INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

DEVELOPING APPLICATIONS THAT USE THE PORTUGUESE CITIZEN CARD (CARTÃO DO CIDADÃO)

The goal of this laboratory is to introduce to the development of JAVA applications that use the Portuguese Citizen's Card (PT-CC). In particular, this lab guide overviews on how to use two of the APIs provided by the PT-CC's middleware library: PTEIDLIB and the PKCS#11.

1 Portuguese Citizen's Card

The Portuguese Citizen's Card (PT-CC) is a document for the electronic identification of citizens that uses *smart card* technology. The PT-CC serves as a unified document that serves as, and replaces, the following documents:

1. Citizen Identity Card
2. Fiscal Identity Card
3. Social Security Card
4. Electoral Card
5. Nation Health Service Identity Card

Visually, the PT-CC exhibits, on its front side, the photo and the elements of civil identification. On its back side, it reports the identification numbers of the five documents that it aggregates and replaces, as well as a optical reading zone and electronic contact chip.

In addition to storing the same information visually printed on the card, the PT-CC's chip stores certificates/private keys for authentication and digital signature, as well as the citizen's fingerprint biometric information.

Figure 1. Back and Front side of the Portuguese Citizen's Card

The PT-CC ensures compatibility with the new documents of electronic identification that are going to be adopted at the European Union level. Further, thanks to the use of smartcard technology, it provides enhanced security levels by increasing the complexity of forging false documents or of unauthorized accesses to the citizens' personal data.

The PT-CC allows the automatic identification via electronic services as well as the authentication of digital documents via digital signatures. This enables the ubiquitous interaction of citizens with diverse services, of both public and private nature. In particular, the PT-CC can be used to grant remote accessto the Public Administration services at anytime and from anywhere via Internet or phone (via *one-time-passwords* generated by the PT-CC).

1.1 Keys and PINs stored in the PT-CC

The PT-CC contains 2 pairs of public/private keys:

- The authentication keys
- The digital signature keys

It is recommended that the digital signature key is exclusively used for generating digital signatures; the authentication key shall always be used when one wants to use the PT-CC to encrypt data (e.g., as part of an authentication protocol). It is potentially insecure to use the same keypair for both signing and encryption. Doing so may enable attacks, depending on the particular public-key scheme you use. For instance, in a poorly designed system, if one can ask for the decryption of any ciphertext C and get back the corresponding Decrypt(C), then it would be possible to forge a signature for a message M by letting C = Hash(M) and then asking for Decrypt(C).

Important note: The digital signature key ("assinatura digital qualificada") has legal value and MUST never be used in the context of this course in any case. In this course, you shall always use the authentication key, also to generate digital

signatures. Also, to be prudent, we advise you NOT to use your own id card in case you have activated the “assinatura digital qualificada”.

The private keys stored in the PT-CC can never leave the PT-CC: they can never be explicitly read and can only be referenced (e.g., when using cryptographic services). The public keys are instead contained in certificates that can be obtained using the programmatic APIs described in the following.

In order to protect against unauthorized usage of the identification data and of the cryptographic services, the PT-CC uses three PINs:

- Authentication PIN: used to obtain permission to use the Authentication (private) Key
- Digital Signature PIN: used to obtain permission to use the Digital Signature (private) Key
- Address PIN: used to obtain information on the address of the PT-CC's holder.

2 Middleware of the Portuguese Citizen Card

The *middleware* of the PT-CC provides a set of features that support both cryptographic operations, like digital signatures, and non-cryptographic ones, like returning provably genuine identification data (e.g., name and address) of the PT-CC holder.

The PT-CC middleware is accessible programmatically via 3 APIs:

- eIDLib: a non-standard/custom API that access **exclusively to identification data and not to the cryptographic operations.** This API offers a common interface across all the various versions of the PT-CC. This allows to develop applications without concerns regarding the format in which data is actually stored in the PT-CC.

- PKCS#11: a standard interface (sometimes called Cryptoki) that provides multi-platform access to the cryptographic features of PT-CC.

- CryptoAPI: a Microsoft API that provides accessto cryptographic operations of the PT-CC's smartcard. Only available for Windows environments, and not further discussed in this document.

Some useful references for the PTEIDLIB and PKCS#11 APIs:

- Technical reference of the PT-CC:

https://www.autenticacao.gov.pt/cc-documentacao

It is strongly recommended to read Chapters 1, 3 and 4.

- Reference Guide of JAVA PKCS#11:

http://docs.oracle.com/javase/7/docs/technotes/guides/security/p11guide.html

3 A JAVA program demonstrating the eIDLib and PKCS#11 APIs

This eIDLib_PKCS11_test Java program demonstrates how to use some of the key features available via the eIDLib and PKCS#11 APIs.

Analyze its source code, whose comments will guide you across the various stages of the program.

The program first uses the eIDLib interface to obtain and display several identification data, and the authentication certificate. Next, it uses the PKCS#11 APIs to generate a digital signature, using the authentication key.

3.1 Install and execute the test program

First, make sure to have installed the middleware of the PT-CC. The middleware of the PT-CC is available here, with installers for different operating systems:

https://www.autenticacao.gov.pt/cc-aplicacao

The installer sets up a library based on the openSC, an open-source project necessary for the communication with the PT-CC.

Next, follow the instructions in the README contained in the archive to compile and run the program. Note that the application should automatically find the openSC libraries, but on some operating systems it may be necessary to use the "Java.library.path" property to define the path to the library, e.g.:

Linux (Ubuntu): -Djava.library.path=/usr/local/lib/pteid_jni/"

MacOS: "-Djava.library.path=/Library/Java/Extensions/"

Note: Make sure to insert a PT-CC in the slot before running the program.

- Analyze the generated output and identify the corresponding code blocks in the test program.

4 Assignments

A. Extend the eIDLib_PKCS11_test.java program to obtain the address information from the PT-CC.
B. Verify the digital signature generated by the PT-CC via the PKCS#11 API using Java Crypto.
C. Integrate the PT-CC with the client library of your project, in order to sign the messages sent to the server-side of the HDS Coin system.