MANUAL DE UTILIZADOR

*Signo*

# INTRODUÇÃO

O sistema ***Signo*** oferece aos seus utilizadores uma forma segura de trocarem mensagens, com um sistema de autenticação robusto, utilizando o cartão de cidadão Europeu e um mecanismo de confidencialidade com base em cifra AES.

Este sistema é muito versátil, dando aos seus utilizadores a capacidade de comprimir as suas mensagens em formato zip, adicionar um carimbo temporal a sua assinatura para que a sua mensagem tenha um prazo de validade e a possibilidade de utilizar mecanismos de cifra externos de forma a que não seja necessário ao utilizador conhecer uma palavra chave para esse efeito.

# REQUISITOS À UTILIZAÇÃO

1. Possuir Cartão do Cidadão e respectivo leitor de cartões
2. Instalar software do Cartão do Cidadão (disponível em <http://www.cartaodecidadao.pt/>)
3. Para utilizar um mecanismo de cifra externo, precisa do respectivo aparelho, neste momento o sistema Signo só suporta o aparelho ***caixaChaves1.0*.**

# FUNCIONAMENTO

1. Instalar o Software do Cartão do Cidadão no seu Computador
2. Ligar o leitor de cartões ao seu computador
3. Inserir o seu Cartão de cidadão
4. Ligar o aparelho **caixaChaves1.0** caso deseje utilizar o sistema de cifra externo
5. Iniciar o programa com as opções que desejar descritas abaixo:

Para executar a interface o utilizador tem ao seu dispor várias opções que poderá optar por chamar consoante as suas necessidades.

* + **–s/r** – flag obrigatória que diz se o utilizador está a operar em modo de envio (-s) ou em modo de recepção (-r)
  + **–p [pathOFfile]** – o campo [pathOFfile] deve ser substituído pelo caminho para o email que pretende enviar, se estiver em modo envio, ou pelo caminho para o email que pretende decifrar, se tiver em modo recepção. Esta flag é obrigatória.
  + **–t** - Caso pretenda utilizar uma assinatura temporal no envio de um email o utilizador deve indicar esta flag. Em modo recepção o utilizador deverá saber se o conteúdo se o conteúdo que está a receber foi assinado temporalmente e assim utilizar esta flag em caso afirmativo.
  + **–z**  - De maneira a zipar o conteúdo de um email, o utilizador deverá usar a flag –z aquando da execução da interface. Em modo recepção o utilizador deverá saber se o conteúdo se o conteúdo que está a receber foi assinado zipado e assim utilizar esta flag em caso afirmativo.
  + **–c**  - Caso pretenda cifrar o conteúdo que está a enviar com o algoritmo AES, o utilizador deverá invocar a flag –c. Em modo recepção esta flag também deverá ser executada se o conteúdo que o utilizador pretende ler tiver sido cifrado com o algoritmo em cima referido.

Um exemplo de execução da interface é o seguinte:

* + **–s –p /sandbox/emailAEnviar.txt –t –z –c** - neste caso o utilizador irá estar a enviar um email (-s) que se encontra na pasta /sandbox/emailAEnviar.txt. Ao enviar esse email o utilizador irá envia-lo com uma assinatura temporal (-t), o seu conteúdo irá zipado (-z) e ainda será cifrado com o algoritmo AES (-c)

1. Ao executar o comando acima o código de autenticação do seu cartão de cidadão será pedido conforme a figura **XX**

**Figura XX – Pedido de codigo de autenticação do Cartão do Cidadão**

Introduza o seu código de autenticação e clique OK.

# Garantias

O ***Signo*** oferece uma garantia vitalícia que quaisquer danos causados durante a sua utilização que sejam provocados por Aliens ou outras situações extremamente improváveis de acontecer