Universidade do Minho

Escola de Engenharia

DSS Demo WebApp

Projeto de desenvolvimento 2 (PD2)

Engenharia de Segurança

Trabalho realizado por:

Duarte Oliveira (pg47157)

Melânia Pereira (pg47520)

Paulo Ricardo Pereira (pg47554)

Junho de 2022

Conteúdo

Capítulo 1

Introdução

1.1 Contextualização

As assinaturas digitais são cada vez mais utilizadas no dia-a-dia atual, tornando cada vez mais necessárias ferramentas e software que permitam a sua criação e validação, tendo sempre em conta o regulamento eIDAS (*electronic IDentification Authentication and trust Services*) e standards relacionados.

A União Europeia disponibiliza uma biblioteca de software *open-source* (*Digital Signature Services* - DSS) para a criação e validação de assinaturas eletrónicas, em linha com o Regulamento eIDAS e standards relacionados.

Assim, este projeto foca-se na utilização e integração de ferramentas disponibilizadas pela DSS, tendo por base a *DSS Demo Web App*, disponibilizada também pela DSS como aplicação de demonstração, para adicionar a esta última algumas funcionalidades de interesse para a criação e validação de assinaturas eletrónicas de forma cada vez mais prática e cómoda para o utilizador, mantendo sempre o máximo de segurança e confiança possível.

1.2 Objetivos

Este projeto de desenvolvimento parte da reutilização do projeto do ano letivo anterior, no qual os alunos alteraram a *DSS Demo WebApp* (v. 5.8.2) de modo a poder ser utilizada com:

- cartão de Cidadão;
- chave Móvel Digital;
- a fonte de *timestmap* do Cartão de Cidadão, de modo a não se utilizar a *dummy timestamp source* que é utilizada nas várias opções da *Demo WebApp* que utilizam *timestamp*.

O objetivo é transpor as alterações referidas em cima (já efetuadas), para a nova versão da *DSS Demo WebApp* (v. 5.10.1 ou superior). Pretende-se também

- Adicionar uma *interface* de autenticação inicial (com utilizador e password);

- Adicionar uma área de utilizador, onde o utilizador (após autenticação) possa definir qual o número de telemóvel que utiliza para a Chave Móvel Digital – sendo os dados do utilizador guardados em Base de Dados;
- Alterar o código efetuado pelos colegas do ano passado, de modo que seja utilizado o número de telemóvel guardado na área de utilizador, sempre que o utilizador efetue uma operação que utilize a Chave Móvel Digital;
- Adicionar a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação na raiz) em ficheiro (formato PEM e/ou DER), nas opções de assinatura: *Counter sign a signature*.

Para além das funcionalidades mencionadas, pretende-se que sejam usadas metodologias de desenvolvimento de software seguro, realçando-se a *Fundamental Practices for Secure Software Development*, o *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*, e o *Microsoft Security Development Lifecycle (SDL)*. É ainda requerida a identificação e melhoria das capacidades do grupo de trabalho nesta vertente, através do modelo de maturidade *OWASP Software Assurance Maturity Model* (SAMM) e que a implementação tenha em conta o *standard* de verificação de segurança de aplicações, *OWASP Application Security Verification Standard*, bem como a utilização de ferramentas de análise de impacto da proteção de dados (*PIA - Privacy Impact Assessment*) para demonstrar *compliance* com o Regulamento Geral de Proteção de Dados (RGPD).

Capítulo 2

Solução

Neste capítulo apresenta-se a implementação das novas funcionalidades pedidas assim como a transposição das alterações já feitas pelos colegas do ano anterior da versão 5.8.2 para a versão 5.10.1.

2.1 Transposição das alterações efetuadas no ano anterior

Para efetuar esta transposição, o grupo começou por analisar o código fornecido dos colegas do ano anterior e compará-lo com o código disponibilizado da *DSS Web App* na sua versão mais recente à data (5.10.1). Desta forma foi necessária uma profunda e repetida comparação das diretorias e ficheiros associados a ambos os projetos, utilizando ferramentas e comandos para analisar cada um e compará-los. Foi necessária alguma paciência pois houve alturas em que se esperava que a compilação do projeto atualizado (5.10.1 com as funcionalidades implementadas no ano anterior) funcionasse, e tal não se verificava. Apesar disso, e depois de alguma persistência, finalmente se conseguiu verificar o funcionamento correto da aplicação, conforme esperado.

2.1.1 Integração do Cartão de Cidadão

Depois de lido também o relatório dos colegas, foi possível perceber que para adicionar esta funcionalidade é apenas necessário instalar o NexU, pois este já permite assinaturas com recurso ao Cartão de Cidadão, no entanto, isto apenas é possível em ambiente Windows. Toda o processo de utilização do NexU para a assinatura com recurso ao Cartão de Cidadão pode ser seguido no relatório dos colegas do ano passado.

2.1.2 Integração da Chave Móvel Digital

Tal como fez o grupo do projeto do ano anterior, o *ApplicationID* foi reutilizado do código dos colegas do ano letivo 2019/2020.

Foi também, à semelhança do que foi feito pelos colegas, gerado um WSDL baseado na versão mais recente da descrição dos serviços Web existentes no servidor da AMA.

Foi ainda necessário adicionar uma dependência no ficheiro `pom.xml` para permitir a

```java
public class CMDService {
    private final static byte[] APPLICATION_ID = "b826359c-06f8-425e-8ec3-50a97a418916".getBytes();
```

Figura 2.1: Valor do ApplicationID

```java
static {
    URL url = null;
    WebServiceException e = null;
    try {
        url = new URL( spec: "https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/CCMovelDigitalSignature.svc?wsdl");
    } catch (MalformedURLException ex) {
        e = new WebServiceException(ex);
    }
    CCMOVELDIGITALSIGNATURE_WSDL_LOCATION = url;
    CCMOVELDIGITALSIGNATURE_EXCEPTION = e;
}
```

Figura 2.2: Bloco de código para a geração do WSDL

comunicação da biblioteca Apache CXF através de canais seguros (HTTPs).

```xml
<dependency>
    <groupId>org.apache.cxf</groupId>
    <artifactId>cxf-rt-ws-security</artifactId>
    <version>2.2.3</version>
</dependency>
```

Figura 2.3: Dependência necessária

Finalmente, foi necessário adicionar um novo *card* ao menu lateral para aceder à opção de assinatura com a CMD e implementar a página, cujo código foi reutilizado do projeto dos colegas do ano passado.

2.1.3 Utilização da fonte de timestamp do Cartão de Cidadão

Para alterar o tipo de timestamp utilizado pela aplicação de *dummy* para a do Cartão de Cidadão, foi necessário alterar o bean que corresponde à fonte do timestamp para o seguinte:

2.2 Interface de autenticação inicial

Para adicionar uma interface de autenticação inicial, que apenas permitisse um utilizador aceder às restantes funcionalidades da aplicação no caso de um *login* de sucesso, foi necessário recorrer à biblioteca `HttpSecurity` que permite dar ou não autorização de acesso a determinadas páginas e, além disso, fazer um *login* que, se bem sucedido, permite então a o acesso a todas as páginas e, consequentemente funcionalidades da aplicação.

Além disto, e também porque um dos requisitos é a utilização de uma base de dados para guardar os dados do utilizador, foi necessário também, então, fazer a conexão com uma base de dados. O software escolhido para a base de dados foi o MySQL e a conexão e autenticação é feita usando a biblioteca `DriverManagerDataSource` e a API JDBC.

```
<bean id="tspSource" class="eu.europa.esig.dss.service.tsp.OnlineTSPSource">
    <constructor-arg name="tspServer" value="http://ts.cartaodecidadao.pt/tsa/server" />
    <constructor-arg name="dataLoader" ref="tspDataLoader" />
</bean>

<bean id="tspDataLoader" class="eu.europa.esig.dss.service.http.commons.CommonsDataLoader">
    <constructor-arg name="contentType" value="application/timestamp-query" />
</bean>
```

Figura 2.4: Alteração da fonte do timestamp

```
http.authorizeRequests() ExpressionUrlAuthorizationConfigurer<...>.ExpressionInterceptUrlRegistry
    .antMatchers( ...antPatterns: "/css/**","/images/**","/fonts/**","/webjars/**").permitAll()
    .antMatchers( ...antPatterns: "/signup", "/signup_process").permitAll()
    .anyRequest().authenticated()
    .and() HttpSecurity
    .formLogin() FormLoginConfigurer<HttpSecurity>
    .loginPage("/login")
    .defaultSuccessUrl("/user-profile")
    .permitAll()
    .and() HttpSecurity
    .logout() LogoutConfigurer<HttpSecurity>
    .logoutSuccessUrl("/login")
    .permitAll()
    .and() HttpSecurity
    .csrf() CsrfConfigurer<HttpSecurity>
    .disable();
```

Figura 2.5: Acessos à View e controlo do fluxo de execução da autenticação

Para ter uma opção de autenticação é necessário também ter uma opção de registo na plataforma. E para ter estas opções é também ainda necessário ter a representação de um utilizador, pelo que foi necessário desenvolver uma classe `User` que contém os atributos necessários para o registo e autenticação, sendo eles:

- Username
- Password
- Número de telemóvel

Então, para implementar esta funcionalidade foram, primeiramente, geradas duas páginas html, usando um layout parecido com o layout base da aplicação, ao qual apenas foi retirado o menu lateral de navegação.

Estas duas páginas são idênticas e apresentam duas caixas de texto onde o utilizador deve inserir o seu nome de utilizador e uma password. O que difere entre o login e um novo registo são os seus *Controllers*.

No caso do login, como é usada a biblioteca `HttpSecurity`, como referido anteriormente, não é necessária a criação de um controlador porque a biblioteca faz essa gestão.

Já para o registo, foi necessário desenvolver um controlador para o método REST GET e para o POST. Para o GET, é apenas criado um novo `User`, enquanto que para o POST é necessário fazer efetivamente o registo e adicionar um novo utilizador à base de dados. Para

```
DriverManagerDataSource dataSourceBuilder = new DriverManagerDataSource();
dataSourceBuilder.setDriverClassName("com.mysql.jdbc.Driver");
dataSourceBuilder.setUrl("jdbc:mysql://localhost:3306/pd2?serverTimezone=UTC&useSSL=false");
dataSourceBuilder.setUsername("root");
dataSourceBuilder.setPassword("root");

this.dataSource = dataSourceBuilder;
auth.jdbcAuthentication()
        .dataSource(dataSource)
        .usersByUsernameQuery("select username,password,1 from users where username = ?")
        .passwordEncoder(passwordEncoder())
        .authoritiesByUsernameQuery("select username,'ROLE_USER' from users where username = ?");
```

Figura 2.6: Conexão à base de dados

isto, foi criada uma classe `LoginService`, que se comporta como um DAO (Data Access Object) e que faz uma conexão com a base de dados, e lança *queries* à mesma, *queries* estas que passam por adicionar um novo utilizador, alterar o número de telemóvel de um utilizador já existente e também obter dados relativos a um determinado utilizador.

```
@GetMapping(value = "/signup")
public String showRegistrationForm(Model model) {
    User user = new User();
    user.setTelemovel("+351 ");
    model.addAttribute( attributeName: "user", user);

    return "signup";
}

@PostMapping(value = "/signup_process")
public String processRegister(@ModelAttribute("user") @Valid User user) throws SQLException {
    boolean f = this.loginService.validateUser(user.getUsername());
    if (f) {
        BCryptPasswordEncoder passwordEncoder = new BCryptPasswordEncoder();
        String encodedPassword = passwordEncoder.encode(user.getPassword());
        user.setPassword(encodedPassword);
        this.loginService.addUser(user.getUsername(), user.getPassword());
        return "login";
    } else{
        return "signup";
    }
}
```

Figura 2.7: pedidos GET e POST para o login

2.3 Área de utilizador

A área de utilizador trata-se apenas de uma nova página que pode ser acedida pelo utilizador através do menu lateral.

Para permitir a alteração do número de telemóvel do utilizador foi criado um novo *Controller* que acede mais uma vez à classe de acesso à base de dados (`LoginService` para fazer uma atualização do número de telemóvel para o utilizador atualmente autenticado.

Para saber qual utilizador que está autenticado, recorreu-se à biblioteca **UserDetails** e à `SecurityContextHolder`, que permitem obter todos os dados relativos à autenticação.

```java
@GetMapping("/user-profile")
public String show(Model model) throws SQLException {

    User user = new User();
    String username = this.getLoggedUser();
    String number = this.loginService.getTelemovel(username);
    user.setUsername(username);
    user.setTelemovel(number);
    model.addAttribute( attributeName: "user", user);

    return "user-profile";
}

@PostMapping("/update-phone-number")
public String update(@ModelAttribute("user") @Valid User user) throws SQLException {
    this.loginService.setTelemovel(user.getUsername(),user.getPassword());

    return "user-profile";
}
```

Figura 2.8: Atualização do numero de telemóvel

```java
private String getLoggedUser(){
    Object principal = SecurityContextHolder.getContext().getAuthentication().getPrincipal();
    String username;
    if (principal instanceof UserDetails) {
        username = ((UserDetails)principal).getUsername();
    } else {
        username = principal.toString();
    }
    return username;
}
```

Figura 2.9: Recolha de dados relativos ao *user* que fez login

2.4 Utilização do número de telemóvel guardado na área de utilizador

Implementar esta funcionalidade mostrou-se bastante simples. Foi apenas necessário alterar no controlador da assinatura com CMD (`CMDSignatureController`) a fonte do número de telemóvel a usar, o qual, em vez de ser introduzido pelo utilizador no *form*, é recuperado através da classe de acesso à base de dados.

```java
signatureDocumentForm.setUserId(loginService.getTelemovel(getLoggedUser()));
```

Figura 2.10

Para além disto foi também removida da página html o campo de introdução do número de telemóvel.

2.5 Assinar com chaves privadas em ficheiro na opção de assinatura Counter sign a signature

Não implementado.

Capítulo 3

Técnicas de desenvolvimento de software seguro

3.1 OWASP *Software Assurance Maturity Model* (SAMM)

O Modelo de Maturidade *Software Assurance Maturity Model* (SAMM) é uma referência do *Secure Software Development Lifecycle (S-SDLC)* para introduzir segurança neste processo de desenvolvimento de software.

O modelo de maturidade permite identificar as capacidades do grupo de trabalho, promover o seu desenvolvimento e avaliar e implementar uma estratégia de segurança para o projeto.

Este modelo foi preenchido de acordo com as instruções da ficha da aula 9. No anexo A, é possível ver os resultados obtidos bem como o *link* para o ficheiro *xlsx*.

3.2 *Microsoft Security Development Lifecycle* (SDL)

3.2.1 Fase de Formação

Dado que todos os elementos do grupo realizaram o perfil de Criptografia e Segurança da Informação no mestrado de Engenharia informática, o grupo adquiriu bons conhecimentos a nível de segurança de software.

3.2.2 Fase de Requisitos

O grupo decidiu desde logo priorizar as questões de segurança do projeto — garantir a integridade, autenticidade e confidencialidade dos dados; ter em conta a legislação em vigor normas definidas pelo RGPD; seguir o *standard* de verificação de segurança de aplicações OWASP.

3.2.3 Fase de Desenho

A identificação de possíveis riscos para o sistema pode ser facilmente percebida pela leitura do presente capítulo, destacando-se a criação do modelo de maturidade *Software Assurance Maturity Model* (SAMM).

3.2.4 Fase de Codificação

O grupo sempre procurou adotar boas práticas de programação. No capítulo 4, pode inclusive ver como instalar a *DSS WebApp* de forma segura.

3.2.5 Fase de Verificação

Vários testes manuais foram feitos de forma a garantir a correta implementação das funcionalidades, procurando sempre descobrir alguma falha no sistema.

3.2.6 Fases de Publicação e de Resposta

Uma vez que se trata de um projeto de âmbito académico, estas fases não se aplicam.

3.3 Vulnerabilidade de inteiros e Validação de Input

Erros com Inteiros podem provocar comportamentos indesejados nos sistemas. Quando explorados, podem causar o *crash* de um programa, corromper dados ou até permitir a execução de software malicioso. Desta forma, optou-se por guardar os valores inteiros (como por exemplo o número de telemóvel) em *Strings*.

Além disso, os *inputs* recebidos são também validados com recurso a expressões regulares. Assim, o número de telemóvel deve ser um número válido em território nacional, i.e., que cumpra os seguintes requisitos:

- começa com o código identificador português +351;
- o identificador deverá ser seguido por nove algarismos, que deverão começar com o algarismo 9;
- o tamanho do input deverá ser 13;
- não pode conter letras.

Também, o PIN da CMD deve corresponder a um conjunto de algarismos de tamanho variável entre 4 e 8. O código de confirmação, por fim, que permite gerar a assinatura, recebido no telemóvel, deve conter apenas 6 algarismos.

Finalmente, de forma a garantir segurança das palavras-chave, é obrigatório que elas possuam as seguintes características:

- mínimo de 8 caracteres;

- pelo menos uma letra maiúscula;
- pelo menos uma letra minúscula;
- pelo menos um número.

3.4 *Buffer Overflow*

Esta vulnerabilidade não é preocupante, uma vez que os programas em Java, como é o caso da *DSS WebApp*, não são vulneráveis a problemas de *Buffer Overflow*, uma vez que é Java é *memory safe*, ou seja, não permite o acesso a regiões de memória não alocadas. Assim, não existe perigo de acesso à memória indevida — exceções são lançadas para impedir que tal aconteça.

Capítulo 4

Utilização da aplicação

4.1 Requisitos de instalação

Os requisitos mínimos exigidos pela documentação da DSS1 para instalar a aplicação com sucesso são os seguintes - (de acordo com a nossa testagem):

- Java Versão igual ou superior a 17.0.2
- Maven Versão igual ou superior a 3.8.6
- (Opcional) wine-5.0
- Um sistema operativo Linux ou *macOS*

4.2 Instalação da DSS WebApp - Linux e macOS

- Aceder à diretoria *AP2-PD2/dss-demonstrations*;
- executar o comando *mvn clean install*;
- na diretoria *AP2-PD2/dss-demonstrations* aceder à diretoria *dss-demo-bundle/target*;
- executar o comando *unzip dss-demo-bundle-5.8.2.zip*;
- aceder à diretoria dss-demo-bundle-5.8.2;
- caso tenha o *wine* instalado;
  - executar o comando *wine cmd*;
  - na consola executar o comando *start Webapp-Startup.bat*;
  - no seu *webrowser* favorito aceder a *localhost:8080*;
- caso não tenha o *wine* instalado:
  - aceder à diretoria *apache-tomcat-8.5.78/bin* ;
  - executar o comando *chmod +x catalina.sh startup.sh shutdown.sh*;
  - executar *./startup.sh* para iniciar a aplicação;
  - executar *./shutdown.sh* para terminar a aplicação;

Capítulo 5

Conclusão

Concluindo existem algumas notas a se terem em consideração. Em primeiro lugar, percebemos todo o carácter de desenvolvimento associado a este projeto prático. Nessa vertente, não podemos deixar de referir as dificuldades que tivemos na conceção da solução deste problema.
Inicialmente foi necessária toda uma familiarização relativamente ao projeto original, bem como perceber de que forma estava dividido e desenvolvido o *DSS*. Para tal, foi preciso entender de que forma compilar e executar o programa, bem como perceber onde realmente fazê-lo. Após isso, foi necessário proceder à passagem de todos os ficheiros que trazem todas as funcionalidades associadas ao projeto do ano passado para a versão atualizada deste projeto. Isto não se revelou tarefa fácil pois, apesar de alguma ambientação a toda a modularidade do projeto original, não tínhamos bem a perceção de onde seriam as diretorias a alterar ou às quais tínhamos que adicionar ficheiros. Deste modo, foi necessário fazer um prolífero e exaustivo processo de verificação de ficheiros, utilizando para tal diferentes ferramentas de comparação de diretorias e ficheiros.
Em segundo lugar, procedeu-se ao desenvolvimento da aplicação em si. Tal como referido no enunciado, esperava-se a reutilização de código de terceiros e utilização da *framework* associada a este projeto. Nessa perspetiva, tivemos **bastantes dificuldades**. Esta foi a fase à qual dedicamos mais tempo e na qual tivemos menos resultados. O nosso grupo sentiu bastantes dificuldades em perceber o **desenvolvimento web** na linguagem *Java* com a *framework Spring*, e apesar de muita pesquisa, muitas horas a ler e a interpretar código, tivemos bastantes problemas ao tentar implementar o que nos era proposto, muitas vezes por problemas que acabavam por gerar outros problemas, o que era dificultado pela falta de conhecimento da nossa parte.
Obviamente não sendo desculpa, isto pôs bastante em causa o nosso desempenho, pois, nesse sentido, dedicamos bastantes horas ao desenvolvimento deste projeto.
Por último, apesar de sentirmos que tivemos um desempenho satisfatório, percebemos totalmente que não conseguimos fazer tudo o que nos era proposto e nesse sentido, assumimos que existiram falhas, não a nível de esforço mas na vertente de perceção no desenvolvimento destas novas características a acrescentar à plataforma, tal como acabamos de justificar.

Apêndice A

SAMM

Os resultados desta avaliação encontram-se aqui.

A.1 Pergunta P2.1

As práticas de segurança escolhidas foram o *Threat Assessment* e os *Security Requirements* da área *Construction*, e o *Security Testing* da área *Verification*. As áreas escolhidas são as mais adequadas e as mais exequíveis ao nosso projeto, dada a dimensão do mesmo e dos recursos humanos e técnicos da equipa de desenvolvimento.

A.2 Pergunta P2.2

O *score* obtido pelo preenchimento do documento *SAMM_grupo8.xlsx* relativamente às práticas de *Threat Assessment* e *Security Testing*, revela o objetivo de alcançar o nível 1 de maturidade. Em relação à prática de *Security Requirements*, uma vez já atingido o nível 1, o objetivo é avançar para o nível 2.

A.3 Pergunta P2.3

Threat Assessment: documentar os piores casos de ataque ao software, bem como os tipos de agentes invasores e atacantes e as suas potenciais motivações para abusar do nosso software.

Security Testing: documentar os casos de teste que são desejáveis executar e informar devidamente os *stakeholders* dos resultados destas operações e das questões de segurança relacionadas com a criação do projeto.

Security Requirements: definir uma equipa para rever, periodicamente, a maioria dos controlos de acesso ao projeto, e fazer *benchmarking* de diferentes atividades de segurança, implementando as que forem consideradas importantes.

Apêndice B

DPIA

B.1 Identifique os nove critérios que devem ser considerados para avaliar se o processamento de dados pessoais irá resultar num risco elevado.

1. **Avaliação ou *scoring*, incluindo caracterização e previsão**, principalmente de aspetos relativos a saúde, situação económica, preferências ou interesses pessoais, localização, movimentações, comportamento ou o desempenho de trabalho.
2. **Tomadas de decisões automatizadas que tenham um efeito legal ou similar significante** na pessoa em causa, por exemplo, cujo processamento possa levar a exclusão ou discriminação de indivíduos.
3. **Monitorização sistemática** dos sujeitos, um processo usado para observar, monitorizar e controlar dados de sujeitos, incluindo dados adquiridos em redes públicas. A recolha dos dados pode ser feita em circunstâncias em que os sujeitos não saibam quem está a recolher os seus dados e como estes serão usados, ainda, pode ser impossível para os indivíduos não serem sujeitos a tal processamento em público.
4. **Dados sensíveis ou de natureza muito pessoal**, que incluem tipos de dados especiais, como as opiniões políticas de um indivíduo, assim como dados relativos a condenações ou infrações criminais. Além destas provisões do GDPR, há outras categorias de dados que são consideradas sensíveis porque estão ligadas a atividades domésticas ou privadas (como comunicações eletrónicas) ou porque impactam o exercício de um direito fundamental (como a localização) ou porque a violação desses dados envolvem sérios impactos na vida do indivíduo. Assim, é importante também perceber se estes dados estão já disponíveis publicamente. Também se incluem dados como documentos pessoais, emails, diários, notas e informação muito pessoal contida em aplicações.
5. **Dados processados em grande escala**, apesar de o GDPR não definir significado de ”grande escala”, há alguns fatores, recomendados pelo WP29, a ter em conta:
   (a) o número de sujeitos de dados implicados, seja como um número específico ou como uma proporção de população relevante;
   (b) o volume de dados ou a gama de itens diferentes de dados a serem processados;
   (c) a duração ou permanência da atividade de processamento;

(d) a extensão geográfica da atividade de processamento.

6. **Correspondência ou combinação de conjuntos de dados**, por exemplo, conjuntos originados de diferentes recolhas e para diferentes propósitos, cuja combinação pode exceder a expetativa razoável do sujeito de dados.

7. **Dados relativos a pessoas vulneráveis**, pela possibilidade da existência de um desequilíbrio de poder entre o sujeito de dados e o controlador, o que significa que os indivíduos podem não ser capazes de consentir ou recusar o processamneto dos seus dados ou mesmo de exercitar os seus direitos. Sujeitos de dados vulneráveis podem incluir crianças, funcionários, segmentos da população que precisam de proteção especial (pessoas doentes, idosos, etc.) e ainda qualquer caso onde se possa encontrar um desequilíbrio na relação entre a posição do sujeito de dados e do controlador.

8. **Uso inovativo ou aplicação de novas soluções tecnológicas ou organizacionais**, como a combinação do uso de impressão digital e reconhecimento facial para controlo de acesso. O GDPR deixa claro que a utilização de uma nova tecnologia pode desencadear a necessidade de realizar um DPIA, devido ao facto de tal tecnologia poder envolver novas formas de recolha e uso de dados pessoais, possivelmente com alto risco para os direitos e liberdades dos indivíduos.

9. **Processamento que proíbe os sujeitos de dados de exercer os seus direitos ou usar um serviço ou contrato**, por exemplo, operações de processamento cujo objetivo é permitir, alterar ou recusar o acesso do sujeito a serviços ou entradas em contratos. Um exemplo disto é quando os bancos avaliam os clientes de acordo com uma base de dados de referência de crédito para decidir se devem, ou não, oferecer-lhes um empréstimo.

B.2 Verifique como é que o PD2 (projeto de desenvolvimento 2, no âmbito da avaliação prática 2) que está a efetuar para esta UC se enquadra nesses nove critérios.

Consideramos que o Projeto de Desenvolvimento 2 que estamos a efetuar se enquadra em quatro dos nove critérios enumerados acima, sendo eles os seguintes:

- **critério 2**, onde os dados processados possam ter um efeito legal significante, devido ao facto de, no projeto, estarmos a tratar de assinaturas digitais de documentos com Cartão de Cidadão que é legalmente vista como uma assinatura manual, ou seja, a realização de uma assinatura digital num documento pode ter implicações legais como as assinaturas manuais em determinados documentos.

- **critério 4**, onde são tratados dados de índole altamente pessoal, pelo facto do projeto necessitar de fazer um processamento dos documentos a assinar, que podem ser documentos pessoais e revelar dados pessoais do indivíduo em causa.

- **critério 7**, onde os dados tratados são relativos a indivíduos vulneráveis do ponto de vista de que estes indivíduos podem não ter a capacidade e consentir ou recusar o tratamento dos seus dados, visto que não temos forma de saber com certeza e exatidão quem são os sujeitos de dados que irão utilizar a aplicação que estamos a desenvolver, pelo que poderão ser cidadãos com necessidade de proteção especial.

- **critério 8**, onde se tem em conta a utilização inovativa de tecnologia, se considerarmos que o uso do Cartão de Cidadão e Chave Móvel Digital para assinatura digital de documentos pode ser considerado como um uso inovador destas tecnologias. Apesar de este já ser um uso comum na sociedade atual, ainda consideramos que seja um uso inovador e que, por isso, o projeto se enquadre este critério.

B.3 DPIA do PD2

Preview

GENERAL INFORMATION

edit

100%

Preview

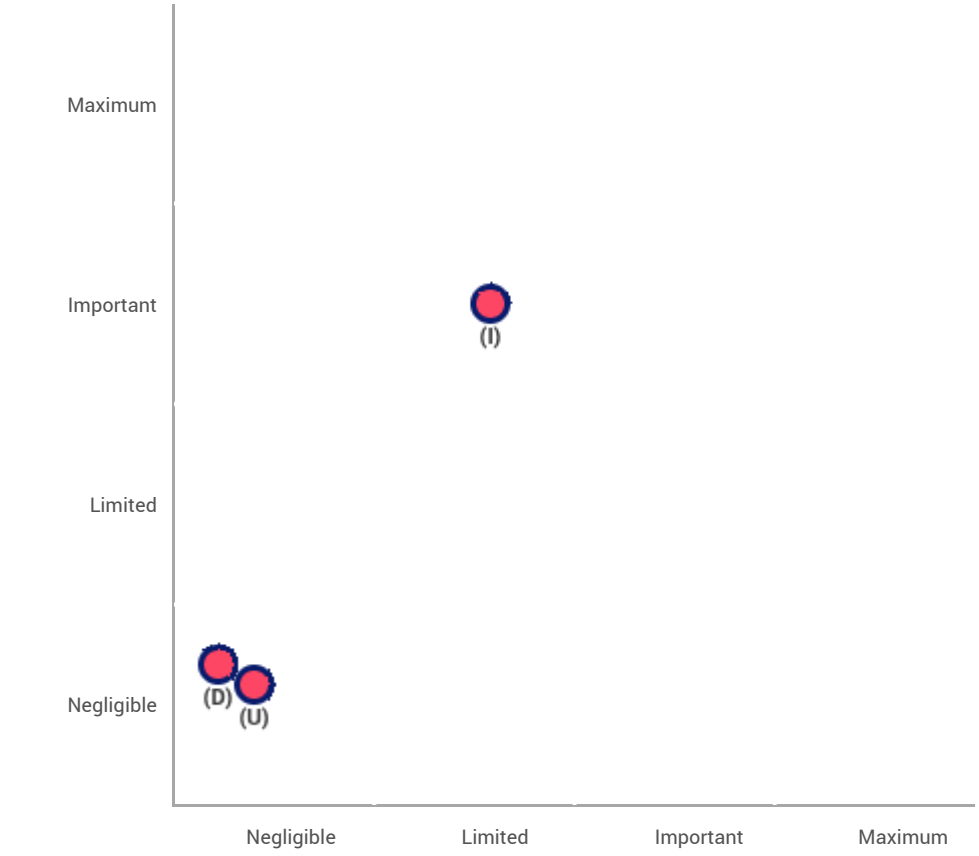
Editing : Grupo 8
Evaluation : Grupo 8
Validation : Grupo 8

Status : Signed validation

Validation

Risk mapping

Risk seriousness



Risk likelihood

- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

6/20/22

Validation

Action plan

Overview

Fundamental principles | Planned or existing measures

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Right of access and to data portability
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers

Redução da acumulação de dados pessoais
Cifragem

Risks

Illegitimate access to data
Unwanted modification of data
Data disappearance

Improvable Measures
Acceptable Measures

Fundamental principles

No action plan recorded.

Existing or planned measures

No action plan recorded.

Risks

No action plan recorded.

Validation

TO TRANSLATE - DPO and data subjects opinion

DPO's name

DPO

DPO's status

The treatment could be implemented.

DPO's opinion

Por respeitar todas as normas, este tratamento pode ser implementado

Search of concerned people opinion

Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested

Não contactável

Não contactável.

Context
Overview

What is the processing under consideration?

Armazenamento dos dados do utilizador para a criação de assinaturas digitais utilizando o Cartão de Cidadão e/ou a Chave Móvel Digital.

What are the responsibilities linked to the processing?

O tratamento de dados vai ser realizado para permitir a criação de assinaturas digitais de documentos, então, é necessário tratar dados do Cartão de Cidadão e da Chave Móvel Digital do utilizador e ainda do documento a ser assinado.

Are there standards applicable to the processing?

As normas descritas pelo Regulamento Geral da Proteção de Dados.

Evaluation : Acceptable

Context
Data, processes and supporting assets

What are the data processed?

Número de telemóvel, sem prazo definido. Os documentos a assinar também são processados e esses dados são conservados apenas durante o tempo de processamento necessário para a realização da assinatura digital.

How does the life cycle of data and processes work?

O número de telemóvel é guardado e consultado e processado quando é necessário realizar a assinatura de um documento. O documento é carregado, os seus dados são processados para realizar a assinatura e depois desta estar gerada, o documento e respetivos dados são descartados.

What are the data supporting assets?

O tratamento feito é integrado numa aplicação da Comissão Europeia, a DSS Web App, por isso, todos os ativos utilizados são os mesmo utilizados por essa aplicação.

Evaluation : Acceptable

Fundamental principles
Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Os dados são tratados apenas para possibilitar a geração da assinatura digital do utilizador, que é a razão pela qual o utilizador os submete à aplicação, então, a finalidade do tratamento é específica, explícita e legítima.

Evaluation : Acceptable

What are the legal basis making the processing lawful?

O fundamento é o consentimento do utilizador para o tratamento dos dados que submete, há um consentimento implícito do tratamento dos dados do documento a assinar visto que, para o assinar,

é necessário utilizá-lo e processá-lo.

Evaluation : Acceptable

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Sim, todos os dados recolhidos são usados para questões de assinatura ou de autenticação, não são recolhidos nem tratados mais dados do que os estritamente necessários.

Evaluation : Acceptable

Are the data accurate and kept up to date?

Sim, o utilizador pode atualizar os seus dados sempre que assim o desejar.

Evaluation : Acceptable

What are the storage duration of the data?

Os dados são conservados apenas durante o tempo necessário para o processamento e realização da assinatura, com exceção do número de telemóvel e credenciais do utilizador, que são armazenados indefinidamente até que o utilizador deseje que estes sejam apagados.

Evaluation : Acceptable

Fundamental principles

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

As informações osbre o tratamento dos dados estão disponíveis na página principal da aplicação e nas páginas onde o utilizador pede a assinatura do documento.

Evaluation : Acceptable

If applicable, how is the consent of data subjects obtained?

O consentimento é obtido quando o utilizador submete o documento na aplicação e efetua login com o Cartão de Cidadão ou Chave Móvel Digital, sendo que estes últimos já pedem o consentimento ao utilizador para a partilha dos dados com a aplicação. O consentimento para o número de telemóvel é obtido quando o utilizador preenche uma caixa de verificação.

Evaluation : Acceptable

How can data subjects exercise their rights of access and to data portability?

O utilizador pode aceder aos seus dados através da aplicação.

Evaluation : Acceptable

How can data subjects exercise their rights to rectification and erasure?

O utilizador pode sempre contactar os responsáveis da aplicação para que os seu dados sejam apagados, e pode retificá-los a qualquer momento através da aplicação.

Evaluation : Acceptable

How can data subjects exercise their rights to restriction and to object?

O utilizador pode sempre contactar os responsáveis da aplicação para alterar as permissões outrora dadas em relação aos seu dados.

Evaluation : Acceptable

Are the obligations of the processors clearly identified and governed by a contract?

Não aplicável.

Evaluation : Acceptable

In the case of data transfer outside the European Union, are the data adequately protected?

Não aplicável.

Evaluation : Acceptable

Risks

Planned or existing measures

Redução da acumulação de dados pessoais

Guardar o mínimo de dados possível, pelo menor tempo possível.

Evaluation : Acceptable

Cifragem

Guardar a "hash" dos dados e não os dados em plaintext.

Evaluation : Acceptable

Risks

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

Possibilidade de assinaturas de documentos com vantagens para o atacante e implicações sérias legais para o utilizador., Roubo de identidade

What are the main threats that could lead to the risk?

Um ataque de Cross-Site Scripting, Um acesso à página fonte da WebApp que possa ser caminho para encontrar uma vulnerabilidade de codificação

What are the risk sources?

Pessoas com conhecimento suficiente e que queiram atacar um utilizador da aplicação.

Which of the identified planned controls contribute to addressing the risk?

Cifragem, Redução da acumulação de dados pessoais

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Um acesso ilegítimo aos dados, neste caso, ao número de telemóvel do utilizador pode ter

um impacto sério muito significativo na vida do mesmo, assim, mesmo com as técnicas de mitigação usadas baixarem a probabilidade de um ataque sucedido, considera-se que o risco é ainda significativo.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, Devido às técnicas de mitigação implementadas, considera-se que a probabilidade de risco é limitada.

Evaluation : Acceptable

Risks

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

O utilizador teria que introduzir o número de telemóvel correto, A autenticcação não é sucedida enquanto o utilizador não efetuar a correção dos dados

What are the main threats that could lead to the risk?

Um ataque de Cross-Site Scripting, Um acesso à página fonte da WebApp que possa ser caminho para encontrar uma vulnerabilidade de codificação

What are the risk sources?

Pessoas com conhecimento suficiente e que queiram atacar um utilizador da aplicação.

Which of the identified controls contribute to addressing the risk?

Redução da acumulação de dados pessoais

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible, Dado um ataque suedido que explore este risco não tem grande impacto para o utilizador, considera-se que a gravidade de risco é insignificante.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, Pelo pouco impacto que tem, considera-se a probabilidade deste risco insignificante.

Evaluation : Acceptable

Risks

Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

O utilizador teria que introduzir o número de telemóvel correto, A autenticc não efetuar a correção dos dados, A autenticcação não é sucedida enquanto o utilizador não efetuar a correção dos dados

What are the main threats that could lead to the risk?

Um acesso à página fonte da WebApp que possa ser caminho para encontrar uma vulnerabilidade de codificação, Um ataque de Cross-Site Scripting

What are the risk sources?

Pessoas com conhecimento suficiente e que queiram atacar um utilizador da aplicação.

Which of the identified controls contribute to addressing the risk?

Redução da acumulação de dados pessoais

How do you estimate the risk severity, especially according to potential impacts and

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible, Este risco tem um impacto muito baixo e pouca utilidade prática para um atacante, por isso, considera-se um risco de gravidade insignificante.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, Devido ao seu baixo impacto e pouca utilidade prática, considera-se a probabilidade deste risco insignificante.

Evaluation : Acceptable

Risks

Risks overview