Algoritmos e Implementações de Sistemas de Segurança
Especificação de Contracto:
Extensão para *Mozilla Thunderbird* com uso de Cartão de 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 âmbito da cadeira de Algoritmos e Implementações de Sistemas de Segurança **(AISS)**, foi pedido a criação de uma extensão de autenticação e confidencialidade para um cliente de email utilizando o cartão de cidadão português. Neste contracto serão específicadas um conjunto de funcionalidades requisitadas pelo cliente, fazendo a avaliação das mesmas.

2. Objectivo

Esta extensão será desenvolvida com o intuito de intensificar a segurança na comunicação via correio electrónico entre utilizadores, recorrendo ao uso do cartão de cidadão e/ou a outros mecanismos criptográficos (baseados em hardware).

3. Funcionalidades

3.1. Essenciais - Pacote Standard

- Plug-in *Mozilla Thunderbird*

Será desenvolvido uma extensão para o cliente de email ***Mozilla Thunderbird*** conforme requisitado pelo cliente. A criação da extensão obriga à utilização de várias linguagens de programação tais como *JavaScript* entre outras. No entanto o cerne da mesma será desenvolvido em *Java*.

- Autenticação via cartão de cidadão

Para garantir a autenticidade do cliente, será utilizado o cartão de cidadão com as respectivas bibliotecas *Java*. A mensagem criada pelo cliente será alvo de duas funções de resumo (***hash***) sendo estas incluídas na assinatura digital, que é gerada conforme as operações suportadas pelo cartão do cliente (tecnologia *SmartCard*), nomeadamente a assinatura usando a chave privada do mesmo.

A utilização de duas funções de resumo (*SHA256* e *RIPEMD160*) permitirá reduzir a probabilidade de encontrar colisões visto que é muito improvável encontrar outro texto que satisfaça ambas as funções de resumo, sendo que estas baseiam-se em algoritmos criptográficos diferentes.

- Confidencialidade

Conforme requisitado pelo cliente, será utilizado um hardware externo (com uma interface baseada em linguagem *C*) que irá permitir a cifra/descifra das mensagens utilizando o algortimo **AES**. O hardware contém uma chave simétrica (gerada previamente pelo cliente) que será utilizada (em conjunto com o hardware) para garantir confidencialidade na troca de mensagens.

Será necessária a implentação de um *binding agent* entre as duas linguagens (*C* e *Java*) de forma a permitir invocações ao hardware.

- Procedimento Geral:

Após o cliente ter finalizado a sua mensagem, poderá escolher qualquer uma das funcionalidades (ou ambas) anteriormente descritas.

Envio: Caso o utilizador escolha ambas as opções, a mensagem , em primeiro lugar, será autenticada com as características mencionadas anteriormente em **Autenticação via cartão de cidadão** e seguidamente iremos cifrar a mesma conforme descrito no ponto **Confidencialidade**. Finalmente o conteúdo gerado é convertido em *Base64* para manter a compatibilidade na tecnologia de transporte de email existente actualmente. Para assinalar o uso de qualquer funcionalidade, o conteúdo cifrado será encapsulado com uma *flag* auto-descritiva das opções utilizadas.

Recepção: Ao receber um email e em função das opções utilizadas (mencionadas através da *flag*), iremos efectuar (se necessário) a descifra e validação do conteúdo.

3.2. Opcionais - Pacote Premium

Para além das funcionalidades anteriormente descritas, este pacote incluirá uma funcionalidade extra a ser descrita de seguida:

- Selo temporal optimizado

Para garantir uma uniformidade temporal, precisamos de recorrer ao uso de uma entidade externa para autenticação temporal das mensagens (**um servidor TSS - *Time Stamp Service***).

O serviço baseia-se na utilização de chaves assimétricas para assinatura do **resumo - *digest*** gerado em função do conteúdo já autenticado pelo utilizador em que a chave pública do servidor **TSS** é conhecida por todos os interlocutores. Deste modo podemos validar o selo temporal obtido utilizando a chave anteriormente mencionada.

3.3. Outras

- Confidencialidade através do Cartão do Cidadão

Em casos em que não temos o aparelho dedicado de cifra **AES**, o cliente pretende uma solução em que quer garantir a propriedade de confidencialidade usando apenas o cartão do cidadão. No entanto, após a análise deste requisito, verificamos que isto só se consegue alcançar tendo acesso à chave pública do destinatário, algo que não é possível obter no sistema implementado actualmente neste tipo de cartões.

Para tal ser possível (uma solução a considerar), será a criação de um *Key Distribution Center* - ***KDC*** que armazenaria as chaves públicas de todos os clientes que pretendam usar esta funcionalidade. No entanto esta funcionalidade incluí vários riscos sendo que esta só e apenas será implementada após aprovação do cliente (mediante renegociação do contracto: **toma de responsabilidade por parte do cliente - serviços mantidos pelo servidor remoto**).

De modo a alcançar a confidencialidade da forma anteriormente indicada, é apresentado em seguida uma descrição (sumária) do procedimento:

- Em contraste à solução proposta (utilização da caixa dedicada com cifra **AES**), para cada mensagem gera-se uma chave simétrica para cifrar o conteúdo da mesma, utilizando a chave pública do destinatário, cifra-se a chave simtrica anteriormente gerada e envia-se o conjunto da mensagem e chave simtrica cifradas para o destinatrio.

- Deste modo, o possuídor da chave privada será capaz de obter a chave simétrica e consequentemente obter a mensagem.

- Anexos

Por forma a permitir a transferência de ficheiros entre interlocutores de um modo autenticado e/ou confidencial, serão utilizados os mecanismos referidos em ***3.1*** e/ou ***3.2***. Os ficheiros serão codififcados em *Base64* e incluídos no corpo da mensagem antes de serem enviados para o destinatário.

- Portabilidade Windows

Por forma a permitir a universalidade de utilização entre os sistemas operativos mais utilizados, em particular o Windows, será necessário a adaptação da extensão criada para o respectivo sistema.

4. Custo

Para a implementação desta aplicação foram considerados os seguintes custos (por pessoa/hora - 50 €/h):

Pacote Standard:
Plug-in para *Mozilla Thunderbird*: 15h
Autenticação: 10h
Confidencialidade c/ caixa AES: 24h

Total Pacote Standard: 2450 €

Pacote Premium:
Pacote Standard
Selo Temporal: +12h

Total Pacote Premium: 3250 €

Funcionalidades opcionais:
Confidencialidade com cartão do cidadão (14h): + 700 €
Anexos (21h): + 1050 €
Portabilidade para Windows: + 1500 €

Table 1. Aceitação de Condições

Especificação	Aceitação
Pacote Standard	
Pacote Premium	
Anexos	
Confidencialidade CC	
Portabilidade Windows	

5. Conclusão

Face aos requisitos especificados pelo cliente, foi apresentada uma solução para a criação de uma extensão para

um cliente de email *Mozilla Thunderbird* com o respectivo custo de implementação base e incluíndo também várias funcionalidades extra (definido como o pacote **Premium**) e/ou opcionais. Esta solução encontra-se pendente para aprovação por parte do cliente, podendo ser alvo de alterações a ser apresentadas no contracto final.

Assinatura: