



DSS Demo Web App

Projeto de Desenvolvimento 2

Engenharia de Segurança

Hugo Marques - pg47848

José Santos - a84288

Nuno Mata - pg44420

Digital Signature Service - DSS

- Projeto software *open-source*, disponibilizado pela União Europeia,
- O principais objetivos é a criação e validação de assinaturas eletrónicas;
 - suporte a 3 principais formatos de assinaturas de documentos (**XadES**, **CAdES** e **PAdES**);
 - validação de certificados;
 - suporte para múltiplas assinaturas de documentos.



Digital Signature Services
(DSS)

DSS Demo Web App

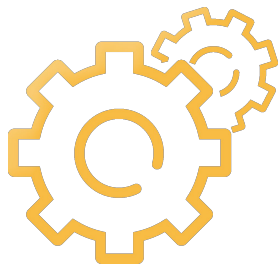
- Exemplo prático da utilização da framework DSS no desenvolvimento de uma aplicação;
- As principais funcionalidades são:
 - assinatura de documentos (XadES, PAdES e CAdES);
 - assinatura de *digests*;
 - extensão de assinaturas;
 - validação de assinaturas;
 - validação de certificados



DSS Demonstration WebApp

Funcionalidades desenvolvidas

- Transposição das alterações efetuadas pelos colegas para a versão 5.11.x;
- Criação de uma interface de autenticação (username e password);
- Criação de uma área de gestão de conta;
- Adicionada a possibilidade de assinatura de digest e documentos usando a CMD



Criação de interface de autenticação

- Interceptar os pedidos para que:
 - o utilizador tenha que estar autenticado se quiser:
 - efetuar uma operação com CMD;
 - aceder à página de gestão de conta;
- Utilização do Spring Security para ajudar na criação desta interface;
- Utilização do *MongoDB*, para guardar os dados do utilizador;

Login



A mockup of a login interface. It features a blue header bar with a white lock icon and the text 'Aceder à CMD'. Below the header, there are two input fields: 'Username' and 'Password', each with a light gray placeholder text. At the bottom right, there is a rounded 'Log In' button.

Criação de área de gestão de conta

- Possibilidade de guardar o nº de telemóvel na base de dados MongoDB;
- Apresentar o nº quando se acede a esta página;
- Modificar o número e atualizar na base de dados MongoDB;

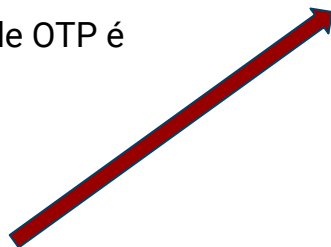
Account Management

Phone Number (Intl.
format)

Sign a digest with CMD

- Aplicação do serviço de CMD à classe do *sign a digest*;
- Adaptação da página exemplo para suportar a assinatura com CMD e lidar com o pedido de OTP da CMD;
- Tal como na assinatura de um documento com CMD, o processo de envio e receção de OTP é idêntico;

e-Signature with CMD
Sign a document
Sign a digest
Account Management



Sign a digest with CMD

Signature format ☐ XAdES ☐ CAdES ☐ JAdES

Digest algorithm ☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512

Digest to sign (Base64)

Level

Allow expired certificate ☐

Add a content timestamp ☐

Phone Number (Intl. format)

PIN

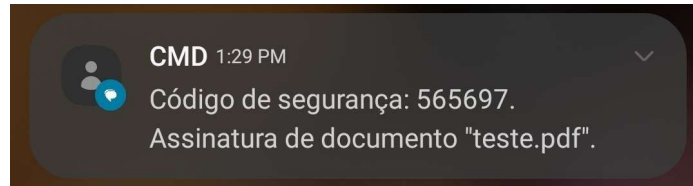
Processo de Validação OTP

Sign a document with CMD

OTP

Submit

Clear



Chave Movel Digital signature process

Done !



Métodos de Desenvolvimento de software seguro

- **DPIA**
 - Para demonstrar como o projeto cumpre as normas do **RGPD**;
 - Utilização da ferramenta **DPIA** para gerar o PIA do projeto;
- **Buffer Overflow**
 - As aplicações em Java não se encontram vulneráveis a este tipo de problema;

Métodos de Desenvolvimento de software seguro

- **Hash da senha de utilizador**

- Recurso ao *Spring Security*, que permite o armazenamento seguro da senha através de um método *"password encoder"*;
- Utilização da função de *hash* "bcrypt"

- **Vulnerabilidade de inteiros**

- Este problema não afeta este projeto;
- Não está a ser guardada nenhuma variável como inteiro;
- N° de telemóvel, Pin da CMD e o código OTP guardados numa string



Métodos de Desenvolvimento de software seguro

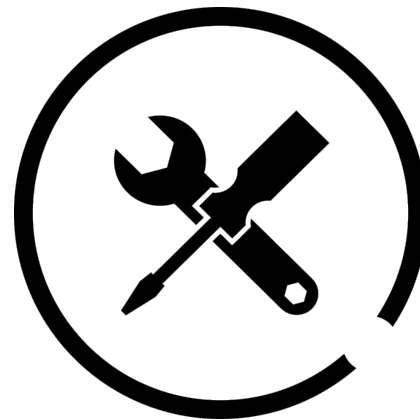
- **Validação de input**

- Campos de login validados (password deve ter entre 8 a 64 caracteres, 1 dígito numérico, uma letra minúscula, uma maiúscula e um caractere especial);
- Validação do nº de telemóvel, Pin da CMD associado e o código OTP recebido no telemóvel



Instalação da aplicação

- Devem ser atendidos os requisitos (detalhado no relatório);
- Instalação da WebApp
 - Em *Windows*;



Utilização da aplicação

Sign a document with CMD

File to sign Nenhum ficheiro selecionado

Container ☒ No ☐ ASiC-S ☐ ASiC-E

Signature format ☐ XAdES ☐ CAdES ☐ PAdES ☐ JAdES

Packaging ☐ Enveloped ☐ Enveloping ☐ Detached ☐ Internally detached

Level

Digest algorithm ☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512

Allow expired certificate ☐

Add a content timestamp ☐

Phone Number (Intl. format)

PIN

Sign a digest with CMD

Signature format ☐ XAdES ☐ CAdES ☐ JAdES

Digest algorithm ☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512

Digest to sign (Base64)

Drag a file here to compute digest

Level

Allow expired certificate ☐

Add a content timestamp ☐

Phone Number (Intl. format)

PIN

Login

Username

Password

Account Management

Phone Number (Intl. format)

Conclusão

- Este projeto exigiu uma compreensão do funcionamento e das funcionalidades da aplicação assim como a necessidade de recorrer a frameworks e APIs de terceiros de modo a simplificar o desenvolvimento;
- Em termos de segurança, procuram desenvolver a aplicação respeitando diversas técnicas e recomendações de segurança que foram lecionados ao longo da UC;
- Uma das partes mais desafiantes foi na instalação da aplicação, visto que obtivemos algumas falhas de compilação devido a dependências que eram necessárias;



DSS Demo Web App

Projeto de Desenvolvimento 2

Engenharia de Segurança

Hugo Marques - pg47848

José Santos - a84288

Nuno Mata - pg44420