DESCRIÇÃO TECNICA DE SOFTWARE

**DESCRIÇÃO DO SISTEMA**

* **Descrição do que o sistema faz**
* **Imagem da nossa arquitectura do sistema**

Os módulos do sistema são classificados de acordo com os workflows **Invocação do Sistema, Assinatura digital usando Cartão do Cidadão, Cifra do conteúdo usando AES, Zip do conteúdo, Invocação do sistema CaixaChaves1.0** e **Utilitários** conforme se segue:

**Invocação do Sistema**

Compreende o modulo **aiac** que abrange todas as funcionalidades necessárias à invocação do sistema.

**Assinatura digital usando Cartão do Cidadão**

Compreende o modulo **aiac.ptcc** que abrange todas as funcionalidades necessárias para fazer assinatura digital do conteúdo de um email, usando o Cartão do Cidadão.

**Cifra do conteúdo usando AES**

Compreende o modulo **aiac.aesJAVA** que abrange todas as funcionalidades referentes à utilização do AES na cifra do conteúdo de um email.

**Zip do conteúdo**

Compreende o modulo **aiac.zip** que abrange a funcionalidade de unzip do conteúdo anteriormente zipado aquando da invocação do sistema.

**Invocação do sistema CaixaChaves1.0**

Compreende o modulo **aiaic.aesC** que abrange todas as funcionalidades que permitem efectuar a cifra AES do conteúdo, usando o sistema CaixaChaves1.0

**Utilitários**

Compreende o modulo **aiac.tools** que abrange funcionalidades relativas à utilização da codificação de base64, conversão de ficheiros para String ou Byte Array e ainda funcionalidades relativas à validação de assinatura temporal.

**DESCRIÇÃO DOS MODULOS**

**aiac**

O modulo aiac é a directoria root de todo o sistema. Neste modulo para além de estarem contidos todos os outros módulos, temos ainda uma classe designada Main.

É através da classe Main que todos os métodos do sistema são invocados. Para a execução do sistema são contemplados 5 argumentos - -s/r -p <pathOfFile> [-t] [-z] [-c].

Descrição dos argumentos:

* -s/-r

Serve o primeiro argumento para diferenciar o modo em que o sistema irá trabalhar. Ao ser invocado a flag –s o sistema irá trabalhar em modo de envio, ou seja, todos as operações resultante a partir desse momento serão reflectidas num email a ser enviado pelo utilizador. De forma análoga se for invocada a flag –r o sistema trabalhará em modo recepção.

* -p <pathOfFile>

O segundo argumento necessário à invocação do sistema indica-nos caminho do ficheiro que queremos enviar ou receber, consoante o que foi passado no argumento acima descrito.

* [-t]

O terceiro argumento diz respeito à utilização de uma assinatura temporal do conteúdo.

* [-z]

Serve o argumento –z para indicar ao sistema se o conteúdo será enviado comprimido será necessário a sua descompressão.

* [-c]

O quinto argumento serve para dizer ao sistema se este irá cifrar o conteúdo usando o algoritmo AES.

Como já foi referido em cima o sistema tem dois modos distintos de operar – envio e recepção – sendo que cada um deles tem as suas características especificas.

Modo de Envio

Ao estarmos a trabalhar em modo de envio, a primeira operação a ser efectuada será a leitura e consequente conversão para base64 do conteúdo do ficheiro que queremos enviar. A conversão do conteúdo do ficheiro para base64 permite-nos enviar qualquer tipo de dados através de uma mensagem de email, pois com ela conseguimos ultrapassar a limitação que nos é imposta pela tabela ASCII neste tipo de mensagens.

Após a leitura e consequente conversão do conteúdo para base64, o sistema irá gerar um timestamp, que servirá para a criação de uma assinatura temporal ao email.

De seguido serão invocadas as bibliotecas de autenticação do cartão de cidadão, de modo a criar uma assinatura digital com o mesmo. Esta assinatura será concatenada de seguida com a assinatura temporal gerada através do timestamp e com o conteúdo em base64.

Ao ser invocada a flag –t o sistema irá comprimir o conteúdo a enviar. Com esta compressão consegue-se assim explorar a entropia do conteúdo na altura da cifra com o algoritmo AES (invocação da flag –c). De notar que a utilização da cifra AES pode ser realizada através do algoritmo desenvolvido pela equipa de trabalho da Signo ou pelo sistema CaixaChaves1.0.

Por fim o conteúdo é novamente convertido em base64 e escrito para um ficheiro que será enviado por email.

Modo recepção

Ao ser iniciado o modo de recepção, o ficheiro recebido é aberto e o seu conteúdo é desconvertido de base64. De seguida é realizada a decifra do conteúdo anteriormente cifrado com o algoritmo AES e ainda a descompressão do mesmo.

Por fim é feita a validação da assinatura (tanto ao nível da assinatura digital com o cartão do cidadão como da assinatura temporal com o timestamp) e conteúdo do email é escrito para um ficheiro.

**aiac.aesJAVA**

O modulo aiac.aesJAVA é constituído pelas classes AES\_API, AESMain, BlockCypherMode, CypherMode e FileRW. É neste modulo que assenta todo o desenvolvimento do algoritmo de AES realizado pela equipa de trabalho da Signo.

**aiac.ptcc**

O modulo aiac.ptcc é responsável pela criação da assinatura digital usando o cartão do cidadão. Dele fazem parte as classes CCAPI e Utils.

**aiac.tools**

O modulo aiac.tools é constituído pelas classes Clock, Convert e ReadWrite. Este modo serve essencialmente para fornecer ferramentas úteis ao desenvolvimento do trabalho realizado pela Signo.

**aiac.zip**

O modulo aiac.zip é responsável por fazer a descompressão do conteúdo de um email. Dele faz parte a classe unzip que recebe como argumento duas Strings, uma referente ao local onde se encontra o conteúdo a descomprimir e outra que indica o local para onde será escrito o conteúdo descomprimido.

**aiac.aesC**

O modulo aiac.aesC é responsável pelo carregamento das funções C que irão suportar a cifra AES usando o sistema CaixaChaves1.0