**CONTRATO DE PRESTAÇÃO DE SERVIÇOS E DE ASSUNÇÃO DE RESPONSABILIDADE TÉCNICA**

**CLIENTE:** Ricardo Chaves, INESC-ID

**PRESTADOR DE SERVIÇOS:** Fábio Domingos, 63520, IST; David Dias, 65963, IST

Pelo presente instrumento particular de Contrato de Prestação de Serviços e de Assunção de Responsabilidade Técnica, as partes acima qualificadas comprometem-se com o seguinte:

**CLAUSULA PRIMEIRA – OBJECTO**

De forma a criar um sistema de email que visa garantir autenticidade, não repudiação e confidencialidade na troca de emails entre os vários utilizadores, são adoptadas as tecnologias presentes no cartão de cidadão para assinatura digital, usando *criptoki*, a interface de tokens criptográficos especificado pela norma *PKCS11* da *RSA* e o algoritmo de cifra *AES*.

Depois de uma analise cuidada às diferentes plataformas de email e de maneira a dar liberdade de escolha aos diferentes utilizadores, será criada uma API, implementável nas varias plataformas. Fará ainda parte do produto final um prótipo funcional que comprove o funcionamento desta API, bem como toda a documentação técnica e manual de utilizador do mesmo.

Poderá ainda ser realizado um serviço premium que contempla a utilização de um timestamp para o envio dos emails. Este ponto será considerado mediante um pagamento extra por parte do cliente.

**Requisitos**

Utilização da interface de tokens criptográficos especificado pela norma *PKCS11* da *RSA*.

Leitores de *smartcard*  para os utilizadores do serviço

**Especificações**

A API resultante do produto final terá 3 componentes:

1. Controlador que permite assinar e validar uma assinatura digital gerada com PKCS11 e o cartão do cidadão.
2. Capacidade de cifra dos conteúdos da mensagem utilizando *AES* para a garantida da confidencialidade
3. Validação temporal de cada email ao ser feito uso de timestamps

**Interface**

O produto final disponibiliza uma interface extensível por um programador, sendo implementável nos vários clients de email:

* **signMail(byte[] email, byte[] timestamp)**

Realiza a assinatura digital sobre o email, adicionando também o timestamp caso este não seja null

* **validateSign(byte[] signature)**

Valida assinatura

* **byte[] generateTimeStamp()**

Devolve um timestamp do preciso momento

* ***void init( int Cipher. int CMode, byte[] key);***

Cifrar/Decifrar parte da Mensagem

* ***byte[] update(byte[] plaintext);***
* ***byte[] update(byte[] plaintext, int inputlen);***

Finalizar a Cifra/Decifra

* ***byte[] doFinal(byte[] plaintext);***
* ***byte[] doFinal(byte[] plaintext, int inputlen);***

O mecanismo a ser usado é iniciado pela função *init.*

Esta interface poderá ser modificada de forma a optimizar o processo e a transparência face aos serviços já em produção na empresa face ao serviço de email.

**CLAUSULA SEGUNDA – RESPONSABILIDADES**

1. O cliente compromete-se a fornecer ao prestador de serviços os leitores de cartão do cidadão, bem como o respectivo middleware.
2. O prestador de serviços compromete-se a utilizar todos os seus recursos computacionais afim de cumprir o contrato estabelecido.

**CLAUSULA TERCEIRA – HONORÁRIOS**

Relativamente ao apresentado na clausula primeira os honorários dividem-se em pagamento base – pagamento relativo à realização do serviço base e pagamento premium – pagamento relativo à realização do serviço premium.

**CLAUSULA QUARTA – PRAZO CONTRATUAL**

O presente contrato é valido até ao próximo dia 10 de Maio não sendo possível qualquer prorrogação do mesmo.