

Utilização de Tokens Criptográficos em Linux/Macintosh

Dada a crescente disseminação de certificados digitais e a necessidade da sua utilização quotidiana, os fornecedores lançam cada vez mais dispositivos criptográficos que visam aumentar a mobilidade dos utilizadores sem colocarem em risco a segurança das suas chaves privadas.

Contudo, dada a mobilidade associada a esses dispositivos, é desejável que possam ser utilizados no maior número de plataformas. Todavia, os fabricantes apenas têm privilegiado a portabilidade entre plataformas **Windows**, negligenciando as cada vez mais expressivas plataformas **Linux** e **Macintosh**.

Nesse sentido, a **MULTICERT** pretende promover a experimentação da utilização de *tokens* criptográficos nas referidas plataformas, de forma a eliminar obstáculos a uma total mobilidade dos utilizadores e, dessa forma, potenciar a utilidade desse tipo de dispositivos.

Objectivo:

Com este projecto pretende-se, aproveitando a experiência da **MULTICERT** na utilização de *tokens* criptográficos (nomeadamente *smartcards*) em plataformas **Windows**, desenvolver uma aplicação em **Java** capaz de comunicar com estes através do protocolo **PKCS#11**, em plataformas **Linux** e **Macintosh**.

Considerandos:

- Em caso de dúvidas na implementação do projecto será possível ter o apoio de colaboradores da **MULTICERT** com vasta experiência em **Java** e **PKCS#11**

Notas:

1. As plataformas preferenciais para testes e funcionamento são **Java** e **Linux/Macintosh**
2. A **MULTICERT** pretende adaptar e utilizar os resultados deste projecto.

Acompanhamento:

Este projecto será acompanhado tecnicamente por um elemento do DIUM e por um elemento da **MULTICERT**, a designar. O acompanhamento será efectuado através de ajuda na concretização do trabalho, assim como através de reuniões com periodicidade mensal (embora possa haver fases do projecto em que a periodicidade seja quinzenal).