into a single group element Q according to the following equation:

$$Q = \frac{Z}{S^v \prod_{i \in M} R_i^{a_i}} \mod n \tag{2.17}$$

where v is a random number.

The actual signature generation process is similar to the RSA signature scheme. The first step is the generation of a random prime e which is used as the ephemeral RSA public key for this signature. Next, the RSA private key $d = e^{-1} \mod (p_0 q_0)$ corresponding to the public key e is computed. Finally, an RSA signature is created over the aggregated messages as follows:

$$A = Q^d \mod n \tag{2.18}$$

As a result, the Camenisch-Lysyanskaya signature over the set of attributes $\{a_i\}_{i \in M}$ is the triplet (A, e, v).

2.2.4.3 CL Signature Verification

To verify a Camenisch-Lysyanskaya signature (A, e, v) over the set of attributes $\{a_i\}_{i \in M}$, the verifier must validate the following equation:

$$A^e = \frac{Z}{S^v \prod_{i \in M} R_i^{m_i}} \mod n \tag{2.19}$$

This verification process resembles that of verifying an RSA signature. The verification equation above can be rearranged as follows to eliminate the need for computing the inverse:

$$Z = A^e \cdot S^v \cdot \prod_{i \in M} R_i^{m_i} \mod n \tag{2.20}$$

The unforgeability of the CL signature scheme hinges on the Strong-RSA assumption, which posits that given an RSA modulus n and an element $u \in \mathbb{Z}_{\kappa}^*$, it is challenging to compute values A and $e > 1$ such that $A^e = u \mod n$.

The CL signature scheme serves as an ideal foundational component for privacy-preserving technologies like ABCs due to its inherent properties:

1. Signers possess the capability to issue signatures on committed values without possessing knowledge of the signed value itself. Essentially, these signatures fall under the category of blind signatures. This feature proves advantageous in an Attribute-Based Credential (ABC) scenario as every credential incorporates the user's secret key as an attribute that must remain concealed from the issuer (signer) during the credential issuance process.

2. Signature owners, or users possessing attributes, retain the ability to demonstrate knowledge of a signature on a committed value. In an ABC context, attribute owners can substantiate the authenticity of the issuer's signature on the credential from which attributes are disclosed to the verifier.

3. Signature owners, or any party, irrespective of being the signer or not, retain the capability to alter a CL-signature without altering the message it authenticates. The resultant randomized (modified) signature remains verifiable against the original public key of the signer. In an ABC framework, the randomizability of CL signatures enables users to maintain unlinkability based on the issuer's CL signature during successive attribute disclosures to verifiers.

2.3 ABCs scheme description

The ABCs scheme constitutes a comprehensive framework designed to enable secure authentication, authorization, and attribute verification processes across various applications. This scheme encompasses multiple protocols, each tailored to specific functionalities within the ABC ecosystem, including verification and issuance. Each of these protocols operates through defined endpoints, request formats, and response formats, facilitating seamless communication between the `irma_api_server`, requestors, and clients. Overall, the ABC scheme provides a robust framework for managing attributes securely and efficiently, contributing to enhanced authentication and authorization processes in various applications [28]. This section outlines the key protocols employed within the ABCs scheme, highlighting how they facilitate secure and privacy-preserving interactions within digital environments. It also includes an overview of the authentication flow using IRMA, which demonstrates the practical implementation of these protocols.

2.3.1 Authentication Flow Using IRMA

The authentication process using IRMA begins when a user attempts to access the web application. The application generates a QR code, which encapsulates a request for certain user attributes relevant to the service being accessed (e.g., age for age-restricted content). Users scan this QR code using the Yivi App, which then communicates with the IRMA server to retrieve the appropriate credentials. Once verified, these credentials are sent back to the web application, which then grants access based on the disclosed attributes. The authentication process can be seen below in Figure 2.4.

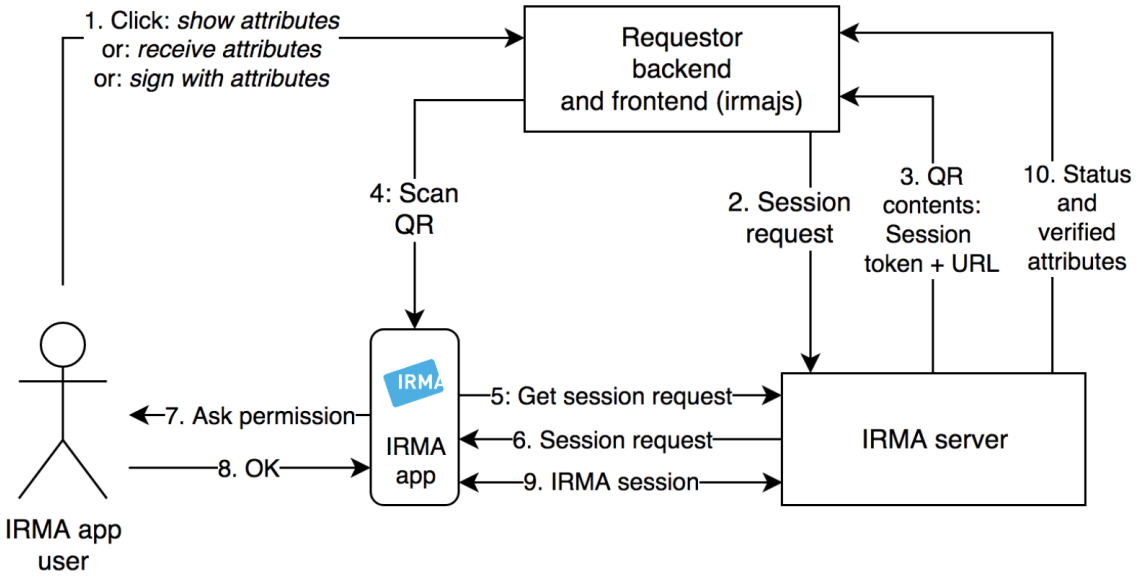

Figure 2.4: A typical IRMA session depicted schematically [13]

2.3.2 IRMA Issuance Protocol:

Request: The IRMA issuance process begins when an identity provider sends a request to the `irma_api_server`, specifying the attributes to be issued.

Response: In response, the `irma_api_server` provides a session token and necessary metadata.

Client Interaction: The identity provider then informs the client about the session token.

Attribute Issuance: Subsequently, the client connects to the `irma_api_server`, sending the session token and receiving the attributes to be issued. The client engages in the issuing protocol.

Verification: The `irma_api_server` verifies the correctness of commitments and returns signatures to the client if they are valid.

Cleanup: Finally, the session is deleted if it exists.

IRMA Issuance Protocol Request and Response Format

Request Format: Identity providers initiate issuance requests to the `irma_api_server` using a signed JWT. The payload of the JWT contains details similar to the verification protocol, along with attributes to be issued and disclosed.

Endpoints:

- `POST /api/v2/issue`: Accepts issuance requests.
- `GET /api/v2/issue/issueID`: Retrieves a nonce for a valid session token.
- `GET /api/v2/issue/issueID/jwt`: Returns the signed JWT along with context, nonce, and issuer public keys.
- `POST /api/v2/issue/issueID/commitments`: Accepts the client's commitments to secret keys and verifies them.
- `DELETE /api/v2/issue/issueID`: Deletes the session and informs the identity provider of failure.

Response Format: Upon successful issuance, the `irma_api_server` returns Camenisch-Lysyanskaya signatures for each credential, along with attributes.

2.3.3 Verification Protocol

Initiation: The verification process begins when a service provider sends a request to the `irma_api_server` in the form of a JSON web token, specifying the attributes required for verification.

Response: The `irma_api_server` responds to the request by providing a session token and necessary metadata, including supported API versions.

Client Interaction: The service provider then informs the client about the session token, initiating client interaction.

Attribute Disclosure: Subsequently, the client connects to the `irma_api_server`, sending the session token and receiving the required attributes. The client may compute a disclosure proof if possible.

Verification: The `irma_api_server` verifies the provided proof and responds to the service provider with the validity status and disclosed attributes.

Cleanup: Finally, the session is deleted if it exists, with no explicit reason provided to the service provider.

Verification Protocol Request and Response Format

Request Format: Service providers initiate verification requests to the **irma_api_server** using a signed JWT. The payload of the JWT includes essential details such as the issuer (`iss`), request type (`sub`), issue time (`iat`), data, validity duration, timeout, and the disclosure proof request.

Endpoints:

- `POST /api/v2/verification`: Accepts verification requests.
- `GET /api/v2/verification/verificationID`: Retrieves a nonce for a valid session token.
- `GET /api/v2/verification/verificationID/jwt`: Returns the signed JWT along with context and nonce.
- `POST /api/v2/verification/verificationID/proofs`: Accepts serialized ProofList object and verifies proofs.
- `DELETE /api/v2/verification/verificationID`: Deletes the session and informs the service provider of failure.

Response Format: Upon successful verification, the `irma_api_server` returns a JSON object indicating the validity of proofs along with disclosed attributes. The status field denotes the outcome of verification.

2.4 Protocols in ABC scheme

This section explains the cryptographic processes involved in the ABC scheme, including Idemix credential issuance and verification via selective disclosure. This section outlines the commitment phase and issuer's signature phase in Idemix credential issuance, providing algorithms for clarity. The subsequent discussion describes Idemix credential verification via selective disclosure, detailing the randomization of the issuer's signature and the formulation of zero-knowledge proofs. Algorithms are presented to illustrate these steps. Overall, the section provides a comprehensive understanding of the cryptographic protocols within the ABC scheme, spanning credential issuance and verification.

2.4.1 Idemix Credential Issuance

An ABC contains a set of attributes, where all the attributes are bound to a user's secret key. For instance, an ABC with four attributes, where sk denotes the user's secret key, $a_1, \ldots, a_4$ denote the attributes that hold for the user, and (A, e, v) denotes the credential issuer's signature. This signature is computed as follows:

$$A = \left(\frac{Z}{S^v R_0^{sk} R_1^{a_1} R_2^{a_2} R_3^{a_3} R_4^{a_4}} \right)^{\frac{1}{e}} \mod n \tag{2.21}$$

In this signature, the elements $(n, S, Z, R_0, R_1, R_2, R_3, R_4)$ collectively form the public key, while the factors of modulus n, denoted as p and q, constitute the private key of the issuer. During issuance, the issuer generates the credential and applies a CL (Camenisch-Lysyanskaya) signature to it. We elaborate on the credential issuance process in Idemix, which is also applicable to the IRMA system since the issuance protocol is implemented in IRMA based on Idemix's cryptographic library.

During the credential issuance process, an interactive protocol unfolds between a user and an issuer. Throughout this protocol, the issuer formulates a new credential for the user, associating it with the user's secret key sk, and performing a blind signature using its private key p, q. This protocol comprises three primary stages:

Commitment phase: Here, the user initiates a commitment U to her secret key sk, represented as:

$$U \leftarrow S^{v_0} \cdot R_0^{sk} \mod n \tag{2.22}$$

where v_0 denotes a randomly selected blinding value. Algorithm 1 in the Appendix outlines the process for creating the commitment U. Following this, the user proceeds to demonstrate to the issuer both the knowledge of sk and the accuracy of her commitment U with the proof:

$$\text{PK } \{(v, \mu) : U = S^v \cdot R_0^{\mu} \mod n\} \tag{2.23}$$

Algorithm 2 details the construction of the aforementioned proof. This proof shares similarities with a non-interactive Schnorr proof of knowledge. The proof's freshness is ensured by a nonce n_U provided by the issuer.

Subsequently, the issuer verifies the proof according to Algorithm 3. Verification succeeds if the signer can effectively reconstruct the commitment $\tilde{U}$ from U, feasible due to the equation:

$$\hat{U} \equiv S^{v_0} \cdot U^{-c} \cdot R_0^{\hat{sk}} \mod n \tag{2.24}$$

Once the proof is successfully verified, the issuer proceeds to sign. The issuer's signature phase involves the blind signing of the user's commitment U along with other attributes a_i, where M represents the maximum number of attributes in the credential. This step entails the generation of a blind Camenisch-Lysyanskaya signature, as depicted in Algorithm 4. A random prime e serves as an ephemeral public key for this signature, and its corresponding private key d is computed as $d \equiv e^{-1} \mod (p_0 \cdot q_0)$. Additionally, the issuer presents the following proof of knowledge to demonstrate that it possesses the private key d and the CL signature has been properly constructed:

$$\text{PK}\{(\delta) : A = \left(\frac{Z}{US^v \prod_{i \in M} R_i^{a_i}}\right)^{\delta} \mod n\} \tag{2.25}$$

Upon successful verification of the issuer's CL-signature, the user can proceed to finalize the credential in the subsequent step. The issuer's role in the issuance process concludes with the creation of this proof, after which it can discard the ephemeral values e and d as they were generated solely for this CL signature.

Credential completion phase: During the credential completion phase, the individual consolidates the credentials by incorporating the issuer's signature. This involves combining the blinding values of the user (v_0) and the signer (v_{00}) as:

$$v = v_0 + v_{00} \tag{2.26}$$

This resultant value v serves as the final randomization value for the Camenisch-Lysyanskaya signature (A, e, v). It's important to note that in subsequent processes, the user demonstrates knowledge of this signature without directly revealing the credential to a verifier during the verification process. The algorithms (1 to 5) for Idemix Credential Issuance can be seen in the Appendix. A diagrammatic representation of Idemix Credential Issuance can be seen in Figure 2.5.

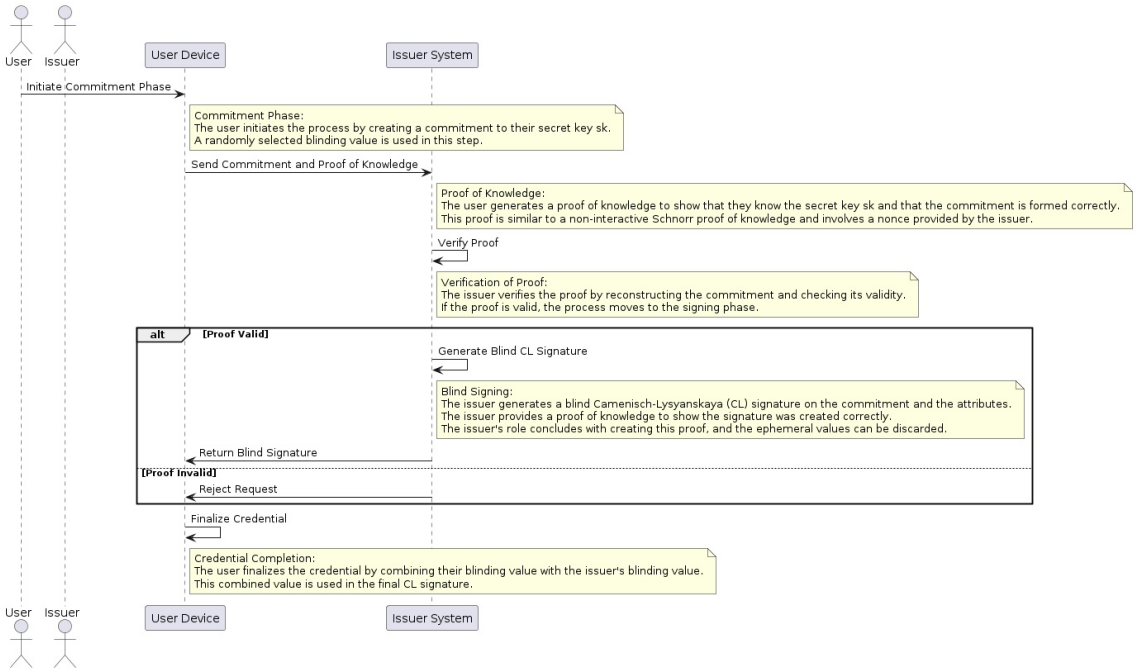

Figure 2.5: Idemix Credential Issuance

2.4.2 Idemix Credential Verification via Selective Disclosure

A user can authenticate to a verifier using her ABCs that were issued as described in the preceding section. This is cryptographically realized by a selective disclosure (SD) protocol. In an SD protocol, the user discloses a subset of attributes from her ABCs and then proves, using a zero-knowledge proof, the validity of the attributes. Let D denote the set of disclosed attributes and H denote the set of hidden attributes, which includes the secret key attribute. Therefore, H and D are disjoint sets of attributes: $H \cap D = \emptyset$, and the number of elements in the union set $H \cup D$ equals the total number of attributes inside the credential.

The SD protocol within both Idemix and IRMA involves a dual-step process. Initially, it encompasses randomizing the issuer's signature on the ABC, the source from which

attributes are disclosed to a verifier. Subsequently, it entails the formulation of a zero-knowledge proof to establish the familiarity with the issuer's signature and the concealed attributes within the ABC. These sequential operations are elucidated extensively below.

• Randomize issuer's signature. When a user discloses non-identifying attributes (e.g., age > 18) from an ABC to a verifier during authentication, the sole means for the verifier to potentially correlate subsequent authentications of the same user is through linking based on the issuer's signature on the ABC. Hence, it is imperative to randomize the CL signature of the issuer on the ABCs to avert this linkability. The CL signature scheme facilitates the user to randomize the signature while leaving the attributes within the credential unaltered. The randomization process is executed using Algorithm 5. Initially, a randomization value r is generated to perturb the signature component A. Subsequently, the value v is adjusted to maintain the validity of the signature, ensuring it continues to satisfy the equation:

$$A^{0e} \equiv (A \cdot S^r)^e \mod n \equiv A^e \cdot S^{er} \mod n$$

$$\equiv \frac{Se^r \cdot Z}{Sv \cdot \prod_{i \in M} R_i^{a_i}} \mod n$$

$$\equiv \frac{S^{-er} \cdot S^{e \cdot r} \cdot Z}{S^{-er} \cdot S^v \cdot \prod_{i \in M} R_i^{a_i}} \mod n$$

$$\equiv \frac{Z}{S^{v-er} \cdot \prod_{i \in M} R_i^{a_i}} \mod n$$

$$\equiv \frac{Z}{S^{v^0} \cdot \prod_{i \in M} R_i^{a_i}} \mod n \tag{2.27}$$

Essentially, following randomization, the issuer's signature (A, e, v) transforms into (A_0, e, v_0), where $A_0 = A \cdot Sr \mod n$ and $v_0 = v - e \cdot r$.

• Formulate a zero-knowledge proof. The randomization of the issuer's signature selectively impacts the A value, leaving e and v_0 susceptible to exposure. Therefore, it becomes imperative to obfuscate the e and v_0 values through a zero-knowledge proof when unveiling this randomized CL signature alongside the attributes $\{a_i | i \in D\}$ to the verifier. Additionally, the ensuing proof conceals the attributes $\{a_i | i \in H\}$ that the user opts not to disclose to the verifier. This proof mechanism is denoted as Selective Disclosure (SD) proof.

$$PK(e \cdot v\{\mu_i\} | i \in H) : Z = A_0^e \cdot S^v \prod_{i \in H} R_i^{\mu_i} \cdot \prod_{i \in D} R_i^{a_i} \mod n \tag{2.28}$$

Algorithm 6 in the Appendix A shows the steps involved in generating the aforementioned proof of knowledge. The SD proof is essentially a non-interactive zero-knowledge proof wherein the user hashes the randomized signature component A_0, the aggregated commitment $\tilde{Z}$, and a nonce transmitted by the verifier. This nonce

binds the SD proof to the authentication session with the verifier, thereby thwarting replay attacks. The outputs of Algorithm 6 comprise the challenge c, the randomized CL signature A_0, and the responses $\hat{e}$, $\hat{v}$, $\hat{a}_i$ for $i \in H$ computed by the user for all the hidden values. These values collectively form the transcript of an SD proof, which is then forwarded alongside the disclosed attributes $\{a_i | i \in D\}$ to the verifier for verification.

The verifier can authenticate the SD proof utilizing Algorithm 7, employing the issuer's public key $(n, S, Z, \{R_i\} | i \in M)$ and the disclosed attributes $\{a_i | i \in D\}$. Essentially, the proof substantiates the accuracy of the issuer's signature over the disclosed attributes. The verification process hinges on the reconstruction of the commitments, feasible due to the equation:

$$\hat{Z} \equiv \tilde{Z} \mod n \tag{2.29}$$

To clarify, let's explain how the equality in the equation above is maintained.

$$\hat{Z} \equiv Z^{-c} \cdot S^{\hat{v}} A_0^{\hat{e}} \cdot \prod_{i \in D} R_i^{c \cdot a_i} \prod_{i \in H} R_i^{\hat{a}_i} \mod n$$

$$\equiv Z^{-c} \cdot S^{\hat{v}+c \cdot v_0} A_0^{\hat{e}+c \cdot e} \cdot \prod_{i \in D} R_i^{c \cdot a_i} \prod_{i \in H} R_i^{\hat{a}_i + c \cdot a_i} \mod n$$

$$\equiv Z^{-c} \cdot S^{\hat{v_0}} S^{c \cdot v_0} A_0^{\hat{e}} A_0^{c \cdot e} \cdot \prod_{i \in D} R_i^{c \cdot a_i} \prod_{i \in H} R_i^{\hat{a}_i} \prod_{i \in H} R_i^{c \cdot a_i} \mod n$$

$$\equiv Z^{-c} (A_0^e \cdot S^{v_0} \cdot \prod_{i \in M} R_i^{\hat{a}_i})^c \cdot A_0^{\tilde{e}} S^{\tilde{v_0}} \prod_{i \in H} R_i^{\tilde{a}_i} \mod n$$

$$\equiv (A_0^e \cdot S^{v_0} \cdot \prod_{i \in M} R_i^{\hat{a}_i})^c \cdot (A_0^e \cdot S^{v_0} \cdot \prod_{i \in M} R_i^{\hat{a}_i})^{-c} \cdot A_0^{\tilde{e}} S^{\tilde{v_0}} \prod_{i \in H} R_i^{\tilde{a}_i} \mod n$$

$$\equiv \cdot A_0^{\tilde{e}} S^{\tilde{v_0}} \prod_{i \in H} R_i^{\tilde{a}_i} \mod n$$

$$\equiv \tilde{Z} \mod n (2.30)$$

The algorithms (5 to 7) for Idemix Credential Verification via Selective Disclosure can be seen in the Appendix A. A diagrammatic representation of Idemix Credential Verification via Selective Disclosure can be seen in Figure 2.6.

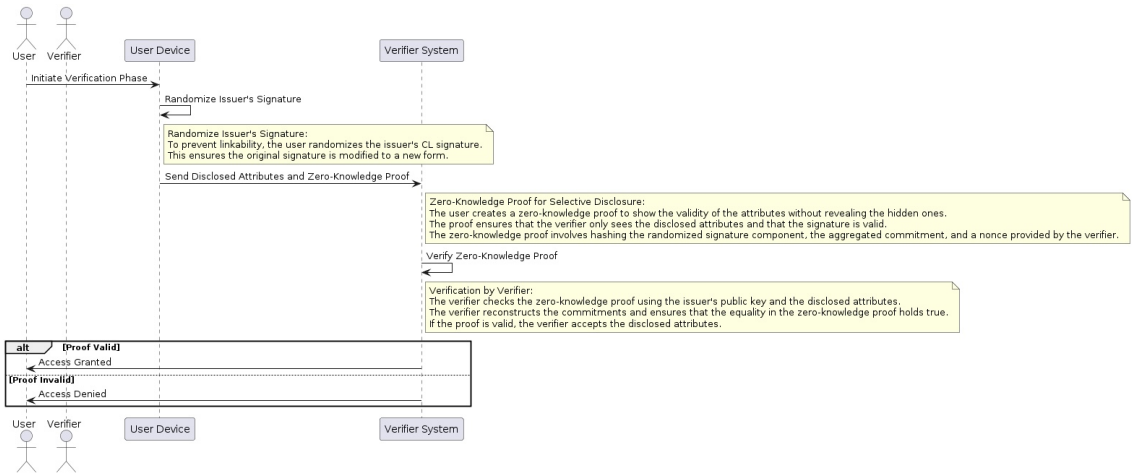

Figure 2.6: Idemix Credential Verification via Selective Disclosure

2.5 Subscription-Based Services

Subscription-based services refer to a business model where customers pay a recurring fee at regular intervals (such as monthly or annually) to access a product or service. This model has become increasingly prevalent in various industries. Subscription services offer customers ongoing access to products, content, or services, often through online platforms. These models are becoming more popular as they provide businesses with a predictable and steady revenue stream while offering consumers the convenience of regular access to products or services without the need for large upfront payments [29].

Subscription-based services encompass a wide range of functionalities designed to enhance user experience and streamline access to the services. Table 2.1 summarizes some of the functionalities provided by these services:

Table 2.1: Functionalities Provided by Subscription-Based Services

Functionality	**Description**
Video Playback	Allows users to stream videos such as movies, TV shows, and other multimedia content based on their subscription plan.
Content Filtering	Provides the ability to filter and restrict content based on user preferences, age ratings, and parental control settings.
Subscription Tier Verification	Verifies the user's subscription level to determine access to premium content and features, ensuring users receive services according to their subscription plan.
User Authentication	Authenticates users through methods such as username and password, ensuring secure access to their accounts and personalized content.
Music Playback	Allows users to stream music tracks, albums, and playlists, offering a wide range of audio content based on subscription plans.
Offline Access	Offers the ability to download content for offline viewing or listening, ensuring users can access their favorite media without an internet connection.
Ad-Free Experience	Provides an option for an ad-free experience, typically available for higher-tier subscription plans, enhancing user satisfaction.
High-Quality Streaming	Delivers high-definition video and audio streaming, including options for HD, 4K, and lossless audio, based on the user's subscription plan.
Early Access to Content	Offers early access to new releases, exclusive content, and features for premium subscribers, keeping them engaged with the latest offerings.

To facilitate user account creation, billing, and personalized service delivery, subscrip-

tion based services often require the collection and utilization of personal data. The list of some common attributes collected by subscription-based services can be seen in Table A.1 in the Appendix A. However, this practice poses significant challenges. Privacy risks emerge as sensitive data – including names and payment details – become vulnerable to breaches, leading to potential identity theft and financial fraud. Additionally, security challenges abound, as subscription services become attractive targets for hackers seeking unauthorized access [30].

2.5.1 Types of Subscription-Based Services and Scenarios for Use of ABCs

Incorporating ABCs into various subscription-based services significantly enhances user privacy and security for service platforms. By enabling selective attribute sharing and minimizing unnecessary data exposure, ABCs serve as a robust tool for managing access and personalization in a privacy-preserving manner. The scenarios outlined in Table 2.2 illustrate the versatility and effectiveness of ABCs across different subscription based services contexts, highlighting their potential to transform industry practices in line with contemporary digital security and privacy standards.

Analysis of Use Case Scenarios

Media Streaming Services: ABCs are particularly advantageous for media streaming services, where managing access to age-restricted content is crucial. By issuing credentials upon age verification, platforms can ensure compliance with age restrictions without storing sensitive information, thus enhancing user privacy. This capability makes media streaming services one of the most suitable subscription based services for utilizing ABCs.

Music Streaming Services: For platforms like Spotify, ABCs facilitate subscription tier verification, enabling seamless access control based on the user's subscription status. This ensures that only users with appropriate credentials can access premium content, thus reducing unauthorized access and ensuring real-time updates to subscription changes. As music streaming services are very similar to media stream services, it is also very suitable for utilizing ABCs.

Academic Journal Subscriptions: ABCs streamline access control for academic platforms by verifying institutional affiliations. This not only enhances security but also promotes interoperability across different platforms, making it easier for users to access resources securely.

Fitness and Wellness Apps: Apps like Peloton benefit from ABCs by verifying memberships and health attributes to offer personalized training plans. This minimizes data exposure by sharing only necessary health information, ensuring compliance with health data regulations.

Professional Software Services: SaaS platforms like Adobe Creative Cloud leverage ABCs for managing licenses and feature access. By issuing credentials corresponding to licenses and enabling feature access based on subscription levels,

Table 2.2: Use Case Scenarios for Attribute-Based Credentials in Subscription Services

Type of Subscription Service	**Scenario**	**Description**	**Technical Aspects**	**Benefits**
Media Streaming Services	Enabling Age-Restricted Access	Media platforms like Netflix use ABCs for managing access to age-restricted content.	Credential Issue: Issued upon age verification. Access Control: Checks credential for age criteria. Privacy Enhancement: Does not store age, only confirms criteria.	Enhanced user privacy and compliance with age restrictions.
Music Streaming Services	Subscription Tier Verification	Platforms like Spotify use ABCs to manage access based on subscription tiers (e.g., free, premium).	Credential Issue: Issued based on tier. Service Access: Checks for premium tier ABC. Dynamic Updating: Updates ABC on subscription changes.	Real-time access control and reduced unauthorized access.
Academic Journal Subscriptions	Access Control Based on Institutional Affiliation	Academic platforms provide access based on institutional affiliation, verified via ABCs.	Credential Issue: Issued by institutions. Access Checks: Credential verification for resource access. Interoperability: Recognized across platforms.	Streamlined access and enhanced security for academic institutions.
Fitness and Wellness Apps	Membership Verification for Personalized Plans	Apps like Peloton use ABCs to verify membership and health attributes for personalized training.	Credential Issue: Issued upon user consent. Access and Personalization: Tailors programs based on verified health attributes. Data Minimization: Shares only necessary health data.	Personalized experiences and compliance with health data regulations.
Professional Software Services	Licensing and Feature Access Control	SaaS platforms like Adobe Creative Cloud manage licenses and feature access via ABCs.	Credential Issue: Corresponds to licenses. Feature Access: Enables features per subscription level. License Management: Simplifies verification of active licenses.	Flexible license management and enhanced feature control.

these platforms can efficiently manage and verify active licenses, enhancing flexibility and control.

By integrating ABCs across these diverse subscription based services scenarios, service providers can offer tailored and secure user experiences, reinforcing the importance of privacy-preserving technologies in today's digital landscape [31].

3

Related Work and Technologies

3.1 Related Work

Several research studies have contributed significantly to the advancement and understanding of ABCs, privacy-preserving technologies, and their applications across various domains. This section delves into the intricacies of some of these research studies.

3.1.1 User-Centric Identity Management and Authentication

The research by Gergely Alpár et al. [32] explores the establishment of secure channels for ABCs, crucial for user-centric identity management systems. Their study emphasizes the role of ABCs in enabling individuals to selectively disclose attributes while maintaining privacy. They highlight vulnerabilities in current attribute-disclosure protocols, particularly regarding data exposure and authentication issues. To mitigate these risks, they propose two efficient and provably secure protocols designed for secure communication between credential holders and verifiers. However, their focus remains largely theoretical, leaving a gap in practical implementation and real-world validation.

In the studies conducted by Jan Camenisch et al. [9], privacy-preserving attribute-based authentication is further explored, focusing on anonymous credentials. Their work is part of the ABC4Trust project, which aims to simplify the adoption of privacy-preserving authentication technologies by defining unified concepts and developing a practical framework. While their research lays a strong foundation, challenges remain in simplifying the complexity of these technologies, standardizing cryptographic mechanisms, designing user-friendly interfaces, and ensuring privacy prioritization in application design. Our research builds on these concepts by creating a proof of concept for ABCs in subscription-based services, contributing to practical implementations.

The research paper by Ahmad Sabouri et al. [33] discusses the challenges of user authentication and access control in online transactions, particularly focusing on the drawbacks of current strong authentication methods like X.509 certificates, which often compromise user privacy. They advocate for Privacy-ABCs as a solution, offering strong authentication while preserving privacy. The ABC4Trust project supports this approach by providing a framework that abstracts the cryptographic

realization of Privacy-ABC modules, promoting broader adoption. However, the diversity of cryptographic schemes in existing implementations has hindered widespread adoption. Our work complements this by demonstrating the feasibility of ABCs in subscription-based services.

3.1.2 ABCs in Smart City Services and Efficiency in Revocation

In their research, J. M. de Fuentes et al. [34] propose the use of ABCs in smart city road traffic services, allowing for the selective disclosure of necessary data and enhancing privacy compared to traditional PKI systems. They evaluate three prominent ABC techniques—U-Prove, Idemix, and VANET-updated Persiano—within the context of Vehicle Ad-Hoc Networks (VANETs), identifying Idemix as the most promising approach due to its performance and compatibility with existing vehicular architectures. Their study, however, remains theoretical. Our research does not directly extend their findings but shows the practical implementation of ABCs in another domain — subscription-based services.

The research by Wouter Lueks et al. [35] addresses the efficiency and practicality of revocation schemes for ABCs, emphasizing low computational costs for both users and verifiers. Their proposed scheme is designed for devices with limited processing capabilities, such as smart cards, and ensures fast verification times. Importantly, the scheme balances anonymity concerns with practical revocation efficiency, integrating seamlessly with systems like Idemix. While we do not focus on revocation schemes, our work can benefit from these insights for future improvements in subscription-based services.

3.1.3 User Acceptance and Integration of Privacy-Enhancing Technologies

The paper by Ioannis Krontiris et al. [36] explores the socio-economic factors influencing the adoption of Privacy-Enhancing Technologies (PETs), focusing on Privacy-ABCs. Their study evaluates user acceptance factors such as perceived usefulness, trust, ease of use, and perceived risk, highlighting the importance of these factors in driving user acceptance. Although our work does not directly evaluate user acceptance, it lays the groundwork for future studies by creating a practical application of ABCs in subscription-based services.

Zinaida Benenson et al. [37] investigate the user acceptance of anonymous credentials through real-world trials, integrating the Technology Acceptance Model (TAM) with security and privacy considerations. Their research offers comprehensive insights into user acceptance factors but is limited by a small sample size. Our research does not conduct user trials but provides a proof of concept that can be used for future user acceptance studies.

The research by Bernd Zwattendorfer et al. [38] explores the integration of anonymous credentials into the Austrian electronic ID (eID) system, aiming to enhance privacy

and enable selective disclosure during authentication. Their proposed architecture utilizes systems like U-Prove and Idemix to allow citizens to authenticate specific attributes without revealing their full identity. While we do not focus on national ID systems, our work shows how similar principles can be applied to subscription-based services.

3.1.4 Comprehensive Overviews and Future Directions

The comprehensive overview provided by Jan Camenisch et al [39]. discusses Privacy-ABC technologies, their architectural framework, legal considerations, and integration with existing identity management systems. Their research offers detailed insights into the implementation and deployment of Privacy-ABC technologies, emphasizing legal implications and architectural design considerations. Our research builds on this by providing practical guidelines for implementing ABCs in subscription-based services, addressing some of the challenges identified in their comprehensive overview.

In summary, while significant progress has been made in the development and application of ABCs and privacy-preserving technologies, challenges remain in areas such as practical implementation, user acceptance, and efficient revocation. This thesis aims to address these challenges by demonstrating a proof of concept for ABCs in subscription-based services, contributing to the broader adoption and understanding of these technologies.

3.2 Related Technologies

This section explores a range of Privacy Enhancing Technologies (PETs) and Identity Management Technologies that align with or differ from ABCs in terms of security and privacy assurances. The goal is to contextualize ABCs within the broader landscape of digital security and privacy solutions, highlighting their unique advantages and potential drawbacks in comparison to other technologies.

3.2.1 Blockchain-based Identity Management

Blockchain-based identity management leverages the decentralized nature of blockchain technology to create identity systems where users have control over their attributes and credentials. By storing identity information on a distributed ledger, these systems provide strong privacy guarantees, as users can selectively disclose only the necessary attributes without revealing unnecessary personal information. One significant advantage of blockchain-based identity management is its resistance to tampering and unauthorized access, thanks to the immutable and transparent nature of blockchain records. Additionally, these systems eliminate the need for centralized authorities, reducing the risk of single points of failure and enhancing user autonomy. However, challenges such as scalability, interoperability, and regulatory compliance may hinder widespread adoption. Moreover, the complexity of blockchain technology and the potential for security vulnerabilities require careful consideration during implementation [40].

Limitations and Comparison with ABCs: Despite its advantages, blockchain-based identity management faces significant limitations. Scalability issues can arise due to the high computational requirements and storage demands of maintaining a distributed ledger. Interoperability with existing systems can be challenging, and regulatory compliance may be difficult to achieve given the nascent state of blockchain regulation and the lack of a responsible entity. Additionally, the complexity of managing blockchain networks and potential security vulnerabilities pose risks. The nascent state of blockchain regulation and the absence of a centralized governing body further complicate regulatory compliance.

ABCs, on the other hand, offer a more scalable solution as they do not rely on a continuously growing distributed ledger. By using cryptographic proofs, ABCs provide privacy without the heavy computational load of blockchain. They also integrate more seamlessly with existing identity systems and offer fine-grained access control, addressing many of the scalability and interoperability challenges faced by blockchain-based solutions.

3.2.2 Self-Sovereign Identity (SSI)

Self-sovereign identity (SSI) systems empower individuals to have full control over their digital identities and attributes, enabling them to manage and share personal information securely and selectively [41]. SSI relies on cryptographic techniques to issue and verify verifiable credentials, allowing users to assert their attributes without relying on centralized authorities. One of the key benefits of SSI is its emphasis on user privacy and autonomy, as individuals can choose which attributes to disclose and to whom. Moreover, SSI systems promote interoperability by adhering to open standards, facilitating seamless integration with existing identity infrastructure. However, challenges such as usability, scalability, and legal recognition may impede mainstream adoption. Additionally, the reliance on cryptographic keys introduces risks related to key management and recovery, necessitating robust security measures.

Limitations and Comparison with ABCs: While SSI provides significant control to users over their identities, it also introduces complexity in key management and recovery. Users must manage cryptographic keys securely, which can be a barrier to adoption due to usability concerns. Scalability remains an issue as well, especially in large systems where managing numerous credentials can become cumbersome.

ABCs mitigate these issues by providing a more user-friendly approach to key management and by utilizing attribute-based systems that simplify credential handling. The fine-grained access control and ease of integration with existing systems make ABCs a more practical solution for large-scale deployments, addressing the usability and scalability challenges faced by SSI.

3.2.3 Decentralized Identifiers (DIDs)

Decentralized identifiers (DIDs) enable self-sovereign identity by allowing individuals, organizations, or things to create and control their identifiers independently of any centralized registry. DIDs are represented as unique strings that are globally

resolvable and cryptographically verifiable, ensuring their integrity and authenticity. By associating DIDs with verifiable credentials, users can prove ownership of specific attributes without disclosing unnecessary personal information [42]. One advantage of DIDs is their decentralized nature, which eliminates reliance on centralized authorities and minimizes the risk of data breaches. Moreover, DIDs promote interoperability and portability by enabling seamless integration with various identity systems and protocols. However, challenges such as scalability, governance, and standardization may hinder widespread adoption. Additionally, the complexity of DID management and the need for robust authentication mechanisms pose implementation challenges.

Limitations and Comparison with ABCs: DIDs face several limitations, including scalability issues, governance challenges, and the need for standardization. Managing a large number of DIDs can be complex, and without a unified standard, interoperability between different systems can be difficult. Robust authentication mechanisms are required to ensure the security of DIDs, adding to their complexity.

ABCs offer a streamlined approach with built-in cryptographic proofs that simplify identity verification and attribute management. By focusing on attribute-based credentials, ABCs reduce the complexity of identity management and provide a more scalable and interoperable solution compared to DIDs. This makes ABCs a more practical choice for widespread adoption in various digital services.

3.2.4 OAuth 2.0 and OpenID Connect

OAuth 2.0 and OpenID Connect are widely used protocols for authentication and authorization on the web [43]. OAuth 2.0 enables delegated access to resources by issuing access tokens with specific scopes, allowing clients to access protected resources on behalf of the resource owner. OpenID Connect adds an identity layer on top of OAuth 2.0, enabling clients to obtain identity information about the end-user. One of the key advantages of OAuth 2.0 and OpenID Connect is their widespread adoption and support by major technology providers, ensuring interoperability and compatibility across different platforms. Additionally, these protocols provide a standardized framework for secure authentication and authorization, reducing the complexity of implementing custom solutions. However, challenges such as token management, security vulnerabilities, and consent management may arise, requiring careful consideration during implementation. Moreover, the reliance on centralized identity providers raises concerns about data privacy and control.

Limitations and Comparison with ABCs: OAuth 2.0 and OpenID Connect, while widely adopted, rely heavily on centralized identity providers, which can be a point of concern regarding data privacy and control. Security vulnerabilities in token management and consent management can also pose risks.

ABCs address these issues by offering decentralized authentication mechanisms that do not rely on centralized providers. This enhances privacy and user control over their credentials. The attribute-based approach of ABCs also provides more granular access control, reducing the risks associated with token management and improving overall security.

3.2.5 Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between identity providers and service providers [44]. SAML enables single sign-on (SSO) functionality by allowing users to authenticate once and access multiple services without re-entering credentials. SAML assertions contain attributes about the user, which can be used for access control purposes. One advantage of SAML is its widespread adoption in enterprise environments, as many identity providers and service providers support the protocol. Moreover, SAML provides a standardized framework for secure identity federation, ensuring interoperability across different systems and platforms. However, challenges such as XML complexity, protocol overhead, and limited support for modern authentication mechanisms may arise, necessitating careful consideration during implementation. Additionally, the reliance on centralized identity providers raises concerns about data privacy and control.

Limitations and Comparison with ABCs: SAML's reliance on XML introduces complexity and overhead, which can impact performance. The protocol's limited support for modern authentication mechanisms can also be a drawback, and the reliance on centralized identity providers poses privacy concerns.

ABCs, in contrast, use more efficient cryptographic methods to provide authentication and authorization. The attribute-based nature of ABCs allows for more flexible and fine-grained access control, reducing the complexity and overhead associated with XML-based protocols like SAML. This makes ABCs a more efficient and privacy-preserving solution for modern digital services.

3.2.6 Federated Identity Management

Federated identity management enables users to access multiple subscription-based services using their existing credentials from a trusted identity provider (IdP). It promotes seamless user experiences and reduces the need for users to create and manage multiple accounts across different services [45]. By using a single set of credentials, users can authenticate across multiple services, enhancing convenience and reducing password fatigue. Federated identity management systems often rely on protocols such as SAML, OAuth, and OpenID Connect to facilitate secure and seamless authentication and authorization processes across different domains.

Limitations and Comparison with ABCs: While federated identity management simplifies user experiences by allowing single sign-on (SSO) across multiple services, it relies heavily on centralized identity providers, which can be a single point of failure and a privacy concern. The centralization of identity information also raises risks related to data breaches and unauthorized access.

ABCs provide a more decentralized approach, reducing reliance on centralized identity providers and enhancing user privacy. By allowing users to manage and disclose specific attributes as needed, ABCs offer greater control and security, addressing many of the privacy and security concerns associated with federated identity management.

3.3 Currently Used Architecture

This section reviews Netflix's current authentication architecture and discusses the potential for integrating Attribute-Based Credentials (ABCs) to enhance system security and user privacy. It begins with an analysis of the existing authentication mechanisms deployed by Netflix, including the innovative use of edge authentication and the adoption of token-agnostic identity propagation. Subsequent subsections explore strategic approaches to incorporating ABCs into this architecture, aiming to leverage their benefits for improved privacy controls and security measures. This integration seeks to refine Netflix's approach to identity management, enhancing both the efficiency and effectiveness of the platform's security protocols in the context of digital content delivery.

3.3.1 Netflix Authentication Architecture - Edge Authentication and Token-Agnostic Identity Propagation

The authentication mechanisms used by Netflix have undergone a significant transformation aimed at reducing complexity, improving security, and enhancing operational efficiency [46]. Traditionally, Netflix faced challenges with managing multiple security protocols and identity tokens across a diverse ecosystem of devices and users. To address these challenges, Netflix introduced a new initiative and formed a dedicated team to centralize authentication and token management. This centralization occurs at the edge of the network, meaning that authentication processes and protocol terminations are managed by services deployed at the network's edge, closer to the user devices. This setup reduces the load on backend systems and allows for faster and more secure handling of authentication requests.

One of the key innovations in Netflix's authentication approach is the adoption of edge authentication and token-agnostic identity propagation. This approach involves moving authentication and protocol termination to the edge of the network, where a set of centralized services manages cryptographic operations and token creation. By doing so, Netflix aims to reduce complexity for service owners, improve security by delegating token management to specialized teams, and enhance auditability and forensic analysis.

The authentication flow at Netflix begins with the user entering their credentials, which are then transmitted to the edge gateway. At the edge, identity filters generate a device-bound Passport, a cryptographically-verifiable identity object, which is propagated throughout the server ecosystem. This Passport contains user and device identity information in a token-agnostic manner, allowing downstream systems to make authorization decisions based on standardized trust levels.

To support edge authentication, Netflix developed the Edge Authentication Services (EAS), a suite of services responsible for handling different types of tokens. These services run as filters in the edge gateway and are designed to be fault-tolerant, ensuring seamless authentication even in failure scenarios. Additionally, Netflix introduced Passport Actions, which are explicit signals sent by downstream services

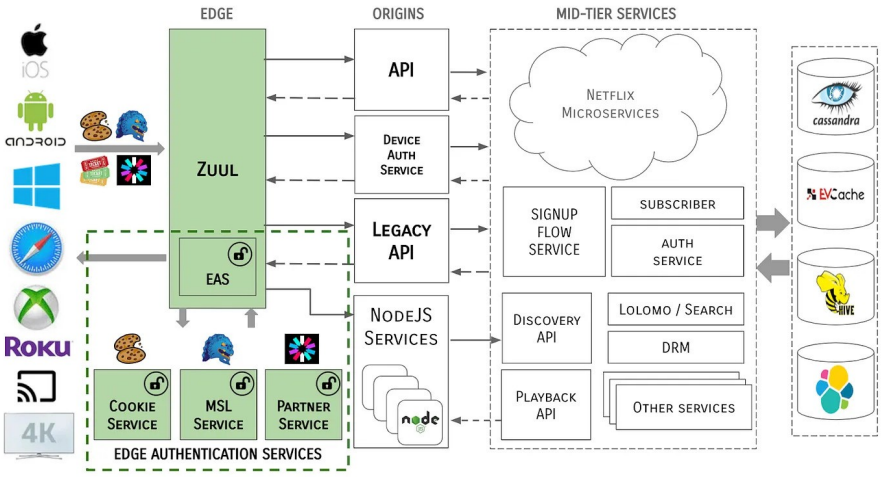

Figure 3.1: Netflix Authentication Architecture [46]

to create or update Passport tokens. A diagrammatic representation of Netflix's authentication architecture can be seen in Figure 3.1.

The Passport, Netflix's internal identity structure, plays a crucial role in authentication and authorization decisions. It contains user and device information, integrity protection via HMAC, and metadata for authorization purposes. Downstream applications use the Passport Introspector to extract and validate Passport contents, ensuring the integrity and authenticity of identity data.

By centralizing authentication and token management at the edge, Netflix has achieved several benefits, including simplified authorization processes, an explicit and extensible identity model, improved operational visibility, and reduced complexity and load on downstream systems. These benefits are evidenced by substantial performance improvements, such as reduced CPU costs, lower response times, and enhanced garbage collection efficiency, as demonstrated in various technical reports and analyses [46].

Looking ahead, Netflix is focused on further enhancing authentication mechanisms, such as introducing multi-factor authentication via a new service called "Resistor" and exploring flexible authorization strategies based on verified identity. Overall, Netflix's approach to authentication demonstrates a commitment to innovation and continuous improvement in securing its streaming platform at scale.

3.3.2 Comparing Netflix Architecture with ABCs

Authenticity (S1): Netflix's approach ensures authenticity by generating integrity-protected token-agnostic identity objects called Passports. These Passports are cryptographically signed (integrity protected by HMAC) and cannot be modified without detection. Verifiers can use HMAC to verify the integrity and authenticity of the Passport.

Unforgeability (S2): Passports are generated and managed at the edge of the network by Netflix's Edge Authentication Services. By employing cryptographic

techniques like HMAC for integrity protection, the Passports are resistant to forgery, preventing malicious third parties from creating valid Passports without proper authorization.

Non-repudiation (S3): With the use of HMAC for integrity protection, the issuer (Netflix) cannot deny that the Passport's signature was produced by them. This ensures non-repudiation, as the authenticity of the Passport can be verified using the issuer's public key.

Non-transferability (S4): Passports are bound to specific devices and users, and their integrity protection prevents unauthorized transfer. Each Passport contains device and user identity information, ensuring that it cannot be transferred to another user or device without detection.

Offline issuer (P1): The issuer (Netflix) is not directly involved in the verification protocol once the Passports are generated. Passports contain all the necessary identity information and integrity protection, allowing downstream services to verify them without needing to contact the issuer.

Issuer unlinkability (P2): Netflix's approach doesn't explicitly address issuer unlinkability as the focus is on ensuring the integrity and authenticity of Passports rather than concealing the identity of the issuer.

Multi-show unlinkability (P3): Passports are short-lived and scoped to individual requests, preventing verifiers from correlating multiple authentication events or tracking user activities across sessions. Each Passport is independent, and there is no linkage between different authentication instances.

Selective disclosure (P4): While Passports contain comprehensive user and device identity information, the Netflix system does not explicitly support selective disclosure of attributes. However, downstream systems can choose to use specific elements of the Passport as needed for authorization or other purposes.

Minimal information (P5): During verification protocols, only the disclosed attributes, credential names, and corresponding issuers are revealed to the verifier. Passports contain essential identity information required for authentication, minimizing the exposure of additional sensitive data during the verification process.

3.4 Comparison of Identity Management Technologies with ABCs

This section presents a comparative analysis of various identity management technologies based on their security and privacy features. The comparison aims to highlight the strengths and limitations of each technology in providing critical security and privacy assurances. Table 3.1 compares the Security and Privacy Features Provided by Various Identity Management Technologies. A detailed comparison can be seen in section A.3 in the Appendix A.

Table 3.1: Comparison of Security and Privacy Features Provided by Various Identity Management Technologies.

Parameters	BBIM	SSI	DIDs	OA/OIC	SAML	NA	FIM	ABCs
Authenticity (S1)	●	●	●	●	●	●	●	●
Unforgeability (S2)	●	●	●	●	●	●	●	●
Non-repudiation (S3)	●	●	●	●	●	●	●	●
Non-transferability (S4)	●	●	●	●	●	●	●	●
Offline issuer (P1)	●	●	●	●	●	●	●	●
Issuer unlinkability (P2)	●	●	●	●	○	○	●	●
Multi-show unlinkability (P3)	●	●	●	●	○	●	●	●
Selective disclosure (P4)	●	●	●	●	○	●	●	●
Minimal information (P5)	●	●	●	●	●	●	●	●

Legend: **Green** indicates full provision of the parameter, **Red** indicates partial provision, and ○ indicates no provision. BBIM - Blockchain-based Identity Management, SSI - Self-Sovereign Identity, DIDs - Decentralized Identifiers, OA/OIC - OAuth 2.0 and OpenID Connect, SAML - Security Assertion Markup Language, NA - Netflix Architecture , FIM - Federated Identity Management

4

Methods

4.1 Conceptual Integration of ABCs into Netflix's Authentication Architecture

The conceptual integration of ABCs into Netflix's existing authentication framework aims to bolster privacy, security, and user experience by leveraging and enhancing the existing robust edge-centric model facilitated by Edge Authentication Services (EAS) and Passport tokens. This proposed enhancement is designed to integrate seamlessly with the current systems, extending their capabilities to manage user identities and access controls with enhanced granularity and security. It is important to note that these modifications have not been implemented on an actual clone of Netflix, but rather represent a theoretical approach to improving their authentication processes.

4.1.1 Modifications to the Current Architecture

1. **ABCs Management Service at the Edge**
    - **Implementation**: Develop and deploy an ABCs Management Service within the existing EAS architecture. This service will handle all operations related to ABCs, including issuance, renewal, revocation, and storage.
    - **Integration with EAS**: The ABCs Management Service should be fully integrated with EAS, utilizing existing security infrastructures for secure communications and scalability.
    - **Cryptographic Operations**: Equip the service to perform necessary cryptographic operations for ABC handling, such as digital signing, verification, and encryption/decryption of ABCs for secure storage and transmission.
2. **Enhancement of the Passport System**
    - **Data Structure Extension**: Modify the data structure of Passports to include a new section for ABCs, which would carry encrypted credentials asserting user properties and permissions.
    - **Passport Issuance and Validation**: Adapt the Passport issuance process to incorporate ABC validation, ensuring Passports accurately

represent the user's current attributes and entitlements.

- **Downstream Integration**: Update downstream systems, such as content delivery networks and microservices, to parse and utilize the extended Passports, possibly requiring updates to the Passport Introspector tool and other related components.

3. **Integration with Service Access Policies**
   - **Access Control Enhancements**: Integrate ABCs into service access policies to allow for more granular and dynamic access control decisions based on the attributes contained within the ABCs.
   - **Service Adaptation**: Modify service logic to understand and enforce access decisions based on ABCs, which will involve training machine learning models or updating rulesets to interpret and act on the attribute data provided by ABCs.
4. **Operational and Performance Optimization**
   - **Load Balancing and Optimization**: Adjust load balancing strategies at the edge to account for the additional processing required for ABC handling, ensuring that performance remains optimal even with the increased computational load.
   - **Fault Tolerance and Reliability**: Implement robust fault tolerance mechanisms for the ABC Management Service to ensure that it remains operational and reliable even under failure conditions, maintaining consistent service availability.

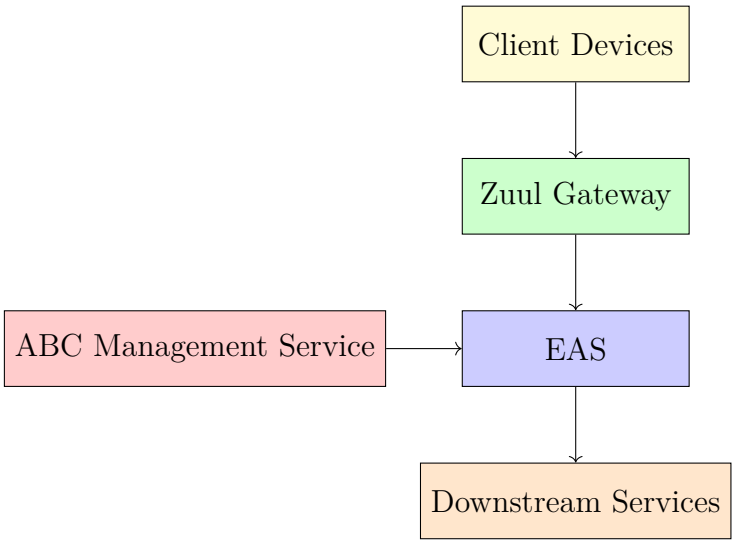

Figure 4.1: Architecture diagram showing the interaction between client devices, Zuul gateway, EAS, ABC Management Service, and downstream services.

These modifications for integrating ABCs into Netflix's authentication architecture aim to create a more secure, private, and user-centric system. By enhancing the

edge architecture to handle the complexities of ABCs, Netflix can provide a more personalized and secure streaming experience, ensuring user data is managed with the utmost integrity and confidentiality. A high level diagram showing the interaction between the different components can be seen in Figure 4.1.

4.1.2 Benefits of ABC Integration

Integrating ABCs into Netflix's architecture offers several significant benefits:

- **Enhanced Privacy**: By using ABCs, personal user information is minimized within the system, as only necessary attributes are encapsulated in the credentials and exposed to the services.
- **Improved Security**: ABCs enhance security by reducing the attack surface associated with user data. Each attribute can be independently verified without exposing other aspects of the user's identity.
- **Flexibility and Scalability**: ABCs provide a flexible and scalable approach to identity management, allowing easy updates to user permissions and attributes without major changes to the underlying authentication infrastructure.
- **Reduced Latency and Overhead**: By verifying credentials at the edge and minimizing back-and-forth communications with central servers for identity checks, system efficiency is improved, reducing latency and overhead.

4.2 ABCs in Subscription-Based Services

ABCs present a powerful framework for enhancing privacy, security, and user control in subscription-based services. By leveraging ABCs, service providers can create a more user-centric system that upholds data integrity and confidentiality. This section delves into the integration of ABCs into subscription-based services.

4.2.1 Overview of the System

The system architecture comprises four main entities: the user, the Attribute Repository (Yivi App), the ABC System (IRMA), and the Subscription-Based Service. These entities can be seen in Figure 4.2. Each entity plays a crucial role in managing, issuing, and verifying credentials while maintaining user privacy.

- **User**: The individual who seeks access to subscription-based services.
- **Attribute Repository (Yivi App)**: A repository where user attributes are stored and managed. It acts as an intermediary between the user and the ABC System.
- **ABC System (IRMA)**: The core system that issues and verifies credentials based on user attributes.
- **Subscription-Based Service**: The service provider that offers various subscription plans and features to users.

4.2.2 Interaction Flow

The interaction between these components can be understood through the sequence of actions depicted in Figure 4.2:

1. **Request Credential with Attributes**:
   - The user initiates a request for a credential by providing specific attributes to the Attribute Repository (Yivi App).
2. **Issue Credential**:
   - The Attribute Repository forwards the request to the ABC System (IRMA), which then issues a credential based on the provided attributes. This credential is digitally signed and includes a unique cryptographic key associated with the user.
3. **Request Attributes**:
   - The Subscription-Based Service requests the necessary attributes from the user to verify the credential. This request is relayed through the Yivi App.
4. **Provide Attributes**:
   - The user selectively discloses the relevant attributes from the issued credential to the Subscription-Based Service via the Yivi App.
5. **Access Subscription-Based Service with Credential**:
   - The user uses the credential to access the subscription-based service. The credential includes proof of the user's attributes.
6. **Verify Credential**:
   - The Subscription-Based Service verifies the credential by checking the validity of the attributes and the digital signature. This verification process ensures that the attributes are authentic and have been issued by a trusted issuer.
7. **Verification Result**:
   - The Subscription-Based Service sends the verification result back to the user. If the credentials are verified successfully, the user is granted access to the requested service.
8. **Provide Subscription-Based Service**:
   - Upon successful verification, the Subscription-Based Service provides the user with access to the subscribed content or features.

By integrating ABCs into their authentication architecture, subscription-based services can create a more secure, private, and user-centric experience. This approach not only enhances user satisfaction but also ensures that data is managed with the utmost integrity and confidentiality.

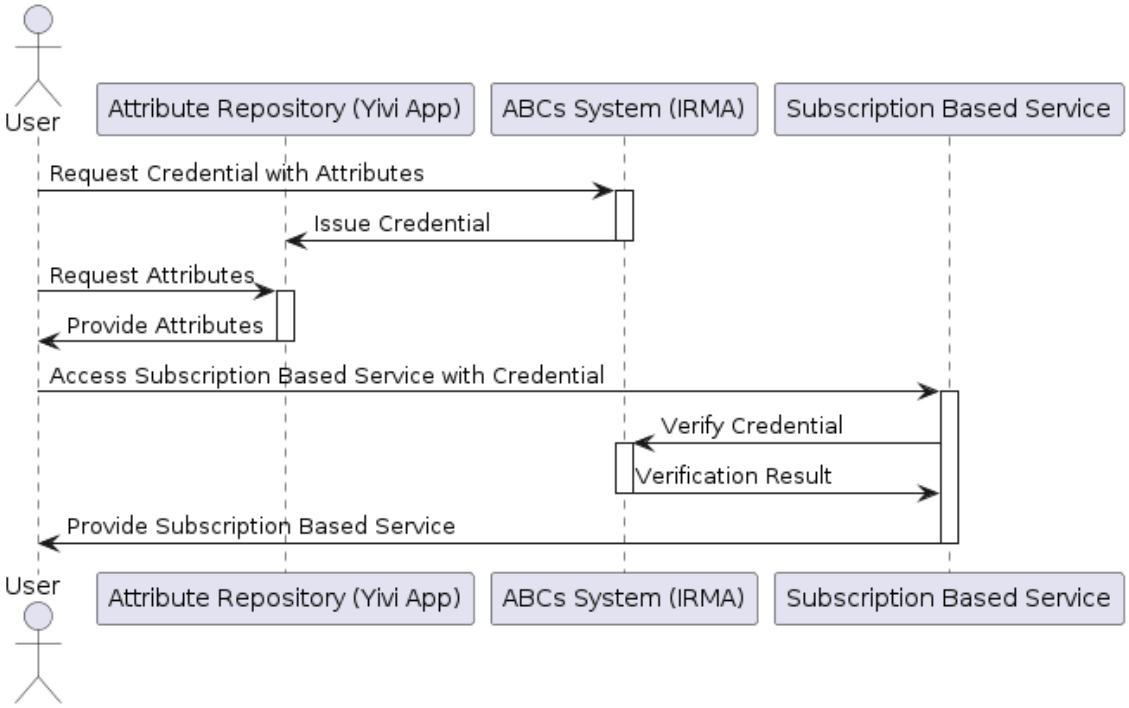

Figure 4.2: ABCs in Subscription-Based Services

4.3 Threat Model for ABCs in Subscription-Based Services

In the development of a PoC for ABCs within subscription-based media streaming services, it is crucial to establish a comprehensive threat model that outlines potential risks and adversarial actions. This model should consider the unique challenges posed by the deployment of ABCs, especially when handled by a service provider who is willing-to-minimize data retention but might inadvertently introduce vulnerabilities.

4.3.1 Assumptions

- **Application Layer Operations**: The PoC operates primarily at the application layer, where user data processing and management of ABCs occur. This includes user authentication, data transmission, and interaction with the IRMA server for credential management.
- **Service Provider's Commitment to Privacy**: The service provider aims to minimize data retention and access but may not have fully secured every aspect of data handling and API access, leaving potential vulnerabilities.
- **Secure Network Communications**: It is assumed that the underlying network infrastructure is secure and that communications between clients and servers are encrypted. However, the application layer itself might have specific vulnerabilities that need addressing.

- **Reliable Credential Issuance and Management**: Credentials are assumed to be issued securely and stored securely by clients; however, the process of credential verification and the security of the storage on client devices can be areas of concern.

4.3.2 Adversarial Model: The Willing-to-Minimize Service Provider

The adversary in this model is not traditionally malicious but is a service provider that prioritizes data minimization. This type of adversary introduces unique challenges:

- **Incomplete Security Measures**: In an effort to minimize data, the provider might implement insufficient security controls that fail to adequately protect the data that is collected and processed.
- **Inadequate Threat Monitoring**: There might be a lack of comprehensive monitoring systems to detect and respond to security breaches promptly.
- **Risks of Data Exposure in Minimized Datasets**: Even minimal datasets might include sensitive or identifiable information that could be exposed due to misconfigurations or security lapses.

4.3.3 Threat Scenarios

1. **API Vulnerabilities**
    - **Threat**: APIs serve as critical gateways between the user devices, the IRMA server, and the service backend. If APIs are not properly secured, they become susceptible to various attacks such as SQL injections, Cross-Site Scripting (XSS), or Cross-Site Request Forgery (CSRF), which could allow attackers to inject malicious requests or retrieve sensitive data.
    - **Example**: Suppose an attacker discovers an SQL injection vulnerability in an API endpoint used to fetch user attributes for content personalization. By exploiting this flaw, the attacker could inject malicious SQL queries to extract ABCs or other user details, leading to data breaches that compromise user privacy and system integrity.
2. **Credential Forgery and Replay Attacks**
    - **Threat**: If credential issuance or transmission lacks robust cryptographic validation, attackers might forge ABCs to gain unauthorized access. Similarly, insufficient protections against replay attacks can allow previously captured credentials to be reused by attackers.
    - **Example**: Consider an attacker intercepting ABCs during a transmission over an insecure channel. Without stringent timestamping or nonce incorporation in the session validation, the attacker could replay these credentials to impersonate a legitimate user, bypassing authentication controls and accessing restricted content or services.

3. **Insider Threats**
    - **Threat**: Insiders with privileged access to the system, such as administrators or developers, might misuse their access to view, alter, or leak ABCs or other sensitive data, either for personal gain or due to external coercion.
    - **Example**: An IT administrator at the streaming service, motivated by personal grievances, deliberately alters the ABCs of several high-profile users, granting unauthorized premium service access to accomplices or selling the altered credentials on dark web markets.
4. **Data Leakage through Misconfiguration**
    - **Threat**: Configuration errors in how data stores or APIs are secured can inadvertently expose sensitive data. These misconfigurations might be due to human error, complex system setups, or lack of awareness about secure configuration practices.
    - **Example**: An incorrectly configured database containing ABCs might be left accessible without proper authentication controls. An external security audit fails to catch this vulnerability, which is then exploited by attackers who gain easy access to the database and extract ABCs, leading to a massive data breach.
5. **Session Hijacking and Cookie Theft**
    - **Threat**: If session management is not handled securely, attackers can hijack user sessions through stolen cookies or session tokens, gaining the same access as the user without needing to authenticate independently.
    - **Example**: An attacker uses a network sniffer on an unsecured Wi-Fi network to capture session cookies from a user accessing the streaming service. The attacker then uses these cookies to hijack the user's session, accessing sensitive content and personal settings without needing the user's credentials.

4.4 Proof of Concept - The Idea

Now that we have a comprehensive understanding of ABCs and their foundational mechanisms, this thesis proceeds to detail the development and implementation of a PoC that integrates ABCs within a subscription-based media streaming service. The PoC is designed to explore the potential of ABCs in enhancing privacy, security, and user experience in digital subscription environments, without sacrificing functionality. Through this implementation, the thesis seeks to provide empirical evidence of how ABCs can be applied in real-world scenarios to manage user access while ensuring that personal data remains secure and private. This approach highlights the viability of ABCs in improving digital interactions within the context of subscription services, offering a practical demonstration of their benefits in maintaining operational effectiveness alongside robust privacy and security measures.

4.4.1 Objective of the Proof of Concept

The primary objective of this PoC is to demonstrate the viability of using ABCs for authenticating and authorizing users within a subscription service. By implementing the PoC, we aim to provide a test-bed to evaluate and answer the research questions posed. This includes validating the system's ability to streamline user access control, safeguard sensitive user information, and maintain full service functionality. This approach supports data minimization and privacy-preserving practices, showcasing how enhanced security measures can coexist with a robust user experience in digital platforms

4.4.2 Components of the Proof of Concept

IRMA Server: We will use the IRMA server as a robust infrastructure for managing ABCs. IRMA (I Reveal My Attributes) is known for its strong privacy features, providing a secure method for users to prove certain attributes without revealing additional unnecessary personal information.

Web Application: The web application will simulate a typical media streaming service with functionalities akin to popular platforms like Netflix or Hulu. It will feature video playback capabilities and different subscription tiers (free and premium). This application will serve as the user-facing component where the ABCs authentication processes are visible and interactable.

Yivi App: This mobile application will be used to interact with the IRMA server. The Yivi App will facilitate the scanning of QR codes generated by the web application to authenticate users by securely disclosing their attributes, such as age, name, and membership details.

4.4.3 Significance and Expected Outcomes

Implementing this PoC is expected to yield significant insights into the practicality of ABCs in real-world applications. We anticipate that ABCs will reduce the need for traditional authentication methods, which often compromise privacy and user control over personal data. This implementation can also serve as a benchmark for evaluating the scalability of ABCs in larger, more complex systems beyond the media streaming model.

5

Implementation and Results

5.1 Attribute Based Credentials for Subscription-based Services - Proof of Concept

This section of the thesis describes the development and implementation of a PoC to illustrate the practical application of ABCs in a subscription-based media streaming service. The PoC demonstrates how ABCs can significantly enhance privacy, security, and user experience by managing access and content personalization dynamically. Below, we delve into each component's setup, functionality, and the technical interactions that underpin this model. The code for the implementation can be found in the GitHub repository [47].

5.1.1 Landing Page Implementation

The PoC begins with the `Landing_Page.html`, which serves as the entry point to the video streaming service. This page is designed to be intuitive and user-friendly, providing two main functionalities:

- **Sign In Button**: Redirects existing users to `index.html`, where a QR code for attribute disclosure is displayed. This QR code is crucial for the authentication process, allowing users to authenticate by scanning the code with the Yivi app. Figure 5.1 showcases the authentication page in the PoC.

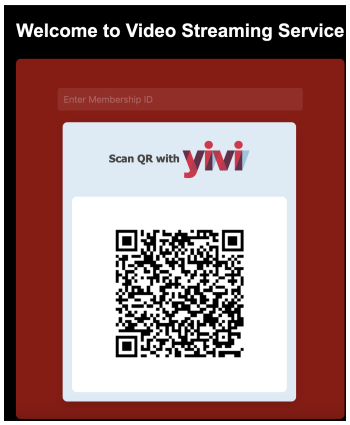

Figure 5.1: Authentication Page

- **Sign Up Button**: Leads new users to `Sign_up_Page.html` for account creation. This step is essential for first-time users to generate and store their ABCs credentials. Figure 5.2 showcases the sign up page in the PoC.

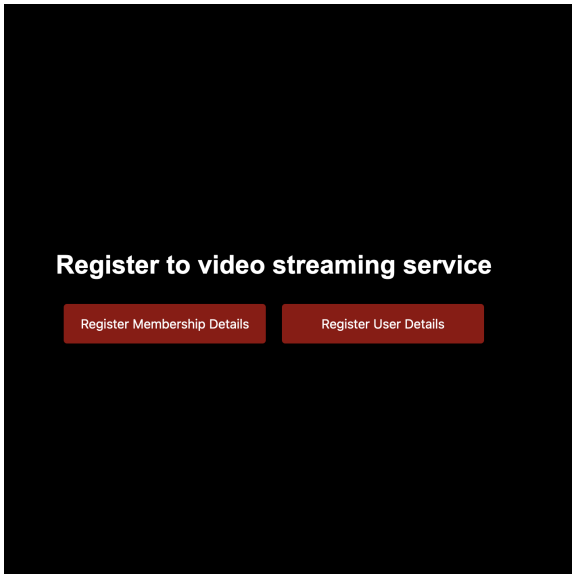

Figure 5.2: Sign up Page

The landing page features a straightforward layout, employing a dark theme and contrasting red buttons that guide users smoothly to the next steps. Figure 5.3 showcases the landing page of the PoC.

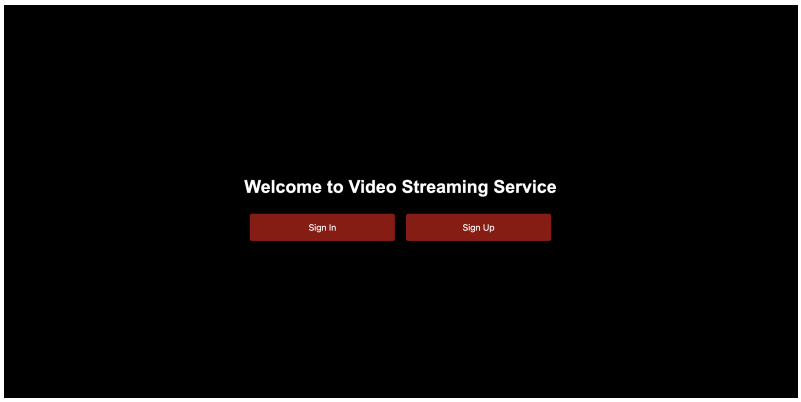

Figure 5.3: Landing Page

5.1.2 Registration and Credential Issuance Process

The sign-up process facilitated through the `Sign_up_Page.html` involves two critical steps for credential creation:

- **Register Membership Details**: Users are directed to an external IRMA demo page where they can register their membership type (free or premium), membership ID, and optionally their full name. Upon completion, a QR code is displayed on the IRMA site, which users scan using their Yivi app to securely

issue and store these details (credentials) on their device, after a code-based authentication process (users have to enter a code in the Yivi app, which is displayed on the webpage). Figure 5.4 showcases the membership details registration page in the PoC.

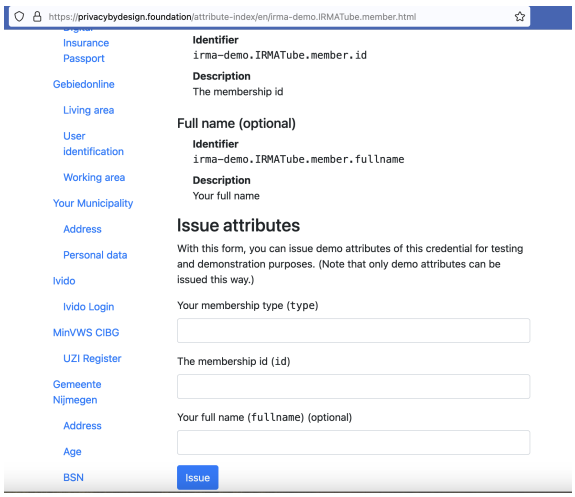

Figure 5.4: Membership Details Registration Page

- **Register Personal Details**: This button links users to a second IRMA demo page to register personal attributes such as name, age (over 12 or 18), and address. Like the membership details, these attributes are also stored in the Yivi app upon scanning the QR code generated post-entry. Figure 5.5 showcases the user details registration page in the PoC.

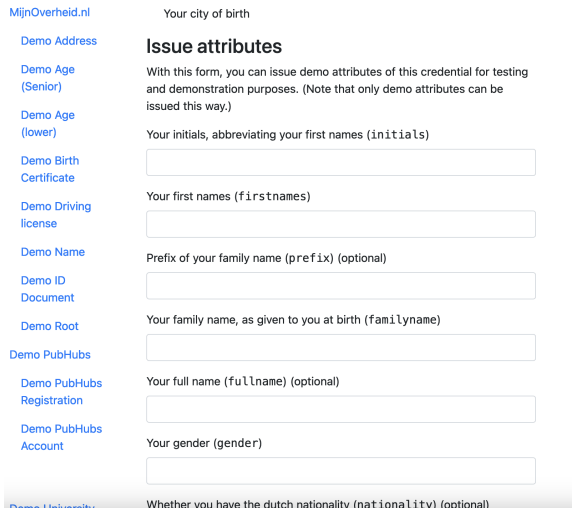

Figure 5.5: User Details Registration Page

Note: In this PoC, users manually enter their details as part of the demonstration. In a production environment, these details would typically be issued as credentials from centralized repositories such as subscription service databases or government repositories like Rijksoverheid (Dutch Population Register) and then stored in the Yivi App. This simulation aims to reflect how the process would operate in a fully

deployed scenario, emphasizing the user's control over their data and the enhanced security provided by ABCs.

5.1.3 User Authentication

After registration, the `index.html` facilitates user authentication via a QR code display:

- **Authentication Sequence**: Users must input their membership ID before scanning the QR code. The attributes disclosed after scanning—such as age, first name, membership type, and ID—must correspond to the membership ID entered to ensure legitimate access. Figures 5.10 and 5.11 showcase this authentication method.
- **Security Measures**: This procedure underscores the robustness of the authentication process, ensuring users cannot access content using another individual's credentials, thereby enhancing security.

This part of the PoC leverages JavaScript for client-side interactions and connects to an IRMA server backend to handle the secure disclosure and verification of attributes.

5.1.4 The Role of the IRMA Server

The IRMA server plays a central role in the PoC, facilitating the secure management and verification of ABCs. It is integrated within the service's infrastructure to:

- **Issue ABCs**: During the registration process, the IRMA server generates the QR codes containing credential requests. Users scan these to obtain their digital credentials that are securely stored within the Yivi app. **Note:** This process is not showcased in the PoC as credential requests can only be sent to authorized government repositories, as we use demo credentials, we register users and issue the credentials, using the process as mentioned in section 5.1.2.
- **Verify Credentials**: During user authentication on the `index.html`, the IRMA server processes the QR code scans to verify that the disclosed attributes match the credentials stored on the user's device. This verification ensures that each login is secure and that users are only able to access content corresponding to their attributes.

The use of the IRMA server underscores the PoC's commitment to privacy and security, ensuring that no personal information is unnecessarily exposed during transactions and that all attribute exchanges are encrypted and authenticated.

5.1.5 Content Filtering and Personalization

Authenticated users proceed to `VideoPlayer.html`, where the service tailors video content based on the disclosed ABCs:

- **Content Filtering**: Depending on the user's age and membership status, the page adjusts the available video content. Adult content is limited to users

verified as over 18, and additional premium content is accessible only to paying members. Figures 5.8, 5.9, 5.6, and 5.7 showcases together showcases this functionality.

- **Dynamic Content Display**: The script on this page dynamically updates the video offerings based on user attributes, demonstrating the capability of ABCs to personalize content delivery effectively.

The page also includes a "Subscribe" button for non-members, which links to the IRMA site for membership upgrades, mimicking real-world functionality where users can enhance their viewing experience by transitioning to a higher service tier. These features are showcased in detail in the subsequent sections.

5.1.6 Assumptions for the PoC

To effectively evaluate and understand the PoC described in this thesis, several critical assumptions have been made. These assumptions are foundational for the implementation and testing phases of the PoC, and they help define the expected operational scope and limitations of the system using ABCs within a media streaming service context.

1. **Credential Issuance and Management**: It is assumed that the IRMA server, used for the demonstration, correctly and securely manages the issuance and storage of ABCs. In a real-world deployment, credentials would be automatically issued from centralized databases, such as those maintained by subscription services or governmental bodies (e.g., Rijksoverheid DigiD Proef or Skatteverket). For the PoC, users manually enter their details, which would not typically be required in a fully operational system.

2. **Secure Authentication Process**: The authentication process assumes that the scanning and verification of QR codes through the Yivi app and IRMA server are secure and error-free. This includes the correct matching of user-entered membership IDs with those stored within the disclosed credentials to ensure legitimate access to the service.

3. **Infrastructure and Integration**: The assumption is made that the existing IT infrastructure and the components integrated into the PoC (like web servers, IRMA server, and client devices running the Yivi app) are robust, secure, and capable of handling the operations described without performance degradation or security vulnerabilities.

4. **User Compliance and Interaction**: It is assumed that users follow the prescribed steps for registration and authentication without attempting to bypass or compromise the established procedures. User interaction with the system is presumed to be in good faith, adhering to the operational guidelines set out in the PoC.

5. **Network and Data Security**: The network infrastructure is assumed to be secure, with all data transmissions between components (e.g., between the IRMA server and clients' devices) being encrypted and protected against

eavesdropping or tampering. For the PoC, it is assumed that the IRMA server and the mobile clients need to be connected to the same network to ensure seamless communication and credential verification.

These assumptions set the framework within which the PoC operates, guiding the expected behaviors and outcomes. Identifying and addressing these assumptions in future development phases will be crucial for enhancing the robustness and scalability of ABCs in subscription-based services.

5.2 Results

This section of the thesis presents the findings derived from the PoC and the analytical exploration of the research questions posed. Through a series of tables and discussions, we showcase how ABCs can be effectively implemented within subscription-based services. Each secondary question is addressed comprehensively, with corresponding evidence from the PoC that supports the feasibility of ABCs in maintaining service functionality, enhancing security, and improving user privacy while minimizing the exposure of personal data. This structured examination provides a clear view of the capabilities and advantages of ABCs

5.2.1 Secondary Research Question 1

Can ABCs maintain the functionalities currently provided by subscription-based services using traditional authentication methods?

The PoC successfully demonstrates that ABCs can maintain the functionalities currently provided by subscription-based services using traditional authentication methods.

Video Playback

Traditional methods support video playback through user credentials and account status checks. In comparison, ABCs verify attributes such as age and membership status to control video playback. The PoC shows that video playback can be managed effectively using ABCs, as demonstrated in the implementation where playback is controlled based on age and membership attributes verified by ABCs in the `VideoPlayer.html` file. Figures 5.8, 5.9, 5.6, and 5.7 demonstrate the effective implementation of video playback through the use of ABCs. These figures illustrate that video playback is controlled by verified attributes, ensuring that appropriate content is shown based on user credentials.

Content Filtering

Content filtering traditionally relies on account settings and user information stored in a database. With ABCs, content is dynamically filtered based on disclosed attributes like age. The PoC implements dynamic content filtering, where content (e.g., adult or non-adult) is shown based on the age attribute verified by ABCs, ensuring that only appropriate content is accessible to users.

Figures 5.6 and 5.7 showcase that content is filtered based on the age attribute: for users under 18, a different category and fewer videos are shown, whereas users over 18 see more videos of a different category. Figures 5.8, 5.9, 5.6, and 5.7 together demonstrate that attributes can be logically combined to display appropriate content.

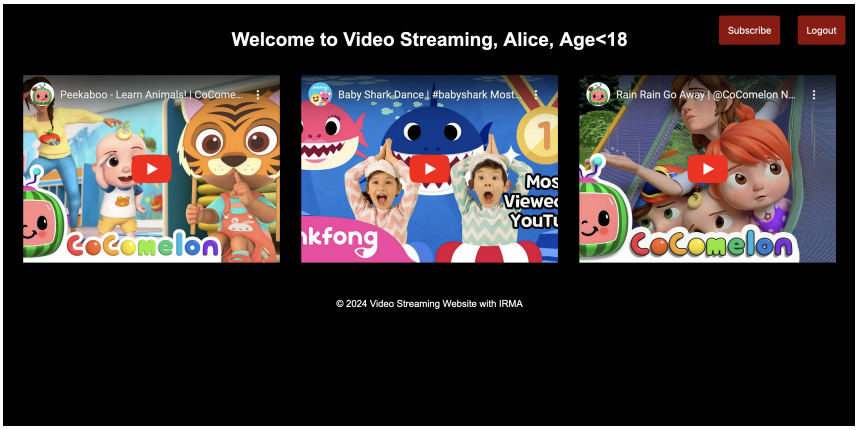

Figure 5.6: Content Filtering for Age<18

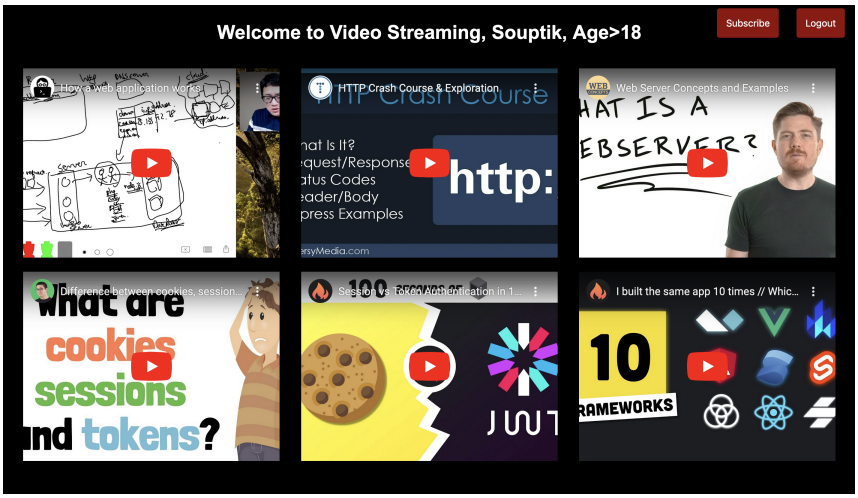

Figure 5.7: Content Filtering for Age>18

Subscription Tier Verification

Verification of subscription tiers using traditional methods involves checking against a database to determine the user's subscription level. ABCs offer an alternative by verifying the subscription level through disclosed membership attributes. The PoC demonstrates this capability by using ABCs to verify different video access levels based on the membership type stored in ABCs and verified through a QR code system.

Figures 5.8 and 5.9 illustrate the video playback functionality for different membership types. For non-premium members, the platform offers access to 4 videos, ensuring a basic level of service. In contrast, premium members enjoy enhanced access with 6 available videos, demonstrating the added value provided by the premium subscription. This differentiation highlights how the service tailors content

availability based on membership status, ensuring an optimal user experience for all members.

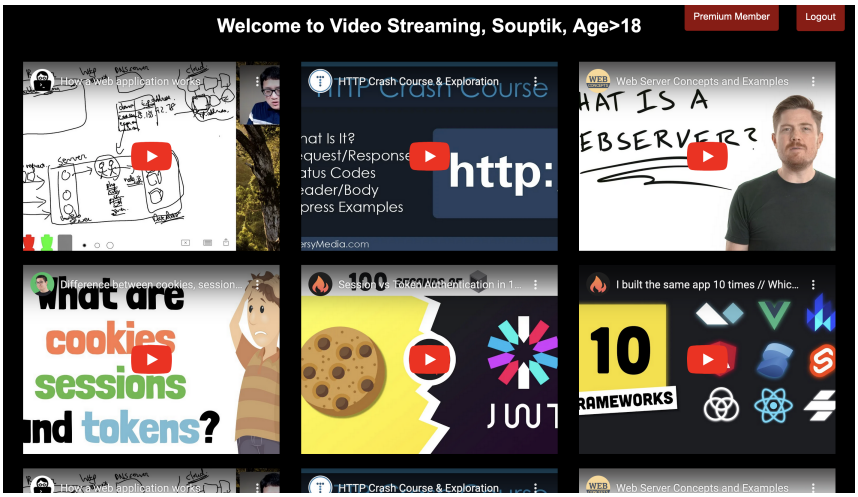

Figure 5.8: Video Playback for a premium member

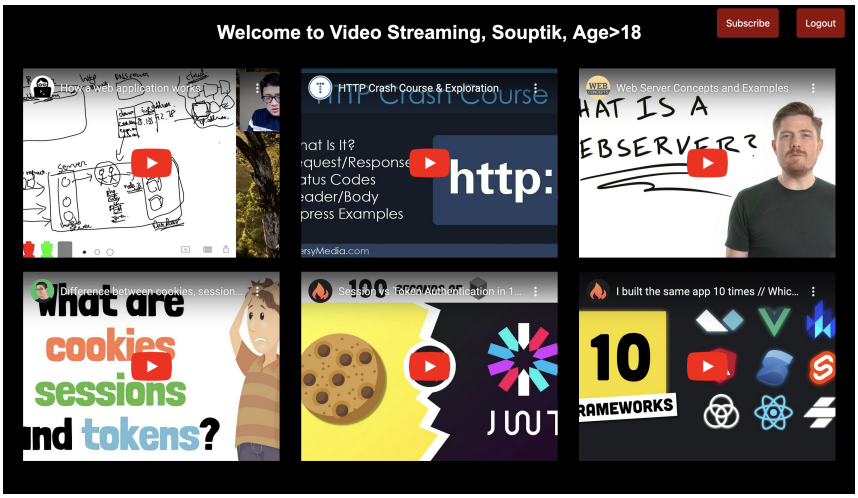

Figure 5.9: Video Playback for a non-premium member

User Authentication

Traditional user authentication typically involves username and password verification. However, ABCs use a QR code to authenticate users based on their credentials without revealing excessive personal information. The PoC successfully implemented this method, where authentication is carried out via a QR code that checks ABCs for matching membership IDs and relevant attributes, as handled in the `index.html` file. Figures 5.10 and 5.11 showcase this authentication method: users are only allowed access if the entered membership ID matches the one in the Yivi app; otherwise, they are denied login. This secure authentication method benefits from the Yivi app's password protection, ensuring that users must both know and be able to disclose their attributes to gain access.

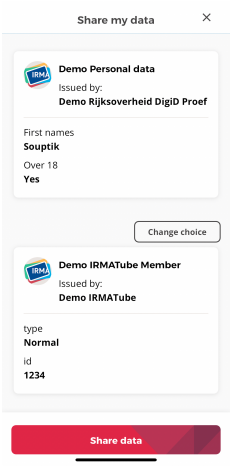

Figure 5.10: Attributes being disclosed

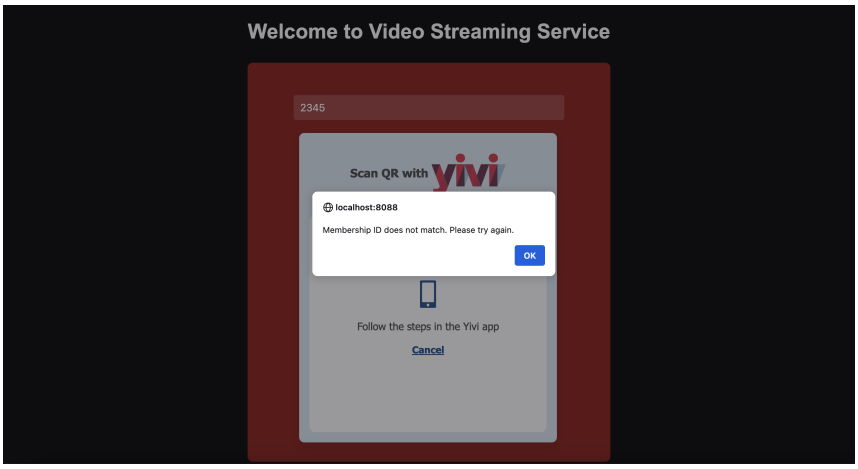

Figure 5.11: Authentication failed due to incorrect Membership ID

In conclusion, the PoC provides strong evidence that ABCs can be effectively integrated into subscription-based services. They not only match but, in some cases, exceed the functionalities provided by traditional methods, offering enhanced security and privacy while maintaining full service functionality. This supports the assertion that ABCs can serve as a viable alternative to traditional authentication mechanisms in these services.

5.2.2 Secondary Research Question 2

What are the intrinsic advantages of ABCs when compared to traditional authentication methods?

ABCs offer several intrinsic advantages over traditional authentication methods, simplifying the authentication process and enhancing user control over personal data. These advantages have been covered from a theoretical standpoint in Table 3.1. Hence, in this section, we cover the advantages from the perspective of the PoC. These advantages are demonstrated through various points, as highlighted below:

User Control Over Attributes: Traditional authentication methods provide users with limited control over how and when their data is used, often allowing service providers full access to user information. In contrast, ABCs empower users with direct control over the disclosure of their attributes during each session. The PoC demonstrates this capability by allowing users to decide what information to share via a QR code, thereby enhancing privacy and user autonomy. Figure 5.12 showcases that users can choose whether they wish to log in as a Normal or Premium user if they are subscribed. While not a typical feature in subscription-based services—since subscribed users would normally always log in as such—this demonstrates the control users have over their attributes.

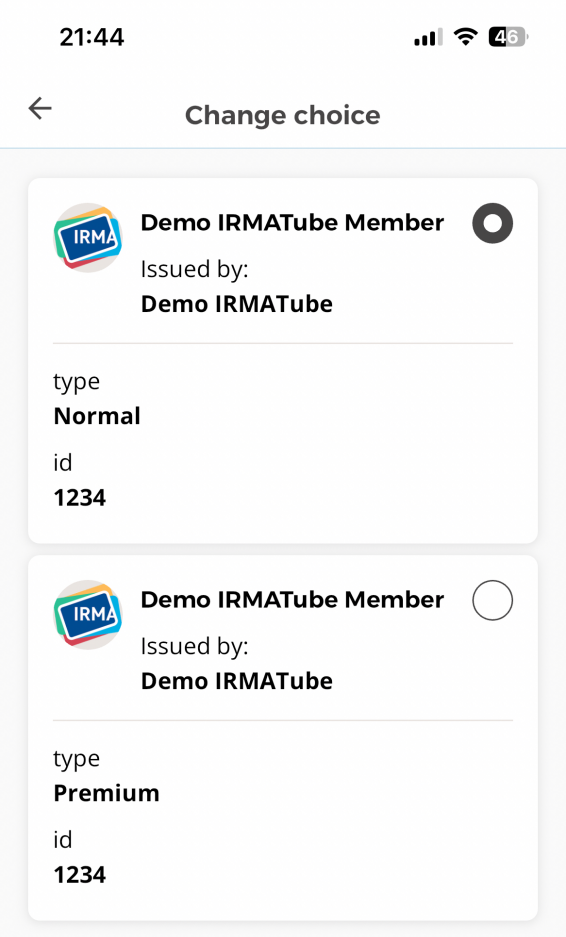

Figure 5.12: User can decide which type of membership to login with.

Single Storage Location for All Attributes: Traditional methods typically scatter user attributes across various databases, increasing the risk of data breaches. ABCs, however, securely store all user attributes in a single location, such as a personal digital wallet or app (e.g., Yivi App in the PoC). This centralized storage reduces exposure and mitigates the risk of data breaches. Figure 5.13 showcases the Yivi app storing different attributes such as personal data from Rijksoverheid (Dutch Population Register), membership attributes, and university student attributes in a single location.

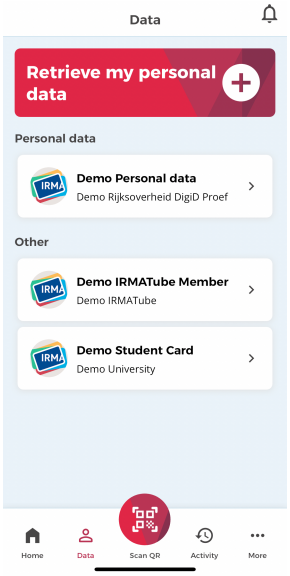

Figure 5.13: Yivi app storing different types of attributes

Selective Disclosure: In traditional authentication, users often have to share more information than necessary. ABCs enable selective disclosure, allowing users to disclose only the attributes required for a particular service or transaction. The PoC illustrates this advantage: when the video streaming service requests proof that the user is over 18 to access adult content, the user uses the Yivi app to select the relevant credential containing their age attribute. Instead of sharing the full date of birth, the system verifies that the age attribute meets the requirement. The video streaming service receives confirmation that the user is over 18 without seeing the exact birthdate or other personal details, granting the user access to the adult content. This demonstrates how ABCs can enhance privacy by disclosing only necessary information. This functionality can be seen in Figures 5.10 and 5.7.

Attributes Verified by Government Agencies: Verification in traditional methods usually requires additional steps for users to prove the authenticity of their information. ABCs simplify this process by using attributes that are pre-verified by trusted entities like government agencies. In the PoC, credentials such as age and membership details, which would be verified by external agencies in a production environment, provide higher assurance of validity. This is illustrated in Figure 5.13, where demo credentials from Rijksoverheid (Dutch Population Register) are used. In a production environment, the data will be fetched from the actual Dutch Population Register, as shown in Figure 5.14.

Reduced Need for Multiple Passwords: Traditional methods require users to remember multiple passwords for different services, increasing cognitive load and security risks. ABCs reduce or eliminate the need for multiple passwords by using digital credentials for authentication. The PoC demonstrates this advantage by employing a single QR scan for authentication and access, streamlining the user experience and enhancing security. This improvement is evident in Figures 5.10 and 5.11, where a QR scan efficiently authenticates users and grants access, highlighting

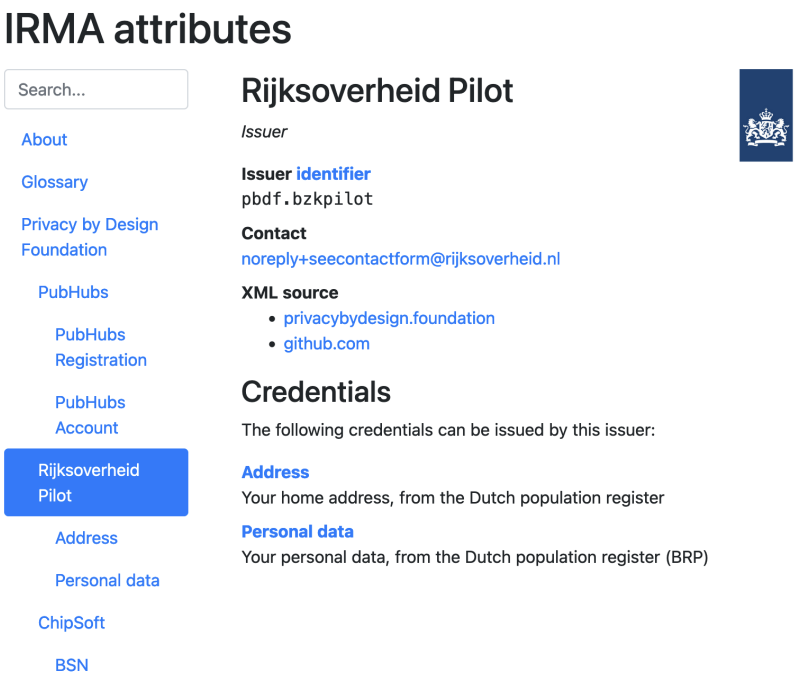

Figure 5.14: IRMA has the capability to fetch data from Rijksoverheid(Dutch Population Register)

the effectiveness of ABCs in simplifying and securing the authentication process. The only password required is for protecting access to the Yivi app, as seen in Figure 5.15.

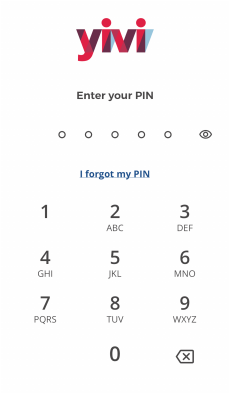

Figure 5.15: Yivi App is Password Protected

5.2.3 Secondary Research Questions 3

Can ABCs reduce the exposure of personal data within subscription-based services?

ABCs are highly effective in minimizing personal data exposure within subscription-based services, aligning with privacy-preserving principles in academic and practical contexts. By leveraging ABCs, services can ensure that only essential information is

disclosed during authentication and authorization processes, significantly reducing the risk of unnecessary data exposure.

Indirect Information Disclosure: This is the same as Selective Disclosure, renamed for better answering the research question. Instead of directly revealing sensitive information such as the exact date of birth, ABCs allow users to disclose generalized attributes like age > 18. This mechanism is demonstrated in the PoC, where the IRMA server verifies that a user is over 18 without exposing their birth date, thereby enhancing privacy. This can be seen in Figures 5.10 and 5.11.

Selective Information Sharing: ABCs allow users to control which attributes they want to share, enabled by storing multiple instances of certain attributes in the Yivi app. Users can choose which attributes to disclose as needed. Figure 5.10 demonstrates this feature, while Figures 5.16 and 5.17 showcase different credentials from the demo and production perspectives respectively, for which multiple instances can be stored.

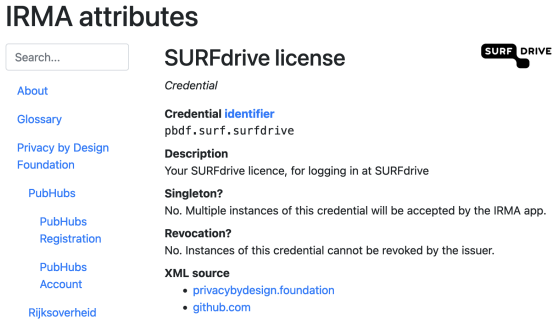

Figure 5.16: Example of Attribute in the production environment that allow multiple instances to be stored.

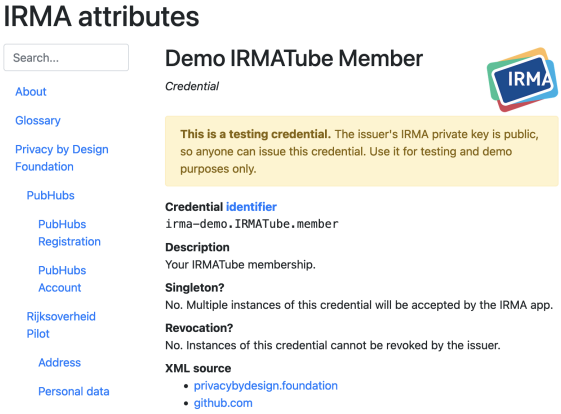

Figure 5.17: Example of Attribute in the demo environment that allow multiple instances to be stored.

Reducing the Need for Storing Information: By utilizing on-the-fly processing, ABCs eliminate the necessity for persistent storage of personal data. This approach not only complies with privacy regulations but also reduces the risk of data breaches.

The PoC illustrates this through functionalities like content filtering and displaying user attributes such as name (as seen in Figure 5.8) without storing personal data on backend databases. This is due to the combination of integrating the user login process with the sharing of attributes. As this process is integrated into one, whenever the user needs to log in (as most SBS tend to remain logged in automatically), a fresh set of user data attributes can be requested which can be used for the computational purposes such as content filtering. This might have additional computational costs on each login, which is a probable limitation.

These features, validated through the PoC, demonstrate that ABCs can substantially reduce personal data exposure while maintaining the full functionality required by subscription-based services, thus proving their efficacy in both enhancing privacy and ensuring compliance with privacy standards.

5.2.4 Secondary Research Question 4

Are ABCs compatible with different operating systems (hosting platforms) and end-user devices (Android, iOS)?

The compatibility of ABCs across diverse operating systems and end-user devices is crucial for ensuring their versatility and accessibility in a variety of application environments. The Table 5.1 demonstrates the broad compatibility of ABCs, particularly with various hosting platforms and mainstream end-user devices. ABCs can be successfully deployed on a range of operating systems including macOS (both Intel and ARM architectures), various distributions and architectures of Linux (32-bit, AMD64, ARM, ARM64), and Windows (32-bit, AMD64, ARM, ARM64). This ensures that ABCs can be integrated into virtually any existing IT infrastructure, facilitating seamless and secure authentication mechanisms.

Additionally, the Yivi App, which serves as a personal digital wallet for storing and managing ABCs, is fully compatible with both Android and iOS platforms. This compatibility allows users to leverage the privacy and security benefits of ABCs directly from their smartphones, making it practical for everyday use in mobile environments. The ease of access to ABCs through the Yivi App on these widely used platforms further enhances user experience and broadens the applicability of ABCs in various digital interactions, ranging from secure logins to complex access control scenarios in subscription-based services.

5.2.5 Secondary Research Question 5

Are ABCs on users' smartphones reliable enough for service providers (verifiers) to trust them as accurate representations of users' true identities?

Attribute-Based Credentials (ABCs) on smartphones provide a reliable and trustworthy method for verifying user identities, making them suitable for service providers. ABCs leverage advanced cryptographic methods to ensure that credentials are issued by trusted authorities and are securely stored and handled on user devices.

Table 5.1: Operating System Compatibility for IRMA Binaries

Hosting Platforms

Operating System	Binaries
macOS (Intel)	irma-darwin-amd64
macOS (ARM)	irma-darwin-arm64
Linux (32-bit)	irma-linux-386
Linux (AMD64)	irma-linux-amd64
Linux (ARM)	irma-linux-arm
Linux (ARM64)	irma-linux-arm64
Windows (32-bit)	irma-windows-386.exe
Windows (AMD64)	irma-windows-amd64.exe
Windows (ARM)	irma-windows-arm.exe
Windows (ARM64)	irma-windows-arm64.exe

End User Operating Systems

Operating System	Proof
Android	`https://play.google.com/store/apps/details?id=org.irmacard.cardemu&pli=1`
iOS	`https://apps.apple.com/nl/app/yivi/id1294092994`

These measures protect the data from unauthorized access and tampering during transactions, which is vital for maintaining security and trust. The following sections demonstrate how specific features of ABCs contribute to their reliability and trustworthiness.

Verification by Trusted Authorities

ABCs are authenticated and issued by reputable entities such as government bodies, ensuring their authenticity. For example, in the Proof of Concept (PoC), age verification credentials were issued by demo government repositories, which reliably controlled access to age-sensitive content. In the production environment, the data will be fetched from actual government repositories such as Rijksoverheid (Dutch Population Register). This robust verification process builds trust in the digital credentials' validity. This functionality can be seen in Figure 5.14.

Secure Storage and Transmission

Credentials are stored securely on users' devices and transmitted using encrypted methods to safeguard against tampering and eavesdropping. The Yivi app demonstrated this in the PoC by securely storing user credentials and using encrypted communications for interactions with service providers. Figure 5.18 showcases the Yivi privacy statement, proving the point on secure storage, and the use of encrypted information is detailed in the Yivi application security practice section in the details of the Yivi app in the Google Play store [48].

Dynamic Credential Management

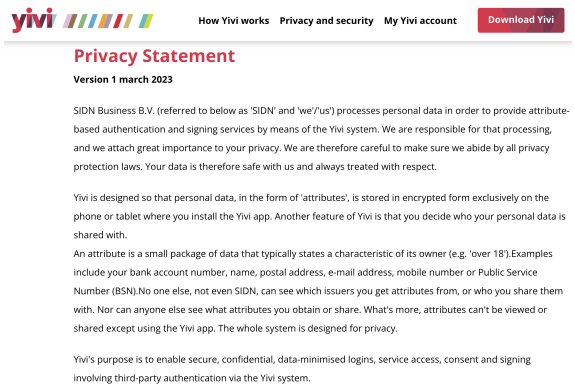

Figure 5.18: Yivi Privacy statement

The infrastructure of ABCs supports the dynamic updating and revocation of credentials, which is crucial for maintaining their accuracy and reliability. This feature ensures that the digital identities are always current and precise, thereby enhancing trust. While the PoC did not show the revocation of demo credentials (as demo credentials cannot be revoked), the capability for easy updates and revocations supports the continued accuracy of the information.

In summary, ABCs offer a highly reliable framework for digital identity verification that service providers can trust to accurately reflect the true identities of their users. These features, demonstrated through the PoC, confirm the capability of ABCs to provide secure, authentic, and dynamically manageable user credentials.

6

Conclusion

This section delves into the conclusions drawn from the comprehensive exploration of Attribute-Based Credentials (ABCs) within subscription-based services, answering the primary research question regarding the potential of ABCs to effectively minimize personal data exposure while ensuring that service functionality remains intact. It also outlines future directions for research that could further enhance the practical application and theoretical understanding of ABCs in various digital environments.

6.1 Conclusion

In addressing the primary research question of this thesis, the analysis and evidence provided in the PoC alongside the insights from the sub-research questions collectively suggest that ABCs can be effectively integrated into subscription-based services. The focus is on whether ABCs can minimize personal data exposure while ensuring that service functionality is not compromised.

The PoC demonstrates that ABCs are capable of maintaining all essential functionalities traditionally managed by conventional authentication methods within subscription-based services. This includes handling video playback, content filtering, subscription tier verification, and user authentication efficiently. This capability ensures that the implementation of ABCs does not detract from the user experience or the operational efficiency of the service.

Furthermore, ABCs offer distinct advantages in managing privacy and data security. They allow users greater control over the disclosure of their attributes, supporting selective information sharing, which minimizes the exposure of unnecessary personal data. This selective disclosure is vital in enhancing data privacy and aligning with best practices for data protection.

Compatibility with a wide range of operating systems and devices, such as Android and iOS, underlines the versatility of ABCs. This compatibility ensures that ABCs can be adopted across different technological environments, making them accessible to a broad user base.

The reliability of ABCs on user smartphones, critical for ensuring the confidence of both users and service providers, is underscored by the robustness of the credential system. ABCs are designed with features that allow for regular updates and the

revocation of credentials, maintaining the accuracy and relevance of the user's digital identity.

Through this examination, it is evident that while ABCs provide a framework that could potentially enhance the security and privacy of digital authentication processes, they also sustain the functionality required by subscription-based services. This balance of functionality and enhanced security features suggests that ABCs can serve as a viable alternative to traditional authentication methods in specific contexts, especially where data privacy is a priority.

Overall, this thesis concludes that ABCs, with their capacity to minimize personal data exposure and adapt to various digital environments, offer a promising direction for the evolution of authentication technologies in subscription-based services. Their effective implementation could lead to significant improvements in how privacy and functionality are managed in digital service platforms.

6.2 Contributions and Analysis

This section discusses the key contributions made throughout the thesis and provides an overview of the critical analyses conducted. The thesis primarily focuses on the application of ABCs within subscription-based services, particularly media streaming platforms, to enhance data privacy while maintaining service functionality. The following points summarize the main contributions and their implications.

Theoretical Framework and Operational Capabilities of ABCs

The thesis delineates the theoretical underpinnings of ABCs, providing a comprehensive overview of their structure and functionality. It details how ABCs enable the verification of necessary user attributes without disclosing personal information, thereby addressing critical privacy concerns. The research extends to the operational capabilities of ABCs, exploring their integration into existing digital infrastructures. This includes an assessment of compatibility across various operating systems and devices, which is crucial for widespread adoption.

Proof of Concept Implementation

A significant contribution of the thesis is the empirical evidence provided through a structured PoC. The PoC within a media streaming service context demonstrates that ABCs can maintain all functionalities of traditional authentication systems while providing additional privacy benefits. This practical demonstration includes secure storage and transmission of credentials, selective disclosure of attributes, and dynamic credential management, showcasing the real-world applicability of ABCs.

Compatibility and Trustworthiness Evaluation

The thesis evaluates the trustworthiness of ABCs on smartphones, considering their potential to accurately represent user identities in a secure and privacy-preserving manner. It includes a detailed analysis of the security features implemented in the Yivi app, such as encrypted storage and communication. Compatibility across

different operating systems and devices is also thoroughly assessed, ensuring that ABCs can be effectively deployed in diverse technological environments.

Addressing Data Privacy Issues

By implementing ABCs, the research proposes a solution that significantly reduces the exposure of personal data within subscription-based services. This aligns with the data minimization principle of the GDPR, emphasizing the collection and processing of only the minimum necessary personal data. The thesis highlights how ABCs enable users to control the information they share, enhancing privacy and reducing the risks associated with data breaches.

6.3 Challenges in Implementing ABCs in Subscription Based Services

Implementing ABCs in subscription based services presents several challenges that must be addressed to leverage their full potential.

Economic Impact of Reduced Data Collection: Collecting user data is often a significant source of revenue for service providers, as it can be used for targeted advertising and other monetization strategies. By minimizing data collection, service providers may face economic losses. This tradeoff between enhancing user privacy and maintaining revenue streams must be carefully managed.

Performance Tradeoffs: While ABCs enhance privacy, they can introduce performance tradeoffs. The processes of verifying and issuing credentials can be computationally intensive, potentially leading to latency issues. Optimizing these processes to ensure a seamless user experience without compromising security is a significant challenge.

Usability and User Experience: The complexity of ABC systems can affect usability. Users must understand how to manage their credentials and interact with services that utilize ABCs. Providing a user-friendly interface and clear instructions is essential to encourage adoption.

Scalability: As subscription-based services grow, the ABC system must scale accordingly. Ensuring that the system can handle a large number of users and transactions without degradation in performance is a significant technical challenge.

Trust Management: Building and maintaining trust between users, service providers, and credential issuers is essential. This involves implementing robust verification processes and ensuring that all parties adhere to established protocols and standards.

Cost of Implementation: The initial cost of implementing ABCs can be high. This includes developing the necessary infrastructure, training personnel, and potentially redesigning existing systems to integrate ABC functionalities. Balancing these costs with the anticipated benefits is a key consideration for service providers.

Less Personalization in Subscription-Based Services: Due to the reduced disclosure of personal information with ABCs, service providers may find it challenging to offer personalized services and recommendations. Personalization often relies on detailed user data, and limiting access to such data could result in a less tailored user experience. Service providers will need to find innovative ways to balance privacy with the desire for personalization.

In conclusion, while the implementation of ABCs in subscription-based services offers numerous benefits, it also involves addressing significant challenges related to security, performance, usability, and regulatory compliance. By carefully navigating these challenges, service providers can enhance privacy and security, ultimately leading to more robust and user-centric subscription models.

6.4 Future Work

This thesis has explored the potential of Attribute-Based Credentials (ABCs) to enhance privacy and preserve functionality in subscription-based services. While the results are promising, several areas warrant further exploration to broaden the scope and applicability of ABCs.

Enhanced Interoperability with Existing Systems Future studies could focus on enhancing the interoperability of ABCs with existing authentication systems, such as OAuth 2.0 and SAML. This integration would facilitate a smoother transition for service providers and potentially increase the adoption rate of ABCs in mainstream applications.

Scalability and Performance Optimization As ABCs gain traction in practical applications, assessing and optimizing their scalability and performance becomes crucial. Future work should aim to develop more efficient protocols and architectures that can handle larger user bases without compromising speed or security.

User-Centric Studies on Privacy and Usability Future work should also include comprehensive user-centric studies to evaluate the privacy and usability aspects of ABCs. Understanding user perceptions and behavior in relation to ABCs can drive improvements in design and functionality, making these systems more user-friendly and widely accepted.

Legal and Regulatory Compliance Another important area for future research is the examination of legal and regulatory challenges associated with the deployment of ABCs. As digital identity systems become more prevalent, ensuring compliance with global data protection regulations, such as GDPR, is imperative. This research could provide valuable insights into the necessary adjustments and best practices for ABC implementation in different jurisdictions.

Broader Application Domains Lastly, expanding the application domains of ABCs to include other areas such as e-government, healthcare, and banking could demonstrate the versatility and robustness of ABCs. Exploring these domains would provide a deeper understanding of the specific requirements and challenges in each sector and how ABCs can be tailored to meet these needs.

Hybrid Model: Coexistence of Traditional Authentication Mechanisms and ABCs Future research could investigate the feasibility of a hybrid model where traditional authentication mechanisms coexist with ABCs. This approach could provide a transitional solution for service providers, allowing them to gradually integrate ABCs while still utilizing established authentication methods. This coexistence could enhance security and user experience by leveraging the strengths of both systems.

Using ABCs in Mobile Apps Exploring the use of ABCs in mobile applications is another promising area for future work. Mobile apps are a dominant platform for user interaction, and integrating ABCs into these apps could significantly enhance privacy and security for a large user base. Research should focus on developing seamless integration techniques, optimizing performance on mobile devices, and ensuring user-friendly interfaces to encourage adoption.

By addressing these areas, future research can build on the foundational work of this thesis, driving forward the practical implementation and theoretical understanding of Attribute-Based Credentials in the digital age.

Bibliography

[1] M. Chew and S. Stamm, "Contextual identity: Freedom to be all your selves," in *Proceedings of the Workshop on Web*, vol. 2, 2013.

[2] "General data protection regulation(gdpr)." (), [Online]. Available: `https://www.edps.europa.eu/data-protection/data-protection/glossary/d_en`.

[3] "General data protection regulation(gdpr)." (), [Online]. Available: `https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement`.

[4] "Spotify data breach 2020." (), [Online]. Available: `https://oag.ca.gov/system/files/Copy%20of%20Spotify%20Breach%20Notice%20Letter%20%28CALIFORNIA%29.DOCX_.pdf`.

[5] "European union data protection." (), [Online]. Available: `https://www.edps.europa.eu/data-protection/data-protection_en`.

[6] "General data protection regulation(gdpr)." (), [Online]. Available: `https://gdpr-info.eu/`.

[7] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[8] V. Seničar, B. Jerman-Blažič, and T. Klobučar, "Privacy-enhancing technologies—approaches and development," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 147–158, 2003.

[9] J. Camenisch, "Concepts around privacy-preserving attribute-based credentials: Making authentication with anonymous credentials practical," in *Privacy and Identity Management for Emerging Services and Technologies: 8th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6 International Summer School, Nijmegen, The Netherlands, June 17-21, 2013, Revised Selected Papers 8*, Springer, 2014, pp. 53–63.

[10] W. Mostowski and P. Vullers, "Efficient u-prove implementation for anonymous credentials on smart cards," in *Security and Privacy in Communication Networks: 7th International ICST Conference, SecureComm 2011, London, UK, September 7-9, 2011, Revised Selected Papers 7*, Springer, 2012, pp. 243–260.

[11] E. R. Verheul, "Self-blindable credential certificates from the weil pairing," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2001, pp. 533–551.

[12] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 21–30.

[13] IRMA Foundation. "What is irma?" (n.d.), [Online]. Available: `https://irma.app/docs/what-is-irma/`.
[14] "Yivi app, https://www.yivi.app/en,"
[15] P. Vullers and G. Alpár, "Efficient selective disclosure on smart cards using idemix," in *IFIP Working Conference on Policies and Research in Identity Management*, Springer, 2013, pp. 53–67.
[16] G. Alpár and B. Jacobs, "Credential design in attribute-based identity management," 2013.
[17] K. S. McCurley, "The discrete logarithm problem," in *Proc. of Symp. in Applied Math*, USA, vol. 42, 1990, pp. 49–74.
[18] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Annual international cryptology conference*, Springer, 1997, pp. 410–424.
[19] N. P. Smart and N. P. Smart, "Zero-knowledge proofs," *Cryptography Made Simple*, pp. 425–438, 2016.
[20] G. Couteau, "Zero-knowledge proofs for secure computation," Ph.D. dissertation, Université Paris sciences et lettres, 2017.
[21] R. Canetti, Y. Chen, J. Holmgren, *et al.*, "Fiat-shamir: From practice to theory," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 1082–1090.
[22] G. Yu, "Simple schnorr signature with pedersen commitment as key," *Cryptology ePrint Archive*, 2020.
[23] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Annual international cryptology conference*, Springer, 1991, pp. 129–140.
[24] R. Metere and C. Dong, "Automated cryptographic analysis of the pedersen commitment scheme," in *Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7*, Springer, 2017, pp. 275–287.
[25] S.-Y. Tan, I. Sfyrakis, and T. Gross, "A relational credential system from q-sdh-based graph signatures," *Cryptology ePrint Archive*, 2023.
[26] J. Han, L. Chen, S. Schneider, H. Treharne, and S. Wesemeyer, "Privacy-preserving electronic ticket scheme with attribute-based credentials," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 4, pp. 1836–1849, 2019.
[27] N. D. Sarier, "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management," *Computers & Security*, vol. 105, p. 102 243, 2021.
[28] D. Ostkamp, "Irma and verifiable creden-tials," 2020.
[29] R. Iyengar, Y.-H. Park, and Q. Yu, "The impact of subscription programs on customer purchases," *Journal of Marketing Research*, vol. 59, no. 6, pp. 1101–1119, 2022.
[30] A. Malhotra and C. Kubowicz Malhotra, "Evaluating customer information breaches as service failures: An event study approach," *Journal of Service Research*, vol. 14, no. 1, pp. 44–59, 2011.

[31] T. Van Letht, "Typologies of subscription-based business models," *Rotterdam School of Management, Erasmus University.—2016*, 2016.

[32] G. Alpár and J.-H. Hoepman, "A secure channel for attribute-based credentials: [short paper]," in *Proceedings of the 2013 ACM workshop on Digital identity management*, 2013, pp. 13–18.

[33] K. Rannenberg, J. Camenisch, and A. Sabouri, "Attribute-based credentials for trust," *Identity in the Information Society, Springer*, 2015.

[34] J. M. de Fuentes, L. González-Manzano, J. Serna-Olvera, and F. Veseli, "Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities," *Personal and Ubiquitous Computing*, vol. 21, pp. 869–891, 2017.

[35] W. Lueks, G. Alpár, J.-H. Hoepman, and P. Vullers, "Fast revocation of attribute-based credentials for both users and verifiers," *Computers & Security*, vol. 67, pp. 308–323, 2017.

[36] I. Krontiris, Z. Benenson, A. Girard, A. Sabouri, K. Rannenberg, and P. Schoo, "Privacy-abcs as a case for studying the adoption of pets by users and service providers," in *Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, Revised Selected Papers 3*, Springer, 2016, pp. 104–123.

[37] Z. Benenson, A. Girard, and I. Krontiris, "User acceptance factors for anonymous credentials: An empirical investigation.," in *WEIS*, 2015.

[38] B. Zwattendorfer, "Using anonymous credentials for eid authentication in the public cloud.," in *WEBIST*, 2015, pp. 156–163.

[39] J. Camenisch, I. Krontiris, A. Lehmann, *et al.*, "D2. 1 architecture for attribute-based credential technologies-version," *Attribute-Based Credentials for Trust*, vol. 105, 2011.

[40] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *Journal of network and computer applications*, vol. 166, p. 102 731, 2020.

[41] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[42] D. Reed, M. Sporny, D. Longley, *et al.*, "Decentralized identifiers (dids) v1. 0," *Draft Community Group Report*, 2020.

[43] W. Li, C. J. Mitchell, and T. Chen, "Oauthguard: Protecting user security and privacy with oauth 2.0 and openid connect," in *Proceedings of the 5th ACM workshop on security standardisation research workshop*, 2019, pp. 35–44.

[44] J. Hughes and E. Maler, "Security assertion markup language (saml) v2. 0 technical overview," *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08*, vol. 13, p. 12, 2005.

[45] A. A. Malik, H. Anwar, and M. A. Shibli, "Federated identity management (fim): Challenges and opportunities," in *2015 Conference on Information Assurance and Cyber Security (CIACS)*, IEEE, 2015, pp. 75–82.

[46] "Netflix architecture." (), [Online]. Available: `https://netflixtechblog.com/edge-authentication-and-token-agnostic-identity-propagation-514e47e0b602`.

[47] S. Paul, *Attribute based credentials for subscription based services*, https://github.com/souptik199 Based-Credentials-for-Subscription-Based-Services.git, 2024.
[48] "Yiviappdetails." (), [Online]. Available: `https://play.google.com/store/apps/datasafety%20id=org.irmacard.cardemu`.
[49] P. Bichsel, C. Binding, J. Camenisch, *et al.*, "Cryptographic protocols of the identity mixer library, v. 1.0," *IBM Research Report*, 2009.
[50] P. Vullers, "Efficient implementations of attribute-based credentials on smart cards," Ph.D. dissertation, SI: sn, 2014.

A

Appendix

A.1 User Data Categories and Attributes for Authentication

Table A.1: User Data Categories and Attributes used in Authentication

Category	**Attributes**
User Identification	Name, Email address, Username
Authentication Credentials	Password or PIN, Security questions/answers
Contact Information	Address, Phone number
Payment Details	Credit/debit card information, Billing address
Subscription Plan	Type of subscription (e.g., basic, premium), Subscription start and end dates, Renewal preferences
Preferences and Settings	Communication preferences (e.g., email notifications), Personalization settings (e.g., language, content preferences)
Usage History	Usage patterns and history of interactions with the service
Device Information	Device type and specifications, IP address for security and access control
Consent and Permissions	User consent for data processing, Permissions for accessing specific features or data
Communication History	Records of communications between the user and customer support
Security and Access Controls	Two-factor authentication preferences, Account activity logs for security monitoring
Subscription Status	Current subscription status (active, inactive), Past subscription history
Feedback and Reviews	User feedback on the service, Ratings and reviews if applicable
Legal and Compliance	Acceptance of terms and conditions, Consent to privacy policies
Data Preferences	Data sharing preferences (opt-in/opt-out), Data deletion and retention preferences

A.2 Algorithms

Algorithm 1 Prepare for a blind Camenisch-Lysyanskaya signature [49] [50]

Function CL-BLIND-COMMIT($sk, (n, S, Z, \{R_i\}_{i=1}^{M})$)
$v_0 \leftarrow$ Random()
$U \leftarrow S^{v_0} \cdot R_0^{sk} \mod n$
Return (U, v_0)

Algorithm 2 Generate a proof of correctness for the user's commitment U [49] [50]

Function CL-Prove-U((U, v_0),n_U,sk,$(n, S, Z, \{R_i\}_{i \in M})$)
$\tilde{v_0} \leftarrow$ Random()
$\tilde{sk} \leftarrow$ Random()
$\tilde{U} \leftarrow S^{\tilde{v_0}} \cdot R_0^{\tilde{sk}} \mod n$
$c \leftarrow \text{Hash}(U, \tilde{U}, n_U)$
$\hat{v}_0 \leftarrow \tilde{v_0} + c \cdot v_0$
$\hat{sk} \leftarrow \tilde{sk} + c \cdot sk$
Return $(c, \hat{v}_0, \hat{sk})$

Algorithm 3 Verify the proof of correctness for U [49] [50]

function CL-VERIFY-U(U, $(c, \hat{v}_0, \hat{s}_k)$, n_U, $(n, S, Z, \{R_i\}_{i \in M})$)
    $\hat{U} \leftarrow U^{-c} \cdot S^{\hat{v_0}} \cdot R_0^{\hat{sk}} \mod n$
    if $c \neq \text{Hash}(U, \hat{U}, n_U)$ **then**
        return Invalid
    end if
    return Valid
end function

Algorithm 4 Generate a blind Camenisch-Lysyanskaya signature [49] [50]

function CL-BLIND-SIGN(U, $\{a_i\}_{i \in M}$, $(n, S, Z, \{R_i\}_{i \in M})$, (p, q))
    $v_{00} \leftarrow$ Random()
    $U \leftarrow U \cdot S^{v_{00}} \mod n$
    for all $i \in M$ **do**
        $U \leftarrow U \cdot R_i^{a_i} \mod n$
    end for
    $Q \leftarrow Z \cdot U^{-1} \mod n$
    $e \leftarrow$ RandomPrime()
    $d \leftarrow e^{-1} \mod (p_0 \cdot q_0)$
    $A \leftarrow Q^d \mod n$
    return (A, e, v_{00})
end function

Algorithm 5 Randomize a Camenisch-Lysyanskaya signature [49] [50]

function CL-RANDOMISE($(A, e, v), (n, S, Z, \{R_i\}_{i \in M})$)
  $r \leftarrow \text{Random}()$
  $A_0 \leftarrow A \cdot S^r \mod n$
  return (A_0, e, v_0)
end function

Algorithm 6 Generation of IRMA selective disclosure proof [49] [50]

function CL-PROVE-D($faigi2D, (A_0, e, v_0), nonce, (n, S, Z, \{R_i\}_{i \in M})$)
  $\tilde{e} \leftarrow \text{Random}()$
  $\tilde{v} \leftarrow \text{Random}()$
  $\tilde{Z} \leftarrow A_0^{\tilde{e}} \cdot S^{\tilde{v}} \mod n$
  for all $i \in H$ **do**
    $\tilde{a}_i \leftarrow \text{Random}()$
    $\tilde{Z} \leftarrow \tilde{Z} \cdot R_i^{\tilde{a}_i} \mod n$
  end for
  $c \leftarrow \text{Hash}(A_0, \tilde{Z}, nonce)$
  $\hat{e} \leftarrow \tilde{e} + c \cdot e$
  $\hat{v} \leftarrow \tilde{v} + c \cdot v_0$
  for all $i \in H$ **do**
    $\hat{a}_i \leftarrow \tilde{a}_i + c \cdot a_i$
  end for
  return $(c, A_0, \hat{e}, \hat{v}, \{\hat{a}_i\}_{i \in H})$
end function

Algorithm 7 Verification of the IRMA selective disclosure proof [49] [50]

function CL-VERIFY-D($(c, A^0, \hat{e}, \hat{v}, \{\hat{a}_i\}_{i \in H}, \{a_i\}_{i \in D}), nonce, (n, S, Z, \{R_i\}_{i \in M})$)
  $\hat{Z} \leftarrow Z^{-c} \cdot A_0^{e} \cdot S^{\hat{v}} \mod n$
  for all $i \in D$ **do**
    $\hat{Z} \leftarrow \hat{Z} \cdot R_i^{c \cdot a_i} \mod n$
  end for
  for all $i \in H$ **do**
    $\hat{Z} \leftarrow \hat{Z} \cdot R_i^{\hat{a}_i} \mod n$
  end for
  if $c \neq \text{Hash}(A_0, \hat{Z}, nonce)$ **then**
    return False
  end if
  return True
end function

A.3 Comparing related technologies to ABCs

A.3.1 Blockchain-based Identity Management - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2):Blockchain-based Identity Management systems leverage cryptographic hashing and consensus mechanisms to ensure the immutability and integrity of identity data stored on the blockchain. This prevents malicious third parties from forging or tampering with identity records without detection. Non-repudiation (S3):Transactions recorded on a blockchain are cryptographically signed by the user's private key, providing irrefutable proof of their origin. This prevents the issuer or any party from denying their involvement in creating or authorizing the transaction. Non-transferability (S4): Each user maintains control over their private keys, which are used to authorize transactions and interact with their identity records on the blockchain. As long as the private keys are kept secure, the user's identity and associated credentials cannot be transferred to another user without explicit consent. Offline issuer (P1): Blockchain-based Identity Management systems operate in a decentralized manner, allowing users to interact with their identity records and perform transactions without requiring direct involvement from a centralized issuer. Users can manage their identity autonomously, even when offline, by signing transactions with their private keys. Issuer unlinkability (P2):In a blockchain network, transactions are pseudonymous, with users identified by cryptographic addresses rather than personally identifiable information. This ensures that the issuer's identity remains unlinkable to specific transactions or identity records stored on the blockchain. Multi-show unlinkability (P3):Blockchain transactions are designed to be unlinkable, meaning that the same user's interactions with the blockchain cannot be easily correlated across different transactions or verification protocols. This provides privacy and anonymity for users by preventing adversaries from tracing their activities on the blockchain. Selective disclosure (P4): Blockchain-based Identity Management systems can support selective disclosure of identity attributes through the use of zero-knowledge proofs or off-chain attestations. Users can reveal specific attributes from their identity records without exposing unnecessary information, enhancing privacy and minimizing disclosure risks. Minimal information (P5): During verification processes, only the necessary attributes required for authentication or authorization are revealed to the verifier. Blockchain-based Identity Management systems ensure minimal information disclosure by providing access to specific identity attributes without exposing additional sensitive data stored on the blockchain.

A.3.2 Self-Sovereign Identity (SSI) - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2):SSI systems utilize decentralized identifiers (DIDs) and verifiable credentials (VCs) that are cryptographically signed by the issuer. This ensures that third parties cannot forge or alter valid credentials without detection, thereby achieving unforgeability. Non-repudiation (S3): Similar to ABCs, in SSI, credentials are cryptographically signed by the issuer. This provides non-repudiation, as the issuer cannot deny their involvement in producing the credential's signature. The cryptographic proof ensures that the credential's origin can be verified.Non-transferability (S4): In SSI, users have control over their digital identities and credentials through the use of decentralized identity wallets. These wallets are secured with the user's private keys, preventing unauthorized transfer of credentials to another user without explicit consent. Offline issuer (P1): SSI systems enable users to interact with their digital identities and credentials offline, as they have control over their identity wallets and private keys. Issuers are not directly involved in the verification process, allowing users to manage their identities autonomously. Issuer unlinkability (P2): SSI systems leverage decentralized networks and cryptographic techniques to ensure issuer unlinkability. Credentials issued by different issuers are stored independently in the user's identity wallet, making it difficult for adversaries to trace the issuer's credentials across different transactions or verification processes. Multi-show unlinkability (P3): SSI systems prioritize privacy and unlinkability by enabling users to present verifiable credentials without revealing unnecessary information. Through zero-knowledge proofs and selective disclosure, verifiers cannot correlate a user's activities across different verification protocols, enhancing multi-show unlinkability. Selective disclosure (P4): Selective disclosure is a fundamental feature of SSI systems, allowing users to selectively reveal specific attributes from their verifiable credentials during verification processes. This minimizes the disclosure of unnecessary information and enhances privacy. Minimal information (P5): During verification processes, SSI systems ensure minimal information disclosure by providing only the necessary attributes required for authentication or authorization. Verifiers receive the disclosed attributes, credential names, and corresponding issuers without revealing additional sensitive information.

A.3.3 Decentralized Identifiers (DIDs) - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2): DIDs are designed to be globally unique and tamper-evident. Once created, a DID cannot be forged or duplicated by a malicious third party due to the decentralized and immutable nature of the underlying distributed ledger technology (DLT) or blockchain. Non-repudiation (S3): DIDs are associated with cryptographic keys that are used to sign and authenticate digital transactions or verifiable credentials. This cryptographic evidence provides non-repudiation, ensuring that the issuer cannot deny their involvement in creating or endorsing a credential associated with a specific DID. Non-transferability (S4): Each DID is owned and controlled by the entity to which it is assigned. Ownership of a DID is cryptographically proven through possession of the associated private keys. Therefore, users cannot transfer their DIDs or associated credentials to another user without explicit authorization. Offline issuer (P1): DIDs allow for offline issuance and verification of credentials. The issuer of a credential can create and sign a verifiable credential offline using their private key. During verification, the integrity and authenticity of the credential can be verified without direct communication with the issuer, as long as the corresponding DID document is available. Issuer unlinkability (P2): DIDs are pseudonymous and do not inherently reveal the identity of the issuer. The decentralized nature of DLT or blockchain ensures that the issuer's identity remains unlinkable to specific DIDs or credentials, providing privacy and confidentiality. Multi-show unlinkability (P3): Verifiers cannot trace the activities of a user across different verification protocols or interactions using the same DID. DIDs facilitate unlinkable interactions, ensuring that no adversary can distinguish whether multiple transactions or verifications were performed using the same DID. Selective disclosure (P4): DIDs support selective disclosure of identity attributes through the use of verifiable credentials and zero-knowledge proofs. Users can reveal specific attributes from their credential without disclosing unnecessary information, enhancing privacy and minimizing disclosure risks. Minimal information (P5): During verification processes, only the necessary information required for authentication or authorization is revealed to the verifier. DIDs ensure minimal information disclosure by providing access to specific identity attributes without exposing additional sensitive data beyond what is required for the transaction.

A.3.4 OAuth 2.0 and OpenID Connect - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2): OAuth 2.0 and OIDC rely on tokens (access tokens, ID tokens) that are issued by trusted authorization servers. These tokens are digitally signed by the issuer (authorization server) using cryptographic methods, ensuring unforgeability. A malicious third party cannot forge a valid token without possessing the necessary cryptographic keys. Non-repudiation (S3): Both OAuth 2.0 and OIDC utilize digital signatures to provide non-repudiation. The issuer (authorization server) signs the tokens, including ID tokens, with its private key. This signature allows relying parties (e.g., resource servers) to verify the authenticity of the tokens and ensure that they were indeed produced by the issuer. Non-transferability (S4): OAuth 2.0 and OIDC tokens are bound to the authenticated user and cannot be transferred to another user without proper authorization. The tokens contain claims that are specific to the authenticated user and are not transferrable between users within the system. Offline issuer (P1): In OAuth 2.0 and OIDC, the issuer (authorization server) is responsible for issuing tokens but is not directly involved in the verification protocol between the client and the resource server. Once tokens are issued, the resource server can independently verify the tokens' validity without direct communication with the issuer. Issuer unlinkability (P2): OAuth 2.0 and OIDC do not inherently provide issuer unlinkability. The issuer (authorization server) is known and trusted by the relying parties. However, the user's identity information is not directly exposed to the relying party, enhancing privacy to some extent. Multi-show unlinkability (P3): In OAuth 2.0 and OIDC, tokens can be used for multiple interactions across different verification protocols (e.g., accessing different resources). However, without additional measures such as token rotation or token binding, there may be risks of correlating multiple token usages to the same user. Selective disclosure (P4): OAuth 2.0 and OIDC support selective disclosure to some extent. OIDC, in particular, allows the client to request specific user information (claims) through scopes during the authentication process. However, the granularity of selective disclosure may vary depending on the implementation and configuration. Minimal information (P5): During verification protocols, OAuth 2.0 and OIDC provide only the necessary information required for authorization and authentication. OIDC, in particular, returns ID tokens containing essential identity information such as user ID and issuer details. However, additional attributes or claims may be requested by the client depending on the scopes and permissions granted.

A.3.5 XACML (eXtensible Access Control Markup Language) - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2): XACML policies and access control decisions can be digitally signed to prevent unauthorized modification or forgery. This ensures that a malicious third party cannot tamper with access control decisions without detection. Non-repudiation (S3): XACML can provide non-repudiation through audit logs and digital signatures on access control decisions. This prevents the issuer from denying that the access control decision was produced by them, as the digital signature can be verified. Non-transferability (S4): XACML access control decisions are typically bound to specific attributes and conditions related to the user's identity, resource, and context. These decisions cannot be easily transferred to another user without meeting the required conditions specified in the access policies. Offline issuer (P1): In XACML, access control policies and decisions can be enforced by policy decision points (PDPs) without direct involvement of the issuer. Once the policies are defined and distributed to the relevant components, the verification process can be performed offline by the PDP. Issuer unlinkability (P2): XACML policies and access control decisions do not inherently provide issuer unlinkability. However, the architecture can be designed to separate the roles of policy decision making (PDP) and policy administration (PAP), limiting the ability of an adversary to trace the origin of the access control decisions. Multi-show unlinkability (P3): XACML does not inherently provide multi-show unlinkability. However, access control decisions can be designed to be stateless or pseudonymous, making it difficult for verifiers to trace the activities of a user across multiple interactions without additional context. Selective disclosure (P4): XACML policies allow for selective disclosure of attributes and conditions required for access control decisions. Policies can be defined to request specific attributes or context information relevant to the authorization process, enabling fine-grained control over information disclosure. Minimal information (P5): During access control decision processes, XACML provides mechanisms to limit the information revealed to the verifier to only the necessary attributes, conditions, and policy names required for making authorization decisions. This ensures that no unnecessary information is disclosed beyond what is specified in the access policies.

A.3.6 Security Assertion Markup Language (SAML) - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2): SAML assertions are digitally signed by the identity provider (issuer) using asymmetric cryptography. This ensures that a malicious third party cannot forge a valid SAML assertion without possessing the private key of the issuer. Non-repudiation (S3): SAML assertions include digital signatures, providing non-repudiation. The issuer cannot deny producing the assertion because the digital signature can be verified using the issuer's public key, thereby confirming the authenticity of the assertion. Non-transferability (S4): SAML assertions are typically bound to a specific user or entity and cannot be easily transferred to another user. The assertions contain attributes and statements that are specific to the authenticated user's session and cannot be reused by another user. Offline issuer (P1): In SAML, the identity provider (issuer) is responsible for issuing assertions but is not directly involved in the verification process between the service provider (verifier) and the user. Once the assertion is issued, the service provider can independently verify its validity without direct communication with the identity provider. Issuer unlinkability (P2): SAML assertions do not inherently provide issuer unlinkability. The issuer (identity provider) is known and trusted by the service provider. However, the identity provider's information is contained within the assertion, allowing the service provider to attribute the assertion to the issuer. Multi-show unlinkability (P3): SAML assertions can be used for multiple interactions across different service providers. However, without additional measures such as token rotation or session management, there may be risks of correlating multiple assertion usages to the same user. Selective disclosure (P4): SAML assertions can contain various attributes and statements about the authenticated user. However, the service provider can request specific attributes through attribute queries or by specifying the required attributes in the authentication request, allowing for selective disclosure. Minimal information (P5): During verification protocols, SAML assertions provide only the necessary information required for authentication and authorization. The assertions contain attributes relevant to the user's identity and authentication context, without revealing unnecessary information to the verifier.

A.3.7 Federated Identity Management - Comparison with Security and Privacy Features Provided by ABCs

Unforgeability (S2): Federated Identity Management systems often employ cryptographic techniques like digital signatures to ensure the unforgeability of credentials. This prevents malicious third parties from forging valid credentials. Non-repudiation (S3): Non-repudiation is achieved in Federated Identity Management systems through the use of digital signatures or other cryptographic mechanisms. This prevents the issuer from denying that they produced the credential's signature. Non-transferability (S4): Federated Identity Management systems typically bind credentials to specific users and entities, preventing users from transferring their credentials to another user within the system. Offline issuer (P1): In Federated Identity Management, offline issuance may be supported, allowing credentials to be issued without direct involvement of the issuer in the verification process. Once issued, credentials can be used for verification without real-time interaction with the issuer. Issuer unlinkability (P2): Federated Identity Management systems can provide issuer unlinkability by employing federated identity protocols that separate the issuer from the verifier. This prevents an issuer from tracing all the credentials they have issued across different verification protocols. Multi-show unlinkability (P3): Multi-show unlinkability can be achieved in Federated Identity Management by using techniques such as pseudonymous identifiers or token-based authentication. This makes it difficult for verifiers to trace a user's activities across multiple authentication transactions. Selective disclosure (P4): Selective disclosure is a key feature of Federated Identity Management systems. Users have control over which attributes or information they disclose during authentication processes, allowing them to reveal only the necessary information required for access. Minimal information (P5): Federated Identity Management systems prioritize minimal information disclosure during authentication processes. Only the necessary attributes, credential names, and issuer information are typically shared with the verifier, ensuring that no unnecessary information is disclosed.

A.3.8 Non-Interactive Zero-Knowledge (NIZK)

Non-Interactive Zero-Knowledge (NIZK) proofs are cryptographic protocols that allow one party, known as the prover, to demonstrate the validity of a statement to another party, known as the verifier, without revealing any additional information beyond the statement's truthfulness. Mathematically, an NIZK proof involves the generation of a proof string π based on the statement x and the prover's secret knowledge w, such that $V(x, \pi) = 1$ if and only if x is true and the prover possesses the secret w, where V is the verification algorithm used by the verifier. Unlike interactive zero-knowledge proofs, NIZK proofs do not require back-and-forth communication between the prover and verifier, making them more efficient and practical for various applications. The verifier then independently verifies the proof using only the proof string and the statement, without requiring any interaction with the prover. NIZK proofs are widely used in cryptographic protocols, such as anonymous credentials, digital signatures, and secure multiparty computation, to ensure privacy, integrity, and authenticity without revealing sensitive information.