FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Portuguese Citizen Card and Digital Mobile Key: the trust required of the citizen

Maria Teresa Queiroz Machado Urbano Ferreira

DISSERTAÇÃO

Mestrado Integrado em Engenharia Informática e Computação

Supervisor: José Manuel de Magalhães Cruz

July 30, 2021

Portuguese Citizen Card and Digital Mobile Key: the trust required of the citizen

Maria Teresa Queiroz Machado Urbano Ferreira

Mestrado Integrado em Engenharia Informática e Computação

July 30, 2021

Abstract

The current tendency regarding governmental operations is to progress towards more electronic, technological, and online solutions for the citizen's needs.

At the moment, the Portuguese government offers several public-key based cryptographic tools for authentication and digital signing. This is done through several available technologies that include a desktop application, a mobile application, and a browser extension.

However, this progress comes with its challenges, as information security cannot be compromised for the purpose of efficiency. With these solutions, the citizens have to accept the conditions they are presented with. This means they lose control over sensitive, personal information that, if accessed, can lead to identity fraud. The citizens are forced to place their trust in the promise of security made by the government and accept the less than full control over their personal information.

This project aims to provide the citizens with proof of trust on the cryptographic methods mentioned, as well as possibly propose an improved and realistic alternative for managing the control the Portuguese government holds over the services provided.

This research requires a deep familiarization with the user experience and the information available to the public, it being: documentation provided, the source code used for some of the technologies, related work, and even information of the approach of other countries with equivalent but different solutions.

Due to time constraints and the lack of viable communication channels with the proper authorities, the work developed did not reach its initial potential, nevertheless improvement points were located. As contribution for the assessment of the quality degree and security perceived by the users, this work revealed a serious governmental effort on the development of these cryptographic tools; however, it also revealed, from the government's side, a minimalist support service lacking in transparency.

This study is beneficial not only for every citizen but also for the government, which should strive to protect its population's privacy, and further work is imperative.

Keywords: Cryptography, Security, Government, Digital Signature, Authentication, Citizen Card, Digital Mobile Key

Resumo

A tendência atual em relação às operações governamentais é avançar para soluções mais eletrónicas, tecnológicas e online para as necessidades do cidadão.

De momento, o governo português oferece várias ferramentas criptográficas de chave pública para autenticação e assinatura digital. Isto é feito por meio de várias tecnologias disponíveis que incluem uma aplicação desktop, uma aplicação móvel e uma extensão para o browser.

No entanto, esse avanço vem com os seus desafios, pois a segurança da informação não pode ser comprometida em favor da eficiência. Com estas soluções, os cidadãos têm de aceitar as condições que lhes são apresentadas. Isso significa que perdem o controlo sobre informações pessoais confidenciais que, se acedidas, podem levar à fraude de identidade. Os cidadãos são obrigados a colocar sua confiança na promessa de segurança feita pelo governo e aceitar o menos que total controlo sobre suas informações pessoais.

Este projecto visa fornecer aos cidadãos uma prova de confiança nos métodos criptográficos mencionados, bem como, eventualmente, propor uma alternativa melhorada e realista para a gestão do controlo do Estado português sobre os serviços prestados.

Esta pesquisa requer uma profunda familiarização com a experiência do utilizador e as informações disponíveis ao público, sendo estas: a documentação fornecida, o código-fonte utilizado para algumas das tecnologias, trabalhos relacionados e até mesmo informações da abordagem de outros países com soluções equivalentes, mas diferentes.

Devido a restrições de tempo e à falta de linhas de comunicação viáveis, o potencial inicial deste projeto nao foi atingido. De qualquer das formas, vários pontos de melhoria foram identificados. Como contribuição para a avaliação da qualidade e da segurança percebida pelo utilizador, este trabalho revelou um esforço sério por parte do governo no desenvolvimento destas ferramentas criptográficas; contudo, revelou também um serviço de apoio minimalista e insuficiente, que carece transparência.

Este estudo é benéfico não só para todos os cidadãos, mas também para o governo, que se deve esforçar para proteger a privacidade da sua população, o que significa que futuro trabalho nesta área é imperativo.

Keywords: Criptografia, Segurança, Governo, Assinatura Digital, Autenticação, Cartão de Cidadão, Chave Móvel Digital

Acknowledgements

Firstly, I would like to thank my supervisor, Professor José Magalhães Cruz, for his guidance and help on the development of this work. I would also like to thank everyone who replied to my incessant emails, calls and questions, your time and help was extremely valuable.

Everyone in both my blood family and my chosen family has played huge part in making me capable of standing up to this challenge, and for that I am eternally grateful.

Lastly I want to thank my friend André, who always believed in me even when I was sure I did not have what it took. Thank you for always helping me when I needed. Thank you for saying you would make time to read my dissertation even though you never got to. And thank you for the great quote.

Maria Teresa Ferreira

“There is an art, it says, or rather, a knack to flying.
The knack lies in learning how to throw yourself at the ground and miss.”

Adam Douglas

Contents

List of Figures

Abbreviations

CA	Certification Authority
CC	Citizen Card
CMD	Chave Móvel Digital
DMK	Digital Mobile Key
DMKS	Digital Mobile Key Service
ICT	Information and Communications Technology
SDK	Software Development Kit
SIM	Subscriber Identity Module
TW4S	Trustworthy System Supporting Server Signing

Chapter 1

Introduction

One of the goals of some current governments worldwide is to make governmental operations increasingly digital. This has many advantages as with an online governance there is a need for fewer workers, people can act directly upon their own needs, and there is a visible reduction of time spent, both on transportation and the operations themselves.

1.1 Context

In this path, the Portuguese government launched two main elements: the *citizen card*, which is a smart card, and the *digital mobile key*. These provide both means for authentication and to perform digital signatures, whose implementations are based on asymmetric cryptography constructions.

To aid the usage of both the citizen card and the digital mobile key, the available means are a desktop application, a mobile application, and a web browser extension, etc. This makes it easy for the common citizen to access all the functionalities they should, provided they have access to a computer, an Internet connection, and, for the citizen card related functionalities, a smart card reader.

Despite the appeal provided by these technologies' comfort, one must not forget the security aspects that might have been slacked to achieve them. In regards to these solutions, the citizen is forced to place their sensitive information on the hands of the Portuguese government.

1.2 Motivation

Every citizen who has the ability to use those tools, should strive to get involved with anything that influences their lives directly, but even more so if it impacts their personal information security.

The authentication and digital signature methods mentioned are only possible with the storage, use, and manipulation of sensitive personal data which, if compromised, can lead to several security breaches such as the ability of impersonation with non-repudiation. This means the security of the data is essential for the usage of the technologies provided.

In addition to this, some of the documentation provided by the government has not been updated in several years. This takes even more of the control away from the user as they are left with somewhat incomplete information that does not allow for a deep familiarization with the risks being taken.

Furthermore, the available documentation is quite obscure and incomplete, limiting the benefit that the common user can take from them. Only someone with experience in the area can understand what is being shared by the government.

1.3 Objectives

The aim of this thesis is twofold. Firstly, there is a goal to assess the trust the government forces the citizens to have. It places few to no choices on their hands when it comes to these cryptographic solutions, so an evaluation will be made regarding if it is actually well-deserved trust, meaning no actual significant risks are being taken.

Secondly, exploring the malleability of the functionalities available. This means evaluating the level of independence a user can achieve and the level of adaptability of these functionalities for each citizen's specific needs and wants.

1.4 Document Structure

The present document is organized into seven main chapters. In the Introduction, the context, motivation and objectives are covered, as well as the document structure, the current section. In the State of the Art chapter, firstly the background section encompasses an exposition of the technologies provided by the government, them being the Citizen Card and the Digital Mobile Key, as well as a brief summary of the functionalities provided by the desktop application middleware. Still in the State of the Art chapter, the case of Estonia is developed as comparison to Portugal, in the Existing technologies section. The third chapter exposes the Problem and the Solution found. The following chapter, titled Implementation, summarizes the practical experiments made on the available SDK code and all the hurdles that were found.

The Questions chapter exposes all the questions that were posed at the beginning of this work and the ones that were answered have the corresponding answer justifications and clarifications.

In the Survey chapter, the questions and answers of the conducted survey are displayed and analysed. It is composed of the sections Survey Questions, Survey Answers, Data Bias, and Survey Conclusions, and it is followed by the last and final chapter that presents the Conclusions of this work and Future Work to be developed.

Chapter 2

State of the Art

Technology is an ever-growing field, and, with this, there is no single correct answer for a specific problem or situation.

Different governments, different companies, or even different developers, despite the fact that all are probably striving to keep user information secure, might take different approaches. This is even more aggravated by the development of more powerful machines, new technologies, new needs for online solutions, and a better common understanding of technology by the general public, which makes constant change and improvement a must.

2.1 Background

Currently, the Portuguese citizens have at their disposal two major technologies: the Citizen Card and the Digital Mobile Key (in portuguese Chave Móvel Digital, or CMD). Both allow for authentication and for digital signatures.

2.1.1 Citizen Card

The Citizen Card (CC) is an authentic document that stores information relevant to the identification of a citizen. The card stores data, both authentication and signature digital certificates, and some applications that are useful for the usage of the card, as is shown in figure 2.1.

The three applications present in the CC are as follows:

- IAS (no specification of this abbreviation was given in the documentation [4]): application responsible for the authentication and digital signature operations; its usage is pin protected;

- EMV-CAP (no specification of this abbreviation was given in the documentation [4]): application responsible for the generation of unique passwords through alternative channels such as by cellphone, for example; its usage is also pin protected; EMV-CAP stands for Europay, Mastercard, and Visa - Chip Authentication Program and it is a solution that was initially used by banks to mitigate online fraud regarding their operations;

- Match-On-Card: application responsible for the biometric verification of the digital fingerprints; this is not pin protected.

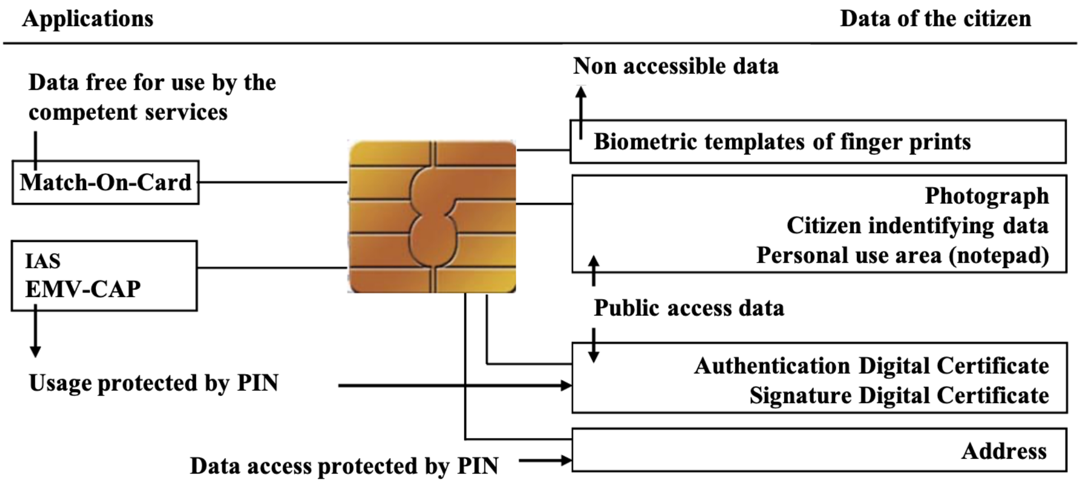

Applications
Data of the citizen
Data free for use by the competent services
Match-On-Card
IAS
EMV-CAP
Usage protected by PIN
Data access protected by PIN
Non accessible data
Biometric templates of finger prints
Photograph
Citizen indentifying data
Personal use area (notepad)
Public access data
Authentication Digital Certificate
Signature Digital Certificate
Address

Figure 2.1: Smart card chip components and respective accessibility [1]

The digital certificates present in the chip are the elements that provide the cryptographic guarantees of security promised as well as the private keys. Despite the fact that in the documentation there were no indicators of the presence of the private key in the chip, in order for the operations promised to be possible, these keys are mandatory. This reflects a lack of transparency in the documentation.

The trust that users put upon these certificates stems from Certification Authorities (CA). These authorities are entities that hierarchically guarantee that the information present in the certificates, namely the public key that corresponds to that specific user.

In the past, the chain of trust was also composed of private entities, as the root CA was a private Portuguese company named "Multicert". This constituted a possible vulnerability as it is very difficult to guarantee anything once the service was outsourced outside the jurisdiction of the government.

However, this vulnerability has already been addressed, as every certificate emitted since April 2020 is now part of a fully state-run chain of trust. Both the new and old root certificates are available for installation [5].

2.1.2 Digital Mobile Key

The Digital Mobile Key (CMD) is a technology implemented in 2015 that allows authentication and digital signatures certified by the Portuguese State, and everything is done with a single login.

It associates a cell phone number (SIM card), or an email address, to the civil identification number of each Portuguese citizen and the passport or title or card of residence for foreign citizens. [1]

The practical information available revolves around activating the DMK, using its functionalities, and some "Frequently Asked Questions". In addition to this, there is some documentation available regarding operation practices, general conditions of usage, and policies for qualified signing.

The user can activate the DMK with their CC, and for that, they need a card reader and the authentication PIN given with the CC, or they can do it through the Portuguese finances portal if they have the Fiscal Identification Number and access passphrase. If none of these options are suitable, the users can also activate their DMK in person.

The security of the DMK is based upon two codes: the PIN the user introduces upon the activation of the DMK and a code that is received through text message to the associated SIM card. All the activities regarding this technology, such as emission, activation, usage, and revocation, are handled by the Service of the Digital Mobile Key (SDMK).

The SDMK is a Trustworthy System Supporting Server Signing (TW4S), which means the digital signing operations are done on the server and not on an environment controlled by the user. This means the private keys that are needed for the operations are obligatorily handled by a remote entity that provides that service.

The SDMK encompasses the following entities:

1. Registration entity;

2. Certification entity;

3. Key pair generation and safekeeping entity;

4. Qualified signature generation entity;

5. Key pair holder, also known as signer;

6. Trusting part, also known as recipient.

Regarding the technical documentation, many times the clarifications are busy with acronyms that make the reading and interpretation hard, and it is frequent that the processes are only said to be "safe", "trusted", or "secure" and do not disclose anything more about the basis of that said safety.

The documentation available presents the steps of the protocols implemented and these follow standardized procedures that are said to allow a high level of security. In these steps, however, the same lack of depth is present and the more technical aspects do not include deeper specification than for example referring to a "Hardware Security Module".

2.1.3 Desktop Application Interface

For easy access to the functionalities promised, the users have at their disposal some applications; however for the purpose of this research the focus will be mainly on the desktop application, despite this, some contrast with the mobile application functionalities is also mentioned. There is a comprehensive middleware manual available for user consultation [6] that aims to aid the interpretation of the functionalities implemented.

The application has three main options:

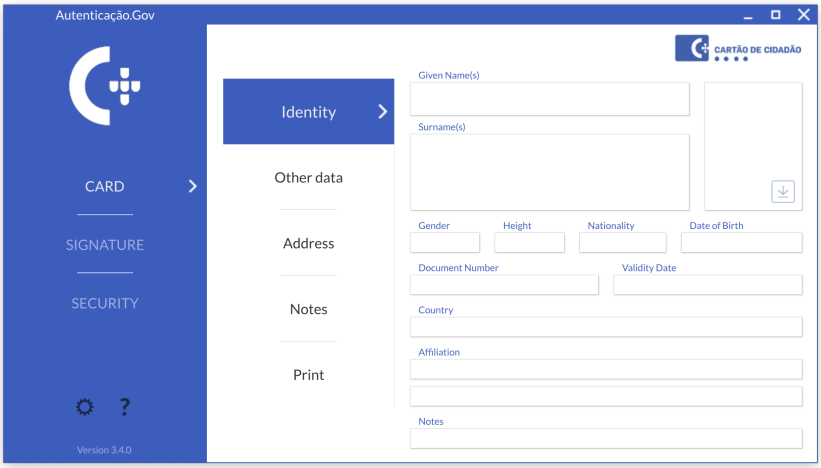


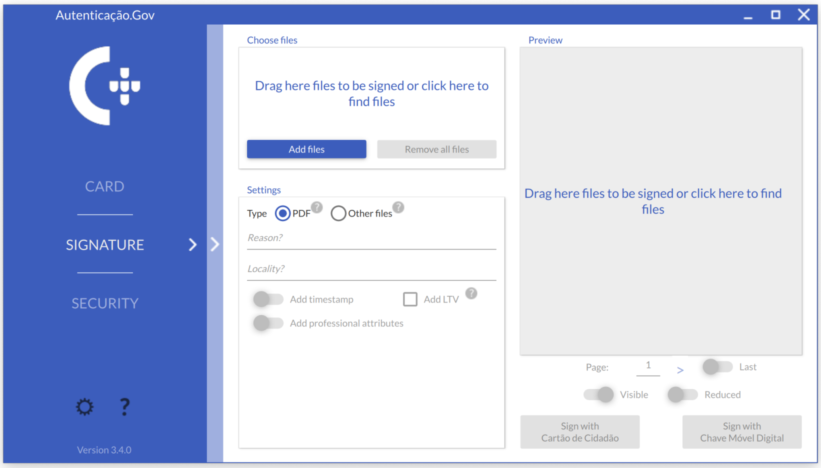
Figure 2.2: Desktop Application User Interface - Citizen Card Option

The Card menu option allows the user to access "all" the personal data stored in the card chip. This includes information like full name, height, document number, date of birth. The address field is pin protected, which allows for an increased level of security if the card is lost and accessed by an unknown party. This section also grants access to a personal notes field that can be edited with a PIN, and an interface for printing is also present. The general interface is as is shown in figure 2.2.

The Signature menu option features a "drag and drop" area that allows for the digital signing of one or more files (PDF or other). The signing can be done through both the Citizen Card or the Digital Mobile Key. The interface is as shown in figure 2.3.

The Security menu option allows the user to access their certificates and check the information regarding the certificates, such as the chain of trust, and also download the certificates as files. This option also includes an area where one can test and modify the three personal pin codes regarding: authentication, digital signing, and the pin to access the address information field. The interface is as is shown in figure 2.4.

As a point of contrast, the mobile application allows for the access of the periodic digital mobile key codes, as well as giving access to pending authorizations and allowing for authentication through QR Code. The mobile app cannot be screenshot due to the presence of the sensitive codes



Drag here files to be signed or click here to find files

Drag here files to be signed or click here to find files

Figure 2.3: Desktop Application User Interface - Digital Signature Option

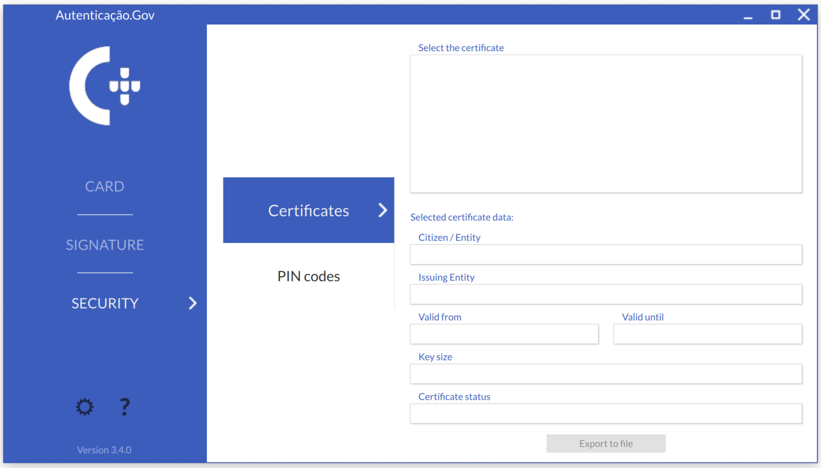


Figure 2.4: Desktop Application User Interface - Security Option

shown, which guarantees some safety regarding the possibility of some user induced vulnerabilities. However, this safety measure can easily be bypassed by taking a photograph of the screen, for example.

2.2 Existing technologies

One way of analysing the approach of the Portuguese government, is comparing and contrasting with the solutions chosen and implemented by other nations. Several countries have been walking towards the adoption of new and more comprehensive integration of online government.

According to the United Nations' E-Government Survey for 2020, the top performers in e-government development are Denmark, the Republic of Korea, Estonia, Finland, Australia, Sweden, the United Kingdom of Great Britain and Northern Ireland, New Zealand, the United States of America, the Netherlands, Singapore, Iceland, Norway and Japan. [7]

Following is an exposition of the country that is placed at the top of the survey.

2.2.1 Estonia

Estonia is sometimes considered the most advanced digital society in the world, and, at the moment, it has 99% of its governmental services online. They also have the goal of serving as an example of success, aiming to inspire other to follow their almost full digital integration of services. [8] Estonia places at the top of the ranking when it comes to this topic, and this has been the case for some time; however, they have had some struggles in the process. [9]

The Estonian implementation focuses on the X-Road, a software solution that interacts with both the public and private sectors and that allows interoperability of services by over 1000 organisations, [8][9] this structure is depicted in figure 2.5. The X-Road is federated, which means there is the possibility for a direct relationship between each part.[8]

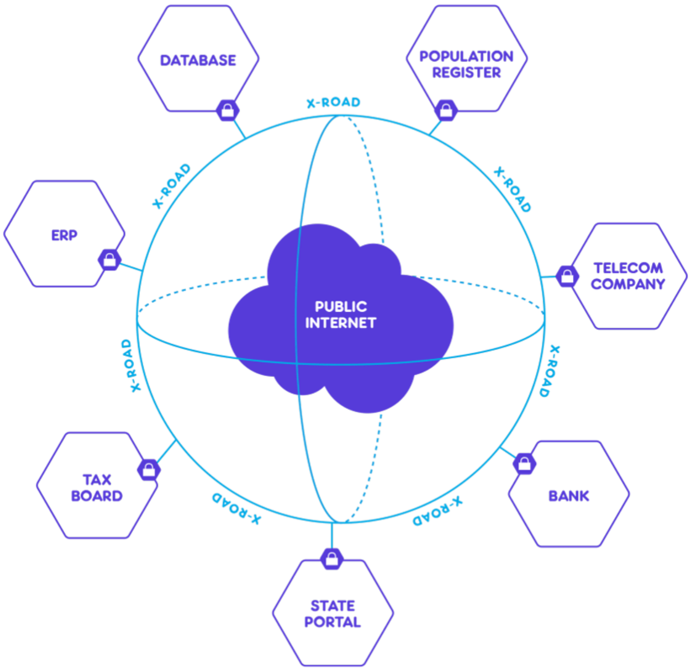


Figure 2.5: X-Road: data exchange layer visualization [2]

In Portugal there is no fully integrated structure, and the Estonian solutions that can be easily paralleled with the Portuguese ones are the ID-card and the Mobile-ID.

The Estonian ID-card is a "smart" identity card, with the digital certificates needed for the features it allows.

The Mobile-ID, similarly to the Digital Mobile Key, allows citizens to authenticate themselves and issue digital signatures through their phone, with a SIM card. [10]

These implementations have had vulnerabilities such as issuing the same private key for different users, or inclusion of information in the certificates that allowed for the retrieval of the private key.[11] These instances underline even more deeply the need to look with a critical eye even at government-approved technologies.

2.2.2 Denmark

In Denmark, the approach taken relies on the "Easy-ID". This was implemented in 2007, and it is a single digital key that allows the citizens to access all the integrated features available that span both the public and private sectors.

Denmark attributes its great success to mainly two factors: the symbiotic relationship between public and private, and most importantly, the trust the population has in the government. [12]

The Easy-ID allows authentication in several portals, and this is done through the User ID, password, and a code. This code is taken from a physical user code card that can be seen in figure 2.6 , and it contains user-specific single-use codes. This duality of online paired with the codes is said to provide strong security. [13]

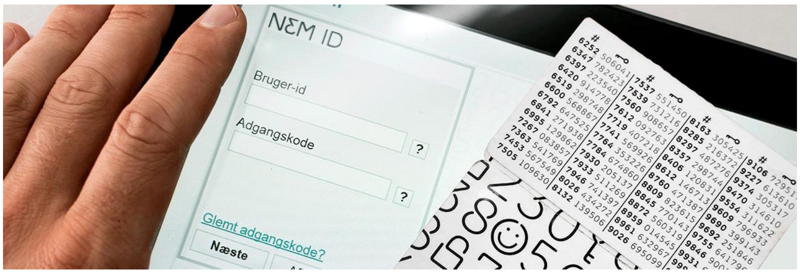


Figure 2.6: Visualization of the needed information for digital authentication in Denmark [3]

Despite the fact Denmark has one of the most deeply integrated digital governments, it is still said that users experience several difficulties. [14] Despite this, the number of users is relatively high, which might not mean the system is well implemented and beneficial to the population and might only represent the mandatory use some actions require. [15]

There was no information found regarding technologies that would provide the citizens of Denmark with the ability to issue digital signatures neither locally, as is done with the CC, or remotely, as is done with the DMK.

2.2.3 Republic of Korea

Despite ranking high regarding the level of digital governance implementation, the fact that South Korea is not part of the European Union makes the information taken from its study more limited. The European Union has legislation covering digital safety measures that Portugal, as well as

Estonia and Denmark, have to follow in order to achieve the minimum sectary enforced for the EU members.

Korea has been implementing an extensive Information and Communications Technology (ICT) infrastructure. The components include:

1. On-nara BPS: a platform that processes the government's work;
2. dBrain: a platform that handles all governmental financial management activities;
3. GIDC: which stands for Government Integrated Data Center and is a platform that integrates the management and operation of national IT resources. [16]

Regarding digital identification, South Korea has not developed a system similar to the ones mentioned previously. Its digitization focuses more on the administrative side and not on user interaction. However, there are active plans to implement a digital ID system that makes use of technologies such as blockchain and biometrics . [17]

2.2.4 Conclusion

Despite the different approaches chosen by the different states, the one factor mentioned throughout all the documentation assessed was trust. Only states that have the trust of the citizens can successfully develop a more integrated system that functions as wanted.

In addition to this, the only country that entirely mirrored the implementation chosen by Portugal is Estonia. This country has an equivalent for both the CC and the DMK, which makes its study the most relevant for the case at hand.

Chapter 3

Problem and proposed solution

The concept of security, when it comes to technology, is relative. For one to decide if something is secure or not, one needs to restrain the scope of the wanted results.

Firstly, the attack model, that defines the power of the attackers. This includes their capabilities of data storage, their capabilities of interaction with the system, and their computational power. These aspects need to be re-analyzed periodically, because as time passes and technological improvements are made, the attack model needs to keep up with the advancements and adapt to constantly more powerful attacks.

Secondly, the security goal needs to be defined. This means specifying what consists of a security breach. The security goal varies mainly on the level of importance one gives to that determined technology, meaning that higher risk elements, will have more ambitious and comprehensive security goals.

Both the attack model and the security goal create the security model, and it is by this security model that one can evaluate if a construction is secure or if it has exploitable vulnerabilities. This also means that we can only have perfect security in theory, and in practice this concept is impossible to achieve.

When it comes to the security of the cryptographic solutions available through the Citizen Card and the Digital Mobile Key, the security model is not always clear and one must fully trust the government is not only making the right choices for all, but also keeping up with the advancements and changes made through time.

3.1 Problem

In regards to the user experience, the biggest problem identified is transparency. Despite having extensive documentation available for the citizen card and its functionalities, mostly regarding common usage practices, and having some documentation for the Digital Mobile Key, there are many questions that still remain unanswered. In order to require trust from the citizens, the state needs to have full transparency concerning each implementation and each step that includes the private key and digital certificates.

In addition to this, it is only logical that user-focused documentation would not include full depth of the elements it covers, as the common citizen would have little to no knowledge to decipher the meaning of technical exposition. But, in most cases there is no redirection to comprehensive documentation that could end up elaborating on all details, if wanted.

The most relevant unanswered questions regarding the Citizen Card are as follows:

- How is the key pair generated?
- How is the key pair inserted in the citizen card?, or
- Is it generated directly onto the card?
- If not, is it safely erased from where it was generated?
- How can the users guarantee it has been successfully deleted and that there are no copies, other than their own, of their private key?
- How can the users control the data stored in the chip of their citizen card, to their specific needs and wants?

The most relevant unanswered questions regarding the Digital Mobile Key are as follows:

- How is the key pair generated?
- How is the key pair stored?
- How is the key pair accessed?
- What is the server side asymmetric key pair generation protocol being used?
- Why are some of the functionalities of the desktop app still not available for public use?
- How is the confirmation SMS code being generated?
- What type of control and access do the people with administrator roles have?
- What are the Hardware Security Module specifications?
- Is it possible for a user to replace their remotely-generated key pair, by a pair generated under their own control?

The questions previously identified reflect the lack of transparency that these services have. Considering that misuse of this information can have grave consequences, the users should have much more knowledge and control over their identifiers.

Heuristic security in the cryptography field is the confidence one can put upon something that is being analysed by the whole community. Despite the fact that it might be counter intuitive to have something be safer if it is more public, full access of the general population allows for a much more exhaustive scrutiny by knowledgeable individuals.

For these solutions to be safe, the only thing private should be the private key of the citizen. All the rest should be public as it would ideally not divulge any information that compromises security of anything. The state, by not sharing everything is not only reducing the heuristic security level but also is removing independence from the users. This secrecy also might make the citizens less inclined to use the Citizen Card and the Digital Mobile Key as it can reduce the general perceived trustworthiness. [18]

3.2 Solution

The solution to the problem is threefold. Firstly, the approach adopted includes a deep familiarization with the user experience. This is truly important as it reflects the communication channels being established with the users. Included in this step is a study of all the usage guidelines provided by the government and all the technical documentation available, as well as interacting with the relevant organizations in order to get some possible clarifications regarding some aspects not addressed previously.

Secondly, there will be an evaluation of the practical dimension. An exploration of the available source code and SDK, paired with the development of an interface that allows access and use of, as much of the user information as possible, directly from the Citizen Card.

Lastly, the goal is to gather the answers to as much of the questions posed as possible. This is not only useful for the answers themselves, as the information is not readily available, but also to allow a more comprehensive understanding of the lack of transparency at hand. The inability to gather all answers is a deep indicator of communication problems with the users.

Chapter 4

Implementation

With the aim of assessing the control that users have over their Citizen Card and its functionalities, it was crucial to perform accessibility and malleability testing. This was done by using the Software Developing Kit available at the official GitHub repository[6].

The programming languages available in the SDK are C++, Java and C#. Despite each language having its strong and weak points C++ was chosen for this assessment as the base code was done in C++. The transition to other languages was done by using wrappers. This choice was made in order to try to mitigate future problems that might surface.

4.1 Objectives

The main objective of this phase was to mimic the official Middleware Desktop Application. This was done to find out if the code provided would not only be useful but also to assess if the user could create his/her own replacement application.

The ability to do so would prove that the user actually has some control over how the information present in the chip of their Citizen Card is accessed and used.

The available categories of functionalities, in order of complexity, are as follows:

- Access elements without a PIN code, for example, name and height;
- Access elements with a PIN code, for example, address and edit notes;
- Access and use the digital signature certificate.

4.2 Results

4.2.1 Elements without PIN code

This category was easily implemented. The code provided was straightforward and the documentation was clear and useful.

The elements accessed were the ones referring to national citizens and they are as follows:

- Given names
- Surnames
- Gender
- Height
- Nationality
- Date of Birth
- Document Number
- Expiration date
- Country
- Father
- Mother
- Accidental Indications (optional)
- Photo (download)
- Tax Number
- Social Security Number
- Health Number
- Document Version
- Emission Date
- Issuing Entity
- Document Type
- Local of Request
- Validation

4.2.2 Elements with PIN code

The functionalities available under this category are:

- Edit and Save Notes
- Access Address
  - Country code (ISO3166 format)
  - District
  - District code
  - Municipality
  - Municipality code
  - Civil Parish
  - Civil Parish code
  - Street type
  - Street type abbreviation
  - Street Name
  - Building type
  - Door number
  - Floor
  - Side
  - Locality
  - Zip4
  - Zip3
  - Postal Locality
  - Is National Address
  - Generated Address Code

This section proved to have its share of complications that needed to be overcome.

Firstly, these functionalities require the establishment of communication with the governmental server for the PIN to be verified; servers on which the user PIN codes are stored. The documentation [19] regarding these actions was quite vague and the code without alterations did not run [6].

As the documentation seemed to be incomplete, the error message printed did not correspond to the errors listed in the documentation[6], and as the code was being used exactly as was said on the SDK, there was doubt if the error was not from the SDK's side.

In order to get some guidance and answers, several emails were sent both to the Agency of Administrative Modernization (in Portuguese "Agência para a Modernização Administrativa") and to several of the contributors listed on the official repository. These emails are listed in Appendix A. The email presented the code that at the time was shown in the SDK manual with the example of accessing the Municipality field, shown bellow:

```
PTEID_EIDCard &card;
unsigned long triesLeft;
//(...)
PTEID_Pins pins = card.getPins();
PTEID_Pin pin = pins.getPinByPinRef(PTEID_Pin.ADDR_PIN);
if (pin.verifyPin("", &triesLeft, true){
        PTEID_Address &addr =  card.getAddr();
        const char * municipio =  addr.getMunicipality();
}
```

Tracing back the error message only pointed to a function of the header file marked with

```
/**< Copy not allowed - not implemented */
```

This situation was fully explained in the email, however the answer received only included links to the official repository and the suggestion to open an issue on the subject.

A few days latter, another answer from the same entity was received and it said that the code previously mentioned had been fixed and the repository was updated. The new and revised version of the code was as follows:

```
PTEID_EIDCard &card;
unsigned long triesLeft;
//(...)
PTEID_Pins &pins = card.getPins();
PTEID_Pin &pin = pins.getPinByPinRef(PTEID_Pin.ADDR_PIN);
if (pin.verifyPin("", &triesLeft, true)){
    PTEID_Address &addr =  card.getAddr();
    const char * municipio =  addr.getMunicipality();
}
```

This solution still did not work and displayed similar errors as before.

Upon further analysis and study of the code, a working solution was developed:

```
PTEID_EIDCard &card;
unsigned long triesLeft;
PTEID_Pins &pins = card.getPins();
PTEID_Pin &pin = pins.getPinByPinRef(PTEID_Pin::ADDR_PIN);
if (pin.verifyPin("", triesLeft, true)){
    PTEID_Address &addr =  card.getAddr();
}
```

Following this breakthrough, another contact was made, in order to inform that the new version still did not work, and the working version was attached. **For this contact no answer was received.**

All functionalities in this category were finally implemented.

4.2.3 Digital Signature

This phase of testing corresponded to trying to sign documents digitally, and this action is also protected by a PIN number.

This step was not fully implemented due to several reasons. Firstly, the code presented in the documentation did not work as intended; then, there was no testing platform or mode through which these functions could be tested; and, lastly, although there was no answer to the request given.

Despite the documentation saying there was a testing mode, no further information is available anywhere else. Information such as how is the test mode used and what are its capabilities and limits where not found, and these questions **got no answer upon email contacts**.

These conditions meant that, for testing purposes, personal cards with sensitive, real information had to be used, which is, in itself, a liability. A trial with the author's own card lead to the blocking of the digital signature PIN code, upon inserting the PIN number regarding digital signatures. This action was not paired with any error message, which meant that there was no way of tracing back to the root of the problem. Another personal card was tested and the outcome was the same.

To control this situation there was an attempt to unlock the PIN code, in order to continue with this evaluation, however this was not possible due to the characteristics of the card and a fully new card would have to be issued. Even in this case, it would be a last-resort solution that would possibly only allow for one more try as there was no indication that the same outcome would not repeat itself. This option was, however, not feasible, as the only available scheduling slots were in the month of July, which was not compatible with the timeline of the current study.

In addition to this, an issue was opened in the GitHub section that addressed two problems: why is the GitHub code provided blocking the digital signature PIN?, and is there a way to test the code without having to use real, valid cards?

The issue was quickly answered by a contributor in the official repository, where the answer given was that the PIN must already have been blocked. This was not the case as the cards used were previously tested in the Desktop Application provided, where there was no problem with any PINs. This information was added to the issue and much later there was finally an answer. The answer included how to unlock the PIN, some information on the availability of testing cards and also the link[20] to where SDK application examples had been added in the meantime.

The option to unlock the PIN had already been explored and was not feasible, like was mentioned previously. The testing cards had also been explored, however only on an authentication testing model, which means that for this case the card obtained was not useful, and further exploration of this option was not possible due to time constraints, as this answer was only given on the . The example implementations present on the GitHub repository were also not thoroughly explored due to time constraints.

4.3 Authentication

This functionality allows for the users to login onto some specific platforms with their Citizen Card. This includes some public and private portals that have adhered to this functionality.

For this case, it was not possible to test this solution, as it is not available to the general public.

Chapter 5

Questions

In this section there will be further analysis of each of the questions presented to the entity that has authority over the SDK, Agency of Administrative Modernization, and the development and maintenance of the CC and DMK. Each question will be followed by the information found on the topic, coupled with the implications of that information.

5.1 Citizen Card questions

5.1.1 How is the key pair generated?

The key pair is generated directly onto the Citizen Card.

5.1.2 How is the key pair inserted in the citizen card?

The key pair is generated directly onto the Citizen Card.

5.1.3 Is the key pair generated directly onto the card?

Yes.

5.1.4 If the pair is not generated directly onto the card, is it safely erased from where it was generated?

Currently without answer.

5.1.5 How can the users guarantee it has been successfully deleted and that there are no copies, other than their own, of their private key?

Currently without answer.

5.1.6 How can the users control the data stored in the chip of their citizen card, to their specific needs and wants?

Currently without answer.

5.2 Digital Mobile Key questions

5.2.1 How is the key pair generated?

The information regarding this topic was found on the document Declaration of Practices of DMKS Operations [19].

Here it is said that the key generation process is activated as soon as the qualified certificate is solicited.

The key pair is generated in cryptographic hardware kept in the server, from where the information cannot be removed. The key pair generation and the certificate emission function as an atomic process. These security claims are made due to the fact that the FIPS 140-2 level 3 and/or Common Criteria EAL 4+ are being followed.

FIPS 140-2 is used as a test to measure the quality and usability of pseudo random number generators [21][22]. This is done to guarantee the randomness level of the values being used, which can compromise the security of the key pair. Level 3 security refers to the strength of the cryptographic primitive. This means some aspects are guaranteed such as, for example, security mechanisms that detect physical tampering or the requirement of identity-based authentication [23].

Common Criteria is an international security standard for certification. In this case, the EAL, or Evaluation Assurance Level needs to at least follow the level 4+ criteria. This means it was "Methodically Designed, Tested, and Reviewed" [24].

5.2.2 How is the key pair stored?

The information regarding this topic was found on the document Declaration of Practices of DMKS Operations [19].

Due to the fact that the DMK's key pair is never in the user's possession, it needs to be safely physically stored on governmental facilities.

All the sensitive data is stored in a Data Center in Lisbon and several rules are followed. These rules include wall, ceiling and floor material specifications, lack of window, and door specifications. These facilities have an uninterrupted power supply with redundancy in case of failure.

There are also guidelines for accessing the rooms, and only high level clearance individuals can actually enter. There are also physical markers that show if an element has been tampered with.

There are also emergency protocols in place that, in extreme cases, lead to the full destruction of the data. The data is also destroyed after the corresponding certificate expires.

5.2.3 How is the key pair accessed?

The key pair is only accessed through the TW4S. This protocol is thoroughly explained on the document Declaration of Practices of DMKS Operations [19].

5.2.4 What is the server side asymmetric key pair generation protocol being used

Currently without answer.

5.2.5 Why are some of the functionalities of the desktop app still not available for public use?

Upon contacting the competent authorities in order to gather information on this topic, the answer gotten was that there are several interfaces available.

The interfaces mentioned were the SDK, Webservices, SAML, and oAuth. Further information would be given if requested regarding which API would be of use for specific needs.

There was no reference made to the want of keeping any functionalities exclusive to the government.

5.2.6 How is the confirmation SMS code being generated?

Currently without answer.

5.2.7 What type of control and access do the people with administrator roles have?

The stored keys are protected with a user-created pin that is added when the user requests the DMK certificate. This means that the information is stored safely.

However, when a user issues a request, for instance, upon requesting the the certificate, the pin is inserted by the user and that information is directly used by the system. This is a risk that is taken based on the fact that the workers are good-natured employees that will not exploit this access.

In addition to this, only a small amount of employees is cleared for that type of access.

This information and the specification of each group of worker, including their functionalities and accesses can be found on the document Declaration of Practices of DMKS Operations [19].

5.2.8 What are the Hardware Security Module specifications?

Upon reviewing the documentation and contacting the competent authorities in order to gather information on this topic, the answer gotten was that the specifications are not available for the public.

This data is kept private as it is seen as liability, however, the system is audited by an external entity regularly.

5.2.9 Is it possible for a user to replace their remotely-generated key pair, by a pair generated under their own control?

Upon contacting the competent authorities it became clear that this is not possible.

A user can ask for the key pair to be replaced and in that case, a new pair will be generated and the respective certificate will be replaced by an updated one.

This means that it is mandatory that the conditions under which the key pair is generated are the ones provided by the government. This can be perceived as positive or negative, however the user is always forced to relinquish their control of the key generation in order to make use of this service.

Chapter 6

Survey

For the benefit of further understanding the perception of the users regarding the topics at hand, a survey containing three questions was elaborated[25]. The aim of this survey is to briefly collect the opinions and experiences of a number of people in order to confirm if the previously assumed perspective of trust in the governmental services was indeed backed up by true experiences.

The survey was sent by email to over nine thousand students (9016), however participant intake was cut off at three hundred answers.

In this section there will be a full presentation of both the questions and answers received as well as the conclusions taken from the extracted data.

The survey was titled "Citizen perception in regards to the cryptographic solutions made available by the Portuguese Government". The introductory text presented aimed to briefly describe the subject under analysis. It read *"Nowadays, any Portuguese citizen, can use their Citizen Card or Digital Mobile Key to generate digital signatures or to authenticate themselves in certain platforms."*

6.1 Survey questions

The survey was elaborated in order to shortly gather relevant information and for this, there were created four questions. Survey screenshots can be found in Appendix B.

The questions and their respective possible answers are as follows:

- Age
  - < 18
  - 18 - 25
  - 26 - 35
  - > 35

- EXPERIENCE: Select the options that apply to your experience with these solutions
  - In the past, I have used the Citizen Card to digitally authenticate myself;
  - In the past, I have used the Citizen Card to digitally sign documents;
  - In the past, I have used the Digital Mobile Key to digitally authenticate myself;
  - In the past, I have used the Digital Mobile Key to digitally sign documents;
  - I have never used any of these solutions.
- PERCEPTION: Select the option that applies to your perception of these solutions
  - I trust that all my personal information is being handled with 100% security;
  - I believe that my information is being handled with enough security;
  - I believe that more could be done, in terms of security, regarding the usage and treatment of my personal information;
  - I believe these solutions are not safe;
  - I feel I do not know enough in order to analyse the security of these solutions.
- INFORMATION: Select the options that better apply to your perception of the accessibility of the information that is available regarding these solutions
  - In the past, I have analysed available documentation and got the answers I needed;
  - In the past, I have analysed available documentation, but I did not get the answers I needed;
  - In the past, I have contacted a competent authority and got the answers I needed;
  - In the past, I have contacted a competent authority, but I did not get the answers I needed;
  - I have never felt the need to further inform myself on these solutions.

The first question aims to gather information on the demographic data of the survey participants. This is relevant, as different age groups react differently to technology and the informatization of governmental resources.

The dimensions of the next questions are three-fold: experience, perception, and information. These three questions allow to assess if the user has come in contact with the functionalities under study, if the user has an overall good impression of the security regarding these functionalities, and lastly if the user has had the need to gather further information and if they were successful in doing so.

6.2 Survey answers

The answers of the three hundred participants were gathered and used to generate the following graphics:

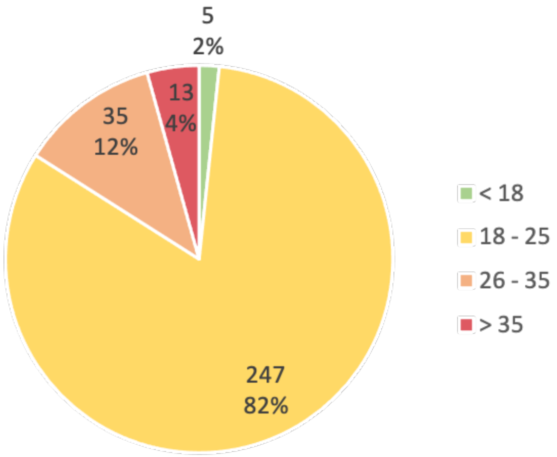


Figure 6.1: Answers received to survey question *"Age"*

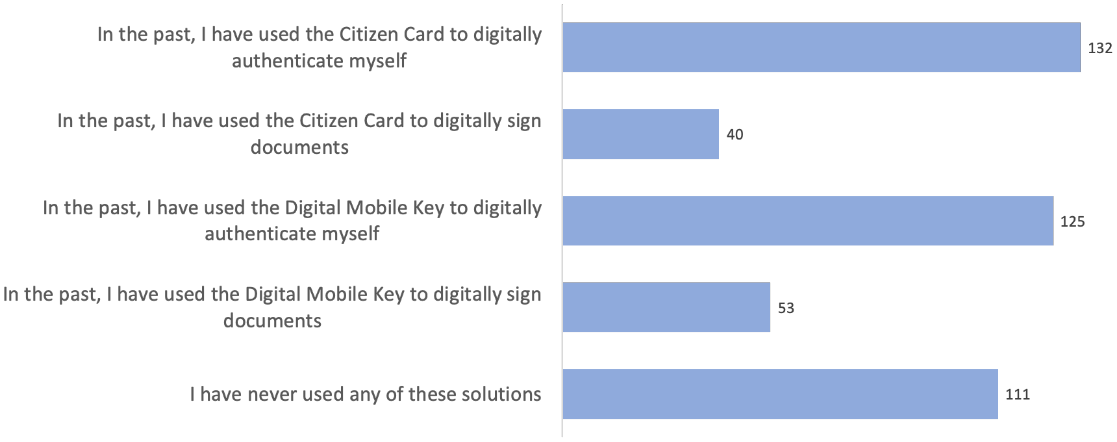


Figure 6.2: Answers received to survey question *"EXPERIENCE: Select the options that apply to your experience with these solutions"*

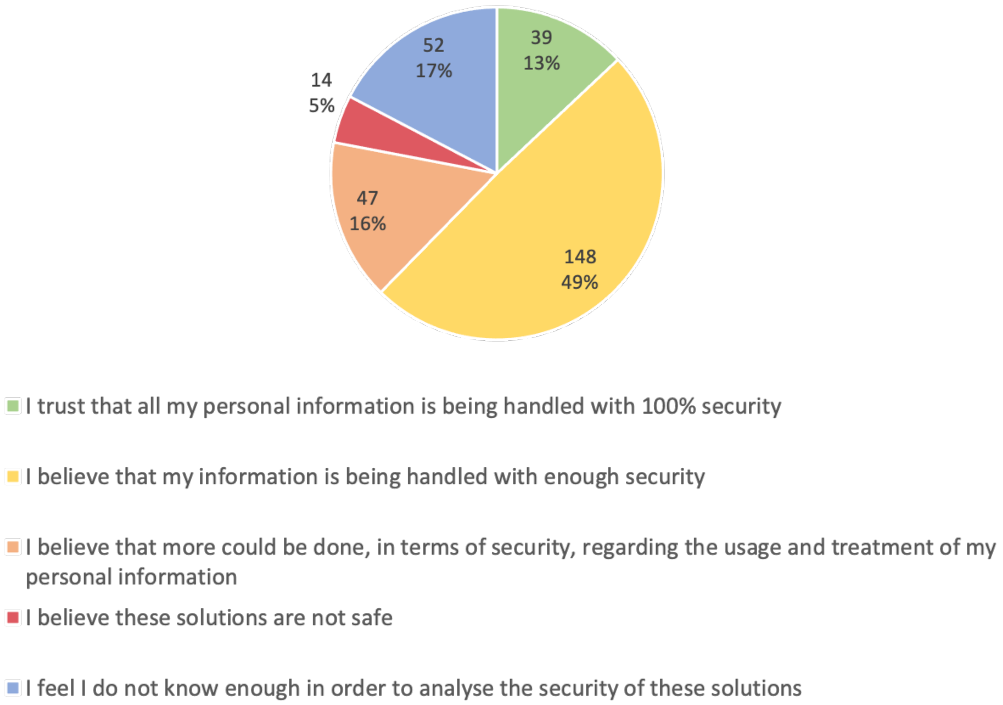


Figure 6.3: Answers received to survey question *"PERCEPTION: Select the option that applies to your perception of these solutions"*

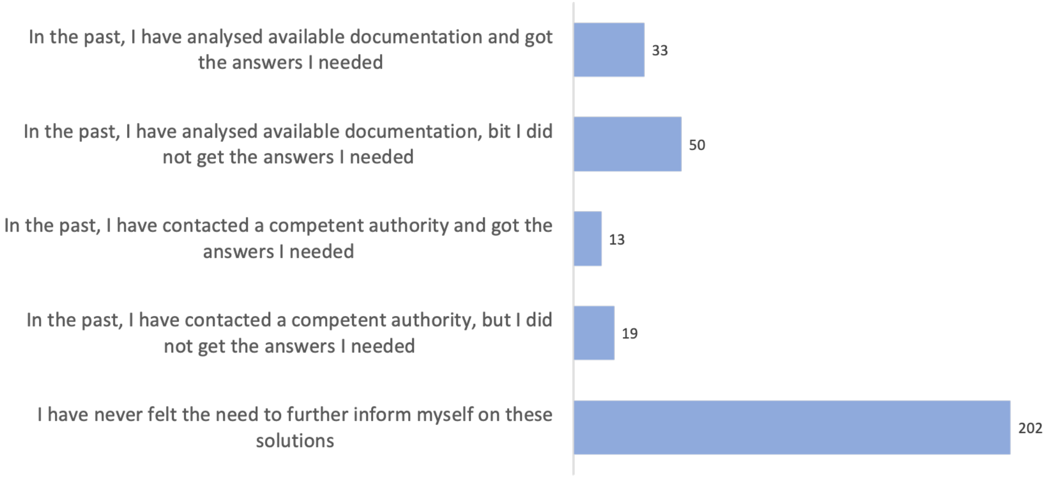


Figure 6.4: Answers received to survey question *"INFORMATION: Select the options that better apply to your perception of the accessibility of the information that is available regarding these solutions"*

6.3 Data bias

Despite striving for impartiality, it is relevant to mention that this survey was spread by institutional email. This means the participant pool is biased towards Engineering students, meaning that the survey takers might be more educated in technological aspects and might have better understanding of software than the general public.

6.4 Survey conclusions

The conducted survey was useful to gather information of the perception of the public and their trust on the services under study.

The first question allowed for the confirmation of the demographic sapmple. Most of the people that took part in this study are young and most-likely have a good understanding of technology. This means that the engagement rate represented from the second to last questions might not be a fully accurate representation of the general public. With this said, the users gathered in this survey are most-likely familiar with these technologies which makes their input and experiences extremely valuable.

The second question, the one regarding experience, shows that a little under two thirds of the participants have used the solutions under study. Despite the numbers for digital authentication being much higher that those of digital signatures, all solutions had positive answers.

This information assures that the answers to the questions that followed in the survey portrayed a diverse array of experiences and not a single specific solution.

The third question, the one regarding perception, shows that almost half of the survey participants believe that their information is being handled with enough security. Despite this being a positive answer, it is also indicative that many people do not fully trust the government's solutions.

This assumption is also backed up by the fact that only 13% of the answers reflected full trust. On a service with complete user transparency, the percentage of users with absolute trust on the service is expected to be higher.

Lastly, on the question regarding information, it is possible to see that the big majority of people have had no contact with the competent authorities and have had no need to search for lacking information on the documentation. This is a positive sign, however, regarding the people who have had issues and have had the need and curiosity to search for further information, the ration between those who actually were satisfied with the information is alarming.

When considering only the people who have analysed the documentation, it is possible to see that 60% of those people did not get the answers they were looking for.

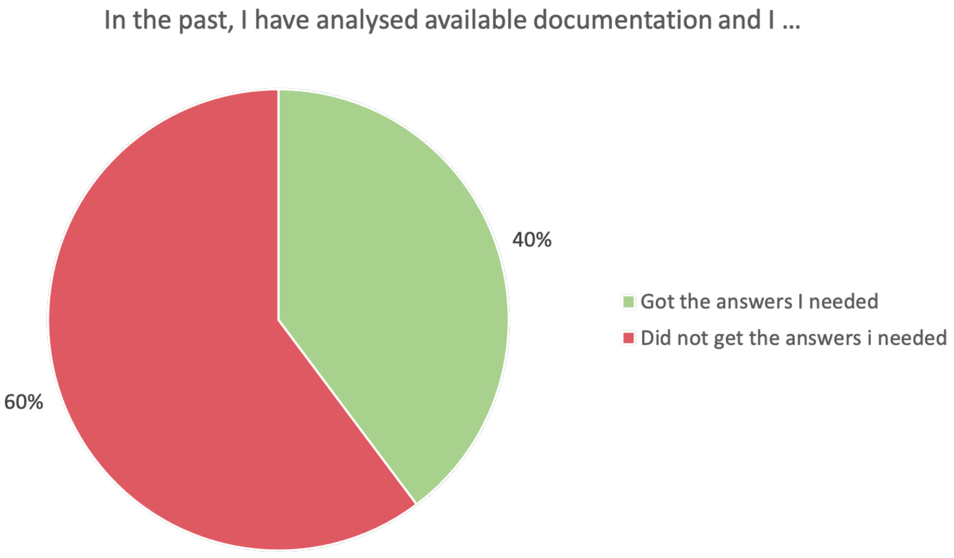


Figure 6.5: Ratio of success upon analysis of governmental documentation

This low rate of success reflects the lack of transparency or, at least, lack of clarity and completeness of the available documentation.

On the same train of thought, when considering only the people who have gotten on contact directly with a competent authority, it is possible to see that 61% could not get the information they needed.

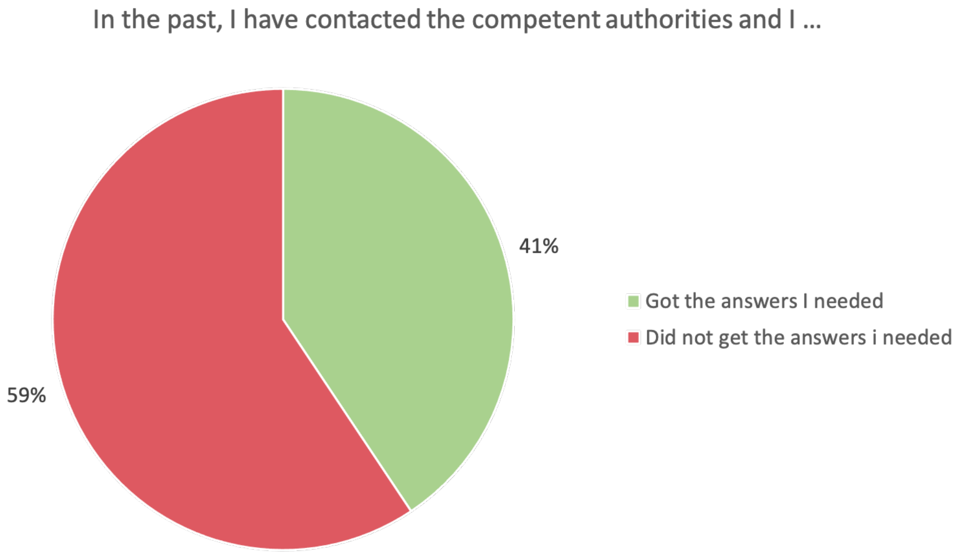


Figure 6.6: Ratio of success upon contact of the competent authorities

This statistic is the most concerning of all because direct contact should be seen as a last resort. Ideally all the information needed by the users should be available online and only small, specific cases should require direct contact. In addition to this, upon contact, all the information should be available and the fact that almost two thirds of the participants who have had the need to do this in the past, did not get clarified, is a big indicator of lack of transparency.

To conclude, this survey reflected the experience the author had during the implementation phase of this project. Functionalities mainly work, and overall there is a semi-well funded basis for trust. However, this trust is compromised upon further investigation as the lack of transparency is evident. It is extremely hard to access any deeper level information and not even direct contact, which should be the last resort and provide all answers, clarified the users sufficiently.

Chapter 7

Conclusions

7.1 Conclusions

The cryptographic "solutions" that the Portuguese government provides to its citizens cannot be the only ones possible or accepted as inevitable, because everything related to technology and security is nuanced and relative to context.

The actualization of concrete, assessable questions made possible the development of a practical and objective evaluation. The documentation was analysed in order to find the answers, and, upon failure, other alternative communication means were used. This way, the comprehensiveness of the documents available to the users was scrutinised and the communication channels such as email and telephone support calls, were also put to the test.

During this study, there was a significant percentage of questions left unanswered after exhausting every previously mentioned possibilities. This fact is a clear indicator that the communication with the users is lacking.

The implementation of the functionalities of the SDK was another clear example of space for improvement. The lack of a testing mode or platform is critical to address, as the use of personal information poses a huge liability to the user.

The questions and the implementation of the functionalities, paired with the deep familiarization of the documentation make up solid ground for evidencing the shortcomings mentioned previously. This fact was also underlined by the results achieved on the conducted survey.

As contribution for the assessment of the quality degree and security perceived by the users, this work revealed a serious governmental effort on the development of these cryptographic tools; however, it also revealed, from the government's side, a minimalist support service lacking in transparency.

To conclude, the transparency the government provides to the users is not sufficient, and there is space for improvement that need to be urgently resolved. Some small improvements, such as providing practical examples online are already being made, but were not checked, as the information was provided only very recently; however there are still several hurdles that require conquering.

7.2 Future Work

It is visible to see that future work is imperative. This would include further communication with the competent entities, preferably without time constraints as rigid as the ones set for this study. It would also be beneficial to explore in more detail the newly added example implementations provided.

Cyber security is ever-changing; this exercise of scrutinizing current technological implementations and its respective documentation needs to be a continuous effort to guarantee transparency.

References

[1] "Autenticação.gov." Available at www.autenticacao.gov.pt. Accessed: 2020-12-04.

[2] A. Veldre, "Introduction of x-tee." https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html, 2016. Accessed: 2021-01-27.

[3] "The Ultimate Guide to Moving to Copenhagen (for EU citizens)." Available at https://www.joinlifex.com/copenhagen/moving-to-copenhagen-denmark. Accessed: 2021-02-09.

[4] "Guia prático de utilização do cartão de cidadão." Available at https://www.autenticacao.gov.pt/web/guest/documentos, 2007.

[5] "Sistema de certificação electrónica do estado - instalação de certificados." Available at https://www.scee.gov.pt/rep/certificados/. Accessed: 2021-02-02.

[6] "Documentação do middleware oficial de identificação eletrónica em portugal." Available at https://amagovpt.github.io/docs.autenticacao.gov/. Accessed: 2021-02-02.

[7] "2020 UN E-Government Survey." Available at https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020, 2020.

[8] "e-Estonia." Available at https://e-estonia.com/. Accessed: 2020-12-04.

[9] M. Kitsing, "Success without strategy: E-government development in Estonia," *Policy & Internet*, vol. 3, no. 1, pp. 1–21, 2011.

[10] P. Laud and M. Roos, "Formal analysis of the estonian mobile-id protocol," in *Identity and Privacy in the Internet Age* (A. Jøsang, T. Maseng, and S. J. Knapskog, eds.), (Berlin, Heidelberg), pp. 271–286, Springer Berlin Heidelberg, 2009.

[11] A. Parsovs, "Estonian electronic identity card: security flaws in key management," in *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pp. 1785–1802, 2020.

[12] "The key to Denmark's digital success." Available at https://denmark.dk/innovation-and-design/denmarks-digital-success. Accessed: 2021-02-09.

[13] "National identity and signing." Available at https://en.digst.dk/digitisation/eid/. Accessed: 2021-02-09.

[14] "NemID & Digital Denmark." Available at https://studycph.dk/nemid-digital-denmark/. Accessed: 2021-02-09.

[15] "Digital Denmark The most digital country in Europe." Available at https://digitaldenmark.dk. Accessed: 2021-02-09.

[16] "Ministry of the Interior and Safety." Available at https://www.mois.go.kr/eng/a01/engMain.do. Accessed: 2021-02-11.

[17] "S. Korea to outline digital ID system to replace old ID cards by Q3." Available at https://pulsenews.co.kr/view.php?year=2020&no=603696. Accessed: 2021-02-11.

[18] S. E. Colesca, "Understanding trust in e-government," *Engineering Economics*, vol. 63, no. 3, 2009.

[19] "Declaração de práticas de operação do SCMD." Available at https://www.autenticacao.gov.pt/web/guest/documentos, 2019.

[20] "Sdk examples." Available at https://github.com/amagovpt/docs.autenticacao.gov/tree/main/SDK_Examples.

[21] L. Min, T. Chen, and H. Zang, "Analysis of fips 140-2 test and chaos-based pseudorandom number generator," *Chaotic Modeling and Simulation*, vol. 2, no. 1, pp. 273–280, 2013.

[22] N. C.-N. H. Family, "Fips 140-2 level 3 non-proprietary security policy," 2016.

[23] K. H. Brown, "Security requirements for cryptographic modules," *Fed. Inf. Process. Stand. Publ*, pp. 1–53, 1994.

[24] "The Common Criteria." Available at https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria. Accessed: 2021-06-10.

[25] "Citizen perception in regards to the cryptographic solutions made available by the portuguese government." Available at https://forms.gle/RivsLiAFzR3qmo8U8.

[26] "Bloqueio do cartão de cidadão por tentativa de assinatura digital." Available at https://github.com/amagovpt/autenticacao.gov/issues/75.

Appendix A

Registry of information exchange

Throughout the development of this work, several emails were exchanged and an issue on the official repository was open. Here is the registry of those interactions.

A.1 Email thread 1: email 1

From: up201603811@fe.up.pt

To: ama@ama.pt

Date: 12/01/2021

Subject: Informações referentes à Chave Móvel Digital

Body: Boa tarde,

Eu sou uma aluna de Engenharia Informática na Faculdade de Engenharia da Universidade do Porto, atualmente a elaborar o meu trabalho de fim de mestrado, sendo que parte deste recai sobre o funcionamento da Chave Móvel Digital. Na minha pesquisa apenas econtrei os três documentos presentes na seguinte página web https://www.autenticacao.gov.pt/documentos.

É possível ser me enviado todo o resto de documentação técnica que exista sobre a Chave Móvel Digital, por favor?

Agradeço desde já a disponibiliadde,

Maria Teresa Ferreira

A.2 Email thread 1: email 2

From: info.cidadao@ama.pt

To: up201603811@fe.up.pt

Date: 25/01/2021

Subject: [Ticket #JRKMZK] Informações referentes à Chave Móvel Digital

Body: Cara Sra. Maria Teresa Ferreira,

A informação técnica da Chave Móvel Digital, encontra-se disponível no link que nos indica.

Caso queira explicitar o propósito e finalidade de outra documentação que necessite, a Agência para a Modernização Administrativa - AMA poderá avaliar a sua disponibilização.

Com os melhores cumprimentos,

Ângela Simões

A.3 Email thread 1: email 3

From: up201603811@fe.up.pt

To: info.cidadao@ama.pt

Date: 30/04/2021

Subject (Original): Re: [Ticket #JRKMZK] Informações referentes à Chave Móvel Digital

Body: Boa tarde,

Após uma análise mais detalhada da documentação da Chave Móvel Digital apresentada, tenho ainda algumas questões que gostaria que fossem esclarecidas ou que me fosse indicado onde se encontra a informação referente aos assuntos em questão.

Os tópicos para os quais não encontrei informação são os seguintes:

- Que tipo de controlo e acesso têm as pessoas com papel de administrador? (apesar da chave privada estar protegida com a passe inserida pelo utilizador, essa passe é enviada na mesma ao servidor pelo que seria possível acesso a esses dados)

- Quais as especificações do modulo de hardware criptográfico? (é possível armazenar as informações referentes a todos os utilizadores de forma segura?)

- Como é feita a verificação dos códigos necessários?

- Qual a razão de haver funcionalidades que ainda não estão disponíveis no SDK? (é apenas uma questão de tempo para haver essa implementação, ou há alguma questão mais impeditiva)

- É possível um utilizador alterar o seu par de chaves de modo a haver um controlo pessoal sobre a sua geração?

Agradeço desde já qualquer ajuda que me possa ser dada,

Maria Teresa Ferreira

A.4 Email thread 1: email 4

From: info.cidadao@ama.pt

To: up201603811@fe.up.pt

Date: 30/04/2021

Subject: [Ticket #JRKMZK] Informações referentes à Chave Móvel Digital

Body: Caro(a) Sr. (a),

Estamos a melhorar o atendimento!

Se está a responder a um pedido que está a ser tratado aguarde pela nossa resposta.

Para novos pedidos submeta a sua questão através do formulário disponível em:

https://eportugal.gov.pt/contactos

Com os melhores cumprimentos,
DIREÇÃO DE PLATAFORMAS E COMPETÊNCIAS DIGITAIS

A.5 Email thread 1: email 5

From: suporte.eportugal@ama.pt

To: up201603811@fe.up.pt

Date: 04/05/2021

Subject: [Ticket #JRKMZK] FW: Informações referentes à Chave Móvel Digital

Body: Cara Sra. Maria Teresa Ferreira,

Agradecemos o seu novo contacto.

No seguimento do email enviado, informamos que as respostas às questões apresentadas são:

- Que tipo de controlo e acesso têm as pessoas com papel de administrador? (apesar da chave privada estar protegida com a passe inserida pelo utilizador, essa passe é enviada na mesma ao servidor pelo que seria possível acesso a esses dados)

[AMA] - https://apps.autenticacao.gov.pt/documents/10179/615532/POL

- Quais as especificações do módulo de hardware criptográfico? (é possível armazenar as informações referentes a todos os utilizadores de forma segura?)

[AMA] - https://apps.autenticacao.gov.pt/documents/10179/615532/POL

Especificações detalhadas não estão disponíveis publicamente, por razões de segurança.

Todo o sistema é alvo de auditoria por entidades externas e reporte dos seus resultados ao Gabinete Nacional de Segurança, nos termos do RE 910/2014.

- Como é feita a verificação dos códigos necessários?

[AMA] - https://apps.autenticacao.gov.pt/documents/10179/615532/POL

- Qual a razão de haver funcionalidades que ainda não estão disponíveis no SDK? (é apenas uma questão de tempo para haver essa implementação, ou há alguma questão mais impeditiva)

[AMA] - Existem várias interfaces disponíveis de acordo com os casos de uso (onde se inclui o SDK, Webservices, SAML, oAuth, ..., entre outros).

Se tivermos informação do caso de uso pretendido poderemos auxiliar na identificação da API mais adequada.

- É possível um utilizador alterar o seu par de chaves de modo a haver um controlo pessoal sobre a sua geração?

[AMA] O controlo "pessoal" pelo utilizador é sempre assegurado (daí a CMD está credenciada como um mecanismo de autenticação com o nível de segurança mais elevado em termos Europeu (high) e ser um serviço de assinatura eletrónica qualificada no contexto EU. E sim, é sempre possível alterar o par de chaves; basta cancelar e emitir uma nova CMD que é gerado um novo par de chaves.

Com os melhores cumprimentos,
Ângela Simões

A.6 Email thread 1: email 6

From: up201603811@fe.up.pt

To: suporte.eportugal@ama.pt

Date: 31/05/2021

Subject: Re: [Ticket #JRKMZK] Informações referentes à Chave Móvel Digital

Body: Boa tarde,

Obrigada pela resposta e os esclarecimentos.

Entretanto deparei-me com um outro problema referente ao SDK e as funcionalidades disponíveis para o Cartão de Cidadão, e agradecia se fosse possível disponibilizar alguma ajuda.

De momento encontro-me a realizar uma avaliação da parte da assinatura digital e do código disponível para esta funcionalidade (usando sempre C++) e estou a ter bastantes dificuldades. Quando utilizo o código fornecido aqui, as opção de XAdES dá-me erro, mas mais impeditivo é tentando o código fornecido para assinatura de documentos PDF, o cartão ficou imediatamente bloqueado (já testei com mais que um cartão e obtive sempre a mesma situação).

Isto é impeditivo visto que tenho de entregar este projeto brevemente e foi-me informado que para desbloquear o meu cartão, tenho de pedir a emissão de um novo e não há horários que acomodem o prazo que preciso de cumprir.

Relacionado com isto, coloco também a questão de como é usado o modo de teste que é dito existir na documentação. Apenas é informado que é necessário colocar o modo de teste a TRUE, mas não encontrei o que esse modo de teste faz nem como o utilizar.

Existe alguma maneira de contornar estas dificuldades que estou a enfrentar?

Obrigada desde já por qualquer ajuda que possa ser fornecida referentemente a estes dois assuntos, Maria Teresa Ferreira

A.7 Email thread 1: email 7

From: suporte.eportugal@ama.pt

To: up201603811@fe.up.pt

Date: 16/06/2021

Subject: [Ticket #JRKMZK] FW: Informações referentes à Chave Móvel Digital

Body: Cara Sra. Maria Teresa Ferreira

Informamos que a sua questão foi encaminhada para a equipa técnica, que está a analisar a situação.

Com os melhores cumprimentos,

Ângela Simões

A.8 Email thread 2: email 1

From: up201603811@fe.up.pt

To: info.cidadao@ama.pt, adrianoribeirocampos@gmail.com

Date: 06/04/2021

Subject: Questão relacionada com o SDK do Middleware autenticação.gov

Body: Boa tarde,

Sou uma aluna da Faculdade de Engenharia da Universidade do Porto de momento a elaborar um projeto de Mestrado em C++ que inclúi uma análise ao middleware de acesso às funcionalidades do Cartão de Cidadão e Chave Móvel Digital.Contudo deparei-me com algumas dificuldades no que toca à utilização do SDK e à sua documentação.

Estes erros são problemas de acesso que não sei se são falhas do meu lado ou são apenas funcionalidades que não estão implementadas. Sabendo que algumas funcionalidades mais básicas estão já implementadas, logo não seria um problema de setup do projeto, quando tento utilizar código fornecido na documentação por vezes não o consigo fazer.

Um exemplo disto é no acesso aos Pins não consigo aceder ao construtor visto que é privado e analisando o header, o construtor que é chamado tem o comentário

```
/**< Copy not allowed - not implemented */.
```

Isto verifica-se por exemplo no acesso à morada em que tem de ser feita a verificação do PIN de acesso e em que o código fornecido no Manual do SDK é o seguinte:

```
PTEID\_EIDCard &card;
unsigned long triesLeft;
//(...)
PTEID_Pins pins = card.getPins();

PTEID_Pin pin = pins.getPinByPinRef(PTEID_Pin.ADDR_PIN);
if (pin.verifyPin("", &triesLeft, true){
        PTEID_Address &addr =  card.getAddr();
        const char * municipio =  addr.getMunicipality();
}
```

Agradeço qualquer ajuda que me possa ser dada em relação a esta questão.

Cumprimentos,

Maria Teresa Ferreira

A.9 Email thread 2: email 2

From: adrianoribeirocampos@gmail.com

To: up201603811@fe.up.pt

Date: 06/04/2021

Subject: Questão relacionada com o SDK do Middleware autenticação.gov

Body: Boa tarde,

Pode consultar o repositório do projecto em:

https://github.com/amagovpt/autenticacao.gov e https://github.com/amagovpt/docs.autenticacao.gov

Se tiver alguma dúvida ou dificuldade pode sempre abrir um issue e respondemos o mais rápido possível:

https://github.com/amagovpt/autenticacao.gov/issues

Coloque o código que está a usar, o que pretende fazer, ... no issue para facilitar a identificar a dificuldade. Obrigado.

Cumprimentos,

Adriano Campos

A.10 Email thread 2: email 3

From: adrianoribeirocampos@gmail.com

To: up201603811@fe.up.pt

Date: 07/04/2021

Subject: Questão relacionada com o SDK do Middleware autenticação.gov

Body: Olá,

Entretanto corrigimos os exemplos que estavas a usar:

https://github.com/amagovpt/docs.autenticacao.gov/commit/4196c47b1ddfd346931d8aaaace55da456cef69b

De qualquer forma, qualquer outra questão avisa. Obrigado.

Cumprimentos,

Adriano Campos

A.11 Email thread 2: email 4

From: up201603811@fe.up.pt

To: adrianoribeirocampos@gmail.com

Date: 06/05/2021

Subject: Questão relacionada com o SDK do Middleware autenticação.gov

Body: Boa tarde,

Obrigada pela resposta.

Penso que a solução apresentada para C++ continua a apresentar falhas, mas de qualquer dos modos, entretanto consegui solucionar.

É possível ser me indicado como é que consigo utilizar o modo de teste, por favor? Tenho estado a utilizar o meu próprio cartão pessoal para fazer esta análise, mas é uma solução longe de ideal visto estar a usar dados/códigos reais. Contudo não consegui encontrar qualquer informação sobre como seria possível usar o modo de teste para além da ativação

```
PTEID_Config::SetTestMode(true);
```

Obrigada por toda a disponibilidade,

Maria Teresa Ferreira

A.12 Email thread 3: email 1

Note: Upon telephonic contact, the information request was said to be best as redirected to the email address presented bellow.

From: mariateresaurbanoferreira@gmail.com

To: cartaodecidadao@irn.mj.pt

Date: 15/06/2021

Subject: Informações referentes à Chave Móvel Digital

Body: Boa tarde,

Sou uma aluna de Mestrado em Engenharia Informática e Computação, e no desenvolvimento da minha tese de Mestrado estou a elaborar um estudo sobre o cartão e cidadão e a chave móvel digital.

É possível serem me indicadas as respostas às seguintes perguntas que dizem respeito ao cartão de cidadão, ou em que documento se encontram essas informações, por favor?

- Como é gerado o par de chaves?

- Como é inserido o par de chaves no cartão de cidadão? É gerado diretamente no chip? Se não for gerado diretamente no chip, o par de chaves é apagado de forma segura do sitio onde foi gerado?

- Como é que os utilizadores conseguem ter a garantia que não há cópias do seu par de chaves pessoal?

- De que forma conseguem os utilizadores controlar a informação presente no cartão?

Toda a ajuda seria muito benéfica para o meu trabalho. Obrigada desde já pela disponibilidade, Maria Teresa Ferreira

A.13 Github issue

Subject (Original): Bloqueio do Cartão de Cidadão por tentativa de assinatura digital [26]

A.13.1 Message 1

From: MariaTeresaFerreira

Date: 31/05/2021

Body: Usando o código fornecido na documentação para assinatura digital com o Cartão de Cidadão, os cartões que usei ficaram imediatamente bloqueados. Não devo estar a chamar nada de forma errada porque chega a aparecer-me a janela de pop-up para inserir o código de assinatura.

Há alguma maneira de contornar isto ou alguma alternativa (pe. algum modo de teste que nao implique usar cartões reais para testar o código)?

Obrigada desde já por qualquer ajuda

A.13.2 Message 2

From: agrr

Date: 01/06/2021

Body: Bom dia,

A nossa suspeita é que os cartões que testou não deveriam ter a assinatura ativa o que significa que o PIN de assinatura estava bloqueado à partida. A ativação da assinatura faz-se normalmente no momento da entrega do CC ou posteriormente se necessário num balcão de levantamento do CC.

O comportamento de aparecer a janela de PIN faz sentido para este cenário porque os métodos de assinatura não validam previamente se os PINs estão de facto desbloqueados.

Essa validação pode ser feita programaticamente com o seguinte código (em Java):

```
 //eidCard é um objecto do tipo PTEID_EIDCard

PTEID_Pins pins = eidCard.getPins();
PTEID_Pin signature_pin = pins.getPinByPinRef(PTEID_Pin.SIGN_PIN);

if (signature_pin.getTriesLeft() == 0) {
     System.out.println("PIN de assinatura bloqueado.");
}
```

A.13.3 Message 3

From: MariaTeresaFerreira

Date: 02/06/2021

Body: Boa tarde,

Eu antes de testar com o meu código, usei a aplicação disponível para testar que estava tudo ok, portanto o PIN estava desbloqueado inicialmente.

A.13.4 Message 4

From: ACamposPT

Date: 21/06/2021

Body: Boa tarde,

Pode desbloquear o Cartão numa loja do Cidadão sem custos. Contudo, dependendo da versão do Cartão pode ser necessário a Carta com os PIN's. Se colocar aqui um excerto do código, podemos tentar identificar o problema.

Entretanto colocamos exemplos completos de usa do SDK, aqui:

https://github.com/amagovpt/docs.autenticacao.gov/tree/main/SDK_Examples

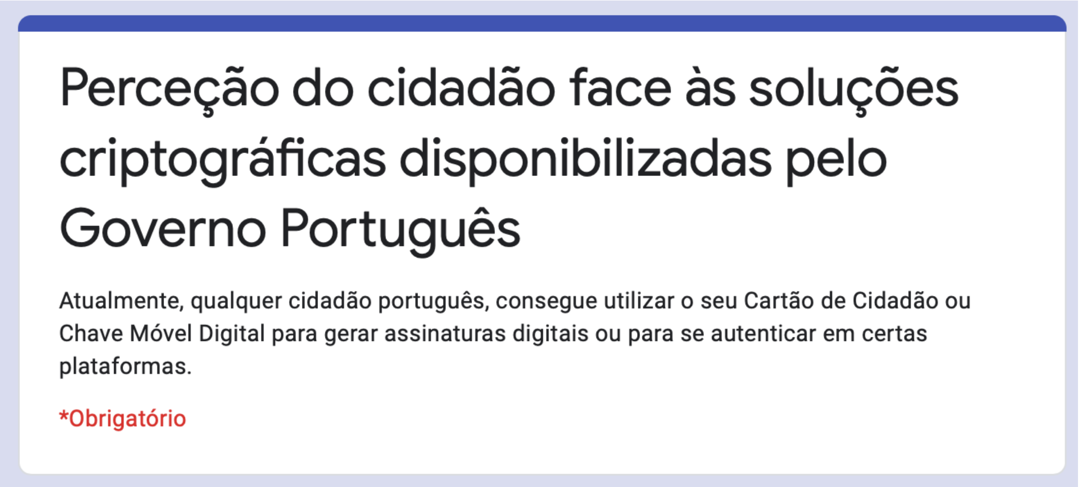
Existe Cartões de Teste para as equipas de desenvolvimento, e também para entidades externas. Sobre os cartões de teste, deverá contactar a AMA e indicar qual o objectivo para o qual pretende os Cartões de Teste. Contactar pelo email:

info.cidadao@ama.pt.

Appendix B

Survey Screenshots

This appendix serves the purpose of registering exactly the online survey developed for this work.

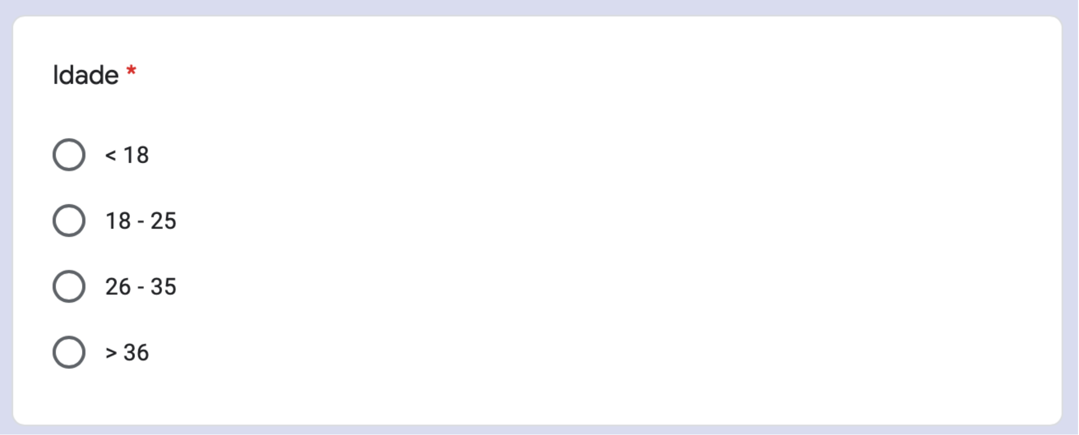


Perceção do cidadão face às soluções criptográficas disponibilizadas pelo Governo Português

Atualmente, qualquer cidadão português, consegue utilizar o seu Cartão de Cidadão ou Chave Móvel Digital para gerar assinaturas digitais ou para se autenticar em certas plataformas.

*Obrigatório

Figure B.1: Online survey introductory text screenshot



Idade *

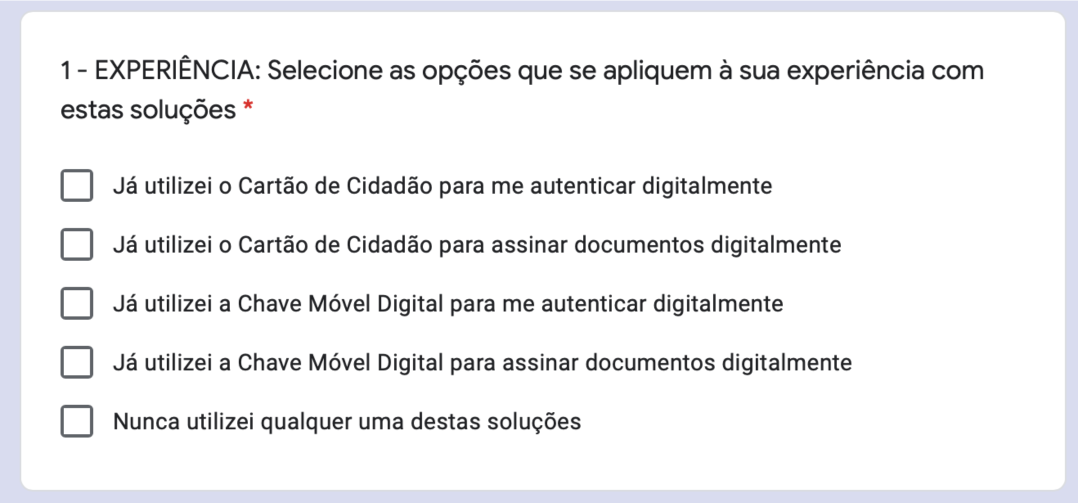
○ < 18

○ 18 - 25

○ 26 - 35

○ > 36

Figure B.2: Online survey age question screenshot



1 - EXPERIÊNCIA: Selecione as opções que se apliquem à sua experiência com estas soluções *

□ Já utilizei o Cartão de Cidadão para me autenticar digitalmente

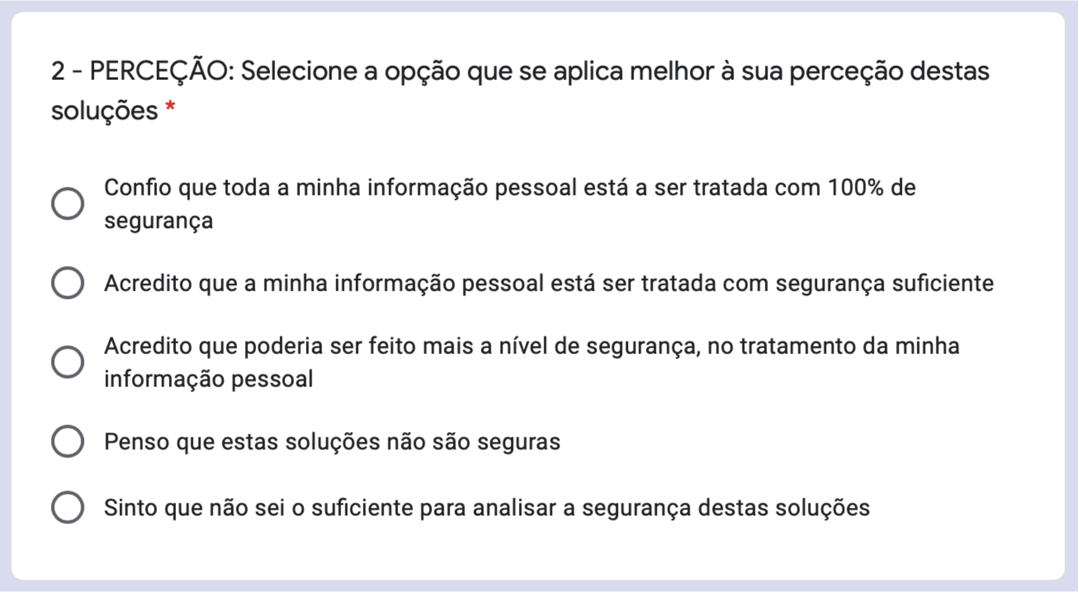
□ Já utilizei o Cartão de Cidadão para assinar documentos digitalmente

□ Já utilizei a Chave Móvel Digital para me autenticar digitalmente

□ Já utilizei a Chave Móvel Digital para assinar documentos digitalmente

□ Nunca utilizei qualquer uma destas soluções

Figure B.3: Online survey experience question screenshot



2 - PERCEÇÃO: Selecione a opção que se aplica melhor à sua perceção destas soluções *

○ Confio que toda a minha informação pessoal está a ser tratada com 100% de segurança

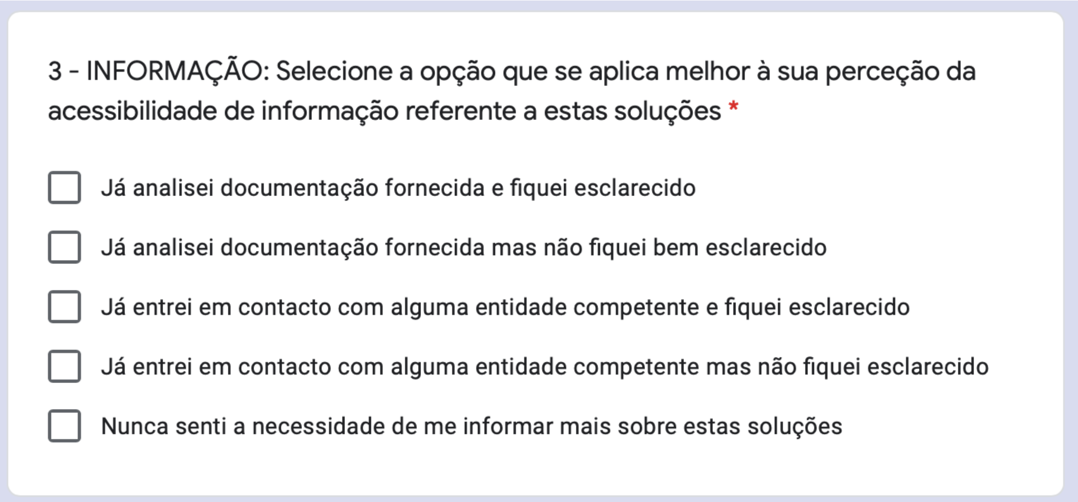
○ Acredito que a minha informação pessoal está ser tratada com segurança suficiente

○ Acredito que poderia ser feito mais a nível de segurança, no tratamento da minha informação pessoal

○ Penso que estas soluções não são seguras

○ Sinto que não sei o suficiente para analisar a segurança destas soluções

Figure B.4: Online survey perception question screenshot



3 - INFORMAÇÃO: Selecione a opção que se aplica melhor à sua perceção da acessibilidade de informação referente a estas soluções *

□ Já analisei documentação fornecida e fiquei esclarecido

□ Já analisei documentação fornecida mas não fiquei bem esclarecido

□ Já entrei em contacto com alguma entidade competente e fiquei esclarecido

□ Já entrei em contacto com alguma entidade competente mas não fiquei esclarecido

□ Nunca senti a necessidade de me informar mais sobre estas soluções

Figure B.5: Online survey information question screenshot