

MEI/MiEI UC de Laboratório de Engenharia Informática

Projetos SCMD¹/SCAP²

Nota: Este enunciado contém vários projetos no âmbito do SCMD e SCAP.

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. Dois desses projetos, o SCMD e o SCAP, estão credenciados (ou em fase de credenciação) de acordo com o regulamento UE 910/2014 (regulamento eIDAS) e permitem respetivamente:

- Assinatura eletrónica qualificada remota, permitindo a qualquer cidadão efetuar a assinatura eletrónica de dados com uma chave privada que se encontra arquivada remotamente e, através de um dispositivo qualificado de assinatura remoto;
- Assinatura eletrónica qualificada na qualidade, através da adição de atributos empresariais a um documento, reconhecendo a qualidade de quem assina.

Encontra uma descrição mais detalhada do SCMD e SCAP nos anexos, na parte final deste documento.

Objectivo:

Com estes projetos pretende-se utilizar as APIs disponíveis para comunicar com o SCMD e SCAP, para desenvolver add-ins/módulos/plug-ins para vários sistemas, permitindo que as funcionalidades do SCMD e SCAP sejam mais facilmente acedidas nas ferramentas utilizadas pelos cidadãos no dia a dia.

Projetos:

As ferramentas às quais se pretende adicionar as funcionalidades do SCMD e/ou SCAP, através de add-ins/módulos/plug-ins, são as seguintes, sendo cada uma considerada como pelo menos um projeto autónomo do Laboratório de Engenharia Informática do MEI/MiEI:

- Adicionar funcionalidade SCMD ao Thunderbird (<https://www.mozilla.org/en-US/thunderbird/>), tendo por objetivo assinar o correio eletrónico com SCMD;
- Estudar como é que se pode adicionar a qualidade/atributo a uma mensagem de correio eletrónico e adicionar funcionalidade SCAP ao Thunderbird (<https://www.mozilla.org/en-US/thunderbird/>);
- Adicionar funcionalidade(s) SCMD e/ou SCAP ao *nextcloud* (<https://nextcloud.com/>) / *owncloud* (<https://owncloud.org/>);
- Adicionar funcionalidade(s) SCMD e/ou SCAP a software de *workflow* de documentos – OpenKM (<https://www.openkm.com/>) ou similar ;

¹ SCMD – Serviço Chave Móvel Digital (assinatura qualificada remota).

² SCAP – Sistema de Certificação de Atributos Profissionais (<https://www.portaldocidadao.pt/web/agencia-para-a-modernizacao-administrativa/sistema-de-certificacao-de-atributos-profissionais-scip-associacao-de-atributos-empresariais>).

- Adicionar funcionalidade(s) SCMD e/ou SCAP a browser web (Chrome, Firefox e/ou Safari);
- Desenvolver app *mobile* que assine documento com SCMD;
- Desenvolver app *mobile* que coloque selo SCAP em documento;
- Desenvolver comando linha (cli) de funcionalidades SCMD/SCAP.

Note-se que os promotores do projeto estão abertos à adição das funcionalidades do SCMD e SCAP a outras ferramentas sugeridas pelos alunos.

Para o desenvolvimento de qualquer um destes projetos, os alunos terão acesso ao ambiente de testes/qualidade do SCAP/SCMD, sendo que após finalização dos testes com sucesso ficará habilitada a ser utilizada em produção.

Colaboração:

Estes projetos têm a colaboração da Devise Futures e da AMA (Agência para a Modernização Administrativa), existindo a possibilidade destes projetos poderem evoluir, numa segunda fase, para temas de dissertação de tese de Mestrado.

Anexos

I – SCAP (Sistema de Certificação de Atributos Profissionais)

O Sistema de Certificação de Atributos Profissionais, através do serviço de associação de atributos empresariais, permite certificar qualidades e poderes do cidadão, no contexto de uma empresa, para autenticação e assinatura qualificada usando o cartão do cidadão.

Com a certificação de qualidades procede-se ao reconhecimento da qualidade presente na certidão permanente da empresa, não necessitando de qualquer documentação adicional. Por exemplo:

- Gerente,
- Administrador.

Com a certificação de poderes procede-se ao reconhecimento dos poderes (ou qualidade profissional) para determinado ato, através de documento específico. Por exemplo:

- Representação de empresa em Procedimento de Contratação Pública,
- Engenheiro.

A assinatura digital qualificada, no âmbito dos atributos profissionais, permite ao titular de um cartão de cidadão, por vontade própria, assumir a autoria de um documento, assinando-o com a chave pessoal existente no seu cartão de cidadão na qualidade das suas funções profissionais.

Um documento assinado pelo titular do cartão de cidadão na qualidade das suas funções profissionais contém:

- Uma assinatura digital qualificada do autor do documento, efetuada através do seu cartão de cidadão (ou outro meio aceite pelo SCAP que permita a um cidadão apor a sua assinatura digital qualificada ao documento);
- Um selo eletrónico qualificado³ aposto pelo Fornecedor de Atributos, por cada atributo qualificador das funções profissionais do autor do documento, que assegura a origem e integridade do atributo, não presumindo a autoria do documento ou a concordância com o seu conteúdo;
- Um selo eletrónico qualificado³ SCAP, por cada atributo qualificador das funções profissionais do autor do documento, que assegura a origem e integridade do atributo, não presumindo a autoria do documento ou a concordância com o seu conteúdo.

³ Selo eletrónico qualificado, de acordo com o regulamento UE 910/2014.

II – 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.