Journal of Digital Media & Interaction
ISSN 2184-3120
Vol. 8, No. 19, (2025), pp. 66-86
DOI: 10.34624/jdmi.v8i19.40196

Integration of Citizen's Card Digital Authentication in Hyperledger Fabric

Carlos Machado Antunes
School of Technology and Management, Polytechnic of Leiria, Portugal
carlos.machado@ipleiria.pt
0009-0005-7010-4328

Marisa Maximiano
School of Technology and Management, Polytechnic of Leiria; CIIC, Portugal
marisa.maximiano@ipleiria.pt
0000-0002-1212-7864

Vítor Távora
School of Technology and Management, Polytechnic of Leiria, Portugal
vitor.tavora@ipleiria.pt
0009-0004-0404-9378

Ricardo Gomes
School of Technology and Management, Polytechnic of Leiria, Portugal
ricardo.p.gomes@ipleiria.pt
0000-0002-0438-9119

Manuel Dias
BioGHP, Portugal
manuel@bioghp.com
0009-0000-1830-6479

Ricardo Correia Bezerra
BioGHP, Portugal
ricardo@bioghp.com
0009-0005-1237-6632

Received: 7 June 2025
Accepted: 24 November 2025

Abstract
This study investigates the integration of the Portuguese Citizen's Card authentication with Hyperledger Fabric blockchain technology, addressing the challenge of bridging traditional government-issued digital identities with blockchain-based systems, particularly focusing on reducing barriers to Web3 adoption for users unfamiliar with decentralized technologies. The proposed solution leverages the Autenticação.gov Software Development Kit (SDK), developed by the Portuguese Agency for Administrative Modernization (AMA) to create a secure bridge between the Citizen's Card authentication system and Hyperledger Fabric's permissioned blockchain framework. The study examines how this approach can facilitate the development of transparent, tamper-proof authentication systems suitable for critical applications such as e-voting and digital government services, and also feasible for on-premises systems. The findings suggest that integrating existing digital identity systems with blockchain technology can promote wider acceptance of decentralized solutions while maintaining security, privacy, and accessibility standards required for public sector applications.

Keywords *Blockchain, Authentication, Smart Card, Private Key Management*

1. Introduction

Hyperledger Fabric (HLF) is a modular and extensible open-source system for deploying and operating permissioned blockchains and one of the Hyperledger projects hosted by the Linux Foundation (George, 2022). As one of the flagship projects under the Hyperledger umbrella, Fabric has emerged as a leading solution for organizations seeking to implement blockchain technology in enterprise environments where privacy, scalability, and controlled access are mandatory.

Unlike public blockchains that operate in a trustless environment with anonymous participants (Hope, 2019), HLF is specifically designed for permissioned networks where all participants have known and authenticated identities. In this system, X.509 certificates are the foundation of identity and authentication (Santhosh & Reshmi, 2023). They are used to represent the digital identity of nodes

(peers, orderers), clients, and administrators, ensuring secure communication and access control within the blockchain network. These certificates are issued by a Certificate Authority (CA) and define the permissions and roles of each participant. HLF includes a CA called Fabric CA that provides certificate management services for the network.

This study investigates the integration of the Portuguese Citizen's Card with Fabric CA and the HLF blockchain, focusing on secure authentication processes. The primary objective is to explore how existing authentication systems, such as digital authentication through the Citizen's Card, can be adapted to enhance user security and accessibility within blockchain environments, addressing the challenge of bridging traditional government-issued digital identities with blockchain-based systems, particularly focusing on reducing barriers to Web3 adoption for users unfamiliar with decentralized technologies. We demonstrate how digital authentication through the Citizen's Card can be accomplished using the Autenticação.Gov Software Development Kit (SDK) (Agência para a Modernização Administrativa, 2025).

The remainder of this document is organized as follows: the next section presents the research questions and describes the research method used. Section 3 provides an overview of the related concepts and work. Section 4 presents our main contribution with the proposed solutions for the integration of digital authentication through the Citizen's Card. Finally, the last section shows the conclusions and future work challenges.

2. Research Questions and Methodology

This document reflects the efforts employed to answer the following research questions:

1. Is it possible to authenticate and control access of an end-user using the digital authentication through a smart card, such as the Portuguese Citizen's Card, in HLF?
2. What processes can be implemented to register and authenticate the end-user through the Portuguese Citizen's Card in HLF?
3. What are the performance impacts of integrating the digital authentication through the Portuguese Citizen's Card in HLF?

The methodology we follow is depicted in Figure 1 and comprises three stages: we start by reviewing the related concepts, followed by a review of existing libraries, frameworks and SDKs. The final stage is dedicated to the implementation of exploratory code to assert the validity of our proposed solutions.

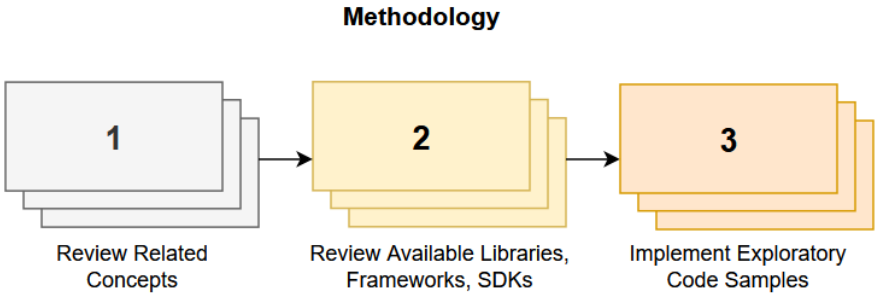

Figure 1. Methodology

The exploratory code samples for Research Question 1 and 2 required the creation of a HLF v2.5 network with one channel and two organizations, including the setup of Fabric CA for each organization, and the development of a desktop client application and a Representational State Transfer (REST) service for testing the authentication processes, as shown in Figure 2.

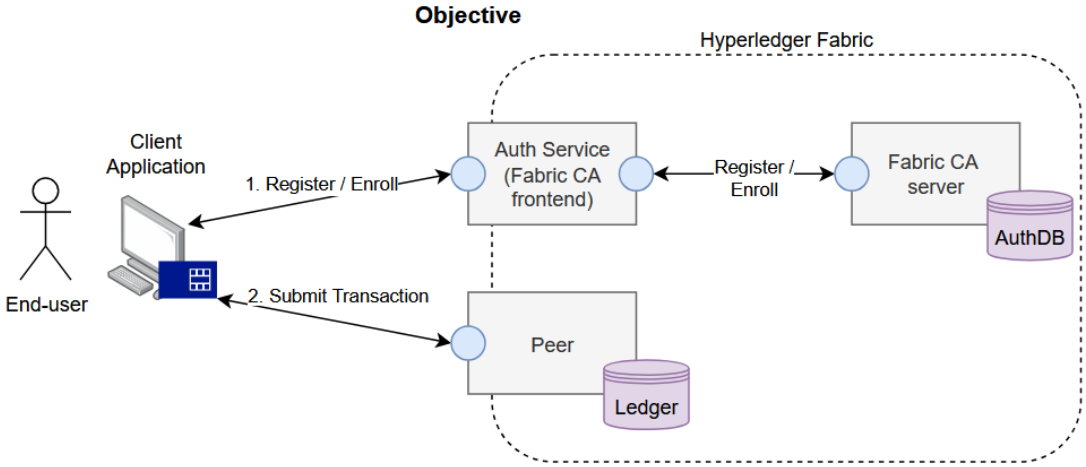

Figure 2. Research Objective

3. Related Concepts and Work

This section begins by presenting the key concepts that are at play in this study. We review three fundamental domains: Distributed Ledger Technology (DLT) and blockchains that enable the creation of decentralized applications, smart card technology allowing for secure authentication processes.

The last sub-section reviews the related work by identifying other blockchain-based platforms that use digital authentication through smart cards and provides a comparison between these platforms and the work presented in this document.

3.1. Blockchain

Blockchain, originally developed for cryptocurrencies, is a decentralized, peer-to-peer ledger technology that distributes data across a network of nodes (Belotti et al., 2019). This structure ensures that no single entity controls the entire system, enhancing security and transparency among all the participants. Transactions are grouped into cryptographically linked blocks, forming an

immutable chain resistant to tampering. Each block contains a hash of the previous block, a timestamp, and transaction data organized in a Merkle tree structure. This design allows for data integrity verification and pseudo-anonymization of transactions while maintaining traceability. The consensus mechanism and the chain's structure make unauthorized modifications practically impossible, as altering one block would require changing all subsequent blocks and gaining network-wide agreement (Gorkhali et al., 2020).

Blockchain networks can be fundamentally categorized into two distinct architectural models: permissionless model operates as open networks where anyone can participate without requiring approval from a central authority, and permissioned model restricts network participation to a predefined set of authorized nodes, organizations, or users. These systems require explicit permission to join the network, validate transactions, or participate in consensus processes (Somma et al., 2024).

Hyperledger Fabric exemplifies the permissioned blockchain approach, serving as a modular enterprise-grade platform specifically designed for business applications. Unlike permissionless networks that rely on anonymous participation, Hyperledger Fabric implements a comprehensive identity management system using X.509 digital certificates to authenticate and authorize all network participants. Each organization, peer node, orderer, and client application must possess valid X.509 certificates issued by CAs before they can interact with the network. This certificate-based identity framework enables fine-grained access control policies, ensuring that only authorized entities can perform specific operations such as invoking smart contracts, querying ledger data, or participating in transaction endorsement processes (Fadele Ayotunde Alaba et al., 2023).

3.2. Smart Cards

Smart cards, such as the Portuguese Citizen’s Card, are a fundamental technology used in modern digital authentication systems, serving as secure hardware tokens that combine portability with robust cryptographic capabilities (Gupta & Quamara, 2019). A smart card is a secure microcontroller that is typically used for generating, storing and operating on cryptographic keys, fundamentally transforming how digital identity verification and transaction authentication are conducted across various domains. These tamper-resistant devices have evolved from simple storage mechanisms to sophisticated cryptographic processors capable of executing complex authentication protocols while maintaining the highest security standards. The cryptographic architecture of modern smart cards, such as the Portuguese Citizen’s Card, enables both authentication and digital signature capabilities through sophisticated key management systems. The Citizen’s Card contains dual-certificate structures, where the authentication signatures allow the card to prove his identity and the certificate also contains privacy-sensitive information such as gender, date of birth, and national number, just to mention a few. The non-repudiation signature is used for generating electronic signatures.

One of the methods available that allows the integration of digital authentication through the Portuguese Citizen’s Card is by using the Autenticação.Gov SDK with a smart card reader to access

the Citizen's Card X.509 certificates and to generate digital signatures, required for signing and submitting transactions to the HLF network. The Portuguese Agency for Administrative Modernization (AMA) is the agency responsible for the development of Autenticação.Gov SDK, a SDK that provides a set of tools and libraries that allow to perform several operations with the Portuguese Citizen's Card, such as signing documents (or any other type of content), secure authentication, and access to citizen's personal data (Agência para a Modernização Administrativa, 2025). The SDK abstracts the Application Protocol Data Unit (APDU) commands used to communicate with the Citizen's Card in a class library originally written in C++ but also available in Java. Besides Typescript and Go, Java is also supported by HLF (Mansour et al., 2024), so this was the programming language we selected for the development of the exploratory code. The code also depends on Bouncy Castle library (Legion of the Bouncy Castle Inc., 2025b) to support some of the cryptographic operations required to implement the authentication process.

3.3. Related Work

The integration of blockchain technology with smart card-based digital authentication represents an emerging frontier in national identity systems. While several countries have implemented advanced smart card identity systems, the degree of blockchain integration varies significantly. This review examines notable implementations including Estonia's ID-card system, the United Arab Emirates' Emirates ID, Luxembourg's EDDITS project, along with their use of distributed ledger technologies.

3.3.1. Estonia's ID-card system

Estonia represents one of the most advanced implementations of blockchain technology in conjunction with smart card identity systems. The Estonian ID-card utilizes Keyless Signature Infrastructure (KSI), a blockchain-like technology that ensures the integrity of digital assets while providing verifiable proof of time, identity, and authenticity (Estonian Business and Innovation Agency, 2025).

The blockchain infrastructure underlying Estonia's digital identity system serves multiple security functions. The immutable ledger records every piece of data interaction, creating an auditable trail that guarantees data has not been tampered with. This technology supports various security features including two-factor authentication and fraud detection mechanisms. The Estonian system has achieved a considerable scale, with over 1.3 billion electronic signatures executed through the platform as of 2021, demonstrating both the robustness and user acceptance of blockchain-integrated smart card authentication (Parsovs, 2020).

3.3.2. United Arab Emirates Emirates ID system

The United Arab Emirates (UAE) has implemented the Emirates ID card as a mandatory identification document for all citizens and residents, featuring advanced biometric security including fingerprint recognition (TDGRA, 2024). While the UAE has articulated ambitious blockchain strategies, including the Emirates Blockchain Strategy 2021, the direct integration of blockchain technology with the physical Emirates ID card itself is less documented compared to Estonia's implementation (TDGRA, 2022).

The UAE government's blockchain strategy envisions using distributed ledger technology for digital transactions, with plans to assign each customer a unique identification number pointing to their information on a secure chain. The Emirates ID has been integrated with various smart services and e-government platforms, including the UAE Pass – a digital identity and signature solution enabling secure login to government and private sector services (TDGRA, 2024).

Recent developments indicate the UAE is moving toward a facial recognition-based digital identity system, with plans announced in 2025 to potentially replace physical Emirates ID cards.

3.3.3. Luxembourg's EDDITS project

Luxembourg has developed an innovative approach to blockchain-based digital identity through the Ethereum Decentralized Digital Identity Trust Services (EDDITS) project. This initiative represents a collaboration between LuxTrust, a government-backed digital identity firm formed in 2005, and INTECH, launching what was described as a world first in the blockchain industry for identity verification (Kuperberg Michael and Kemper, 2019).

EDDITS operates on INFRACHAIN, Luxembourg's governance-trusted permissioned blockchain platform, and provides a solution to one of blockchain's persistent challenges: identity verification. The service allows users to link their LuxTrust strong identity credentials to their blockchain identity (specifically Ethereum addresses), enabling any Ethereum service provider to verify such identity through cryptographic claims (Tanzim Nawar et al., 2023). This bridge between traditional trusted identity systems and decentralized blockchain applications represents a significant architectural innovation.

Users can prove specific attributes such as their name, email, or postal address to online service providers without revealing unnecessary information. The system enables users to manage their digital identity through smart contracts, control access keys, review claims, and even digitally sign documents using their blockchain identity.

EDDITS demonstrates a practical model for integrating existing national eID infrastructure (Luxembourg's electronic identity cards and LuxTrust certificates) with blockchain-based identity systems. Rather than replacing the physical smart card infrastructure, EDDITS creates a trusted linkage layer that extends traditional identity credentials into the blockchain ecosystem, providing strong authentication guarantees for decentralized applications.

3.3.4. Comparative analysis

The examination of these systems reveals several architectural approaches to integrating distributed ledger technologies with smart card authentication:

- Estonia employs a hybrid model where blockchain technology (KSI) provides an immutable audit trail and integrity verification layer, while smart cards handle the actual authentication and digital signing operations. This separation allows for robust security while maintaining user privacy.

- The UAE is pursuing a more ambitious transformation, with blockchain infrastructure planned for the backend of digital identity services, though the extent of integration with physical smart cards remains evolving. The emphasis on mobile digital identity suggests a transition toward software-based authentication that may eventually supersede physical cards.
- Luxembourg's EDDITS represents a bridging architecture that connects existing trusted identity systems (smart cards and digital certificates) to blockchain platforms. Rather than replacing physical credentials, EDDITS extends their utility into decentralized ecosystems, demonstrating how legacy infrastructure can be preserved while gaining blockchain benefits.

Luxembourg's EDDITS project is close to what we demonstrate in this paper, but in comparison with all these systems, we show in the following section that it's also possible to integrate smart card digital authentication, such as the Portuguese Citizen's card, with Hyperledger Fabric platform, a platform that is not used by any of the national identity systems mentioned. The use of this platform is significant, mainly due to the private and permissioned nature of Hyperledger Fabric blockchain. Anyone can use this platform for any business purpose other than providing government services, with complete control over the blockchain infrastructure, and still use smart card digital authentication that is trusted nation-wide.

4. Research

Following our comprehensive review of the relevant concepts and work, and extensive testing, we confidently respond to Research Question 1 affirmatively, it is technically possible to use X.509 certificates stored in a smart card, such as the Portuguese Citizen's Card, to authenticate, sign and submit transactions to the HLF blockchain, as long as the following two core requirements are met:

1. The cryptographic algorithm supported by the smart card X.509 certificates must match the algorithm used by HLF for transaction signature and validation, which is Elliptic Curve Digital Signature Algorithm (ECDSA) with curve P-256. Since June 2024, and in compliance with the EU Regulation 2019/1157 of the European Parliament (European Parliament & European Council, 2019), the Portuguese State began issuing a new version of the Portuguese Citizen's Card (Governo da República Portuguesa, 2024), which includes X.509 certificates generated with ECDSA with curve P-256 key pairs (Agência para a Modernização Administrativa, 2025). Previous versions of the Citizen's Card used Rivest-Shamir-Adleman (RSA) cryptography with 3072-bit key size.
2. If HLF Node Organizational Units (OU) are enabled, the OU of the certificate's Distinguished Name (DN) must match one of the supported roles by HLF, which are named as "peer", "orderer", "admin", or "client".

Besides these requirements, it's also important to consider that HLF uses Attribute Based Access Control (ABAC) to allow or deny access to chaincode functions based on the attributes of the caller's identity certificate. These attributes are defined as key-value pairs associated with user identities during enrollment with Fabric CA and some are reserved for use by HLF itself. The attributes are

added to the X.509 extensions section of the certificate as a Javascript Object Notation (JSON) document with Object Identifier (OID) “1.2.3.4.5.6.7.8.1”, as in the following example shown in Figure 4.

```
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Basic Constraints: critical
                CA:FALSE
            1.2.3.4.5.6.7.8.1:
                {"attrs":{"hf.Affiliation":"","hf.EnrollmentID":"org1admin","hf.Type":"admin"}}
```

Figure 4. HLF X.509 extension attributes

The knowledge of these requirements is critical to provides answers to Research Question 2, which focuses on the processes to implement end-user registration and authentication processes through the Portuguese Citizen’s Card. The next sections detail the steps required to implement these processes.

4.1. End-user Registration

Typically, the end-user is registered with Fabric CA by an administrator, but this operation can also be performed autonomously. The proposed solution is a two-step process detailed on the sequence diagrams shown in Figure 5 and 6, where a client application obtains the required data from the Citizen’s Card inserted on a smart card reader using Autenticação.Gov SDK.

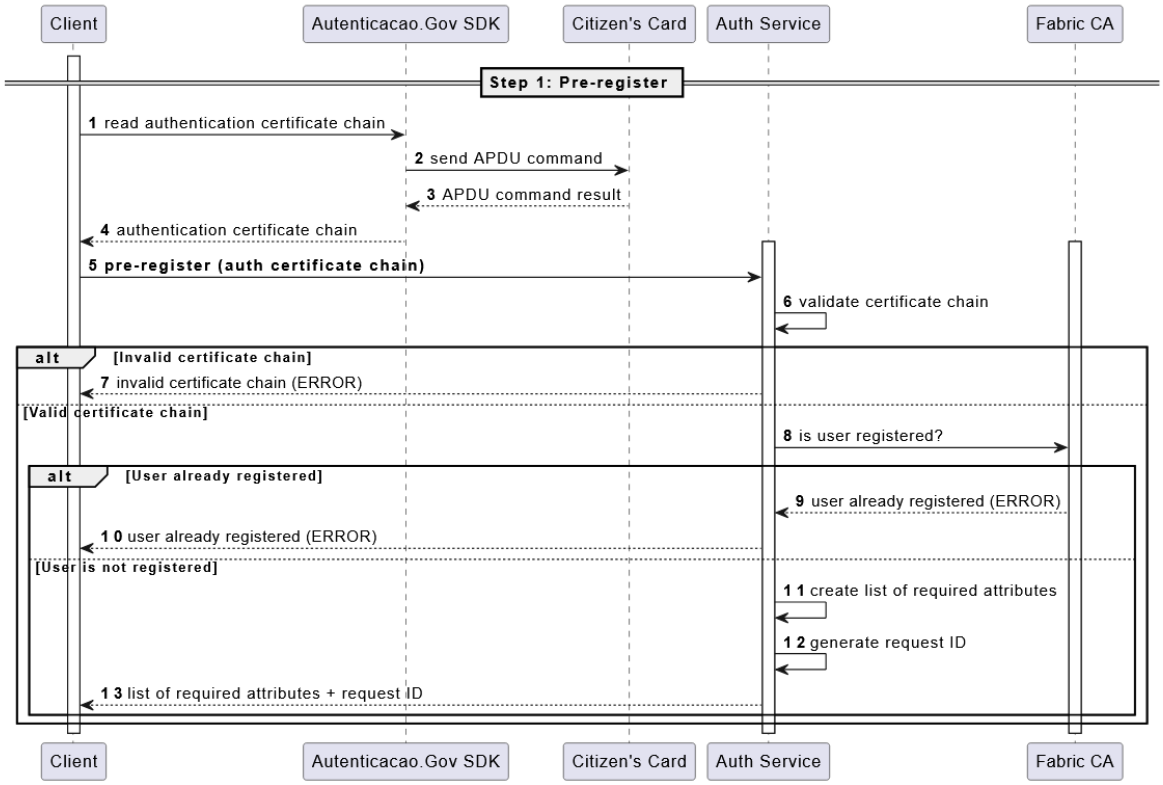

Figure 5. End-user pre-registration through Citizen’s Card (step 1)

In the first step, the certificate chain is read from the Citizen's Card and sent to the authentication service. The service then validates the certificate chain and, if it's valid, replies to the client application with a list of attributes that the end-user must provide to complete the registration (for instance, date of birth). It is recommended to also include an attribute that corresponds to some identifier that is unique to the end-user, such as the Citizen's Card Number, the Social Security Number, etc. to be used as the user ID that is going to be registered in Fabric CA. A nonce should also be sent to the client application to be included in the signed document to prevent replay attacks.

In the second step, depicted in Figure 6, the client application reads the attribute values from the Citizen's Card that corresponds to the list of attributes requested by the authentication service.

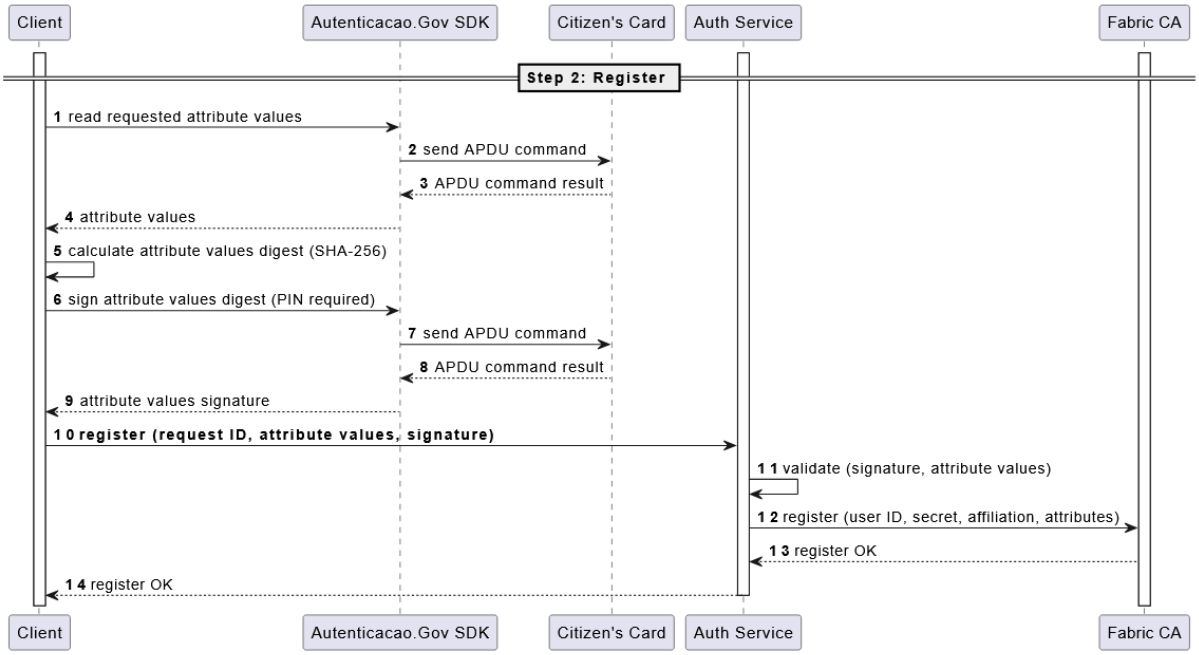

Figure 6. End-user registration through Citizen's Card (step 2)

The client application collects all the attribute values in an Extensible Markup Language (XML) document, adds the nonce to the document, and asks to digitally sign that document with the Citizen's Card. The end-user must insert the Personal Identification Number (PIN) to successfully sign the XML document. Afterwards, the client application sends the XML document and the digital signature to the authentication service to complete the registration process. Fabric CA also requires an enrollment secret to be provided in order to fulfill the registration request, which is automatically generated by the authentication service based on the SHA-256 thumbprint of the Citizen's Card certificate sent by the client application in step 1. When the registration process is completed, a new record is added to the 'users' table in Fabric CA database with the following example data presented in Table 1 (some columns omitted for brevity).

Table 1. 'Users' table in Fabric CA database

id	token	type	attributes
123456789	$2a$10$IbaN7AWIGnKk FdIBl81ieOtBrpJ5KEp9Z	client	[{"name":"hf.EnrollmentID","value":"123456789", "ecert":true},

	azC433E27ytWpxHYuEeq		{"name":"hf.Type","value":"client","ecert":true},{"name":"hf.Affiliation","value":"","ecert":true}, {"name":"birthDate","value":"20010203","ecert":true}]

Table 1 shows that, along with the end-user attributes, Fabric CA also adds the attributes reserved by HLF to the table record when the user is registered.

4.2. End-user Authentication

Following the registration process, the end-user identity must be created, and this is accomplished by enrolling the end-user with Fabric CA. The proposed solution for this operation is also a two-step process detailed on the sequence diagrams shown in Figures 7 and 8, and it also starts with a client application reading the authentication certificate chain from the Citizen's Card and sending it to the authentication service.

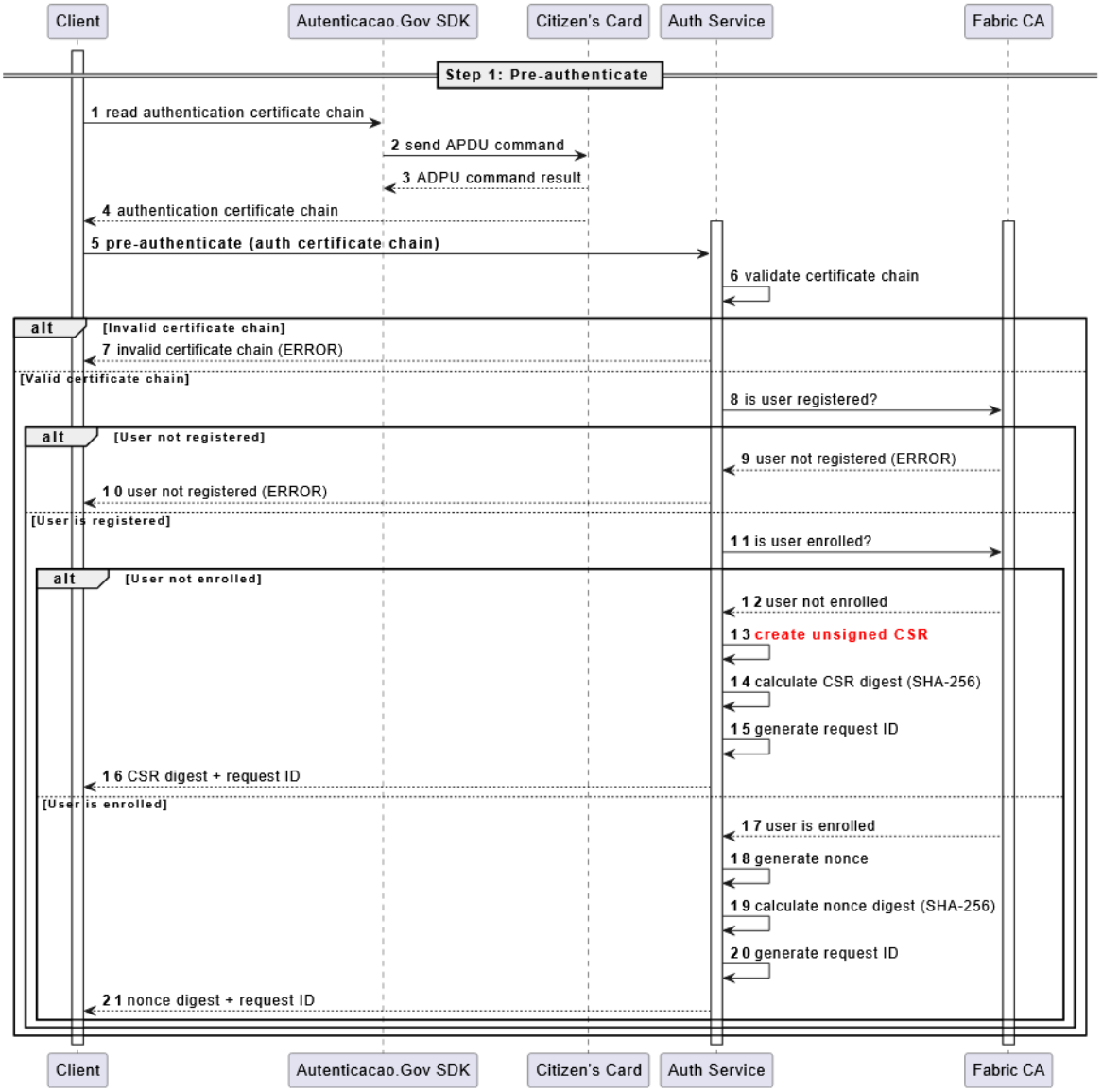

Figure 7. End-user pre-authentication through Citizen's Card (step 1)

The first time the end-user tries to authenticate to the authentication service, Fabric CA is requested to issue a X.509 certificate with the appropriate DN and user attributes. The critical action is emphasized in bold red in Figure 7 (action number 13), which is the action of creating an unsigned Certificate Signing Request (CSR). A private key is not required to create an unsigned CSR because, as the name implies, it is created without a signature. Nevertheless, it is possible to calculate the unsigned CSR's digest and request the end-user to sign that digest. The resulting signature is then embedded in the CSR, thus completing its definition. Neither the JDK nor Bouncy Castle (for Java) provides support to create this type of CSR, but the .NET implementation of the Bouncy Castle library provides this feature (Legion of the Bouncy Castle Inc., 2025a), so we ported the CSharp code to Java.

The unsigned CSR is created with the same public key and DN defined in the certificate sent by the end-user, except that:

- The Organizational Unit (OU) attribute value of the DN is replaced with the term "client".
- The Common Name (CN) attribute value of the DN must match the user ID registered in Fabric CA, so it is also replaced if needed.

The CSR's SHA-256 digest is calculated and then sent back to the client for the end-user to digitally sign it. As depicted in Figure 8, the digital signature is sent to the authentication service to sign the CSR and send it to Fabric CA for enrolling the end-user by issuing a new X.509 certificate. If the operation succeeds, the issued certificate includes the attributes that were previously recorded in the 'users' table during end-user registration process.

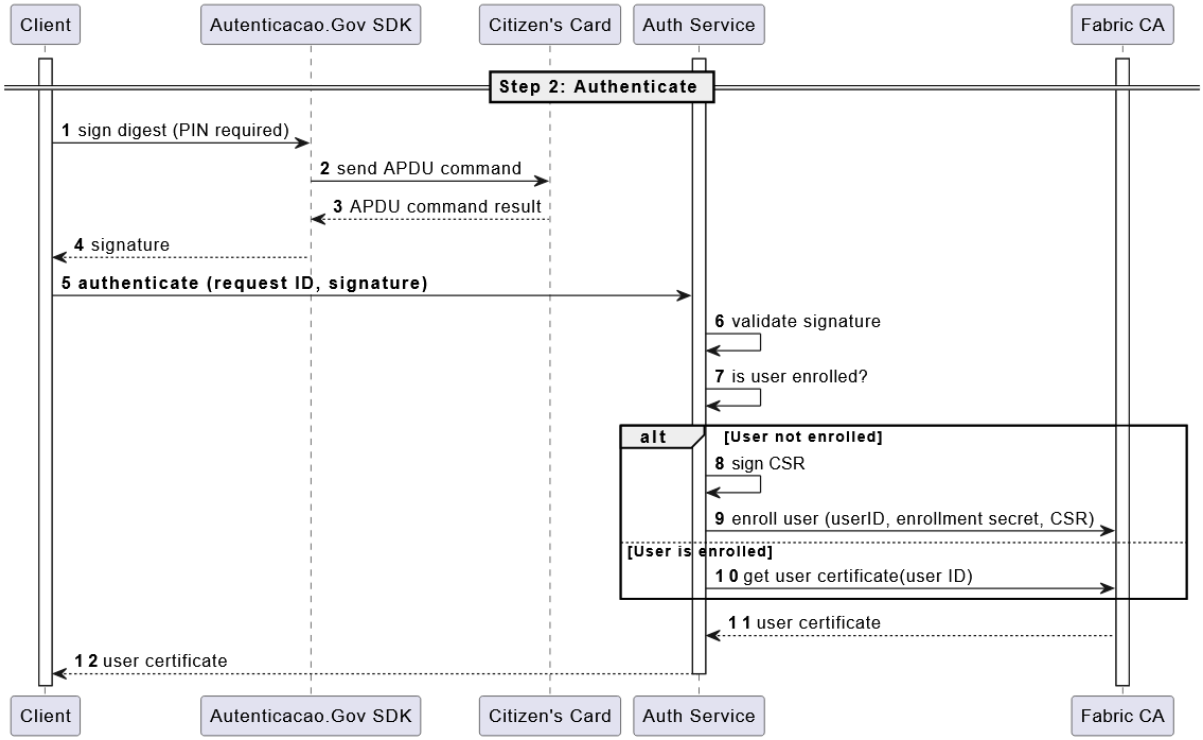

Figure 8. End-user authentication through Citizen's Card (step 2)

If the end-user is already enrolled, the authentication service simply generates a nonce, calculates its SHA-256 digest and sends it to the client for the end-user to digitally sign it. The digital signature is sent back to the authentication service, validates it and gets the X.509 certificate from Fabric CA.

In the end of this process, the client application gets the X.509 certificate provided by Fabric CA and can use the Citizen's Card private key, through the Autenticação.Gov SDK, to sign and submit transactions to HLF network. To achieve this, the client application uses the Hyperledger Fabric Gateway Client Application Programming Interface (API) to connect to a HLF peer and invoke chaincode to submit transactions to the HLF network (Hyperledger, 2025). In order to connect to a HLF peer, the client application must specify an instance of Identity and Signer, which are two interfaces that are included in the Gateway Client API. The Identity is an abstraction of the X.509 certificate provided by Fabric CA and the Signer is a custom implementation that signs a digest using the Citizen's Card through the Autenticação.Gov SDK. An example of such an implementation is presented in Figure 9:

```java
package ...;

import java.security.GeneralSecurityException;
import org.hyperledger.fabric.client.identity.Signer;
import pt.gov.cartaodecidadao.*;

public class CitizenCardSigner implements Signer {

    @Override
    public byte[] sign(byte[] digest) throws GeneralSecurityException {
        try {
            PTEID_ReaderSet readerSet = PTEID_ReaderSet.instance();
            PTEID_ReaderContext reader = readerSet.getReader();
            if (reader == null) {
                throw new GeneralSecurityException("Smart card reader not found.");
            }
            if (!reader.isCardPresent()) {
                throw new GeneralSecurityException("Citizen's card not present.");
            }
            PTEID_Card card = reader.getCard();
            // PIN is requested to the end-user whenever Sign() method is called.
            PTEID_ByteArray signature = card.Sign(new PTEID_ByteArray(digest, digest.length));
            return signature.GetBytes();
        } catch (PTEID_Exception ex) {
            throw new GeneralSecurityException("Smart card error.", ex);
        }
    }
}
```

Figure 9. Custom implementation of Signer interface

Whenever the client needs to sign a transaction, the code presented in Figure 9 is executed, thus requiring the end-user to provide the PIN to fulfill the signature request. This means that, to submit a transaction, the client must wait for user input, and this has a great impact on the overall time to complete the transaction, as we demonstrate in the following section.

The next section tries to answer Research Question 3, where we show the performance tests and corresponding results that allow us to estimate the performance impacts of the proposed integration of smart card digital authentication in Hyperledger Fabric.

4.3. Performance Analysis

To measure the performance of the proposed integration, we implemented another version of the authentication service to serve as our reference. This version simply acts as a proxy to Fabric CA to register and enroll users with randomly generated enrollment secrets, and without performing any data validations. All the charts presented in this section show the time in microseconds and simulate the sequential registration and authentication of 1000 users.

The chart depicted in Figure 10 shows the time to register and enroll users with our reference version. On average, it takes around 68 milliseconds to register and 64 milliseconds to enroll a user.

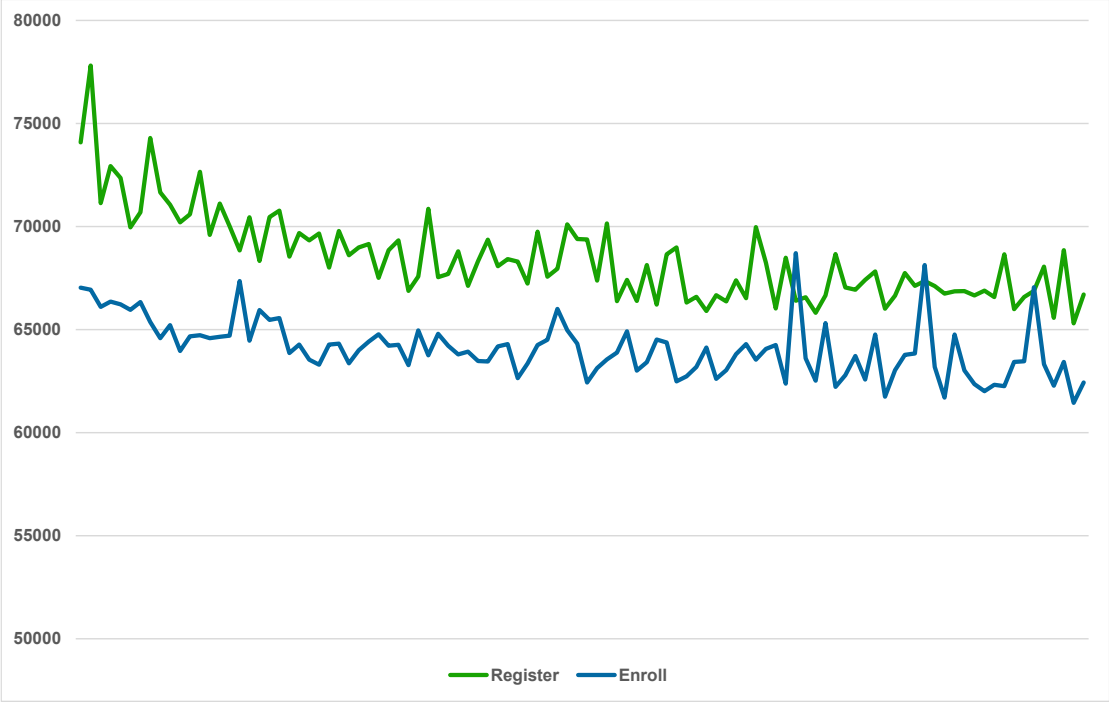

Figure 10. Reference time to register and enroll users

To compare the values with our reference version, we used the version of the authentication service that integrates smart card authentication with Fabric CA to run tests and measure the time to register and authenticate users. With this version, we executed the tests with three different configurations, all concerned with certificate revocation validation of the Citizen's Card certificate: i) without revocation validation, ii) with revocation validation and without Certificate Revocation List (CRL) caching and iii) with revocation validation and with CRL caching. The main reason for having these three configurations is to allow us to better estimate the time the authentication service takes to process the request and the time it takes to download the CRLs to check if the Citizen's Card was revoked.

4.3.1. Test results without revocation validation

Figure 11 shows a stacked line chart with the time to pre-register and register users with the authentication service that integrates smart card authentication with Fabric CA with revocation validation disabled. On average, it takes around 76 milliseconds to pre-register and register a user.

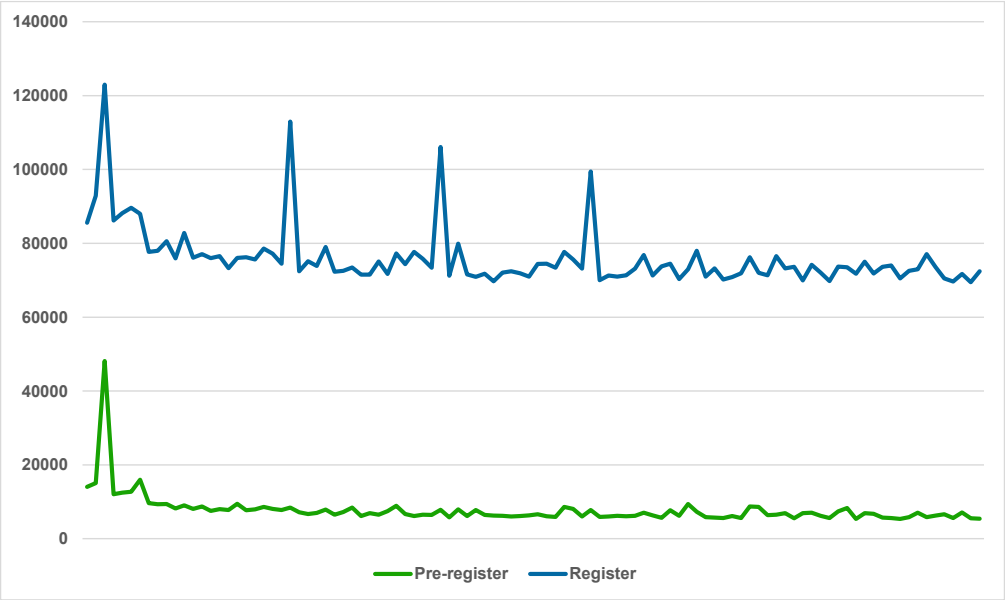

Figure 11. Time to register users with revocation validation disabled

Figure 12 shows a stacked line chart with the time to pre-authenticate and authenticate users with revocation validation disabled. On average, it takes around 28 milliseconds to pre-authenticate and authenticate a user, which is less than our reference version. This is because neither our service nor Fabric CA is required to generate a new key pair for the user's certificate.

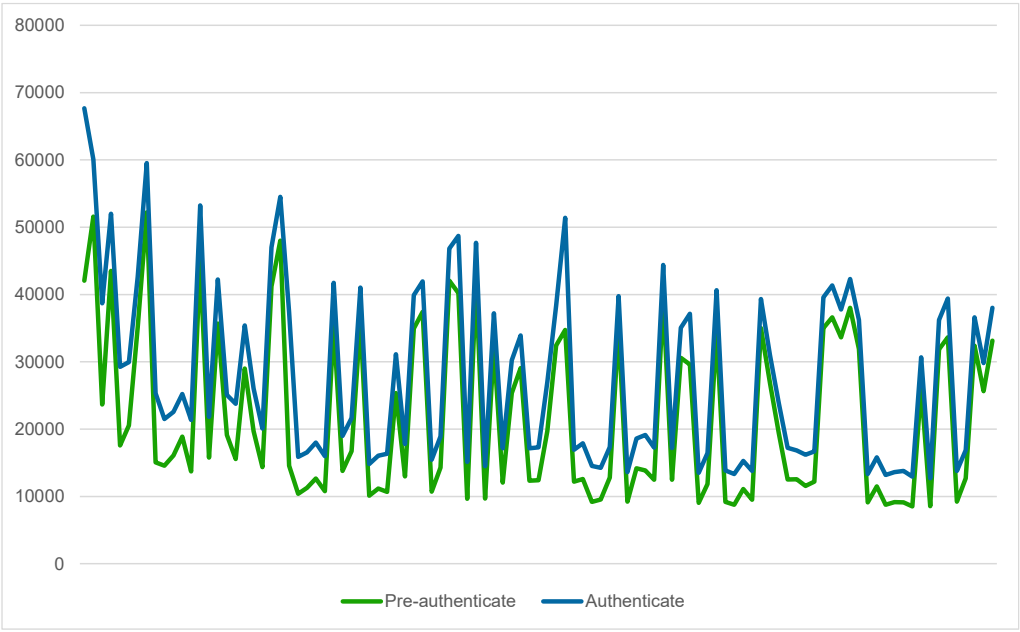

Figure 12. Time to authenticate users with revocation validation disabled

4.3.2. Test results with revocation validation

Figure 13 shows a stacked line chart with the time to pre-register and register users with revocation validation enabled. On average, it takes around 1.1 seconds to pre-register and register a user which is more than 14 times greater than the times measured with the reference version. Whenever the service needs to validate a Citizen's Card certificate it also downloads the CRLs from the Portuguese Citizen's Card CA to check if the certificate was revoked, causing this drastic increase of time to process the request.

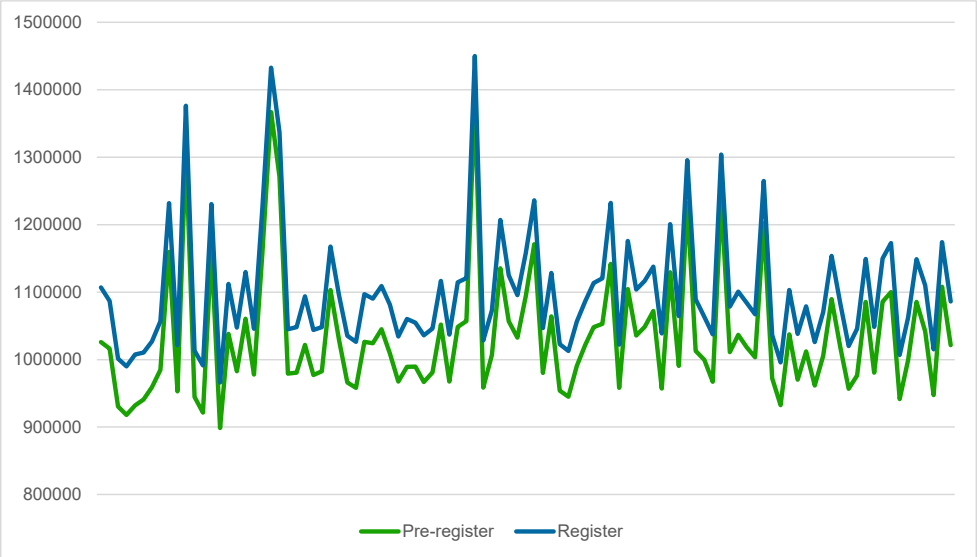

Figure 13. Time to register users with revocation validation enabled

Figure 14 shows a stacked line chart with the time to pre-authenticate and authenticate with revocation validation enabled. On average, it takes around 1.02 seconds to pre-register and register a user which also represents a drastic increase of time to process the request in comparison with the results obtained with the reference version.

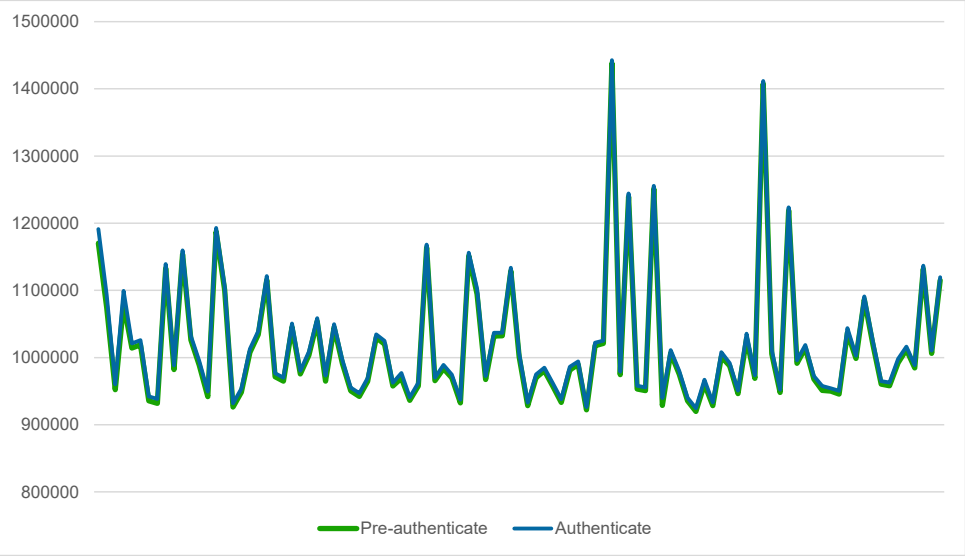

Figure 14. Time to authenticate users with revocation validation enabled

4.3.3. Test results with revocation validation and caching

Figure 15 shows a stacked line chart with the time to pre-register and register users with revocation validation and CRL caching enabled. This means that service downloads a CRL to check if the user's certificate is revoked and stores the CRL in cache for two minutes. Whenever a new CRL is required for validation, the service first checks if it is in the cache and it only tries to download the CRL again if it is missing. The chart shows that on average, it takes around 245 milliseconds to pre-register and register a user, nevertheless it also reveals that after caching all the required CRLs, the time it takes to process the request is well below 100 milliseconds.

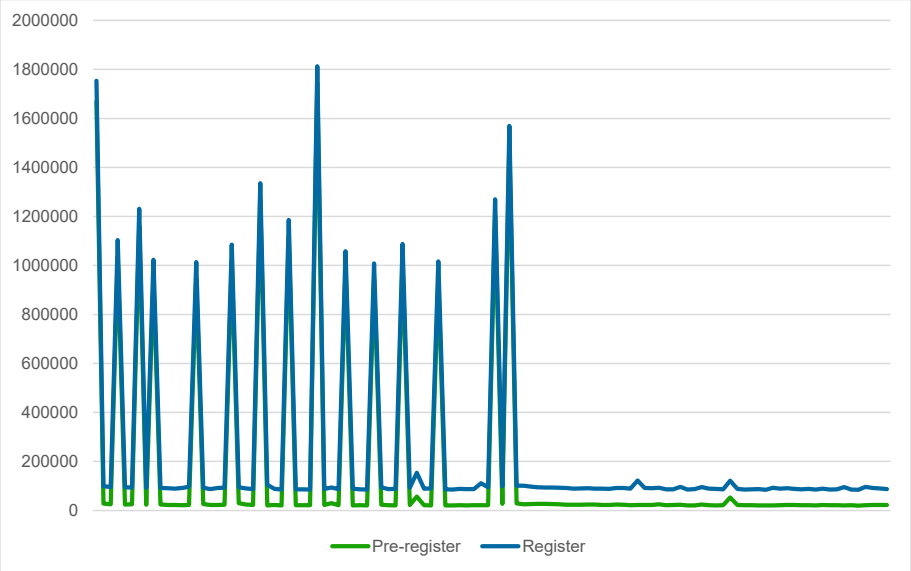

Figure 15. Time to register users with revocation validation and CRL caching enabled

Figure 16 depicts a stacked line chart with the time to pre-authenticate and authenticate with revocation validation and CRL caching enabled. On average, it takes around 67 milliseconds to complete the request. Although with less spikes than the chart in Figure 15, it also shows that there is a drastic increase in time to process the request whenever there is a cache miss.

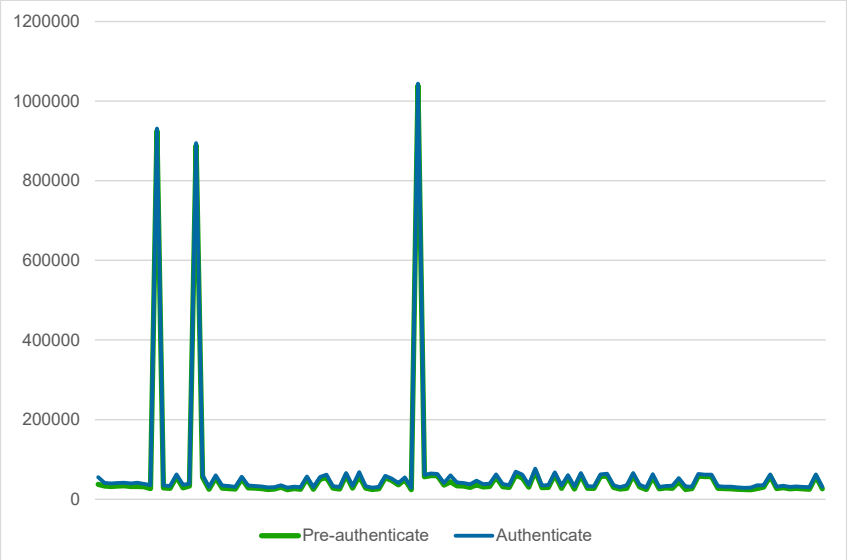

Figure 16. Time to authenticate users with revocation validation enabled

The test results we presented in this section show that the authentication service performs well when revocation validation is disabled, with response times similar or even better than our reference version. It also shows that running the service with revocation validation enabled and with CRL caching can be considered a good compromise between security and performance.

Finally, we also measured the time it takes to sign a transaction on the client side, with and without user's PIN input. The results are shown in Figure 17 which reveals that it takes, on average, 7.4 seconds to sign a transaction when PIN input is required, whereas without PIN it takes around 2 milliseconds. Besides the time user spends typing the PIN and press the 'Enter' key, the time the smart card takes to sign the transaction's digest must also be accounted for.

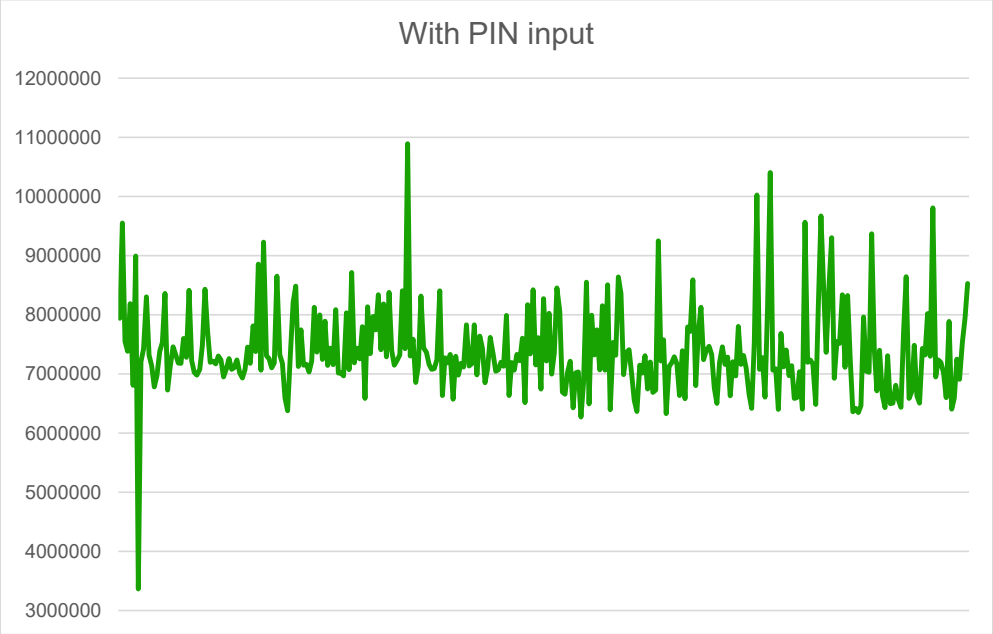

Figure 17. Time to sign a transaction with PIN input

The chart depicted in Figure 17 should be interpreted with some caution because it always depends on the user's ability to type the PIN correctly and expeditiously. Nevertheless, the obvious consequence of this requirement is that the overall time to completely process the transaction by the blockchain network increases dramatically, albeit without spending CPU cycles, because on the client-side the application is simply waiting for user input and on the server-side the transactions are processed asynchronously.

5. Conclusions

This study investigated the integration of the Portuguese Citizen's Card with Hyperledger Fabric (HLF) blockchain technology to enable secure authentication processes in enterprise blockchain environments. Through a comprehensive methodology involving literature review, technical analysis, and exploratory implementation, we addressed three primary research questions concerning the feasibility, implementation processes, and broader applicability of smart card-based authentication in blockchain systems.

Our investigation confirmed that it is technically feasible to authenticate and control access for end-users using digital authentication through the Portuguese Citizen's Card in Hyperledger Fabric environments. This feasibility is contingent upon two critical requirements: compatibility between the cryptographic algorithms used by the smart card X.509 certificates and HLF's transaction signature validation mechanisms (specifically ECDSA with curve P-256), and proper configuration of Organizational Unit attributes in certificate Distinguished Names to match HLF's supported roles. The recent adoption of ECDSA cryptography in Portuguese Citizen's Cards issued since June 2024, in compliance with EU Regulation 2019/1157, addresses the first requirement and enables seamless integration with modern blockchain systems.

We developed and validated comprehensive processes for both end-user registration and authentication through the Portuguese Citizen's Card in HLF networks. The registration process involves a two-step authentication mechanism where users provide certificate chains and digitally signed attribute documents using the Autenticação.Gov SDK. The authentication process similarly employs a two-step approach, utilizing Certificate Signing Requests and digital signatures to establish user identity within the Fabric CA framework. These processes leverage existing government-issued digital identity infrastructure while maintaining the security and access control requirements of permissioned blockchain networks.

The technical contributions of this work include the development of a custom Signer interface implementation that integrates smart card operations with HLF's Gateway Client API, enabling seamless transaction signing using Citizen's Card private keys.

5.1 Limitations and Practical Considerations

Despite the technical feasibility demonstrated in this research, several important limitations affect the practical deployment of smart card-based authentication in blockchain environments. The most significant constraint stems from HLF's transaction execution model, which requires multiple cryptographic signatures throughout the transaction lifecycle. End-users must provide their PIN at least once for read operations and twice for write operations: first to endorse the transaction and subsequently to submit the endorsed transaction to the network. Depending on the transaction submission approach – whether synchronous or asynchronous – a third signature may be required to verify the commit status of the transaction (Hyperledger, 2023).

This multi-signature requirement creates substantial usability challenges that limit the applicability of our proposed solution. For applications with minimal user interactions, such as electronic voting systems or infrequent credential verification scenarios, the authentication overhead remains acceptable. However, for applications requiring frequent blockchain interactions or real-time user engagement, the repeated PIN entry significantly degrades user experience and may discourage adoption.

These constraints highlight the tension between security and usability in blockchain-based authentication systems. While smart card integration provides enhanced security through hardware-

based private key protection and established government identity verification, the associated user experience challenges may limit practical deployment to specific use cases where security requirements outweigh convenience considerations.

5.2 Future Work

Future research should address these usability limitations through several potential approaches. Investigating session-based authentication mechanisms that reduce the frequency of PIN entry while maintaining security standards could significantly improve user experience. For instance, depending on the criticality of data, we could replace the authentication service with a complete frontend to the Hyperledger Fabric network, and all read operations would be carried out by the service itself. Only write operations would require the end-user to input the PIN to sign and submit transactions.

Additionally, exploring mobile-compatible authentication alternatives, such as integration with mobile secure elements or trusted execution environments, could extend the applicability of government-issued digital identity integration to mobile platforms.

The development of hybrid authentication models that combine smart card security with mobile convenience represents another promising research direction. Such approaches might investigate how emerging technologies like contactless authentication and biometric verification could complement existing smart card infrastructure.

Another topic to take into consideration for future studies concerns the planning and execution of a thorough threat model analysis which this paper currently lacks.

This research demonstrates the practical viability of integrating established government digital identity infrastructure with cutting-edge blockchain and decentralized identity technologies. While current limitations constrain immediate widespread deployment, the foundation established here provides a pathway for more accessible and secure blockchain-based applications that can evolve to leverage existing user authentication familiarity while maintaining the security and decentralization benefits of distributed ledger systems.

Acknowledgments

This work was financially supported by Project BlockchainPT – Decentralize Portugal with Blockchain Agenda, WP 2: Health and Wellbeing, 02/C05-i01.01/2022.PC644918095-00000033, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

References

Agência para a Modernização Administrativa. (2025). *Manual do SDK – Middleware do Cartão de Cidadão*. https://amagovpt.github.io/docs.autenticacao.gov/manual_sdk.htm

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys and Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/COMST.2019.2928178

Estonian Business and Innovation Agency. (2025). *KSI Blockchain - e-Estonia*. https://e-estonia.com/solutions/cyber-security/ksi-blockchain/

European Parliament, & European Council. (2019, July 12). *Regulation (EU) 2019/1157*. https://eur-lex.europa.eu/eli/reg/2019/1157/oj/eng

Fadele Ayotunde Alaba, Hakeem Adewale Sulaimon, Madu Ifeyinwa Marisa, & Owamoyo Najeem. (2023). Smart Contracts Security Application and Challenges: A Review. *Cloud Computing and Data Science*. https://doi.org/10.37256/ccds.5120233271

George, J. T. (2022). Hyperledger Fabric. *Introducing Blockchain Applications*, 125–147. https://doi.org/10.1007/978-1-4842-7480-4_6

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics*, *7*(3), 321–343. https://doi.org/10.1080/23270012.2020.1801529;WGROUP:STRING:PUBLICATION

Governo da República Portuguesa. (2024, June 11). *Novo Cartão de Cidadão a partir de 11 de junho*. https://www.portugal.gov.pt/pt/gc24/comunicacao/noticia?i=novo-cartao-de-cidadao-a-partir-de-11-de-junho

Gupta, B. B., & Quamara, M. (2019). *Smart Card Security*. CRC Press. https://doi.org/10.1201/9780429345593

Hope, J. (2019). What Is Blockchain and How Does It Work? *The Department Chair*, *29*(4), 11–11. https://doi.org/10.1002/DCH.30250

Hyperledger. (2023). *Architecture Reference - Hyperledger Fabric Documentation*. https://hyperledger-fabric.readthedocs.io/en/release-2.5/architecture.html

Hyperledger. (2025). *Fabric Gateway - Hyperledger Fabric Docs*. https://hyperledger-fabric.readthedocs.io/en/release-2.5/gateway.html

Kuperberg Michael and Kemper, S. and D. C. (2019). Blockchain Usage for Government-Issued Electronic IDs: A Survey. In J. Proper Henderik A. and Stirna (Ed.), *Advanced Information Systems Engineering Workshops* (pp. 155–167). Springer International Publishing.

Legion of the Bouncy Castle Inc. (2025a). *Bouncy Castle CSharp - Pkcs10CertificationRequestDelaySigned source code*. https://github.com/bcgit/bc-csharp/blob/31a3d18e4b38c53f49d71d08ee3f83e22d939615/crypto/src/pkcs/Pkcs10CertificationRequestDelaySigned.cs

Legion of the Bouncy Castle Inc. (2025b). *Bouncy Castle open-source cryptographic APIs*. https://www.bouncycastle.org/

Mansour, M., Salama, M., Helmi, H., & Mursi, M. (2024). A Survey on Blockchain in E-Government Services: Status and Challenges. *ArXiv Preprint ArXiv:2402.02483*.

Parsovs, A. (2020). Solving the Estonian ID Card Crisis: the Legal Issues. In Amanda Hughes, Fiona McNeill, & Christopher W. Zobel (Eds.), *ISCRAM 2020 Conference Proceedings* (pp. 459–471). Virginia Tech.

Santhosh, M. G., & Reshmi, T. (2023). Enhancing PKI Security in Hyperledger Fabric with an Indigenous Certificate Authority. *2023 IEEE International Conference on Public Key Infrastructure and Its Applications, PKIA 2023 - Proceedings*. https://doi.org/10.1109/PKIA58446.2023.10262412

Somma, A., De Benedictis, A., Esposito, C., & Mazzocca, N. (2024). The convergence of Digital Twins and Distributed Ledger Technologies: A systematic literature review and an architectural proposal. *Journal of Network and Computer Applications*, *225*, 103857. https://doi.org/10.1016/j.jnca.2024.103857

Tanzim Nawar, T., Khan, F. J., Akter, J., Authro, A. S., Ullah, S. M. W., & Hossain, M. N. (2023). A Design for Managing Smart National Identity Cards Securely through the Utilization of Blockchain Technology. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4638825

TDGRA. (2022). *Emirates Blockchain Strategy 2021*. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/emirates-blockchain-strategy-2021

TDGRA. (2024a). *Emirates ID* . https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id

TDGRA. (2024b). *The UAE Pass*. https://u.ae/en/about-the-uae/digital-uae/digital-transformation/platforms-and-apps/the-uae-pass-app