Instituto Superior Técnico, Tagus Park

Disciplina de Aplicações e Implementações de Algoritmos Criptográficos

MERC: 1º ano, 2º semestre, 2012/13

65963 – David Dias
63520 – Fábio Domingos

Data: 16/04/2013, Terça-feira

Autenticação com Cartão de Cidadão

Abstract: *Sistema de autenticação em serviços por validação da assinatura digital produzida com o Cartão de Cidadão português*

1. Introdução

O Cartão de Cidadão português oferece serviços de assinatura digital através de um mecanismo de criptografia de chave assimétrica. Ao contrário da assinatura digital tradicional, em que usamos a chave privada para assinar o documento, no caso do cartão do cidadão o acesso a esta é impossível, tendo apenas acesso a *tokens* criptográficos gerados a partir da chave privada que vão ser usados para fazer a assinatura. Desta forma garantimos a não repudiação das mensagens trocadas e impossibilitamos que a identidade seja forjada.

A implementação realizada neste contracto, prevê um mecanismo de autenticação usando o sistema descrito, de forma distribuída em que temos um agente a comunicar com um serviço de autenticação para esta ser validada.

2. Pressupostos e objectivos

É assumido para o desenvolvimento deste serviço, que os utilizadores têm acesso a um dispositivo de leitura do cartão de cidadão e que tenham em sua posse o seu cartão de cidadão. Não serão fornecidos mecanismos de autenticação alternativa.

Este projeto tem como objectivos:

- Mecanismo de Autenticação de um utilizador com chave assimétrica
- Garantir a não repudiação das mensagens
- Confidencialidade na troca de mensagens
- Mitigar os *Reply Attacks*

3. Arquitetura

O sistema desenvolvido implementa uma arquitetura cliente servidor composta por 4 partes:

- um *AuthAgent* - presente no lado do cliente que funciona de interlocutor com o servidor para proceder a autenticação do cliente
- um *AuthService* - serviço disponibilizado pelo servidor para a validação das assinaturas digitais do cliente
- uma *API* para o Cartão do Cidadão, partilhada entre o Cliente e o Servidor de maneira a ter acesso aos serviços oferecidos pelo Cartão de Cidadão
- um pacote *Utils*, que oferece à aplicação mecanismos para guardar chaves públicas de forma persistente na memoria, para futuras autenticações

Podemos observar a arquitetura na figura 1.

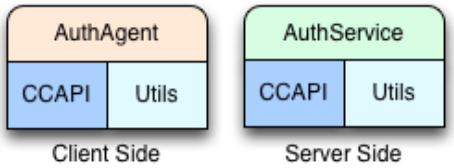

Figure 1 - Arquitetura do sistema

4. Modo de Funcionamento

De maneira a que a autenticação possa ser feita de forma remota, são usadas *sockets TCP* para a partilha de mensagens entre o *AuthAgent* e o *AuthService*. Estas mensagem podem ser:

- ***AUTH_REQUEST*** – Enviado para fazer um pedido de autenticação
- ***NOUNCE*** – número gerado pelo servidor para que o cliente possa fazer a autenticação
- ***NOUNCE_SIGNED*** – *nounce* cifrado com o *token* criptográfico gerado pela chave privada do cliente, também conhecido como assinatura digital
- ***AUTH_APPROVED*** - Mensagem de informação com a validação da autenticação
- ***AUTH_DENIED*** – Mensagem de informação com a não validação da autenticação

A ordem com que são trocadas estas mensagem pode ser observada na figura 2

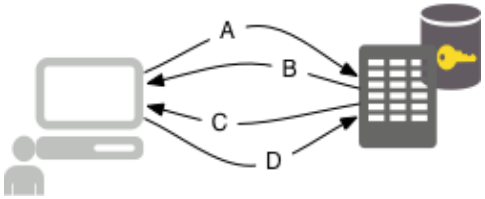

Figure 2 - Troca de mensagens entre o *AuthAgent* e o *AuthService*

A – O *AuthAgent* envia uma mensagem de pedido de autenticação ao *AuthService*
B – O *AuthService* gera um nounce de 128 bits e devolve ao *AuthAgent* para este o assinar como challenge
C – O *AuthAgent* devolve ao *AuthService* o nounce assinado com o seu token criptográfico gerado com o cartão de cidadão
D – Após verificação, o *AuthService* envia uma mensagem *AUTH_APPROVED* ou *AUTH_DENIED* conforme o resultado da validação.

Uma vez que não está disponível um repositório centralizado com as chaves públicas de cada cliente, foi necessário recolher previamente a chave pública do cartão de cidadão com qual realizamos o teste e assim coloca-la de forma persistente no lado do servidor.

5. Trabalho Futuro

De forma a tornar o sistema mais robusto, teremos de implementar um sistema de carimbos temporais, para que um agente malicioso que esteja a fazer escuta de pacotes, não possa usar a nossa mensagem de autenticação, uma vez que ela tem uma validade muito reduzida.

6. Conclusões

O cartão de cidadão é um serviço com um grande nível de rigor para um sistema de autenticação e não repudiação, no entanto, devido ao pouco desenvolvimento sobre este, a sua API pode conter erros e incompatibilidades com alguns sistemas.