



Escola de Engenharia
Universidade do Minho

DSS *Demo Web App*

Projeto de Desenvolvimento 2020/2021
Engenharia de Segurança



29/6/2021

Grupo 3:

Constança Elias – PG42820

Diogo Rio – A84752

Filipe Freitas – PG42828

Maria Araújo – PG42844



Estrutura do Relatório

- *DSS Demo Web App*
- Solução Desenvolvida
 - Cartão de Cidadão
 - Chave Móvel Digital
 - Fonte de *timestamp* do cartão de cidadão
 - Guardar configurações do utilizador
- Técnicas de Desenvolvimento de *Software Seguro*
- Conclusão



DSS (*Digital Signature Services*)

- É um projeto *open-source*, em Java, que permite assinar, validar e estender assinaturas eletrônicas avançadas (AdES).
- As principais funcionalidades são:
 - assinatura de documentos em diversos formatos (XML, PDF, ODT, TXT, ZIP...);
 - três formatos principais de assinatura digital (XAdES, CAdES e PAdES);
 - validação de certificados.



Digital Signature Services
(DSS)



DSS Demo Web App

- A DSS Demo WebApp consiste numa integração da *framework* DSS, sendo um exemplo concreto da utilização da mesma.
- Principais funcionalidades:
 - assinar documentos
 - extender uma assinatura
 - validar uma assinatura
 - validar um certificado



DSS Demonstration WebApp



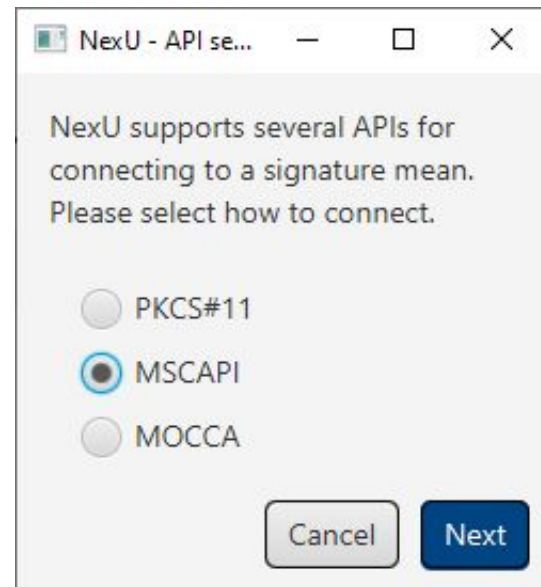
Solução Desenvolvida

- Integração das funcionalidades pedidas:
 - Integração do Cartão de Cidadão
 - Utilização do NexU
 - Integração da Chave Móvel Digital
 - Utilização do *Timestamp* do Cartão de Cidadão
 - Guardar configurações e dados do utilizador



Integração do Cartão de Cidadão

- Em *Windows*, o NexU já permite assinaturas com o Cartão de Cidadão português.
- Basta utilizar a API *MSCAPI* do *Windows* para interação com *Smart Cards* (não existe ligação automática com o CC português)



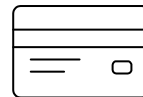


Timestamp do Cartão de Cidadão

- Utilizado em todos os tipos de ficheiros que a aplicação permite assinar.
- Foi necessário alterar a configuração do **Timestamp Protocol (TSP)**, de modo a utilizar o servidor do Cartão de Cidadão português.
- No ficheiro *tsp-config.xml* alterou-se o *bean* que corresponde à fonte do *timestamp*.

Alteração do servidor do timestamp

```
22 <bean id="tspSource" class="eu.europa.esig.dss.service.tsp.OnlineTSPSource">
23   <constructor-arg name="tspServer" value="http://ts.cartaodecidadao.pt/tsa/server" />
24   <constructor-arg name="dataLoader" ref="tspDataLoader" />
25 </bean>
26
27 <bean id="tspDataLoader" class="eu.europa.esig.dss.service.http.common.CommonsDataLoader">
28   <constructor-arg name="contentType" value="application/timestamp-query" />
29 </bean>
```





Integração da Chave Móvel Digital

- Com base no projeto desenvolvidos por alunos do ano passado.
- Foi necessário adicionar uma dependência.
- Foi criada uma nova área na página de aplicação.





Integração da Chave Móvel Digital

- Esta nova página tem 3 estados diferentes:
 - **Página Principal** – contém a introdução dos dados da CMD e da assinatura a gerar;
 - **Página de OTP** – onde é se introduz o OTP recebido;
 - **Página de *Download*** – onde é feito o *download* do ficheiro assinado.
- Validação das entradas utilizando a *framework Spring*.
- Funciona para todos os tipos de validação e *hash* disponíveis.



Login na DSS Web App

- Último requisito do projeto: guardar dados e configurações do utilizador de modo a que quando fizesse *login* pudesse usar os seus dados perante a CMD.
- Optou-se por guardar apenas o nº de telemóvel no lado do cliente, para cumprir com as leis de proteção de dados pessoais
- Fica guardado na *localStorage* do *browser* do cliente.
- Caso já esteja lá guardado é recuperado automaticamente.
- O utilizador escolhe se quer guardar o número através de uma *checkbox*.



Técnicas de Desenvolvimento de Software Seguro

- OWASP Software Assurance Maturity Model (SAMM)
- Microsoft Security Development Lifecycle (SDL)
- OWASP Application Security Verification Standard
- PIA
- *Buffer Overflow*
- Vulnerabilidade de inteiros
- Validação de *Input*



Microsoft SDL

Este modelo de desenvolvimento de *software* seguro divide-se em 7 fases.

- **Fase de Formação**
 - Todos os elementos do grupo adquiriram conhecimentos a nível de segurança de software no perfil de Criptografia e Segurança da Informação.
- **Fase de Requisitos**
 - Garantir que as normas definidas pelo RGPD são cumpridas;
 - Seguir o standard de verificação de segurança de aplicações (*OWASP Application Security Verification Standard*)



Microsoft SDL

- Fase de Desenho

Procurou-se identificar possíveis riscos para o sistema.

- *Denial of Service*
 - Os invasores podem congestionar a rede com ruído que pode provocar colisões de sinal e produção de erros.
 - Se a rede for sobrecarregada por utilizadores da aplicação pode levar a uma desconexão do serviço.



Microsoft SDL

- **Fase de Codificação**
 - Teve-se em atenção o processo de codificação, procurando adotar boas práticas.
- **Fase de Verificação**
 - Revisão e testes manuais das funcionalidades, procurando descobrir alguma abertura no sistema que necessitasse de ser corrigido.
- **Fases de Publicação e de Resposta**



OWASP Application Security Verification Standard

Tendo em conta a lista *standard* mais recente, (2017).

- **A1 - Injeção de Código**
 - Adequada validação de *input*.
- **A2 - Quebra de autenticação**
 - Contacto telefónico não é uma informação que por si só traga vantagens a um atacante.
- **A3 - Exposição de dados sensíveis**
 - Não foram armazenados dados confidenciais.



OWASP Application Security Verification Standard

- **A6 - Configuração incorrecta de segurança**
 - Procurou-se que os erros do sistema não sejam expostos ao utilizador.
- **A7 - *Cross-Site Scripting***
 - Todos os dados recebidos são validados e nenhuma informação é enviada para o *browser* sem ter sido previamente verificada e filtrada.



Outras práticas de segurança

- **PIA**
 - Para demonstrar *compliance* com o RGPD (Regulamento Geral de Proteção de Dados)
- ***Buffer Overflow***
 - Programas em Java, como é o caso da DSS WebApp, não são vulneráveis a problemas de *Buffer Overflow*.



Outras práticas de segurança

- **Vulnerabilidade de Inteiros**
 - Não se aplica
 - N° de telefone, Pin da CMD e o código de confirmação guardados numa *string*
- **Validação de *Input***
 - Validação do n° de telemóvel, o PIN da CMD associada e o código OTP recebido no telemóvel.





Instalação da App

- Requisitos
- Processos de instalação detalhados no relatório.
 - Em *Windows* e *Linux*
- **Nota:** A funcionalidade de assinatura com Cartão de Cidadão apenas está disponível em Windows.





Utilização da App

Digital Signature Services > Sign a document with CMD

e-Signature	Sign a document with CMD
Sign a document	File to sign <input type="button" value="Browse..."/> 150.pdf
Sign a digest	Container <input checked="" type="radio"/> No <input type="radio"/> ASIC-S <input type="radio"/> ASIC-E
Sign a PDF	Signature format <input type="radio"/> XAdES <input type="radio"/> CAdES <input checked="" type="radio"/> PAdES <input type="radio"/> JAdES
Sign with JAdES	Packaging <input checked="" type="radio"/> Enveloped <input type="radio"/> Enveloping <input type="radio"/> Detached <input type="radio"/> Internally detached
Sign multiple documents	Level <input type="text" value="PAdES-BASELINE-LTA"/>
Counter sign a signature	Digest algorithm <input type="radio"/> SHA1 <input checked="" type="radio"/> SHA256 <input type="radio"/> SHA384 <input type="radio"/> SHA512
Standalone application	Allow expired certificate <input type="checkbox"/>
REST/SOAP WebServices	Add a content timestamp <input checked="" type="checkbox"/>
e-Signature with CMD	Phone Number (Intl. format) <input type="text" value="+351 931744118"/>
Sign a document	PIN <input type="text" value="*****"/>
Server side	<input type="button" value="Submit"/> <input type="button" value="Clear"/>
Extend a signature	
Timestamp document(s)	



Simple Report	Detailed Report	Diagnostic tree	ETSI Validation Report
Validation Policy : QES AdESQC TL based <input type="button" value="Print"/> <input type="button" value="Download as PDF"/>			
Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).			
Signature S-FFC8D4EA4D327B8F50497CDA75F3118C4AC1BB4A6BA8E1F17CF27CD12A455D4			
Qualification:	QESig ⓘ		
Signature format:	PAdES-BASELINE-LTA		
Indication:	TOTAL PASSED ✓ The authority info access is not present!		
Certificate Chain:	🔗 Diogo Miguel Pinto Rio 🔗 EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão 00003		
On claimed time:	2021-06-21T13:41:33		
Best signature time:	2021-06-21T12:44:18 ⓘ		
Signature position:	1 out of 1		
Signature scope:	Partial PDF (PARTIAL) The document ByteRange : [0, 85179, 123069, 494]		
Document Information			
Signatures status:	1 valid signatures, out of 1		
Document name:	150-signed-pades-baseline-lta.pdf		



Conclusão

- Este projeto permitiu **integrar/utilizar APIs** e código de terceiros de modo a simplificar o processo de desenvolvimento ou **aumentando a sua segurança**.
- Parte **mais desafiante**: instalação da *DSS Demo WebApp*
 - falhas na compilação das várias dependências que eram necessárias para construir as várias partes que compõem a aplicação
- A nível de **segurança**, foram tidos em conta as estratégias e recomendações que foram lecionadas ao longo da unidade curricular.





Conclusão

- **Trabalho futuro:**
 - **integrar sessões** na plataforma, para permitir guardar outros dados além do seu contacto, como um histórico das operações realizadas (para poder reutilizar acções);
 - **Implementar diretamente a configuração**, no NexU, para a assinatura com o Cartão de Cidadão, sem ser necessário configurá-la nenhuma vez.
 - Implementar as outras **páginas da aplicação DSS WebApp** no separador do **CMD**.
 - Aplicação de outras estratégias de *software* seguro, como o recurso a programas de detecção de **vulnerabilidades de software**.

