Algoritmos e Implementações de Sistemas de Segurança - Relatório do Segundo Contracto:
Manipulação de dados do Cartão do Cidadão Português
Instituto Superior Técnico - Taguspark

Bernardo Santos
57437, MERC
bernardompsantos@ist.utl.pt

Artur Balanuta
68206, MERC
artur.balanuta@gmail.com

1. Introdução

No ãmbito da cadeira de Algoritmos e Implementações de Sistemas de Segurança **(AISS)**, foi realizado um trabalho experimental dedicado à manipulação de dados existentes no cartão de cidadão português, mais concretamente a obtenção de elementos e também a verificação (em termos de autenticidade) dos mesmos.

2. Objectivo

O objectivo deste trabalho foi criar uma pequena aplicação (com métodos criados para a obtenção e/ou verificação de dados existentes de modo a explorar a biblioteca disponibilizada (middleware) no site do cartão de cidadão, utilizando a linguagem Java e poder criar um algoritmo de autenticação que utilize as propriedades existentes no cartão do cidadão (tecnologia *SmartCard*).

3. Metodologia Experimental

Esta aplicação foi realizada em linguagem Java e foi testada num computador com as seguintes características:

- **Processador:** Intel Core 2 Duo 2.4 GHz;
- **RAM:** 4 GB DDR3;
- **Sistema Operativo:** Mac OS 10.8.3 - 64Bits;
- **Disco Rígido:** SSHD;

3.1. Obtenção de Dados

Neste trabalho experimental foi requisitado um método para obter a chave pública existente no cartão do cidadão. Para que tal seja possvel é necessário aceder aos certificados existentes no cartão e seleccionar o que tem o nome ***CITIZEN AUTHENTICATION CERTIFICATE***.

Utilizando as bibliotecas nativas de segurança e criptografia do Java, exportamos o certificado para um objecto do tipo ***X509Certificate*** e seguidamente extraímos a chave pretendida, inserindo a mesma para um ficheiro (apenas para efeitos de confirmação).

3.2. Verificação/Autenticação de Dados

Neste trabalho experimental foi requisitado tambm um mtodo de autenticação para validar/verificar a veracidade dos dados obtidos.

1 - Para tal o utilizador/possuidor do cartão do cidadão deverá autenticar-se (através do código respectivo de autenticação), gerando um ***nounce*** - número aleatório usado para comunicações criptográficas.

2 - Com este ***nounce*** (**1**) ser gerada uma assinatura usando a chave privada existente no cartão do cidadão. Para tal ser possível, recorremos a outra biblioteca de segurança/criptografia existente no Java, desta feita ***PKCS11*** - geração e gestão de chaves criptográficas. Ao criar uma sessão ***PKCS11*** é então gerada uma assinatura para o ***nounce*** anteriormente criado.

3 - Seguidamente, para verificar/validar a assinatura criada criamos um objecto do tipo *Signature* e iniciamos o processo de verficação usado a chave pública anteriormente obtida. Este objecto será actualizado com o mesmo ***nounce*** (**1**) usado para gerar a assinatura mencionada em **2**.

4 - A verificação/validação de assinaturas/dados ocorre quando utilizamos o método ***verify*** (que faz parte da API do objecto *Signature*). Se de facto o utilizador/possuídor do cartão autenticou-se correctamente, esta verificação confirma/valida a mesma, ou seja o ***nounce*** que foi gerado e as assinaturas correspondentes (para a criação usando a chave privada do cartão e para a validação usado a chave pública do mesmo) confirmam a autenticidade do utilizador.

4. Conclusão

Foi apresentada uma aplicação que permite a manipulação dos dados existentes no cartão de cidadão português, que nos permitiu adquirir conhecimentos para a criação de um sistema de autenticação utilizando este sistema. Os resultados obtidos foram razoáveis, ficando em consideração a sua utilização para futuros trabalhos.