

Trabalho Prático - 02

Gestor de *Passwords*

Joel Francisco, Rúben Santos

2121000@my.ipleria.pt, 2130725@my.ipleria.pt

ESTG-IPLeria, Leiria, Portugal

Resumo: O presente projeto de gestão de *passwords* tem o objetivo de guardar credenciais de forma centralizada utilizando um serviço *web*, com autenticação por certificado ou nome de utilizador e *password*, pois a maioria destes serviços só permite a segunda opção. Como foi pedido, a aplicação foi desenvolvida usando aplicações universais do Windows 10, para o lado do cliente, e um serviço *WebApi*, para o lado do servidor. Grande parte do cliente e do servidor ficou implementado com alguma segurança, nomeadamente encriptação de *passwords* com o algoritmo Sha256 e duplo *salt*, um salt contante e um *salt* individual por utilizador, para evitar ataques por força bruta (com uso de Rainbow Tables). E ainda, proteção das principais funcionalidades do serviço apenas para utilizadores autenticados. A aplicação ficou com o registo, login (por utilizador/password ou certificado) e acesso a todos os dados do utilizador a funcionar (cada registo de credenciais é guardado num campo Blob binário totalmente encriptado). Não foi implementado um mecanismo (Https) de maneira a garantir confidencialidade e integridade do transporte de dados entre o servidor e o cliente.

Palavras-chave: Segurança, Informação, Certificados, Encriptação, Algoritmos, Autenticação, Hash, Passwords, WinRT, UWP.