Avaliação prática 2 - Projeto de desenvolvimento 2 (PD2)

De seguida são apresentados os vários projetos de desenvolvimento 2. O relatório final e o código fonte deverá ser colocado na área do Grupo no github até ao dia 23/06/2022, na subdiretoria "AP2-PD2" (**Note que no relatório tem de indicar os passos necessários para se poder testar o código fonte, incluindo o ambiente (que se espera que seja preferencialmente Linux)**).

.

Data e horário de apresentação do trabalho

Para além da apresentação oral do trabalho, também se vai querer ver o trabalho a funcionar, assim como aceder ao código fonte para que possam explicar código desenvolvido ou algumas das alterações efetuadas.

Local: remoto via Zoom, em https://us02web.zoom.us/j/84769107997?pwd=Qi9KbXNQOXlqWG9DQ2RNSVorKzFPdz09 Data e hora:

- Grupo 1 - 27/06/2023 às 10h00
- Grupo 2 - 27/06/2023 às 10h30
- Grupo 3 - 27/06/2023 às 11h00
- Grupo 4 - 27/06/2023 às 11h30

- Grupo 5 - 27/06/2023 às 12h00
- Grupo 6 - 27/06/2023 às 12h30
- Grupo 7 - 27/06/2023 às 16h00
- Grupo 8 - 27/06/2023 às 16h30
- Grupo 9 - 27/06/2023 às 17h00
- Grupo 10 - 27/06/2023 às 17h30
- Grupo 13 - 27/06/2023 às 18h00

Caso exista algum grupo não identificado, por favor contactem o docente da UC.

Avaliação do PD2

A avaliação do PD2 será efetuada entre 0 e 20 valores. Quem entregar antes da data limite tem uma valorização de 1% na sua nota por cada dia de antecipação.

Note que o projeto de desenvolvimento, para além do desenvolvimento em si, inclui componentes de:

- Identificação do "*Software Assurance Maturity Model* (SAMM)" da equipa,
- RGPD PIA, e
- *Compliance* com boas práticas de desenvolvimento.

Para algumas destas componentes terão questões no âmbito das fichas de trabalho (avaliação prática 1), na sequência de aulas teóricas sobre o tema. Esses relatórios farão parte do relatório final deste projeto de desenvolvimento.

Objectivos

O objetivo destes projetos de desenvolvimento não é aprender a programar (esse poderia ser o objetivo se fosse um projeto no âmbito da licenciatura), mas

- Integrar/utilizar/alterar frameworks, APIs, código de terceiros, ..., que sejam relevantes para o seu projeto, de modo a simplificarem o desenvolvimento e/ou aumentarem a segurança;
- Utilizar metodologia 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);
- Identificar e melhorar as capacidades do grupo de trabalho no desenvolvimento de

software seguro, através do modelo de maturidade OWASP *Software Assurance Maturity Model* (SAMM);

- Seguir o standard de verificação de segurança de aplicações (OWASP *Application Security Verification Standard*), no desenvolvimento do projeto;
- Utilizar ferramentas de análise de impacto da proteção de dados (PIA - *Privacy Impact Assessment*), de modo a demonstrar compliance com o RGPD (Regulamento Geral de Proteção de Dados).

Utilização/integração de ferramentas disponibilizadas no âmbito do Digital Signature Services (DSS)

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.

O código fonte do DSS encontra-se disponível no repositório Bitbucket do DSS e, no github em https://github.com/esig/dss.

Também são disponibilizadas várias aplicações de demonstração da utilização do DSS, que pode encontrar no repositório Bitbucket do DSS e, no github em https://github.com/esig/dss-demonstrations.

DSS Demo WebApp

Como aplicação de demonstração, o DSS disponibiliza a DSS Demo WebApp que pode fazer download e instalar a partir de https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Signature+Service+-+++DSS.

Os seus colegas alteraram a DSS Demo WebApp - versão 5.8.2 - (pode ver no projeto dos seus colegas), de modo a poder ser utilizada com:

- Cartão de Cidadão,
- Chave Móvel Digital, e
- 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*.

Pretende-se que pegue no trabalho dos seus colegas, e:

1. Transponha as alterações que eles já tinham efetuado, para a nova versão da DSS Demo WebApp (versão 5.11.1 ou superior);
2. Adicione interface de autenticação inicial (com utilizador e password);
3. Adicione 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 -;
4. Altere o código efetuado pelos seus colegas, de modo que seja utilizado o número de telemóvel guardado na Base de Dados, sempre que o utilizador efetue uma operação que utilize a Chave Móvel Digital.

Nota: Para testar com a sua Chave Móvel Digital necessita de a ativar (componente de autenticação e assinatura), existindo as seguintes alternativas (entre outras, como pode ver em https://eportugal.gov.pt/servicos/ativar-a-chave-movel-digital):

- em https://www.autenticacao.gov.pt/,
- utilizando a aplicação móvel (app) AutenticaçãoGov (https://www.autenticacao.gov.pt/aplicacao/autenticacao-gov-movel), ou
- por videochamada (processo a iniciar em https://eportugal.gov.pt/servicos/ativar-a-chave-movel-digital).

Este trabalho será efetuado pelos Grupos:

- Grupo 1, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados, em hierarquia até à Entidade de Certificação raiz) em ficheiro (formato PEM), nas opções de assinatura: *Sign a document*.
- Grupo 2, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados, em hierarquia até à Entidade de Certificação raiz) em ficheiro (formato DER), nas opções de assinatura: *Sign a document*.
- Grupo 3, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação raiz) em ficheiro (formato PEM), nas opções de assinatura: *Sign a PDF*.
- Grupo 4, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação raiz) em ficheiro (formato PEM), nas opções de assinatura: *Sign a digest*.
- Grupo 5, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação raiz) em ficheiro (formato PEM), nas opções de assinatura: *Sign with*

JAdES.

- Grupo 6, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação na raiz) em ficheiro (formato PEM), nas opções de assinatura: *Sign multiple documents*.
- Grupo 7, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação na raiz) em ficheiro (formato DER), nas opções de assinatura: *Sign multiple documents*.
- Grupo 8, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação na raiz) em ficheiro (formato PEM), nas opções de assinatura: *Counter sign a signature*.
- Grupo 9, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação raiz) em ficheiro (formato DER), nas opções de assinatura: *Sign a PDF*.
- Grupo 13, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação raiz) em ficheiro (formato DER), nas opções de assinatura: *Sign a digest*.
- Grupo 14, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação raiz) em ficheiro (formato DER), nas opções de assinatura: *Sign with JAdES*.
- Grupo 15, que para além do que é pedido acima, adiciona a possibilidade de assinar com chaves privadas (e respetivos certificados na hierarquia até à Entidade de Certificação na raiz) em ficheiro (formato DER), nas opções de assinatura: *Counter sign a signature*.

Caso exista algum Grupo não identificado, poderão escolher o trabalho a efetuar e deverão indicar qual a sua escolha no relatório final.