Projeto 2 - Relatório

Carlos Luz - 73492
Diogo Nunes - 70502

December 2025

1 Introduction

O sistema implementa um armazenamento seguro de ficheiros baseado em blocos, garantindo confidencialidade e controlo de acesso. Os clientes podem registar-se, autenticar-se e armazenar ficheiros encriptados no servidor OBSS, que valida o acesso através do OAMS. O OAS gere a autenticação e emite tokens digitais assinados para validar os utilizadores. Palavras-chave encriptadas e índices locais permitem pesquisa e partilha segura de ficheiros entre utilizadores.

2 Architecture

2.1 OAS Server - Autenticação

O OAS Server funciona como controlo de acesso entre users, onde numa fase inicial, os utilizadores comunicam com o OAS de forma a criarem os tokens de acesso.

Cada utilizador partilha a sua chave publica, o Hash da sua Password e o salt durante a fase de registo.

Na fase de autenticação o utilizador fornece o nonce, o timestamp atual e uma assinatura digital e recebe um token ECDSA assinado que vai ser utilizado para todo o controlo de acessos a ficheiros entre o cliente e o OAMS e OBSS.

2.2 OAMS Server - Controlo de acessos

Gere toda a gestão de acessos do cliente a ficheiros, mantém informações relativas a ficheiros partilhados e valida acesso a ficheiros a partir de tokens verificados com assinaturas digitais do OAS. A identidade dos Clientes é fortemente baseada na geração de um ID anónimo derivado da chave publica de cada utilizador.

2.3 OBSS Server - Block Storage Server

Servidor de armazenamento de Blocos, baseado no desenvolvimento feito no Projeto 1, que nesta segunda fase usa o Servidor OAMS para realizar a gestão

de acesso de utilizadores a ficheiros. Guarda também metadados dos clientes donos dos ficheiros e keywords dos ficheiros.