eIDAS Qualified services – serviço de preservação

Contexto

O Regulamento eIDAS (Regulamento UE n.º 910/2014) estabelece uma lista de serviços de confiança qualificados que são reconhecidos (e fazem prova em justiça em todos os Estados-Membros) por todos os Estados Membros independentemente do Estado Membro onde o serviço é prestado, a saber:

a) Serviços de criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais,
b) Serviços de envio registado eletrónico e certificados relacionados com estes serviços,
c) Serviços de criação, verificação e validação de certificados para a autenticação de sítios web,
d) Serviços de preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços.

Esta dissertação foca-se no serviço de preservação de assinaturas eletrónicas (e selos eletrónicos) qualificadas (que doravante designaremos simplesmente por serviço de preservação), que devem começar a ser utilizados massivamente nos próximos anos.

O serviço de preservação, associados a documentos assinados com assinatura eletrónica, podem ter as seguintes alternativas:

- Serviço de preservação com armazenamento (os documentos ficam armazenados do lado da entidade que presta o serviço);
- Serviço de preservação com armazenamento temporário (funciona de modo assíncrono, sendo feito o *upload* dos documentos a preservar, que são "processados" e colocados num *container* em conjunto com relatório de preservação e relatório de validação. No momento em que o dono do *container* levanta ou recebe o *container*, todos os documentos a preservar são apagados);
- Serviço de preservação sem armazenamento (funciona de modo síncrono, e o *container* é devolvido da resposta do pedido de preservação de documentos, não ficando documentos guardados do lado do serviço).

Como os documentos assinados têm que ser "re-preservados" sempre que o *timestamp* está a acabar a validade ou quando há grandes evoluções nas ameaças criptográficas, a preservação com armazenamento permite que a entidade que presta o serviço faça essa operação sem intervenção do titular dos documentos.

No caso da preservação com armazenamento temporário ou sem armazenamento, é necessário existir algum tipo de inteligência do lado da aplicação cliente para ver se os documentos necessitavam de "re-preservação".

Já foi efetuado trabalho prévio no âmbito de uma tese de mestrado[1] finalizada em Abril de 2021, tendo sido desenvolvida uma prova de conceito (aplicação *standalone*) do serviço de preservação.

[1] *eIDAS Qualified Trust Services – Serviço de Preservação*, Dissertação de Mestrado em Engenharia Informática, João Fernandes, Universidade do Minho, 2021

Objetivo

Com esta proposta para dissertação de mestrado pretende-se:

1. Identificar/Analisar requisitos e definir arquitetura e componentes para as várias alternativas do serviço de preservação identificadas anteriormente, de modo que estejam de acordo com o Regulamento eIDAS;
2. Desenvolver *web services* para as alternativas identificadas no ponto anterior;
3. Desenvolver aplicação cliente com algum tipo de inteligência, para casos de uso (a identificar/analisar) de preservação com armazenamento temporário ou sem armazenamento.

Espera-se que no desenvolvimento desta dissertação sejam utilizadas as boas regras de programação, que poderão incluir ferramentas que permitam aquilatar da qualidade do código desenvolvido/utilizado, no que diz respeito a vários factores, como por exemplo: *Code Coverage*, *Abstract Interpretation*, *Compiler Warnings*, *Coding Standards*, *Code Duplication*, *Security*, *Dead Code*.

Preferência:

Dado que a *Digital Signature Service (DSS) library*[2] já disponibiliza muitas das funcionalidades necessárias para um serviço de preservação base, tem-se preferência por candidatos que já tenham tido contacto com essa biblioteca.

Desenvolvimento da Dissertação de Mestrado

A dissertação de mestrado será desenvolvida nas instalações da Devise Futures, em Braga.
Note-se que estão a ser contactadas várias entidades para patrocinarem este desenvolvimento, sendo o trabalho de dissertação remunerado quando isso ocorrer.

Bibliografia

Identifica-se alguma bibliografia (especialmente standards ETSI e RFC) potencialmente relevante:

- Regulamento eIDAS: *REGULAMENTO (UE) N.o 910/2014 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE*[3], em especial o:
  - Artigo 33, e
  - Artigo 40.
- ETSI EN 319 401, Electronic signatures and infrastructures (ESI); General policy requirements for trust service providers
- ETSI SR 019 510, electronic signatures and infrastructures (esi);scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures.

[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Digital+Signature+Service+-++DSS
[3] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32014R0910&from=EN

- ETSI TS 119 511, electronic signatures and infrastructures (esi); policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
- ETSI TS 119 512, electronic signatures and infrastructures (esi); protocols for trust service providers providing long-term data preservation services
- IETF RFC 4998: "evidence record syntax (ers)".
- IETF RFC 6283 (2011): "extensible markup language evidence record syntax (xmlers)".
- ETSI TS 102 918 Associated Signature Containers (ASiC). Electronic Signatures and Infrastructures, (ESI), 2013.

Outra bibliografia:

- Futuretrust - scalable preservation service
- BSI technical guideline 03125 preservation of evidence of cryptographically signed documents, v.1.2.2. 2019.
- Qualified preservation services for qualified electronic signatures and seals - Criteria for assessing compliance with the eIDAS regulation. Agence nationale de la sécurité des systèmes d'information, 2017.
- Tina Hühnlein Mike Prechtl Detlef Hühnlein Florian Otto, Tobias Wich. Towards a standardised preservation service for qualified electronic signatures and qualified electronic seals.