Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 237 (2024) 923–930

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Industry Sciences and Computer Science Innovation

Enhancing e-IDs authentication with NFC

Tariq Youssef[a], Adriano Campos[b], André Guerreiro[b], Carlos Coutinho[b,c]

[a]*Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal*
[b]*Caixa Mágica Software, Lisboa, Portugal*
[c]*Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR, Lisboa, Portugal*

Abstract

In the modern times, the heavy footprint of Information and Communication Technologies in the everyday life brings multiple challenges to the ordinary citizen, like having a digital profile on numerous services and institutions. The spread of authentication services that need to be verified to perform simple tasks is thus overwhelming. Many countries hence developed elaborated solutions to unify some of the authentication services around a single e-ID card to help performing different everyday tasks. The burden associated with carrying a smartcard reader to authenticate, or the time spent and complexity of the authentication using Mobile Digital Tokens represent an adversity for citizens who are not so digitally educated. NFC is a technology that is growing in usage every year and is widely adopted now. It is easy and fast to use. This paper proposes a safe, easy, and fast way to implement NFC-based authentication in an e-ID card and discusses its benefits.

Keywords: Authentication; e-ID; NFC; PKI;

1. Introduction

Electronic Identification (e-ID) cards have become an essential part of our daily routines, facilitating identity verification and access to crucial services. As we increasingly move towards a digital world, many of these functionalities have transitioned online. This shift underscores the importance of authentication, a topic thoroughly examined in this research [1].

The integration of Near-Field Communication (NFC) into e-ID authentication is a transformative step. With NFC-enabled e-ID cards, the authentication process is streamlined. A simple tap, a PIN, and the added layer of multi-factor authentication replace the complexities of traditional login methods. This approach not only eliminates the need for smartcard readers but also fortifies security by mandating the physical presence of the card. The critical role of multi-factor authentication in enhancing security measures is further detailed in various studies [2].

Examining the Portuguese Citizen Card (PCC) offers insights into the potential future of e-ID cards. The PCC is currently undergoing a transition to incorporate NFC technology, a move that could significantly transform online authentication. Once fully implemented, this innovative approach is expected to provide a more intuitive, faster, and secure authentication experience for users. The anticipated benefits are not limited to individual users. Government

10.1016/j.procs.2024.05.180

services are projected to experience a reduction in authentication-related queries, potentially leading to decreased footfall at physical service centers, notably the "Lojas do Cidadão". For businesses, this evolving technology promises a more reliable and enhanced authentication process for their clientele.

In conclusion, the marriage of NFC technology with e-ID cards marks the dawn of a new era in online authentication, promising enhanced security, efficiency, and user experience for individuals, government entities, and businesses.

2. Research methodology

Diving deeper into the research methodology, the Design Science Research Methodology (DSRM) [3] was identified as the ideal framework for this study due to its alignment with the research's objectives. A central aspect of this research revolves around understanding how contactless authentication can be seamlessly integrated into an e-ID card using NFC technology. Additionally, the study seeks to determine the tangible benefits citizens will experience when utilizing the e-ID card's contactless authentication feature.

Through this research, we aim to present a method for NFC integration that not only addresses existing challenges but also significantly enriches the user experience.

3. State of the art

3.1. Near-field communication

NFC is a group of standardised wireless protocols that enable one and two way communication between devices that are within a very short distance of each other (the max range is 10cm). This technology is widely implemented nowadays in many devices we commonly use, like our smartphones, tablets, cards, and a lot more.

An NFC connection always has an initiator and a target. The initiator starts the interaction by sending a request, and the target answers it [4].

NFC devices can have two types, active and passive; Active devices are battery-powered, passive devices are powered through the electromagnetic field created while an active device communicates with them. Another difference worth stating is that a passive device can only be a connection target, never an initiator, whereas an active device can be both [4]. An example of an active device is a smartphone with NFC support, and an example of a passive device is a NFC tag or and e-ID card with NFC support. The adoption of NFC authentication with E-ID is growing in popularity, offering a streamlined and secure method for identity verification [5].

3.2. Usage of public key cryptography for authentication

Authentication is the act of proving our identity to someone or something.

Challenge-response authentication is a set of protocols where a party that wants to be authenticated is asked a question (also called challenge) by another party that must be answered correctly for the authentication to be successful [6].

Consider, for example, that party A wants to authenticate itself to party B; A starts by requesting authentication from B, after which B will send a challenge to A, who will answer the challenge, and if the answer is right then A will be authenticated.

In a public key cryptography system, each party has a set of two keys, one public[1] and the other private[2]. Challenges are signed with the private key, and the public key is used to verify the signature (verify if the answer is correct).

In a public key cryptography system, if party A wishes to authenticate itself to party B then it must first send its ID to B in order for B to obtain A's public key, after which B will send a challenge, which A will sign with its private key and send back to B, and B will verify the signature with A's public key. All entities need access to the public keys to verify the challenge answers; this can be done using or without using certificates.

[1] Every party can access it

[2] Only the owner knows it, no other party can know it

3.2.1. Certificateless public key infrastructure

This method is simple and consists of having a single central database with a pair of keys and IDs for all parties; therefore, when some entity requests a public key from the central database, it must trust the integrity of the information in it. Table 1 shows an example database.

Table 1. An example of a central database.

ID	Public Key
1	”public key of the identity 1”
2	”public key of the identity 2”
3	”public key of the identity 3”

After a party sends its ID and public key to the central database it can be authenticated by other parties. In the authentication process, the authenticating party just needs to send to the Public key infrastructure (PKI) Server the ID of the party requesting authentication to get its public key to verify its signature. Figure 1 shows the interaction between *B* and *A* for the authentication of *A*.

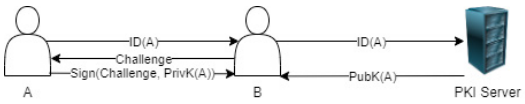

Fig. 1. Interaction between *B* and *A* for the authentication of *A*

Whenever there is need to stop an entity from being able to authenticate itself, its entry can just be removed from the PKI Server central database.

3.2.2. Public key infrastructure with certificates

Another common method of authentication is by using certificates. Firstly, we need a certification authority (CA) which needs to be trusted by every verifying/authenticating party. The CA also has a private-public key pair.

In the registration act, a party sends its ID and public key to the CA, which will sign them with its private key; the output of the signature is called a certificate. Then the generated certificate is sent back to the party that is being registered. After this process the party can be authenticated by others. Figure 2 shows the interaction between the CA and *A* for the registration of *A*. Figure 3 shows the interaction between *B* and *A* for the authentication of *A*.

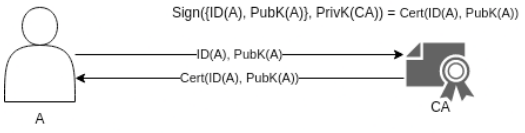

Fig. 2. Interaction between the CA and *A* for the registration of *A*

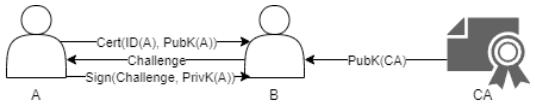

Fig. 3. Interaction between *B* and *A* for the authentication of *A*

During the authentication process, the authenticating party will receive the certificate of the party that wants to be authenticated and verify its validity. The authenticating party uses the public key of the CA to verify the signature on the certificate to ensure that it is genuine and hasn't been tampered with. If the certificate is valid, the authenticating party will send a challenge to the party that wants to be authenticated. The party that wants to be authenticated will sign (encrypt) the challenge with its private key and send it back. The authenticating party then verifies the digital signature of the challenge using the public key retrieved from the valid certificate. If the verification is successful, the party is authenticated.

When using this method, it's common to have a database where all revoked certificates are listed; Whenever a certificated is revoked it is added to that database so that its revoking status can be verified in the authentication process. It's also possible to have something called an OCSP responder, which will be talked about later.

In conclusion, a certificate-based PKI system holds a significant edge over a certificateless PKI system. The primary advantage lies in the robust authentication and verification mechanisms facilitated by certificates issued by a trusted CA. Certificates serve as a reliable means of associating a public key with the identity of the entity it represents, thereby establishing a chain of trust. This trust framework is essential for secure communications in a myriad of digital interactions today. Moreover, the use of certificates enables the implementation of additional security measures such as certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) for real-time verification of certificate validity. These features contribute to the overall integrity and trustworthiness of the system, making certificate-based PKI a superior choice for ensuring digital security and trust in an increasingly interconnected world.

3.3. The Portuguese Citizen Card

The actual PCC is a smartcard used as form of physical identification valid in Portugal and in the EU. It contains a chip that helps in the identification process of its owner, in person or online [7].

The PCC is also used to authenticate in Portuguese public administration portals and others using ”autenticação.gov” to perform different tasks, like taxes, getting a criminal record, banking, performing digital signatures, and others.

It is important to highlight the compelling reasons for utilizing the PCC for authentication. Firstly, it is an official document recognized by the authorities. Secondly, it is backed by a reputable state institution, the INCM (Imprensa Nacional-Casa da Moeda). Moreover, the PCC incorporates certified security features, ensuring a high level of data protection and integrity, like public key certificates.

3.3.1. Current online authentication processes

Nowadays the authentication in Portuguese public administration portals and others can be done with a smartcard reader or with a service called Chave Móvel Digital (CMD).

Online authentication using a smartcard reader. This is the most used and method is done using a smartcard reader and a browser plugin[3]. We need to connect our Citizen Card (CC) to our computer through the smartcard reader and introduce our authentication pin when requested [8]. This authentication pin is generated upon the creation or renewal of the PCC and shipped in a letter to a given address [9]; if this letter is lost and the pin forgotten, a duplicate must be requested in person at a physical government service site (like ”Loja do Cidadão”) [10].

The plugin that is needed for the authentication does not work on smartphones, making the aforementioned authentication process impossible on a smartphone. A company called SmartCardOnMobile (SCOM) tried to solve that problem by creating a mobile application that can perform the authentication using a compatible mobile smartcard reader, though this authentication can only be used to consult/share the card information and perform a digital signature [11]. They also created a SDK that can be used by other developers to perform a similar PCC authentication to be used in their applications [12].

The information in the PCC that can be consulted from the SCOM application or using the SCOM SDK is both the public information and the protected data that the PCC contains [11].

Online authentication with CMD. CMD is the most recent way to authenticate. First, we need to activate the service; this can be done online, mainly using a smartcard reader and our PCC, or in person at a physical government service site [13]. In both cases, we need to create a pin and select a contact form[4] that will be used in the authentication process.

Once the service is activated, to authenticate we just need to input the selected contact, the pin and the one-time-pin which will be delivered through the contact [14]. It’s possible to authenticate using a computer or a smartphone.

3.3.2. Issues with the current online authentication processes

Using a smartcard reader to authenticate has some issues. First, it needs a smartcard reader device, which needs to be bought, and most people don’t have one.

[3] This plugin is called Autenticação.Gov

[4] A contact can be a phone number, email, or others.

Another problem worth mentioning is that the SCOM solution for smartphone authentication solves only half of the smartphones problem; it is still impossible to login into Portuguese public administration portals using a smartcard reader in a smartphone even via CMD.

CMD also has some issues. It needs a subscription to a service, which, as said before, needs to be done in person or online with a smartcard reader. Another problem is that the authentication can be done without the physical PCC, raising security concerns.

As stated above, the current online authentication processes using the PCC have many issues. Research and exploration have been done in other countries to provide solutions for similar problems that the PCC online authentication processes face nowadays. In fact, research on Spain's DNIe system investigates the potential of using NFC in e-ID cards for authentication [15]. If this approach were to be implemented, it would provide similar benefits to the implementation in the PCC, such as not needing additional hardware. Research like the one stated above and this paper provide valuable solutions for improving e-ID card authentication with NFC.

3.3.3. Portuguese public key infrastructure

In this section of this paper, the way the PCC authentication works regarding its PKI will be discussed. The Portuguese PKI uses certificates to help the authentication process.

Each PCC has 2 certificates [16]:

1. A certificate to perform digital signatures.
2. A certificate for authentication (identification of the cardholder).

Another certificate, that is used to authenticate via CMD, exists but is not present in the physical PCC, since this authentication method doesn't require the physical card.

Each certificate type has its own CA:

1. The Digital Signature CA issues the certificates used to perform digital signatures.
2. The CC authentication CA issues the certificates used to authenticate with the CC.
3. The CMD CA issues the certificates needed to authenticate via CMD.

Figure 4 shows the certification authority tree of the Portuguese PKI.

The Portuguese PKI consists of a hierarchical trust model, where the topmost CA is the CA Root. The CA Root issues certificates for the remaining subordinate CAs, which in turn issue certificates for the PCC and the CMD.

In this PKI model, each CA issues digital certificates with different expiration dates, with the highest expiration dates being at the top of the chain. For example, certificates issued by the CA Root have a higher expiration date than the ones issued by the CMD CA. This ensures that the digital certificates can be trusted and used for secure electronic transactions.

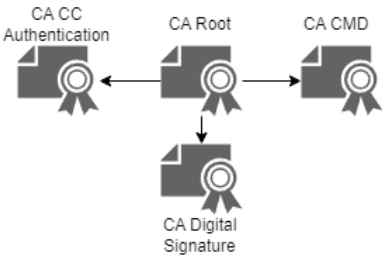

Fig. 4. Certification authority tree of the Portuguese PKI

When a CA issues a new certificate, all subordinate CAs below it in the hierarchy must also issue new certificates. This is because each CA uses its own certificate to issue other certificates, and all certificates in the chain must be valid and trustworthy to ensure secure electronic transactions.

There are various reasons why a CA may issue a new certificate. One reason is to minimize risk, as certificates are often only valid for a limited time period and may need to be replaced if compromised. Another reason is to improve security features, such as using stronger encryption algorithms or key management practices. Additionally, changes in policy or technology may require updating certificates, such as when the validity period of a Citizen Card in Portugal increased from 5 to 10 years. It is crucial for CAs to keep their certificates up-to-date to ensure the security of the

PKI and the digital certificates issued to users. Valid and properly managed certificates are also important for secure electronic transactions and communications.

Checking the validity of a certificate To ensure the security of digital transactions, it is important to check the validity of certificates. There are two primary methods for checking certificate validity. The first method is called Online Certificate Status Protocol (OCSP), which is a protocol used to check the validity of a certificate through a POST request. OCSP is a faster and more efficient way of checking certificate status because it queries the CA directly for information on the certificate, rather than requiring the download of a large Certificate Revocation List (CRL).

The second method is called a CRL, which is a list that contains all revoked certificates and can be downloaded online. CRLs are typically updated frequently, with a new version available each week. Additionally, there is a type of CRL called a Delta CRL, which is a smaller list that is updated more frequently, often on a daily basis. The Delta CRL only contains the differences (entries added and removed) from the previous CRL, making it more efficient for checking the status of recently revoked certificates.

Both OCSP and CRL are important tools for ensuring the validity of digital certificates and for maintaining the security of the PKI. It is essential for users and applications to regularly check the validity of certificates before accepting them as authentic to prevent fraudulent use of certificates or other security breaches.

4. Proposed Solution

The proposed solution explores the integration of NFC technology with e-ID cards to facilitate a secure, efficient, and user-friendly authentication process. This innovative approach leverages the universality of smartphones and the robust security attributes of e-ID cards to create a streamlined authentication paradigm. The following sections delve into the high-level requirements, architectural design, and the proof of concept developed to realize this novel authentication solution.

4.1. High-level requirements for a safe NFC-Based authentication using e-ID cards

The requirements to build a system that makes a secure authentication possible using NFC with an e-ID card are the following:

The e-ID card Composition The e-ID card must be equipped with an NFC tag. Additionally, it must incorporate a secure microprocessor chip responsible for storing the certificate, as well as the private and public keys of the entity utilized in the authentication process. This microprocessor chip must be able to perform the necessary cryptographic operations for the authentication. For added security, the private key must be encrypted when stored within the card, ensuring its protection against unauthorized access.

NFC Initiator The NFC initiator, such as an NFC card reader or a smartphone with NFC support, establishes a secure connection with the authentication server. Once this connection is established, the initiator serves as the primary communication bridge between the e-ID card and the authentication server.

Authentication Server Behaviour The authentication server plays a pivotal role in verifying the authenticity of the e-ID card and ensuring the rightful authentication of its owner. Upon receiving an authentication request, the server initiates a challenge, subsequently verifying the response alongside the certificate's authenticity and revocation status. Should the challenge be signed with a legitimate key and the certificate be confirmed as genuine and valid, the server is obliged to invoke multifactor authentication. The mandatory implementation of multifactor authentication significantly bolsters security, ensuring that even in scenarios where the e-ID card is misappropriated or an unauthorized NFC initiator is nearby even with knowledge about the local decryption pin, access remains restricted. The authentication server is integrated with a PKI server. This PKI server manages the CAs responsible for issuing and supervising certificates. Furthermore, it upholds the protocols and policies related to the issuance and revocation of digital certificates, ensuring the authentication server can consistently verify the status of these certificates.

User Interface and Experience For an authentication system to be embraced by its users, the interface must be as seamless as the technology behind it. The interface should be designed with the user in mind, ensuring that it is intuitive and straightforward. This entails clear prompts for user actions, feedback on successful or failed authentication attempts, and adherence to modern usability and accessibility standards. Given the sensitive nature of authentication, the interface must also maintain stringent security measures, ensuring that user data remains protected at all times.

4.2. Architecture

A proof of concept (POC) has been developed for an innovative authentication solution that leverages the capabilities of Near Field Communication (NFC) to validate e-ID cards using smartphones.

This POC utilizes the advantages of NFC, the robust security attributes of e-ID cards, and the ubiquity of smartphones, paving the way for a transformative approach to digital identity verification.

At the heart of this POC lies an authentication server, crafted in C++, encompassing a custom protocol built upon the robust foundation of Transport Layer Security (TLS). Recognized for its ability to ensure secure communication across computer networks, TLS was the preferred choice to safeguard the transmission of critical authentication information.

The custom protocol is designed to accommodate three distinct types of requests. It's crucial to note that while each request has a specific function, they are not necessarily sequential. The client can directly make an authentication request, as the requisite certificate validation processes are embedded within it. This design choice offers flexibility and ensures a streamlined and efficient authentication process.

1. **Certificate request**: This request issues a certificate for the client. It creates a critical piece of information necessary for the subsequent steps in the authentication process, representing the client's identity in digital form.
2. **Certificate validation request**: This request plays the role of verifying the validity of the issued certificate. It checks if the certificate was issued by a trusted CA and whether it remains active, i.e., it has not been revoked. This request essentially informs the client about the current status of their certificate.
3. **Authentication request**: this request performs a challenge-based authentication using certificates. This request is the main entry point for the client when it seeks to authenticate. It includes validation checks and provides an interface for the client to authenticate securely.

The client application is developed in Kotlin, a statically-typed programming language known for its efficiency in modern Android applications. Kotlin's concise syntax, safety features, and seamless compatibility with Java are notable advantages. This application interfaces with a custom native library, crafted in C++. This library employs the Resource Acquisition Is Initialization (RAII) paradigm [17], a principle that ensures resources, particularly memory, are acquired upon object creation and released upon object destruction, guaranteeing efficient memory management. Due to the unavailability of a smart card for testing purposes, the library includes a custom emulator. This emulator was specifically designed to replicate the behavior of a genuine smart card, allowing for comprehensive testing in the absence of an actual smart card.

The Android client boasts an intuitive design, ensuring that the authentication process is not only easy and fast but also secure for the end-users. This user-centric design approach prioritizes user experience, making the authentication journey seamless. With this Android application, the client simply needs to open the app, scan their e-ID, input the local pin to decrypt the private key, and then click on the authentication button sending an authentication request to the server. This streamlined process ensures a hassle-free and efficient authentication experience for the users.

Ensuring the integrity of cryptographic operations is the OpenSSL C library—a thorough, open-source toolkit renowned for implementing the Secure Sockets Layer (SSL) and TLS protocols.

The foundational principles and imperatives of secure communication and cryptography that influenced the selection of OpenSSL are elaborated upon in seminal texts on network security [18].

5. Conclusion and future work

This implementation significantly improves the authentication process, marking a substantial stride towards modernized digital authentication practices. The elimination of the need for a smartcard reader not only streamlines the authentication process but also reduces the dependency on additional hardware, thereby promoting a user-friendly experience. Requiring the physical presence of the e-ID card during authentication enhances security by ensuring only authorized individuals can gain access, addressing a critical concern in digital authentication. Although the current Proof of Concept (POC) does not yet incorporate multi-factor authentication, a stipulated requirement, it sets the stage for future enhancements in this direction, as future work. The results, obtained using the DSRM [3], underline the effectiveness of the proposed solutions in addressing the identified issues. The broader implication of this work lies in its potential to significantly reduce authentication-related challenges for both individuals and organizations, paving the way for a safer and more efficient digital authentication ecosystem.

Acknowledgements

This work was supported by Fundação para a Ciência e a Tecnologia, I.P. (FCT) [ISTAR Projects: UIDB/04466/2020 and UIDP/04466/2020].

References

[1] Tavares, M., Veiga, F., Guerreiro, A., Campos, A., and Coutinho, C., "WalliD: secure your ID in an Ethereum Wallet", in Proceedings of the 9th IEEE-TEMS international Conference on Intelligent Systems 2018 (IS-2018), Funchal, Portugal, 2018-09-26, DOI:10.1109/IS.2018.8710547.

[2] N. Alyousif and S. Alhabis. "The Necessity of Multi Factor Authentication." In: Interna- tional Journal of Computer Science and Information Technology Research 10.2 (Apr. 2022). Research Publish Journals (Publisher), Website: www.researchpublish.com, International Journal of Computer Science and Information Technology Research, ISSN 2348-1196 (print), ISSN 2348-120X (online), pp. 46–49. doi: 10 . 5281 / zenodo . 6472757. ur l: https://doi.org/10.5281/zenodo.6472757.

[3] Ken Peffers et al. "Design Science Research Process: A Model for Producing and Presenting Information Systems Research". In: CoRR abs/2006.02763(2020). arXiv: 2006.02763. url:https://arxiv.org/abs/2006.02763.

[4] Sandra Dominikus and Manfred Aigner. "mCoupons: An Application for Near Field Communication (NFC)". English. In: 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07). Vol. 2. 2007, pp. 421–428. doi: 10.1109/AINAW.2007.230.

[5] V. Seth. "Why NFC is a rising star in digital ID." In: Biometric Technology Today 2021.9 (2021), pp. 5–7. doi: 10.1016/S0969-4765(21)00094-1.

[6] Sushil Jajodia Henk C. A. van Tilborg, ed. Encyclopedia of Cryptography and Security. English. 2nd ed. Springer New York, NY. isbn: 978-1-4419-5905-8. doi: 10.1007/978-1-4419-5906-5.

[7] O Cartão de Cidadação. Portuguese. url: https://www.autenticacao.gov.pt/web/guest/o-cartao-de-cidadao. (accessed: 08/11/2022).

[8] Autenticação com Cartão de Cidadão. Portuguese. url: https://www.autenticacao.gov.pt/cartao-cidadao/autenticacao. (accessed: 06/11/2022).

[9] Carta e códigos PIN do Cartão de Cidadão. Portuguese. url: https://www.autenticacao.gov.pt/web/guest/cartao-cidadao/codigo-pin. (accessed: 06/11/2022).

[10] Request a duplicate of the pin letter - ePortugal.gov.pt. English. url: https://eportugal.gov.pt/en/servicos/pedir-a-segunda-via-da-carta-pin. (accessed: 06/11/2022).

[11] SmartCardOnMobile. Portuguese. url: https://scom.pt/. (accessed: 06/11/2022).

[12] sdk – SmartCardOnMobile. Portuguese. url: https://scom.pt/sdk/. (accessed: 06/11/2022).

[13] Ativar a Chave Móvel Digital. Portuguese. url: https://www.autenticacao.gov.pt/web/guest/cmd-pedido-chave. (accessed: 06/11/2022).

[14] Autenticação com Chave Móvel Digital. Portuguese. url: https://www.autenticacao.gov.pt/web/guest/chave-movel-digital/autenticacao. (accessed: 06/11/2022).

[15] J. León-Coca, D. Reina, S. Toral, F. Barrero, and N. Bessis. "Authentication Systems Using ID Cards over NFC Links: The Spanish Experience Using DNIe." In: Procedia Computer Science 21 (2013). The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013) and the 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH), pp. 91–98. issn: 1877-0509. doi: https://doi.org/10.1016/j.procs.2013.09.014. url: https://www.sciencedirect.com/science/article/pii/S1877050913008077.

[16] PKI cartão de cidadão. Portuguese. url: https://pki.cartaodecidadao.pt/. (accessed: 06/03/2023).

[17] B. Stroustrup. The C++ Programming Language. 4th. Boston, MA, USA: Addison-Wesley Professional, 2013. isbn: 978-0-321-56384-2.

[18] W. Stallings. Network Security Essentials: Applications and Standards. 7th. Hoboken, NJ, USA: Pearson Education, Inc., 2017. isbn: 978-0-13-444428-4.