Instituto Superior de Engenharia de Lisboa
Mestrado de Engenharia Informática e Multimédia

Carteira Eletrónica Segura

Unidade Curricular: Cibersegurança

Docente: Professor Tiago Dias

Alunos:
Miguel Azenha, nº 47708
Marta Ferreira, nº 50775

25 de novembro de 2025

Índice

Introdução

O presente trabalho prático tem como objetivo explorar a tecnologia Intel Software Guard Extensions (SGX) no desenvolvimento de uma aplicação de carteira eletrónica, destinada ao armazenamento seguro de credenciais de acesso a plataformas informáticas. A segurança e confidencialidade das credenciais são fatores críticos, dado que estas contêm informações sensíveis como nomes de utilizador, senhas de acesso e descrições dos contextos de utilização.

A aplicação a desenvolver deverá permitir a gestão de até 100 credenciais diferentes, disponibilizando funcionalidades essenciais ao utilizador, tais como:

1. criação de uma nova carteira;
2. visualização do conteúdo da carteira;
3. adição de novas credenciais;
4. remoção de credenciais existentes;
5. geração de senhas de acesso seguras, com comprimento variável entre 8 e 100 caracteres.

Para cada credencial, devem ser armazenados o nome de utilizador (até 100 caracteres), a senha de acesso (8 a 100 caracteres) e uma descrição identificativa do cenário de utilização (até 100 caracteres). A persistência dos dados deverá ser garantida através de armazenamento em ficheiro, utilizando cifra AES-GCM de 128 bits para assegurar confidencialidade e integridade, incluindo a senha de acesso que protege a carteira.

Adicionalmente, a funcionalidade de *sealing* deverá ser utilizada para garantir a proteção dos dados no ficheiro, permitindo a sua recuperação segura em execuções posteriores. A minimização da *Trusted Computing Base* (TCB) é recomendada, de forma a reduzir a superfície de ataque e aumentar a segurança global da aplicação.

Este trabalho permite aplicar na prática os conceitos aprendidos em aula, incluindo:

- criação e destruição de enclaves SGX;
- comunicação segura entre aplicação não confiável e enclave (*ECALLs* e *OCALLs*);
- implementação de mecanismos de confidencialidade e integridade em dados persistentes;
- utilização de técnicas de selagem (*sealing*) para armazenamento seguro de dados sensíveis.

A realização deste projeto reforça a compreensão da utilização de enclaves SGX em cenários de segurança real e a importância da proteção de dados sensíveis em aplicações práticas.

Enquadramento Teórico

0.0.1 Título

Conclusões