MEI/MiEI UC de Laboratório de Engenharia Informática

Validação/verificação do protocolo SAP[1] do SCMD[2]

Contexto:
Portugal, por intermédio da AMA (Agência para a Modernização Administrativa), tem desenvolvido um conjunto de projetos inovadores na área da desmaterialização de documentos e desburocratização de serviços, que se encontram na vanguarda do que é feito a nível europeu e mundial. Um desses projetos, o SCMD, está credenciado (ou em fase de credenciação) de acordo com o regulamento UE 910/2014 (regulamento eIDAS) e permite efetuar assinatura eletrónica qualificada remota, i.e., assinatura eletrónica de dados com uma chave privada que se encontra arquivada remotamente e, através de um dispositivo qualificado de assinatura remoto.
Para garantir que as assinaturas digitais criadas remotamente ("*server-side*") têm o mesmo reconhecimento jurídico que as assinaturas digitais criadas num ambiente totalmente gerido pelo titular da chave privada de assinatura (por exemplo, usando cartões inteligentes), os dados de ativação da assinatura (SAD – *Signature Activation Data* – na nomenclatura anglo-saxónica) são obtidos de acordo com o protocolo de ativação de assinatura (SAP – *Signature Activation Protocol* – na nomenclatura anglo-saxónica), de modo a garantir um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesma.

Encontra uma descrição mais detalhada do SCMD no anexo, na parte final deste documento.

Objectivo:
O protocolo de ativação de assinatura (SAP) tem de garantir um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesmas, assim como tem de ser desenhado para garantir que não está sujeito a várias vulnerabilidades (e.g., ataques *man-in-the-middle*, *online guessing*, *offline guessing*, *credential duplication*, *phishing*, *eavesdropping*, *replay*, *session hijacking*, *man-in-the middle*, *credential theft*, *spoofing* e/ou *masquerading*) que podem comprometer o acesso à chave privada de assinatura.
Com este projeto pretende-se analisar o protocolo SAP e validar/verificar que o mesmo está de acordo com os requisitos elencados no *CEN 419241-1 (prEN 419241-1:2017) – Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements*, através de métodos formais apropriados.

Colaboração:
Este projeto tem a colaboração da Devise Futures e da AMA (Agência para a Modernização Administrativa), existindo a possibilidade de poder evoluir, numa segunda fase, para tema de dissertação de tese de Mestrado.

[1] SAP – *Signature Activation Protocol*
[2] SCMD – Serviço Chave Móvel Digital (assinatura qualificada remota).

Anexo – SCMP (Serviço Chave Móvel Digital)

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS.

Tendo por base a importância da experiência de utilização, conjugado com as novas possibilidades de assinatura eletrónica qualificada "*server-side*" previstas no regulamento europeu 910/2014, o Serviço Chave Móvel Digital (SCMD) disponibiliza o serviço de assinatura qualificada "*server-side*".

Neste contexto, o SCMD gere todos os fluxos de mensagem inerentes ao processo de emissão, ativação e revogação do certificado CMD de assinatura qualificada, assim como da sua utilização para assinatura qualificada "*server-side*" de documentos.

Para garantir que as assinaturas digitais criadas remotamente ("*server-side*") têm o mesmo reconhecimento jurídico que as assinaturas digitais criadas num ambiente totalmente gerido pelo titular da chave privada de assinatura (por exemplo, usando cartões inteligentes), o prestador de serviços de assinatura remota (neste caso, o gestor do SCMD) aplica procedimentos específicos de gestão e segurança administrativa e, utiliza sistemas e produtos confiáveis, incluindo canais de comunicação eletrónicos seguros, para garantir que o ambiente de assinatura do servidor é confiável e que as chaves de assinatura são usadas com um alto nível de confiança sob o exclusivo controle do titular das mesmas.

O sistema confiável para assinatura "*server-side*" (TW4S) devolve, ao assinante ou a uma aplicação, a assinatura digital criada com base nos dados a serem assinados. I.e., o objetivo do TW4S é criar a assinatura digital sob o controlo do titular da chave de assinatura, a partir da representação dos dados a serem assinados (DTBS/R – *Data To Be Signed Representation* – na nomenclatura anglo-saxónica). O TW4S do SCMD é composto por:

- Aplicação de assinatura em servidor (SSA – *Server Signing Application* – na nomenclatura anglo-saxónica), e
- Dispositivo remoto de criação de assinatura/selo (*remote* SCDev – *Signature/Seal Creation Device* – na nomenclatura anglo-saxónica).

A SSA utiliza o *remote* SCDev para utilizar a chave privada de assinatura, sob o exclusivo controle do titular da mesma. Desse modo, quando a SSA utiliza o *remote* SCDev, o assinante autorizado (i.e., o titular da chave de assinatura) controla remotamente a chave de assinatura com um alto nível de confiança.

O *remote* SCDev é um SCDev aumentado com o módulo de ativação de assinatura (SAM – *Signature Activation Module* – na nomenclatura anglo-saxónica), executado num ambiente protegido contra adulteração (*tamper protected environment*, na nomenclatura anglo-saxónica). Este módulo utiliza os dados de ativação da assinatura (SAD – *Signature Activation Data* – na nomenclatura anglo-saxónica), obtidos de acordo com o protocolo de ativação de assinatura (SAP – *Signature Activation Protocol* – na nomenclatura anglo-saxónica), de modo a garantir um alto nível de confiança de que a chave de assinatura é utilizada sob o controlo exclusivo do titular da mesma.