MEI/MiEI UC de Laboratório de Engenharia Informática

Avaliação de Usabilidade/Compatibilidade de Cadeias de Certificação Heterogéneas

Contexto:

Os mecanismos de certificação de chaves públicas são um componente crucial na segurança dos sistemas informáticos, estando presentes nas mais variadas actividades sociais/cidadania (e.g. navegação web, interacção com organismos do estado, cartão de cidadão, etc). Estes mecanismos pretendem-se estáveis por forma a minimizar interferências no funcionamento das múltiplas actividades que deles dependem, mas avanços recentes na área da Computação Quântica vieram colocar uma pressão elevada para a substituição de algoritmos e tamanhos de chaves a serem contemplados nesses certificados.

Objectivo:

Com este projeto pretende-se realizar um estudo de viabilidade e compatibilidade de sistemas de certificação heterogéneos, que possibilite acomodar na mesma hierarquia diferentes algoritmos e tamanhos de chaves.

Projeto:

O projecto irá avaliar o grau de suporte, por parte dos sistemas operativos actuais (Windows, MacOS, Linux, Android), de uma hierarquia de certificação heterogénea em que se recorrem a diferentes algoritmos e tamanhos de chaves nos diferentes níveis da hierarquia. A hierarquia adoptada deverá replicar a envolvida no cartão de cidadão, possibilitando assim aferir a margem de manobra na adopção de diferentes algoritmos/ tamanhos de chaves nesses dispositivos sem perturbar o eco-sistema envolvente.
Será desenvolvido um protótipo emulando as entidades certificadoras dos diferentes níveis, assim como o próprio cartão (possivelmente recorrendo a um emulador).

Acompanhamento:

Este projeto será acompanhado por José Carlos Bacelar (jba@di.uminho.pt), e por José Eduardo Miranda (Devise Future). É integrado num projecto mais alargado em que está envolvido o HASLAB e a INCM.