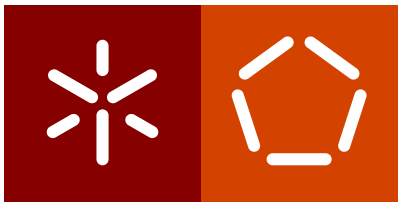
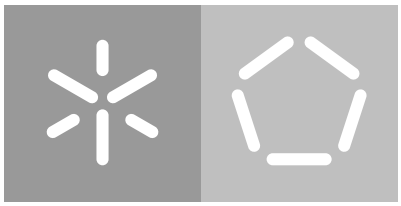


**Universidade do Minho**
Escola de Engenharia
Departamento de Informática

João Manuel da Silva Gomes Fernandes

# eIDAS Qualified Trust Services
# Serviço de Preservação

Janeiro de 2021



**Universidade do Minho**
Escola de Engenharia
Departamento de Informática

João Manuel da Silva Gomes Fernandes

# eIDAS Qualified Trust Services
# Serviço de Preservação

Dissertação de Mestrado
Mestrado em Engenharia Informática

Dissertação supervisionada por
**Professor José Carlos Bacelar Almeida**

Janeiro de 2021

## DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

# AGRADECIMENTOS

Terminada uma fase muito importante da minha formação académica, cabe-me deixar umas palavras de agradecimento.

Este é o momento de expressar a minha gratidão a todos aqueles que estiveram mais próximos no meu processo de construção humana e cívica. Sem essas preciosas ajudas, a caminhada teria sido, com toda a certeza, mais penosa.

Aos meus pais, pelo apoio, pelo amor incondicional e também pela compreensão quando os problemas foram surgindo. Com eles aprendi que os erros também nos ensinam e que devemos ter objetivos de vida bem definidos, traçando metas difíceis, mas alcançáveis.

À minha irmã, que, apesar de ser uma chata e uma autêntica "pica miolos", sempre me apoiou em tudo que foi necessário para que eu pudesse ter uma caminhada tranquila.

Às minhas avós, Filomena e Maria do Céu, que sempre me incentivaram a perseguir os meus sonhos. Sinto muita tristeza que a avó Filomena tenha partido sem ter oportunidade de ver o seu neto "formado" (como dizia na sua simplicidade), desejo que permanentemente me manifestava...

Aos meus amigos que me acompanharam neste processo académico, com especial atenção à Joana e ao Saimon, o meu muito obrigado por me terem aturado em alguns momentos de maior "stress", dando-me sempre ânimo para seguir em frente.

Ao Doutor José Eduardo Pina Miranda que teve a perspicácia para propor o tema de dissertação e a paciência para orientar a minha tese de Mestrado. Sem a sua permanente disponibilidade para ajudar a melhorar o meu trabalho, o resultado final teria sido muito menos ambicioso.

Ao Professor José Carlos Bacelar Almeida que, desde a primeira hora, validou toda a temática que sustenta esta tese de Mestrado.

*Esta conquista*
*não seria possível*
*sem todos vocês.*

*Eternamente grato,*
*João M. Fernandes*

## DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducentes à sua elaboração.

Mais declaro que conheço e que respeito o Código de Conduta Ética da Universidade do Minho.

# RESUMO

De forma a uniformizar o mercado Europeu e conseguir mais confiança nas transações eletrónicas (*sic* Considerando 2º do Regulamento eIDAS (2014)), a União Europeia publicou o Regulamento UE nº 910/2014 (Regulamento eIDAS (2014)), também conhecido como Regulamento *Eletronic Identification, Authentication and Trust Services (eIDAS)*. Este normativo legal pretende regular as assinaturas e selos electrónicos, a identificação eletrónica e os serviços de confiança dentro do Espaço Europeu. O objetivo deste regulamento é permitir transações seguras e eficazes entre negócios, pessoas e as autoridades públicas.

Para atingir o seu objetivo, o Regulamento eIDAS introduziu o conceito de serviços de confiança qualificados. Os serviços de confiança qualificados permitem às assinaturas eletrónicas o efeito legal equivalente a uma assinatura manuscrita, quando baseadas num certificado qualificado de assinatura eletrónica emitido por uma entidade que está integrada na lista de confiança de um determinado Estado Membro. Estas assinaturas são intituladas de assinaturas eletrónicas qualificadas e são reconhecidas nos restantes Estados Membros. Tribunais (ou outros órgãos encarregados de procedimentos legais) não podem descartá-las como prova apenas porque são eletrónicas, têm de avaliá-las da mesma forma que fariam com o seu equivalente em papel. (*sic* Artigo 25º do Regulamento eIDAS (2014))

A necessidade de preservação de longo prazo de assinaturas eletrónicas é reconhecida no seio da União Europeia (UE). No Regulamento eIDAS, entre os serviços de confiança qualificados introduzidos, encontra-se o serviço de preservação qualificado. Um serviço de preservação qualificado tem como objectivo preservar o estado de validade de uma assinatura eletrónica qualificada ao longo do tempo.

Esta dissertação tem o seu foco no desenvolvimento de uma Prova de Conceito do serviço de confiança qualificado de preservação de assinaturas e selos eletrónicos qualificados, que se antecipa que comece a ser utilizado massivamente nos próximos anos.

PALAVRAS-CHAVE União Europeia, Assinatura Eletrónica Qualificada, Serviço Preservação de Longo Termo, eIDAS, Validade das Assinaturas Eletrónicas, Lista de Confiança.

## ABSTRACT

In order to standardise the European market and achieve greater confidence in electronic transactions (*sic* Recital 2º eIDAS (2014), the European Union has developed EU Regulation No 910/2014, also known as eIDAS. This regulation aims to regulate electronic signatures and seals, electronic identification and trust services in Europe. The aim of this regulation is to enable secure and efficient transactions between businesses, individuals and public authorities.

So as to achieve its objective, the eIDAS Regulation introduced the concept of qualified trust services. Qualified trust services allow subscribers and electronic signatures the legal effect equivalent to a handwritten signature when based on an electronic signature qualified certificate issued by an entity which is part of the trust list of a given Member State. These signatures are entitled qualified electronic signatures and are recognised in the other Member States. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence just because they are electronic, they have to assess them in the same way as they would for their paper equivalent. (*sic* Article 25º of the Regulation eIDAS (2014))

The need for long-term preservation of electronic signatures is recognised within the UE. In the Regulation eIDAS, among the qualified services of trust introduced, is the qualified preservation service. A qualified preservation service aims to preserve the validity status of a qualified electronic signature over time.

This dissertation focuses on the development of a Proof of Concept for the qualified electronic signature and seal preservation trust service, which is expected to start to be used massively in the coming years.



KEYWORDS Europian Union, Qualified Electronic Signature, Long-Term Preservation Service, eIDAS, Eletronic Signature Validity, Trust List.

# CONTEÚDO

# LISTA DE FIGURAS

# LISTA DE ACRÓNIMOS

**AIP** Archival Information Package.
**ASN.1** Abstract Syntax Notation One.
**CEN** Comité Europeu de Normalização.
**CRL** Certificate Revocation List.
**CTESI** Comité Técnico (CT) para Eletronic Signatures and Infrastructures (ESI).
**DC** Dublin Core.
**DI** Departamento de Informática.
**EAD** Encoded Archival Description.
**EC** Entidades de Certificação.
**eIDAS** Eletronic Identification, Authentication and Trust Services.
**ENISA** European Union Agency for Network and Information Security.
**ETSI** Instituto Europeu de Normas de Telecomunicações.
**ISO** Organização Internacional de Normalização.
**ITU** União Internacional das Telecomunicações.
**MEI** Mestrado em Engenharia Informática.
**METS** Metadata Encoding and Transmission Standard.
**OAIS** Open Archival Information System.
**OCSP** Online Certificate Status Protocol.
**PREMIS** PREservation Metadata – Implementation Strategies.
**UE** União Europeia.
**UM** Universidade do Minho.
**UNESCO** United Nations Educational, Scientific and Cultural Organization.
**UUID** Universally Unique Identifier.
**XML** Extensible Markup Language.

# GLOSSÁRIO

**A**

**ASSINATURAS ELETRÓNICAS** os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar.

**ASSINATURAS ELETRÓNICAS AVANÇADAS** uma assinatura eletrónica que obedeça aos requisitos especificados no Artigo 26º do Regulamento (UE) 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**ASSINATURAS ELETRÓNICAS QUALIFICADAS** uma assinatura eletrónica avançada criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica.

**C**

**CERTIFICADO QUALIFICADO DE ASSINATURA ELETRÓNICA** um certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento (UE) nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**CERTIFICADO QUALIFICADO DE SELO ELETRÓNICO** um certificado de selo eletrónico, que seja emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento (UE) nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**D**

**DADOS DE VALIDAÇÃO** dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico, como por exemplo, certificados qualificados de assinaturas eletrónicas, listas de revogação, entre outras.

**DADOS PARA A CRIAÇÃO DE UMA ASSINATURA ELETRÓNICA** o conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica.

**DISPOSITIVO QUALIFICADO DE CRIAÇÃO DE ASSINATURAS ELETRÓNICAS** o dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento (UE) nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**DOCUMENTOS ELETRÓNICOS** qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual.

**E**

**ENTIDADE SUPERVISORA** entidade eleita pelo Estado Membro, para desempenhar as atividades de supervisão previstas no Regulamento (EU) nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**ESQUEMA DE PRESERVAÇÃO** conjunto de mecanismos de preservação selecionados para implementar um objetivo de preservação.

**EVIDÊNCIAS DE PRESERVAÇÃO** evidências produzidas pelo serviço de preservação, que podem ser usadas para demonstrar que um objetivo de preservação foi alcançado.

**L**

**LISTA DE CONFIANÇA** lista que fornece informações sobre o status e o histórico dos serviços qualificados de confiança fornecidos por prestadores qualificados de serviços de confiança relativamente ao cumprimento dos requisitos aplicáveis e das disposições relevantes do Regulamento (UE) Nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**LONGOS PERÍODOS DE TEMPO** período de tempo durante o qual as mudanças tecnológicas podem ser uma preocupação.

**O**

**OBJETIVOS DE PRESERVAÇÃO** objetivo alcançado durante o período de preservação. Um dos seguintes: estender por longos períodos de tempo o estado de validade de uma assinatura ou estender evidências de preservação.

**OBJETOS PARA PRESERVAÇÃO** dados a preservar. Neste caso o objeto para preservação é a assinatura qualificada, ou o selo qualificado, e os respetivos dados de validação.

**ORGANISMO DE AVALIAÇÃO DE CONFORMIDADE** o organismo definido no artigo 2º , nº 13, do Regulamento (CE) nº 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**P**

**PERFIL DE PRESERVAÇÃO** conjunto univocamente identificado de detalhes pertinentes ao modelo de armazenamento, especifica quais os objetivos da preservação, como as evidências de preservação são criadas e validadas, assim como o período de preservação, se existir.

**PERÍODO DE PRESERVAÇÃO** para um serviço de preservação com armazenamento, período durante a qual o serviço de preservação resguarda os objectos de preservação submetidos e as provas associadas.

**PERÍODO DE RETENÇÃO DAS EVIDÊNCIAS DE PRESERVAÇÃO** termo utilizado no serviço de preservação com armazenamento temporário, onde é especificado o período de tempo onde o utilizador pode levantar as evidências de preservação do serviço..

**PESSOA COLETIVA** um corpo de pessoas ou uma entidade considerada como tendo muitos dos direitos e responsabilidades de uma pessoa singular e especialmente a capacidade de processar e ser processada.

**PESSOA SINGULAR** ser humano capaz de direitos e obrigações na esfera civil.

**PRESTADORES DE SERVIÇOS DE CONFIANÇA** a pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança.

**PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA** o prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora.

**PROVAS DE EXISTÊNCIA** evidência que prova que um determinado objeto existiu numa determinada data/tempo.

**PROVAS DE INTEGRIDADE** evidências que provam que os dados não foram alterados desde que foram preservados.

**S**

**SELOS ELETRÓNICOS** os dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos.

**SELOS ELETRÓNICOS AVANÇADOS** um selo eletrónico que obedeça aos requisitos estabelecidos no artigo 36º do Regulamento (UE) nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**SELOS ELETRÓNICOS QUALIFICADOS** selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico.

**SELOS TEMPORAIS QUALIFICADOS** dados em formato eletrónico que vinculam outros dados, também em formato eletrónico, a uma hora específica, criando uma prova de que esses outros dados existiam pelo menos até a essa hora indicada. Têm também que satisfazer os requisitos estabelecidos no artigo 42º do Regulamento (UE) Nº 910/2014.

**SERVIÇOS DE CONFIANÇA** um serviço eletrónico geralmente prestado mediante remuneração.

**SERVIÇOS DE CONFIANÇA QUALIFICADOS** serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento (UE) nº 910/2014 (*sic* Artigo 3º do Regulamento eIDAS (2014)).

**SIGNATÁRIO** a pessoa singular que cria uma assinatura eletrónica, ou a pessoa coletiva que cria um selo eletrónico.

**U**

**UTILIZADOR** a pessoa singular ou coletiva que utiliza o serviço de confiança.

**V**

**VALIDAÇÃO** o processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico.

Parte I

# MATERIAL INTRODUTÓRIO

# 1

# INTRODUÇÃO

Esta dissertação tem como finalidade o estudo aprofundado de um dos serviços de confiança qualificados, estabelecidos pela UE no Regulamento eIDAS (Regulamento (EU) nº 910/2014 (eIDAS (2014))) e descreve o trabalho de Mestrado, desenvolvido no contexto do *Mestrado em Engenharia Informática (MEI)*, realizado no *Departamento de Informática (DI)*, *Universidade do Minho (UM)*. Trata-se do serviço de confiança qualificado de preservação de assinaturas e selos eletrónicos qualificados.

Este tema de dissertação foi proposto pela empresa *DeviseFutures Lda.*[1], com a orientação do Dr. José Eduardo Pina Miranda.

## 1.1 CONTEXTUALIZAÇÃO

A transformação digital que temos vindo a assistir introduz uma nova forma de fazermos negócios, de acedermos a serviços e de nos identificarmos. Contudo, existe ainda falta de confiança, por parte das pessoas e empresas, em aderir a esta transformação digital na sua plenitude, dificultando assim o desenvolvimento económico e social.

A confiança no mundo digital é essencial para que indivíduos e organizações usem e adotem serviços electrónicos.

"Criar confiança no ambiente em linha é fundamental para o desenvolvimento económico e social. A falta de confiança, nomeadamente devido à perceção de incerteza jurídica, leva os consumidores, as empresas e as autoridades públicas a hesitarem em realizar transações por via eletrónica e em adotar novos serviços." (*sic* Considerando 1º do Regulamento eIDAS (2014))

Neste contexto surge o Regulamento (UE) Nº 910/2014 eIDAS (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. Este normativo legal, que revoga a Diretiva 1999/93/CE relativa a um quadro legal comunitário para as assinaturas electrónicas, é geralmente conhecido como Regulamento eIDAS, com efeitos

1 https://www.devisefutures.com

reportados a 1 de Julho de 2016, sendo obrigatória a sua total adoção por parte dos Estados Membros da UE.

A Diretiva 1999/93/CE tratava das assinaturas eletrónicas sem oferecer um quadro transfronteiriço e transetorial geral que garantisse a segurança, a fiabilidade e a facilidade de realizações das transações eletrónicas. (*sic* Considerando 3º do Regulamento eIDAS (2014))

O Regulamento eIDAS melhora e desenvolve as disposições daquela diretiva, "criando uma base comum para as transferências electrónicas em condições seguras entre cidadãos, empresas e as autoridades públicas", conseguindo assim interoperabilidade e transparência entre os estados-membro da UE e, consequentemente aumentar a confiança das pessoas e empresas nas transações *online*.

Uma componente importante do Regulamento eIDAS são as assinaturas e selos electrónicos. Nos Artigos 25º e 35º do Regulamento, relativos aos efeitos legais das assinaturas eletrónicas e selos eletrónicos, respectivamente, é declarado que a ambos "não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial". Também é definido que as assinaturas eletrónicas qualificadas têm o mesmo efeito legal que uma assinatura manuscrita e, quando baseada num certificado qualificado de assinatura eletrónica emitido (para uma pessoa singular) por um Estado-Membro, é reconhecida como assinatura electrónica qualificada em todos os outros Estados-Membros. No caso dos selos eletrónicos qualificados, estes beneficiam "da presunção da integridade dos dados e da correcção da origem dos dados aos quais estão associados", e, tal como as assinaturas eletrónicas qualificadas , quando são baseados num certificado qualificado de selo eletrónico emitido (para uma pessoa coletiva) por um Estado-Membro, são reconhecidos como selos electrónicos qualificados em todos os outros Estados-Membros.

A titulo de exemplo, em Portugal, as assinaturas efectuadas com o Cartão de Cidadão são assinaturas eletrónicas qualificadas.

Com vista à interoperabilidade entre os Estados-Membros, o Regulamento define requisitos que os prestadores de serviços de confiança qualificados devem cumprir para poderem ter essa designação. Dentro desses serviços encontra-se o serviço qualificado de Preservação de assinaturas e selos qualificados (*sic* Artigos 34º e 40º do Regulamento eIDAS (2014)), que vai ser o foco do presente documento.

Os serviços de preservação qualificados são particularmente importantes no sentido em que o seu maior objetivo é manter o estado de validade técnica de assinatura durante longos períodos de tempo.

## 1.2 MOTIVAÇÃO

### 1.2.1 *Desmaterialização de Processos*

A desmaterialização processual é a base para a simplificação administrativa, conduzindo, de uma forma geral, ao aumento de eficiência dos serviços do Estado e à prestação de serviços por via eletrónica. (*cf.* AMA-Agência para modernização administrativa)

A desmaterialização permite a eliminação do suporte de papel em todos os processos dentro de cada organismo público, entre organismos públicos e, sempre que possível, na relação com cidadãos e empresas, potenciando, simultaneamente, a modernização administrativa.

A prestação de serviços por via eletrónica permite a eficiência e modernização administrativa, o que potencia a satisfação do cidadão.

Assim, o impacto de desmaterialização de processos abrange uma redução substancial ao nível dos consumíveis de impressão, papel, áreas alocadas a arquivo físico e recursos humanos afetos a atividades de circulação do papel. (*cf.* AMA-Agência para modernização administrativa)

A tendência é que todos os processos judiciais em versão de papel venham, paulatinamente, a ser desmaterializados. Esta realidade estará cada vez mais presente nos Tribunais portugueses. O Código de Processo nos Tribunais Administrativos (CPTA[2]), tendo em vista o combate à morosidade processual e a simplificação de procedimentos na tramitação dos processos da jurisdição administrativa e fiscal, previu uma intensificação do processo de desmaterialização através do recurso às tecnologias da informação na relação dos tribunais com as partes e demais intervenientes (*vide* Portaria nº 380/2017 - Diário da República).

Outra situação análoga é o Decreto-Lei nº 28/2019, de 15 de Fevereiro, que vem regulamentar as obrigações fiscais relativas ao processamento das faturas, obrigação de conservação de livros, registos e documentos de suporte, bem como dos programas de contabilidade.

Entre as novidades, está a criação de condições para a desmaterialização de documentos, incentivando a adoção de um sistema de faturação eletrónica e de arquivo eletrónico de documentos. Estas novidades vão permitir às empresas uma redução dos custos administrativos e vão estimular o desenvolvimento e a utilização de novos instrumentos tecnológicos, incorporando uma filosofia de inovação e desburocratização.

Assim, as faturas e demais documentos fiscalmente relevantes recebidos em papel passam a poder ser digitalizados e arquivados em formato eletrónico, e posteriormente destruídos. A digitalização deve garantir a sua consulta e reprodução em papel ou outro suporte eletrónico; para efeitos fiscais, as reproduções integrais em papel obtidas a partir dos arquivos em formato eletrónico, têm o valor probatório dos documentos originais; os documentos devem

2 http://www.ministeriopublico.pt/iframe/codigo-de-processo-nos-tribunais-administrativos

ser guardados de forma sequencial e respeitando um plano de arquivo e individualização de cada exercício.

### 1.2.2 *Preservação do Património Documental*

Face ao risco crescente de perda de informação preciosa que determina o património mundial em termos de conhecimento, de identidade, de história e de valores humanos, a *United Nations Educational, Scientific and Cultural Organization (UNESCO)* envida esforços no sentido de sensibilizar os governos, as instituições competentes e o público em geral para a importância de preservação da informação para as gerações atuais e futuras. O património documental representa a memória da humanidade mas é ameaçado e corre o risco de desaparecer para sempre.

Também é importante tornar esse património acessível ao maior número de pessoas através da utilização das tecnologias mais apropriadas. Este é o motivo pelo qual a UNESCO toma as medidas necessárias para conservar o património documental e audiovisual através do Programa Memória do Mundo[3]. Segundo a visão da UNESCO, o património documental mundial pertence a Todos, devendo ser inteiramente preservado e protegido, e constantemente acessível a todos, sem qualquer obstáculo.

A necessidade da criação deste programa nasceu da crescente tomada de consciência do estado preocupante de conservação do património documental e da precariedade do seu acesso em diferentes regiões do mundo.

### 1.2.3 *Digitalização da Economia*

Outro aspeto relevante é o facto de em todos os estados membros da UE, os organismos públicos, quando actuam oficialmente através de documentos eletrónicos, terem de os arquivar durante longos períodos de tempo.

De maneira a confirmar e garantir a validade e veracidades destes documentos eletrónicos, foi crescendo o uso de assinaturas e selos eletrónicos nos mesmos.

Muitos destes documentos que contêm assinaturas eletrónicas ou selos eletrónicos, recorrem a técnicas de assinaturas digitais, para que possam ser unicamente ligados a um signatário. A validade destas assinaturas tem que ser garantida antes e durante a sua retenção.

Isto para que, caso apareça algum tipo de litígio em que haja a necessidade de testar a veracidade e validade destes documentos, fazendo a validação das assinaturas eletrónicas qualificadas presentes nos mesmos, esse suporte esteja disponível.

3 https://en.unesco.org/programme/mow

### 1.2.4 *Preservação de Informação a Longo Prazo*

O período de retenção, às vezes muito longo, levanta questões sobre as assinaturas presentes nos documentos eletrónicos, como a força e a aptidão dos mecanismos criptográficos usados. É sabido que, à medida que o tempo avança, estes mecanismos vão ficando cada vez mais vulneráveis a ataques, sendo necessária a aplicação de mecanismos de preservação aptos para manter o estado de validade da assinatura durante longos períodos de tempo. (*cf.* ETSI TS 119 511)

Tal como as peças de arte, uma assinatura eletrónica precisa de ser sujeita a manutenção periódica para garantir a sua frescura.

"O presente regulamento deverá assegurar a preservação das informações a longo prazo, para assegurar a validade legal das assinaturas e dos selos eletrónicos durante períodos alargados e garantir que possam ser validados independentemente da evolução tecnológica futura." (*sic* Considerando 61º do Regulamento eIDAS (2014))

O Regulamento eIDAS, dentro da gama de serviços de confiança qualificados que introduziu, estabeleceu o serviço qualificado de preservação de assinaturas eletrónicas qualificadas.

"Os serviços de preservação de assinaturas eletrónicas qualificadas só podem ser prestados por prestadores qualificados de serviços de confiança que utilizem procedimentos e tecnologias capazes de prolongar a fiabilidade das assinaturas eletrónicas qualificadas para além do prazo de validade tecnológica." (*sic* Artigo 34º do Regulamento eIDAS (2014))

## 1.3 Objetivos da dissertação

No que diz respeito a esta dissertação de mestrado, relevam-se os seguintes objetivos:

- Identificar requisitos, definir a arquitetura e componentes para um serviço de confiança qualificado de preservação de assinaturas e selos eletrónicos qualificados, de modo que estejam de acordo com o Regulamento eIDAS e com as normas gerais da comunidade internacional para proporcionar confiança nos serviços de preservação;
- Desenvolver um protótipo do serviço de confiança referido no ponto anterior.

## 1.4 ESTRUTURA DO DOCUMENTO

Este documento está organizado em 4 capítulos.

O estado da arte é abordado no **segundo capítulo**, onde são distinguidos os diferentes tipos de assinaturas e selos eletrónicos, assim como todos os componentes envolventes à preservação de assinaturas e selos eletrónicos qualificados (como técnicas de preservação, normas associadas e projetos úteis).

O **terceiro capítulo** descreve uma visão da solução criada para o protótipo da Prova de Conceito, como os seus objetivos, o *design* da arquitetura, assim como o desenvolvimento das componentes utilizadas na solução proposta.

Finalmente, o **quarto capítulo** apresenta uma descrição das conclusões que podem ser extraídas deste trabalho, assim como de alguns trabalhos futuros.

Parte II

# NÚCLEO DA DISSERTAÇÃO

# 2

# ESTADO DA ARTE

Neste capítulo será exposto o atual estado da arte e uma revisão da literatura relativa aos conceitos associados ao serviço de preservação de assinaturas eletrónicas qualificadas.

## 2.1 ASSINATURAS E SELOS ELETRÓNICOS QUALIFICADOS

### 2.1.1 *Assinaturas Eletrónicas*

O Regulamento eIDAS distingue três classes diferentes de assinaturas electrónicas, nomeadamente a classe das assinaturas eletrónicas, a classe das assinaturas eletrónicas avançadas e a classe das assinaturas eletrónicas qualificadas.

Segundo o regulamento eIDAS, às assinaturas electrónicas e selos electrónicos não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial pelo simples facto de se apresentarem em formato electrónico.

As assinaturas eletrónicas simples ou, simplesmente, assinaturas eletrónicas estão estabelecidas como "os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar"(*sic* nº5 do Artigo 3º do Regulamento eIDAS (2014)). O signatário tem de ser obrigatoriamente uma pessoa singular.

As assinaturas eletrónicas avançadas, segundo o Regulamento eIDAS, são assinaturas eletrónicas que obedecem aos requisitos especificados no Artigo 26º, nomeadamente:

(a) Estar associada de modo único ao signatário;

(b) Permitir identificar o signatário;

(c) Ser criada utilizando dados para a criação de uma assinatura eletrónica;

(d) Estar ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados.

O signatário possui o controlo total e exclusivo dos dados referidos no ponto (c). A chave privada, usada para o acto da assinatura, é um exemplo de dados para a criação de uma assinatura eletrónica, que se não forem bem geridos e armazenados pelo signatário (por

exemplo, no caso de perda ou no caso de sofrerem algum tipo de ataque), este não poderá voltar a usar os dados para criar a assinatura.

Este tipo de assinaturas é tipicamente usado para garantir a integridade e o não-repúdio dos dados assinados.

A última classe definida sob o Regulamento eIDAS é a das assinaturas eletrónicas qualificadas, que engloba todas as assinaturas eletrónicas avançadas, criadas recorrendo a um dispositivo qualificado de criação de assinaturas eletrónicas, que se baseiem num certificado qualificado de assinatura eletrónica.

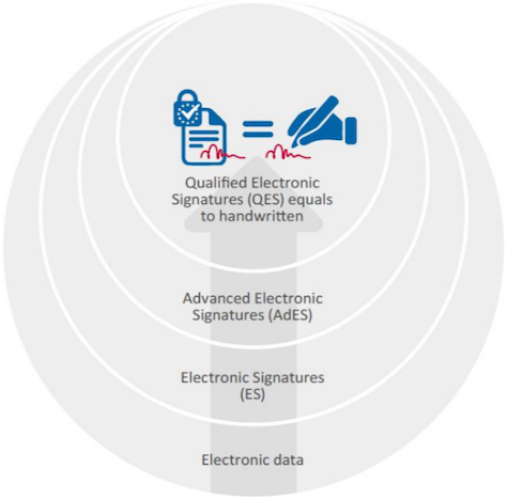



Figura 1: Tipos de assinaturas electrónicas (Fonte: ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures)

Com o eIDAS, as assinaturas eletrónicas qualificadas têm o mesmo valor legal que uma assinatura manuscrita. (Considerando 49º do Regulamento eIDAS (2014)) Para além disso, assinaturas eletrónicas qualificadas baseadas num certificado electrónico qualificado emitido num Estado-Membro são reconhecidas como tal em todos os outros Estados-Membros. (*sic* nº3 do Artigo 23º do Regulamento eIDAS (2014)). Este estatuto legal das assinaturas electrónicas qualificadas abre novas portas ao desenvolvimento económico-social de negócios e serviços na Europa, garantindo maior segurança às transacções *online* e serviços na Europa (*cf.* ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures).

Actualmente, as assinaturas eletrónicas qualificadas são implementadas através de criptografia assimétrica. A chave privada, usada pelo signatário, corresponde aos dados para a criação de uma assinatura eletrónica referida no eIDAS (*cf.* ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures).

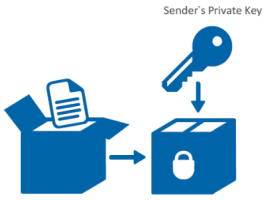



Figura 2: Assinatura de dados com uma chave privada para produzir uma assinatura electrónica (Fonte: ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures)

Para verificar a assinatura o verificador usa a chave pública do signatário. A verificação com uma chave pública significa que a assinatura foi gerada com a chave privada correspondente. Assim, a origem da assinatura só pode ser do signatário que tem em sua posse a chave privada. Desta forma é alcançada a característica do não-repúdio.

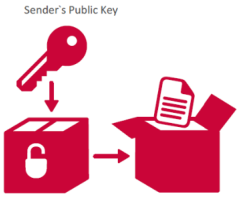



Figura 3: Verificação de uma assinatura com a chave pública do signatário (Fonte: ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures)

Outra característica importante desta técnica é a integridade dos dados assinados, pois se os dados assinados forem alterados a verificação falhará.

Mas criptografia assimétrica apenas não é suficiente para garantir que uma dada chave pública pertence a um signatário, único proprietário e usuário da chave privada (*cf.* ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures). Para obter essa garantia são usadas *Entidades de Certificação (EC)*, que asseguram a ligação chave pública –> signatário com um certificado de chave pública. Para as assinaturas eletrónicas qualificadas esse certificado deve ser um certificado qualificado de assinatura eletrónica.

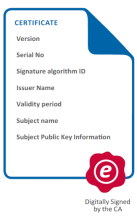



Figura 4: Certificado de chave pública (Fonte: ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures)

### 2.1.2 *Selos Eletrónicos*

Como já foi mencionado anteriormente, as assinaturas eletrónicas apenas podem ser usadas por uma pessoa singular. O Regulamento eIDAS também introduziu o reconhecimento de selos eletrónicos. São similares às assinaturas eletrónicas e estão divididos em 3 classes: selos eletrónicos simples, ou selos eletrónicos, selos eletrónicos avançados e selos eletrónicos qualificados.

Tal como para as assinaturas eletrónicas, o Regulamento eIDAS, estabelece normas e requisitos para os selos eletrónicos. Se os primeiros só podem ser usados por uma pessoa singular, os segundos só podem ser usados por uma pessoa coletiva. Simultaneamente às assinaturas eletrónicas qualificadas, a criação dos selos eletrónicos qualificados tem que se basear num certificado qualificado de selo eletrónico, e tem que ser criado através de um dispositivo qualificado de criação de selo electrónico.

Os selos eletrónicos qualificados gozam da presunção de integridade dos dados e da correção da origem dos dados a eles associados (*sic* nº2 do Artigo 35º do Regulamento eIDAS (2014)).

Tal como a assinaturas eletrónicas qualificadas, também os selos eletrónicos qualificados vieram ajudar o desenvolvimento dos negócios e serviços *online* na Europa, tornando as transações *online* e os serviços mais seguros.

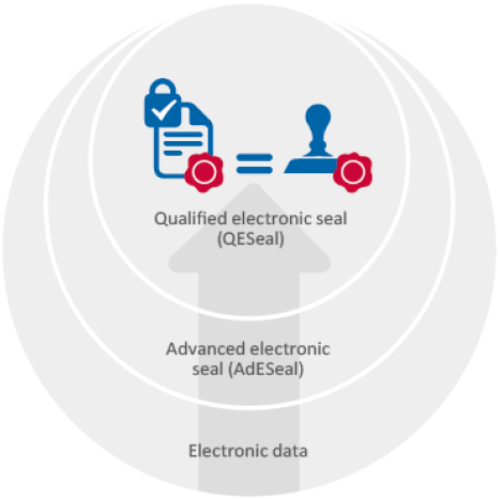



Figura 5: Tipos de selos electrónicos (Fonte: ENISA (2016) Security guidelines on the appropriate use of qualified electronic seals)

### 2.1.3 *Emissão de Certificados Qualificados de Assinaturas/Selos*

O Regulamento eIDAS, exige que o certificado qualificado de assinatura eletrónica e o certificado qualificado de selo eletrónico sigam as regras impostas no mesmo e que as EC

responsáveis pela emissão dos certificados sejam prestadores qualificados de serviços de confiança.

Nos termos do Regulamento eIDAS, uma EC, que emite certificados qualificados de assinaturas eletrónicas ou certificados qualificados de selos eletrónicos, está sujeita a auditorias por parte do organismo de avaliação de conformidade. Se a entidade supervisora do Estado Membro, onde essa EC está estabelecida, receber um relatório de auditoria e verificar que os requisitos do Regulamento eIDAS são cumpridos, a EC recebe a marca de confiança da UE e é adicionada à lista de confiança da UE como prestadores qualificados de serviços de confiança.

Este assunto é aprofundado na secção 2.2.1.

## 2.2 SERVIÇOS DE CONFIANÇA QUALIFICADOS

Os prestadores de serviços de confiança são muitas vezes um elemento essencial para fortalecer a confiança entre as partes que realizam transações eletrónicas (*cf.* ETSI EN 319 401).

O eIDAS estabelece normas aplicáveis a todos os serviços de confiança. No entanto é necessária uma distinção entre serviços de confiança qualificados e não qualificados devido ao tipo de serviço que prestam.

De maneira a garantir um alto nível de segurança dos serviços de confiança qualificados o eIDAS prevê um esquema de supervisão activa dos prestadores qualificados de serviços de confiança e também dos serviços de confiança qualificados que eles providenciam (*cf.* ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures).

### 2.2.1 *Prestadores qualificados de serviços de confiança qualificados*

O Regulamento eIDAS define diferentes tipos de serviços de confiança qualificados, sendo eles:

- emissão de certificados qualificados para assinaturas eletrónicas e selos eletrónicos;
- emissão de certificados qualificados para a autenticação de sítios *web*;
- serviço de preservação qualificado para assinaturas e selos eletrónicos qualificados;
- serviço de validação qualificado para assinaturas e selos eletrónicos qualificados;
- serviço de criação de selos temporais qualificados;
- serviço qualificado de envio registado eletrónico.

(*cf.* ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures)

Este Regulamente exige também a cada Estado Membro que estabeleça, mantenha e publique uma lista de confiança com informações sobre os prestadores qualificados de serviços de confiança que atuam no seu território, juntamente com informações sobre os serviços de confiança qualificados que providenciam.

De forma a distinguir os serviços de confiança qualificados dos não qualificados, foi criada uma marca de confiança da União Europeia (Figura 6). Esta marca pretende contribuir para a transparência do mercado.

Os prestadores de serviços de confiança, que queiram obter o estatuto de qualificado, necessitam de passar por uma avaliação por parte de um organismo de avaliação de conformidade, que irá determinar e avaliar se estão em conformidade com os requisitos impostos pelo Regulamento eIDAS. O organismo de avaliação de conformidade produzirá um relatório de avaliação de conformidade, indicando se os requisitos foram cumpridos. Documentos, como o ETSI EN 319 401 e Criteria for assessing compliance with the eIDAS regulation, especificam normas e controlos de conformidade, para que os prestadores de serviços possam atingir o título de qualificado.

O relatório elaborado pelo organismo de avaliação de conformidade é entregue à entidade supervisora do Estado Membro onde o serviço se encontra.

De acordo com o documento ENISA (2016) Mapping of requirements of eIDAS to existing standards, para que um prestador qualificado de serviços de preservação qualificados consiga providenciar o seu serviço, será avaliado se o serviço está em conformidade com os requisitos especificados nos Artigos 5º, 13º, 19º, 24º, 34º e 40º do Regulamento eIDAS, de que se destaca:

- Artigo 5º Tratamento e proteção dos dados;
- Artigo 13º Responsabilidade e ónus da prova;
- Artigo 15º Acessibilidade para as pessoas com deficiência;
- Artigo 19º(1) e Artigo 19º(2) Requisitos de segurança aplicáveis aos prestadores de serviços de confiança ;
- Artigo 24º(2).a Informar a entidade supervisora de todas as alterações à prestação dos seus serviços de confiança qualificados, inclusivamente da intenção de cessação de atividades;
- Artigo 24º(2).c Face ao risco da responsabilidade por danos prevista no artigo 13. , conservam recursos financeiros suficientes e/ou adquirem um seguro de responsabilidade adequado, de acordo com a legislação nacional;

- Artigo 24º(2).d Antes de estabelecerem uma relação contratual, informam, de forma clara e completa, as pessoas que pretendam utilizar serviços de confiança qualificados dos termos e condições exatos da utilização de tais serviços, incluindo de qualquer limitação à sua utilização;
- Artigo 24º(2).e Utilizam sistemas e produtos fiáveis que estejam protegidos contra modificações e garantam a segurança e a fiabilidade técnicas dos processos de que são suporte;
- Artigo 24º(2).f Utilizam sistemas fiáveis de armazenamento dos dados que lhes são fornecidos, num formato verificável;
- Artigo 24º(2).g Tomam as medidas adequadas para prevenir a falsificação e o roubo dos dados;
- Artigo 24º(2).h Registam e mantêm acessíveis durante um prazo adequado, incluindo depois de o prestador qualificado de serviços de confiança ter deixado de prestar esses serviços, todas as informações pertinentes relativas aos dados emitidos e recebidos pelo prestador qualificado de serviços de confiança, em particular para efeitos de apresentação de provas em processos judiciais e para garantir a continuidade do serviço. Esse registo poderá ser feito eletronicamente;
- Artigo 24º(2).i Conservam um plano de cessação de atividades atualizado que garanta a continuidade do serviço;
- Artigo 24º(2).j Garantem um tratamento lícito dos dados pessoais em conformidade com a Diretiva 95/46/CE;
- Artigo 24º(5) A Comissão pode, por meio de atos de execução, estabelecer os números de referência das normas relativas aos sistemas e produtos fiáveis que cumprem os requisitos constantes do nº 2, alíneas e) e f).

No que diz respeito aos serviços de confiança qualificados de preservação de assinaturas e selos qualificados, em específico, para além dos requisitos anteriores acrescem os seguintes:

- Artigo 34º (1) Os serviços de preservação de assinaturas eletrónicas qualificadas só podem ser prestados por prestadores qualificados de serviços de confiança que utilizem procedimentos e tecnologias capazes de prolongar a fiabilidade das assinaturas eletrónicas qualificadas para além do prazo de validade tecnológica.

  De acordo com o Artigo 34º (2), a Comissão pode, por meio de atos de execução, estabelecer os números de referência das normas relativas ao serviço qualificado de preservação de assinaturas eletrónicas qualificadas.

- Artigo 40º *Mutatis mutandis*, aplicação do Artigo 34º à preservação de selos eletrónicos qualificados.

Para além dos requisitos especificados nos artigos anteriores, será também avaliada a conformidade com as normas e requisitos estabelecido no ETSI EN 319 401, relativo às evidências de preservação mencionadas no Artigo 24º (2).h e ao plano de cessação mencionado no Artigo 24º (2).i, assim como com os requisitos aplicáveis expostos no ETSI TS 119 511 e no ETSI TS 119 102-1. Outros aspetos, como módulos criptográficos, também são alvo de análise, segundo Criteria for assessing compliance with the eIDAS regulation.

Em suma, será avaliada a conformidade com as normas genéricas para os prestadores qualificados de serviços de confiança, assim como as normas específicas para cada serviço de confiança qualificado (neste caso, para o serviço de preservação qualificado).

Se a avaliação, mencionada anteriormente, for aceite positivamente pela entidade supervisora, os prestadores de serviços de confiança podem usar a marca de confiança da UE (Figura 6) e são adicionados à lista de confiança do Estado Membro como prestadores qualificados de serviços de confiança, lista essa que é gerida pela entidade supervisora. Em Portugal, o Gabinete Nacional de Segurança é a entidade supervisora.

Figura 6: Marca de confiança da UE (Fonte: ENISA (2016) Security guidelines on the appropriate use of qualified electronic signatures)

Na lista de confiança encontram-se identificados vários tipos de serviços de confiança qualificados, que podem e devem ser usados para auxiliar a preservação de assinaturas eletrónicas qualificadas, assim como serviços qualificados de criação de selos temporais qualificados e serviços qualificados de validação de assinaturas eletrónicas qualificadas.

### 2.2.2 *Normas*

O Regulamento eIDAS abrange um vasto leque de serviços. Para apoiar a implementação deste regulamento altamente técnico, foi necessário um maior trabalho de normalização.

"A Comissão pode, por meio de atos de execução, estabelecer os números de referência das normas relativas ao serviço qualificado de preservação de assinaturas eletrónicas qualificadas" (*sic* Artigo 34º Nº2 do Regulamento eIDAS (2014)).

Os trabalhos de normalização anteriores, no âmbito do mandato M/460 Fase II, destinado a apoiar a antiga Diretiva 1999/93/EC, forneceram um conjunto central de normas necessárias para as assinaturas electrónicas. No entanto, com a entrada em vigor do Regulamento eIDAS, foram introduzidas novas características que precisam de ser tomadas em linha de conta. São necessárias normas adicionais para assegurar que estas novas funcionalidades sejam suportadas.

"Quando adotar atos delegados ou de execução, a Comissão deverá considerar as normas e especificações técnicas estabelecidas pelas organizações e entidades europeias e internacionais de normalização, nomeadamente o *Comité Europeu de Normalização (CEN)*, o *Instituto Europeu de Normas de Telecomunicações (ETSI)*, o *Organização Internacional de Normalização (ISO)* e a *União Internacional das Telecomunicações (ITU)*, a fim de assegurar um nível elevado de segurança e de interoperabilidade da identificação eletrónica e dos serviços de confiança." (*sic* Considerando 72º do Regulamento eIDAS (2014)).

Entidades como CEN, ETSI e *European Union Agency for Network and Information Security (ENISA)* trabalharam e apresentaram uma coletânea de normas, que satisfazem o Regulamento eIDAS, para ajudar os prestadores qualificados de serviços de confiança a cumprir os requisitos exigidos pelo Regulamento. O ETSI, por exemplo, elaborou o documento ETSI TS 119 403-3 *Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers*, onde apresenta uma colectânea de normas que cada serviço de confiança deve respeitar. Na imagem seguinte estão expostas as normas especificas para o serviço qualificado de preservação de assinaturas e selos eletrónicos presentes nesse documento.

| Qualified trust service in Regulation (EU) No 910/2014 [i.1] | Standards |
|---|---|
| Qualified preservation service for qualified electronic signatures | ETSI EN 319 401 [i.10], ETSI TS 119 511 [i.24], ETSI TS 119 512 [i.25] |
| Qualified preservation service for qualified electronic seals | ETSI EN 319 401 [i.10], ETSI TS 119 511 [i.24], ETSI TS 119 512 [i.25] |

source: ETSI TS 119 403-3

Figura 7: Normas disponíveis em apoio ao Regulamento eIDAS (Fonte: ETSI TS 119 403-3)

Como se pode confirmar na figura acima exposta, os documentos propostos quer para o serviço qualificado de preservação de assinaturas eletrónicas qualificadas, quer para o serviço qualificado de preservação de selos eletrónicos qualificados são os mesmos. Trata-se dos documentos ETSI EN 319 401 *General Policy Requirements for Trust Service Providers*, ETSI TS 119 511 *Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques* e ETSI TS

119 512 *Protocols for trust service providers providing long-term data preservation services*. Estes documentos serão abordados e explorados ao longo desta dissertação.

## 2.3 PRESERVAÇÃO DE ASSINATURAS ELETRÓNICAS E SELOS QUALIFICADOS

É reconhecido que as assinaturas eletrónicas qualificadas, selos eletrónicos qualificados, selos temporais eletrónicos qualificados e respetivos dados assinados precisam de ser preservados por longo prazo, através de medidas adequadas, que mantenham a validade legal e a conclusividade das assinaturas qualificadas e dos dados assinados (*cf.* Towards a standardised preservation service for qualified electronic signatures and qualified electronic seals). O Considerando 61º do Regulamento eIDAS indica explicitamente a necessidade de preservação a longo prazo.

"O presente regulamento deverá assegurar a preservação das informações a longo prazo, para assegurar a validade legal das assinaturas e dos selos eletrónicos durante períodos alargados e garantir que possam ser validados independentemente da evolução tecnológica futura."

O Artigo 34º do mesmo Regulamento introduz um tipo especifico de serviço de confiança qualificado: o serviço de preservação qualificado de assinaturas e selos eletrónicos qualificados.

Segundo a Agência Nacional de Segurança de Sistemas de Informação (ANSSI) do Estado Françês, duas abordagens são reconhecidas de maneira a assegurar a preservação de assinaturas e selos qualificados:

1. uma abordagem sistemática baseada na proteção, em termos de integridade do sistema de arquivo eletrónico onde as assinaturas e os selos qualificados serão preservados. Neste caso, as normas sobre o Arquivo Eletrónico, ISO 14641-1, devem ser tomadas em linha de conta;

2. uma abordagem específica baseada na proteção em termos de integridade, de forma unitária, de cada assinatura ou selo electrónico qualificado que seja objeto de preservação, através da extensão regular da assinatura ou do selo ou da recolha regular dos dados de validação dos mesmos.

   (*cf.* ANSSI (2017))

Na segunda abordagem que vai de encontro às normas ETSI, que determinam as características técnicas do serviço de preservação de acordo com o eIDAS, resumidamente, a preservação de assinaturas e selos qualificados significa:

1. a recolha de todos os dados de validação necessários para validar a assinatura ou o selo;

2. validar a assinatura e o selo, recorrendo, ou não, a serviços de confiança qualificados de validação externos;

3. recolher as evidências usadas na validação, e protegê-las em conjunto com a assinatura ou o selo, usando provas de existência, como por exemplo, selos temporais qualificados, de maneira a que seja possível provar o estado de validade de uma assinatura ou de um selo no momento em que a prova foi criada. Estas provas são denominadas por evidências de preservação.

### 2.3.1 *Serviço Arquivo Eletrónico vs Serviço de Preservação Qualificado*

Se o Regulamento eIDAS foi necessário para acrescentar uma dimensão complementar de confiança, também pode causar alguma confusão. Não se pode confundir "arquivo eletrónico de documentos"com "preservação de assinaturas". O Regulamento estabelece regras para a preservação qualificada de assinaturas eletrónicas, que é distinto de arquivo eletrónico, que não é um serviço abrangido pelo Reguamento eIDAS. Os objetivos de cada processo fazem a diferenciação entre estas duas atividades. Note-se contudo que tal não significa que não possam ser complementares.

O serviço de preservação qualificado visa garantir a confiabilidade numa assinatura eletrónica qualificada ou num selo eletrónico qualificado ao longo do tempo, daí que as tecnologias subjacentes a este processo tenham como alvo as assinaturas ou os selos, isto é, o não-repúdio e integridade do documento assinado.

O serviço arquivo eletrónico visa assegurar que um documento eletrónico é armazenado de forma a garantir a sua integridade. A tecnologia subjacente ao arquivo eletrónico é, portanto, dirigida ao documento em si.

Por outras palavras, o arquivo eletrónico de documentos e a preservação de assinaturas eletrónicas e selos eletrónicos são de natureza diferente, baseiam-se em soluções técnicas diferentes e diferem na sua finalidade.

Dentro do **serviço de preservação**, foram normalizadas três variantes principais, o serviço de preservação com armazenamento, sem armazenamento ou com armazenamento temporário. Aspetos que serão aprofundados na secção 2.4.2.

O serviço de preservação com armazenamento guarda os objetos de preservação, em conjunto com as respetivas evidências de preservação como, por exemplo, o certificado qualificado de assinatura eletrónica usado para a criação, durante o período de preservação estabelecido. Este serviço disponibiliza a funcionalidade de apagar e atualizar os objetos de preservação antes do fim do seu período de preservação.

Um serviço de preservação tem dois objetivos:

1. estender por longos períodos de tempo a capacidade de validar uma assinatura eletrónica, mantendo o seu estado de validade;

2. poder providenciar provas de existência da assinatura e dos dados a ela associados.

Para ser possível estender a validade de uma assinatura eletrónica por longos períodos de tempo, o serviço de preservação necessita de providenciar provas de existência da assinatura, dos dados assinados e dos dados de validação.

Para um **serviço de arquivo**, as demonstrações de provas de existência são realizadas através de uma auditoria baseada em critérios específicos como, por exemplo, o ISO 14721:2012 e o ISO 16363:2012.

É importante referir que nos serviços de preservação, as demonstrações de provas de existência, são realizadas através de uma auditoria baseada em critérios específicos. Refiro, a título de exemplo, os critérios expostos no ETSI TS 119 511, recorrendo ao uso de técnicas de assinaturas digitais para demonstrar que os dados não foram alterados desde uma determinada data, fazendo uso de selos temporais qualificados.

Um serviço de preservação pode fazer parte de um serviço de arquivo.

Uma das diferenças entre um serviço de preservação e um serviço de arquivo é o facto do segundo, sem o primeiro, não capturar nem verificar nenhum dado de validação associado a uma assinatura eletrónica, isto é, não garante o não-repúdio dos documentos arquivados, nem a validação técnica da integridade dos mesmos.

Uma das relações entre estes serviços está no facto do serviço de arquivo poder usar um serviço de preservação de maneira a providenciar provas de existência de dados relacionados com assinaturas. E o serviço de preservação com armazenamento poder usar um serviço de arquivo com o objetivo de armazenar dados.

O *consultative Committee for Space Data Systems (CCSDC)* desenvolveu o modelo de referência OAIS, vertido na norma ISO 14721:2012, onde são identificadas as características essenciais de um sistema de arquivo. Este modelo contém um *OAIS Information Model* como conceito de alto nível de um *Information Package* que organiza os objectos de informação geridos por um serviço de arquivo OAIS. O *Information Package*, que é armazenado num arquivo digital, é autónomo, inclui toda a informação necessária, como *Content Information* que agem como *Data Objects(s)* , juntamente com a sua *Representation Information*, e outros metadados para satisfazer o propósito da sua criação (por exemplo, requisitos legais, requisitos de documentação, regras de conformidade, provas de integridade contra terceiros, utilizando assinaturas digitais, selos temporais ou *evidence records*). A *Representation Information* transporta informação semântica e estrutural.

Este modelo distingue entre:

- o que é submetido ao arquivo, um *Submission Information Package* (SIP);
- o que é preservado, um *Archival Information Package* (AIP);
- e o que é devolvido aos clientes do arquivo, um *Dissemination Information Package* (DIP).

Os metadados específicos da preservação, no OAIS, chamam-se *Preservation Description Information* e incluem *Reference Information* (identificador interno e/ou externo que identifica o *Content Information*), *Provenance Information* (histórico detalhado do *Content Information*), *Context Information* (relação com outra informação), *Fixity Information* (assegurando que o *Content Information* não foi alterado de forma não documentada, utilizando mecanismos de autenticidade ou integridade como, por exemplo, assinaturas, selos temporais).

Além disso, existem *Packaging Information*, que vinculam o *Content Information* com o *Preservation Description Information* num único pacote lógico, e *Descriptive Information* que facilitam a descoberta e recuperação de *Content Information* por um cliente do serviço de arquivo OAIS.

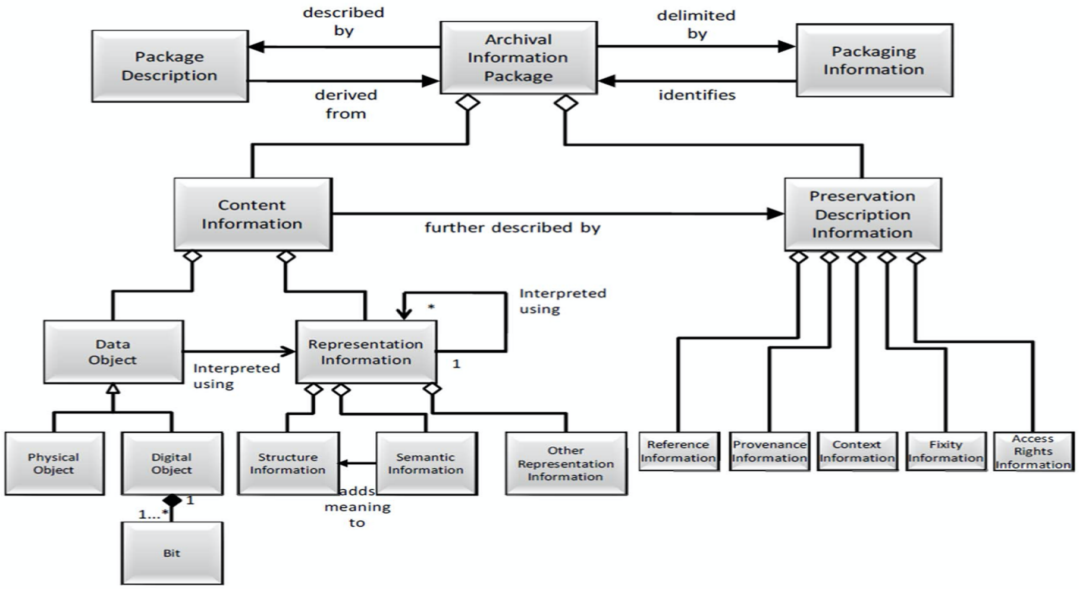



Figura 8: Visão geral do OAIS Information Model (Fonte: ETSI SR 019 510)

O Modelo OAIS contém também um *OAIS Function Model* que descreve um conjunto de serviços e funções para atingir os seus objetivos, entre eles, os seguintes:

- *Ingest:* Aceitar informação submetida pelo seu produtor e prepará-la para arquivo;
- *Archival Storage:* Gestão e manutenção do armazenamento de longo termo;
- *Data Management:* manutenção das bases de dados e descrição da informação armazenada no Archival Storage;
- *Access:* Pedir e devolver informação arquivada do Archival Storage;
- *Preservation Planning:* monitorização de alterações e riscos, por exemplo, inovações no armazenamento e nas tecnologias de preservação;

- *Administration:* gestão das operações diárias do sistema OAIS;

A imagem abaixo mostra uma visão geral do sistema OAIS.

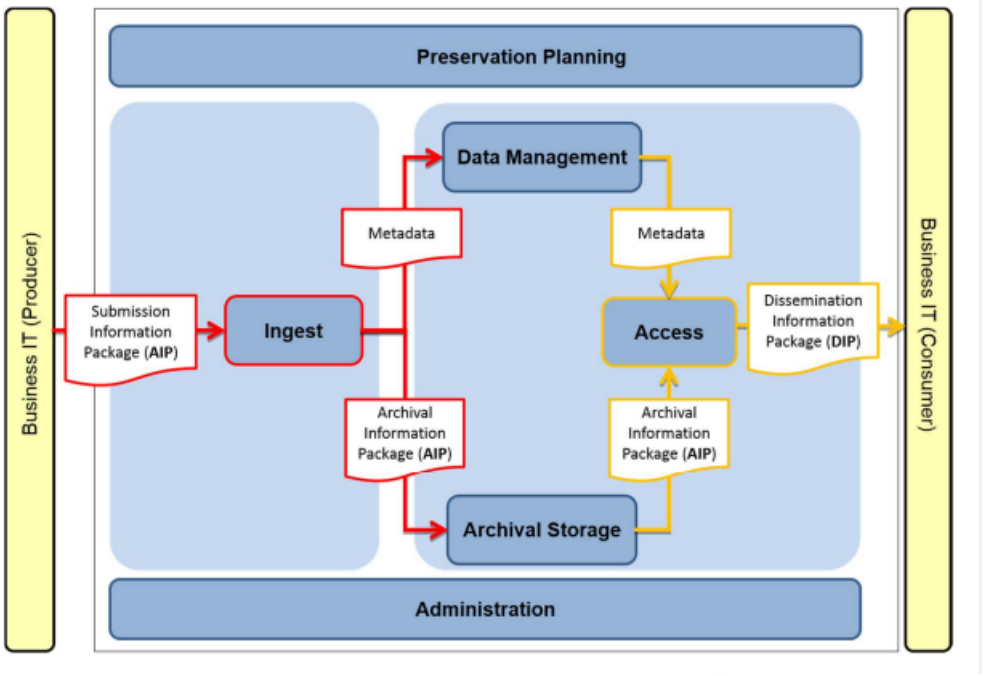



Figura 9: Visão geral do modelo funcional OAIS (Fonte: ETSI SR 019 510)

Como foi mencionado anteriormente nesta secção, o serviço de preservação e o serviço de arquivo podem ser complementares. Caso o serviço qualificado de preservação tenha um perfil de preservação com armazenamento ativo, pode fazer uso de um repositório digital que esteja em conformidade com o modelo de referência OAIS.

Na figura seguinte, os retângulos a branco representam um serviço de preservação com armazenamento.

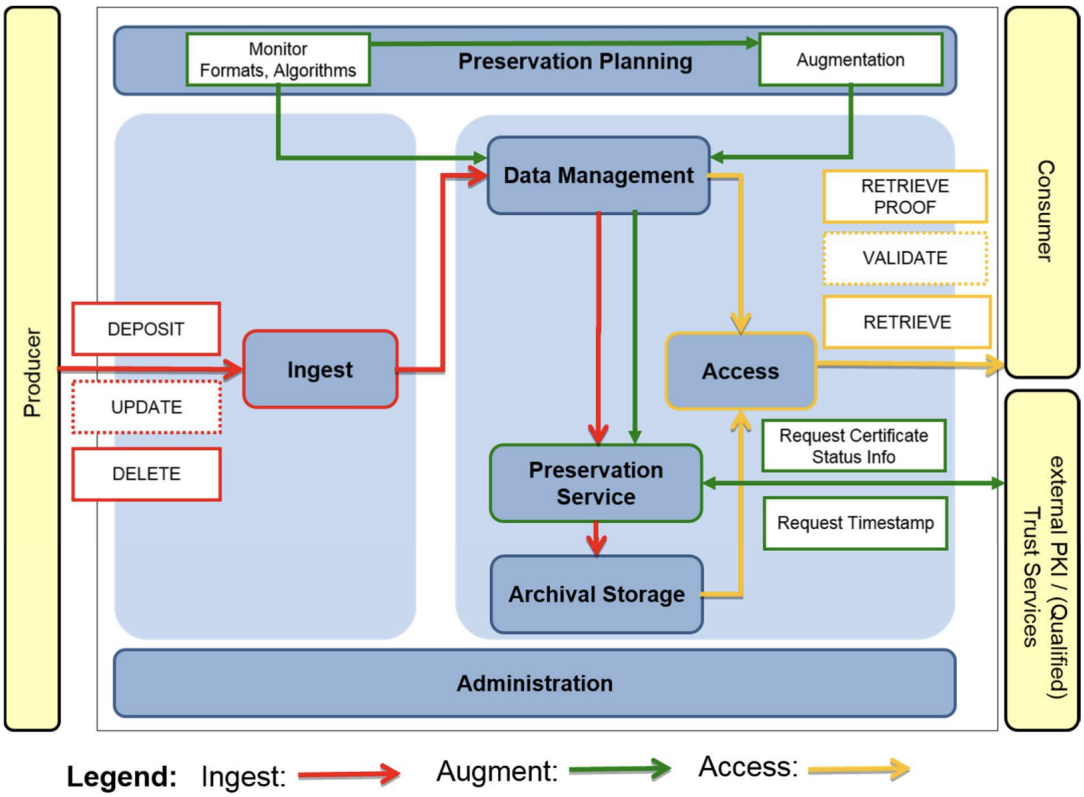



Figura 10: Serviço de preservação, incluindo o modelo de ingestão e de acesso em conformidade com o modelo OAIS (Fonte: ETSI SR 019 510)

Um serviço de preservação que permita a opção de armazenamento, terá de garantir que o cliente possa realizar certas ações, tais como ações de *depósito*, de *apagar*, de *recolher evidências*, entre outras. Este assunto será aprofundado na secção 2.4.2.

## 2.4 Visão geral das normas do sistema de preservação ETSI

Para normalizar algumas políticas e alguns aspetos técnicos dos serviços de preservação qualificados, o *Comité Técnico (CT) para Eletronic Signatures and Infrastructures (ESI) (CTESI)*, pertencente ao ETSI, começou por fazer um estudo, que resultou no ETSI SR 019 510 *Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures*, com o objetivo de estabelecer uma boa base para o subsequente processo de desenvolvimento de normas, no qual são apresentados requisitos, políticas (*cf.* ETSI TS 119 511) e protocolos técnicos para serviços de preservação (*cf.* ETSI TS 119 512).

Este documento fornece um estudo no âmbito da preservação de dados a longo prazo, incluindo a preservação de/com assinaturas digitais e cobre dois casos principais:

1. a preservação do estatuto de validade das assinaturas (utilizando selos temporais, *evidence records*, etc.) e dos dados assinados associados;

2. preservação da integridade dos objectos digitais, sejam eles assinados ou não, utilizando técnicas de assinaturas digitais (como assinaturas digitais, selos temporais, evidence records).

Fornece também um inventário das normas existentes sobre o tema dos serviços de preservação e uma proposta para um quadro de normas. (*cf.* ETSI SR 019 510)

Daqui resultaram as políticas e os requisitos de segurança expostos no ETSI TS 119 511 *Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*. Este documento baseia-se nos requisitos de política geral especificados no ETSI EN 319 401 *General Policy Requirements for Trust Service Providers*, especifica requisitos de política e segurança para os prestadores de serviços de confiança que fornecem o serviço de preservação a longo prazo de assinaturas eletrónicas e de dados gerais, ou seja, dados assinados ou dados não assinados, utilizando técnicas de assinaturas digitais.

Especificamente, mas não exclusivamente, as assinaturas digitais abordadas no documento ETSI TS 119 511 abrangem assinaturas electrónicas, assinaturas electrónicas avançadas, assinaturas electrónicas qualificadas, selos electrónicos, selos electrónicos avançados, e selos electrónicos qualificados nos termos do Regulamento eIDAS. O serviço de preservação abordado neste documento visa apoiar serviços de preservação qualificados para assinaturas ou selos electrónicos qualificados, de acordo com o Regulamento eIDAS (*cf.* ETSI TS 119 511).

O documento ETSI TS 119 511 resume-se a dois casos principais:

1. a preservação durante longos períodos de tempo, utilizando técnicas de assinatura digital, da capacidade de validar uma assinatura digital, da capacidade de manter o seu estatuto de validade e da capacidade de obter uma prova da existência dos dados assinados associados tal como estavam no momento da submissão ao serviço de preservação, mesmo que mais tarde a chave usada na assinatura fique comprometida, ou o certificado expire, ou ataques criptográficos se tornem viáveis no algoritmo de assinatura.

2. o fornecimento de provas da existência de objectos digitais, sejam eles assinados ou não, utilizando técnicas de assinatura digital (como assinaturas digitais, selos temporais, *evidence records*).

São abrangidas diferentes estratégias para o serviço de preservação. Os requisitos aplicáveis dependem da estratégia escolhida pelo serviço de preservação (*cf.* ETSI TS 119 511).

O Comité Técnico também elaborou protocolos técnicos para os prestadores de serviços de preservação qualificados que estão expostos no ETSI TS 119 512 *Protocols for trust service providers providing long-term data preservation services*, que complementa o ETSI TS 119 511.

O documento ETSI TS 119 512 aborda primeiro aspectos gerais, tais como uma arquitectura de sistema para preservação. Numa segunda fase, o documento especifica métodos e objectos de dados que constituem um protocolo entre um cliente e um serviço de preservação para a emissão e manutenção de evidências de preservação.

### 2.4.1 *Arquitetura do Sistema*

De acordo com o ETSI TS 119 512, o serviço de preservação qualificado disponibiliza uma *interface de preservação*, onde o utilizador pode submeter objetos para preservação ao serviço, com a finalidade de serem protegidos e preservados pelo serviço de confiança qualificado. Como podemos observar na Figura 11, a entidade *Client* comunica com o serviço de preservação através da *Preservation Interface*.

O serviço de preservação pode fazer uso de serviços de confiança qualificados externos, como serviços que emitam selos temporais qualificados ou que recolham todos os dados de validação, como *Certificate Revocation List (CRL)* e *Online Certificate Status Protocol (OCSP)*, e façam uma validação qualificada de assinaturas e selos qualificados e de todos os dados a eles associados, tal como é demonstrado na Figura 11 (*ValS - Validation Service*, *TSA - Time Stamping Authority* e *SigS - Signature or Seal Creation Service*, por exemplo).

Como foi mencionado anteriormente na secção 2.3.1 , existem três variantes principais para o modelo de armazenamento de um serviço de preservação qualificado:

- com armazenamento;
- com armazenamento temporário;
- sem armazenamento.

O serviço de preservação qualificado, se optar por um modelo de preservação com armazenamento, pode usar um armazenamento interno ou externo sob o seu controle. Aspetos mais relevantes serão abordados na próxima secção.

Opcionalmente, o serviço de preservação pode entrar em contacto com o utilizador, através de uma interface de notificações, de maneira a informá-lo de acontecimentos relevantes.

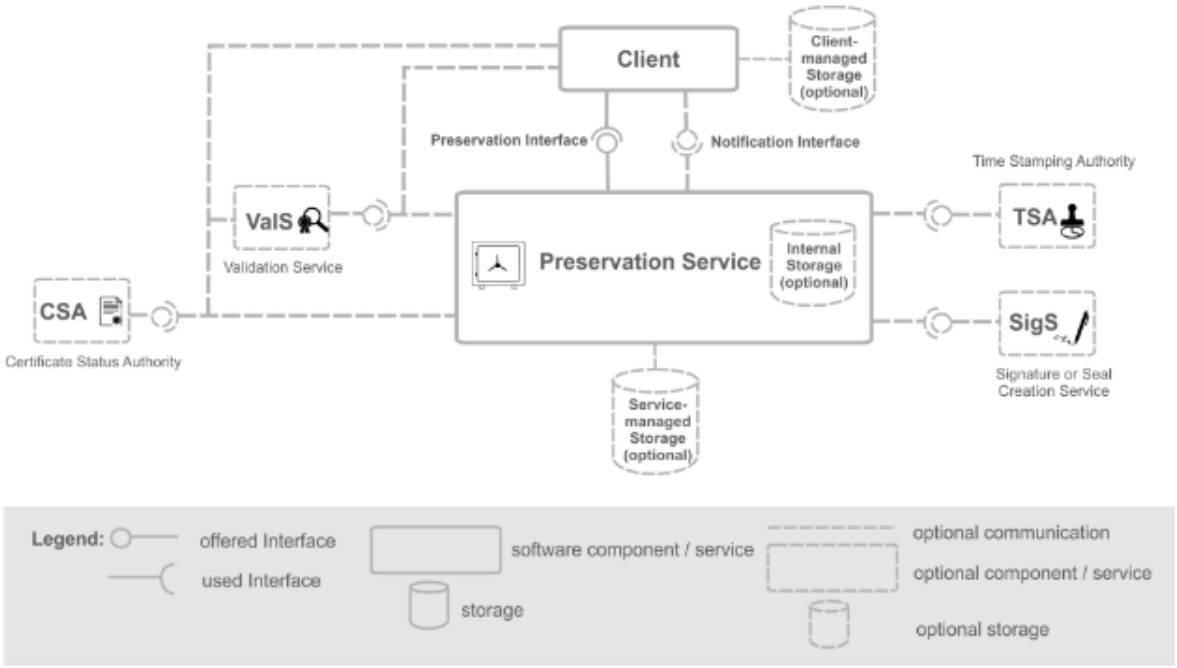



Figura 11: Arquitetura do sistema de preservação ETSI

### 2.4.2 *Modelos de Armazenamento*

Um serviço de confiança qualificado de preservação pode escolher o modelo de armazenamento que queira implementar no seu serviço. O CTESI distingue três variantes principais de modelos de armazenamento nos documentos ETSI SR 019 510 e ETSI TS 119 511:

- **Serviço de Preservação com Armazenamento**

  Os objetos para preservação e as evidências de preservação associadas, são armazenados pelo serviço de preservação. Quando requisitados pelo utilizador, o serviço de preservação entrega o pedido, quer seja a submissão original ou as evidências de preservação.

  Quando o serviço de preservação é munido com armazenamento, as operações seguintes são identificadas e devem ser implementadas. Estas operações podem ser realizadas pelo utilizador através da interface de preservação mencionada anteriormente.

  A operação de **depósito** é o processo em que o utilizador envia os objetos para preservação ao serviço de preservação. O serviço executa o processo interno de preservação onde aplica os respetivos mecanismos de preservação, devolvendo um identificador ao utilizador, que representa as evidências de preservação.

Neste caso, quando os objetos para preservação são assinaturas eletrónicas qualificadas e o objetivo de preservação é estender a capacidade de manter o estado de validade da assinatura por longos períodos de tempo, antes de proceder com algum tipo de preservação, a validação da assinatura tem de ser garantida, no momento da sua entrega, pelo utilizador ao serviço de preservação.

A operação **recuperar**, realizada pelo utilizador ou por um utilizador autorizado previamente especificado, quando quiser recuperar algum tipo de informação, quer sejam a submissão original ou as evidências de preservação, envia o identificador, que foi recebido na operação de depósito, ao serviço e requer o pretendido.

Uma operação opcional para os serviços de preservação, é a de **atualizar elementos armazenados**. O utilizador envia o identificador dos dados armazenados em conjunto com um delta-objetos para preservação, que basicamente é uma atualização dos dados armazenados. O serviço de preservação, após recepção, cria uma nova versão e envia outro identificador referente à nova versão. O serviço de preservação guarda todas as versões existentes.

Outra operação necessária neste modelo é a de **apagar**, onde o utilizador envia o identificador recebido na operação de depósito, e após autenticado, todos os dados relacionados com esse identificador são apagados.

O serviço de preservação com armazenamento deve dispor também da operação de **aumentar/estender**, que é um mecanismo ativado internamente para assegurar a validade dos dados armazenados, renovando algum aspeto específico para cumprir os objetivos de preservação e para estender o período no qual as evidências de preservação podem ser validadas.

A última operação a ser mencionada é opcional, mas importante. É a execução de **recuperar passos de operações**, que consiste no envio do identificador, por parte do utilizador, pedindo todos os passos das operações, como aumentos internos nas evidências de preservação ou simplesmente um registo com os pedidos realizados pelo utilizador ao serviço de preservação.

Para alcançar os objectivos de disponibilidade, confidencialidade e integridade o serviço de preservação pode ter de cifrar os dados armazenados, aplicando mecanismos adicionais de protecção da integridade.

- **Serviço de Preservação com Armazenamento Temporário**

  Com este modelo, o utilizador é inteiramente responsável pelo armazenamento e gestão, quer dos objetos para preservação, quer das evidências de preservação criadas pelo serviço.

O serviço de preservação recebe os objetos para preservação, mantendo-os em sua posse apenas o tempo necessário para criar as evidências de preservação. Uma vez produzidas as evidências, o serviço de preservação mantém-nas durante um período de tempo, denominado período de retenção das evidências de preservação, para permitir ao utilizador o levantamento das mesmas. As evidências de preservação são produzidas assincronamente.

Após o levantamento das evidências pelo utilizador, quer a submissão original, quer as evidências de preservação criadas são apagadas do serviço.

- **Serviço de Preservação sem Armazenamento**

  Neste modelo, os objetos para preservação, os objetos já preservados e as evidências de preservação são armazenados por parte do utilizador. O serviço de preservação não armazena nada. As evidências de preservação são produzidas sincronamente e enviadas na resposta.

  O serviço de preservação apenas faz um registo de todas as suas ações, para que esteja apto a apresentar registos das suas atividades. É da inteira responsabilidade do utilizador o armazenamento das evidências de preservação.

Em qualquer modelo, o serviço de preservação cria as evidências de preservação com base no perfil de preservação ativo (*cf.* secção 2.4.3). Os serviços de preservação podem contactar serviços de confiança qualificados externos para obter as informações necessárias para criar as evidências de preservação (por exemplo o serviço de confiança que emitiu o certificado de assinatura qualificado, o serviço de confiança que emitiu selos temporais e o serviço de confiança de validação qualificada).

Em qualquer dos modelos referidos acima, o serviço de preservação monitoriza todos os eventos que podem levar à impossibilidade de validar os objetos preservados ou as evidências de preservação, como por exemplo, os algoritmos criptgráficos usados na criação das evidências de preservação.

Quando se fala em estender a validade de uma assinatura qualificada ou de um selo qualificado, basicamente significa o aumento do período de tempo no qual é possível validar uma assinatura. Este objetivo pode ser alcançado, por exemplo, fazendo uso de selos temporais qualificados. Se já existirem, procede-se à sua renovação.

### 2.4.3 *Esquemas de preservação, Perfis de preservação e Políticas*

As normas de preservação do ETSI permitem a implementação de diferentes estratégias de preservação, que são descritas num esquema de preservação abstrato.

Um esquema de preservação é um conjunto genérico de procedimentos e regras pertinentes ao modelo de armazenamento do serviço de preservação e a um ou mais mais objetivos

de preservação, que descrevem como as evidências de preservação são criadas e validadas. Pode ser suportado por um ou mais perfis de preservação.

Um perfil de preservação identifica um conjunto de detalhes sobre a implementação, que especifica como as evidências de preservação são geradas e validadas, que são pertinentes a um modelo de armazenamento e a um ou mais objetivos de preservação.

O anexo F do ETSI TS 119 512 disponibiliza exemplos de esquemas de preservação, distinguidos pelo modelo de armazenamento, o objetivo de preservação e a maneira como as evidências de preservação são criadas. Um exemplo de um esquema de preservação para um serviço de preservação qualificado é: um serviço de preservação com armazenamento, com o objetivo de preservar a assinatura qualificada, recorrendo a *Evidence Record Syntax*. Este tipo de conceito é desenvolvido na secção 2.4.4.

#### ***Políticas***

O objectivo da política do serviço de preservação é declarar com precisão o que o serviço faz, ou seja, que objectivos de preservação suporta, que métodos aplica, que objectos aceita para preservar, que política de validação, etc. É igualmente importante especificar o formato das evidências de preservação para permitir a interoperabilidade e a movimentação dos dados preservados de um serviço para outro, se necessário.

- *Política de criação da assinatura*

  A política de criação de assinaturas estabelece quais as regras a serem aplicadas para criar a assinatura eletrónica qualificada. Pode ser usada como informação para decidir quais as regras a ser aplicadas para a validação. Esta política pode indicar, entre outras informações, qual a âncora de confiança que é usada para validar a assinatura. Como define o RFC 5280, uma âncora de confiança é o ponto final de um processo de validação de um caminho de certificados.

  A validade dessa âncora de confiança é vital para a integridade da cadeia como um todo. Qualquer caminho de certificação válido tem de terminar num certificado âncora de confiança.

- *Política de validação de assinaturas*

  A política de validação de assinaturas é um conjunto de regras estabelecido para a recolha e validação da assinatura e dos dados de validação. Esta informação é útil no processo de validação, para que se obtenham resultados iguais a validações anteriores.

- *Política das evidências de preservação*

  Esta política contém informações relativas à criação das evidências de preservação, assim como informações sobre como podem ser validadas.

Todas estas políticas devem estar presentes num perfil de preservação de um serviço de preservação.

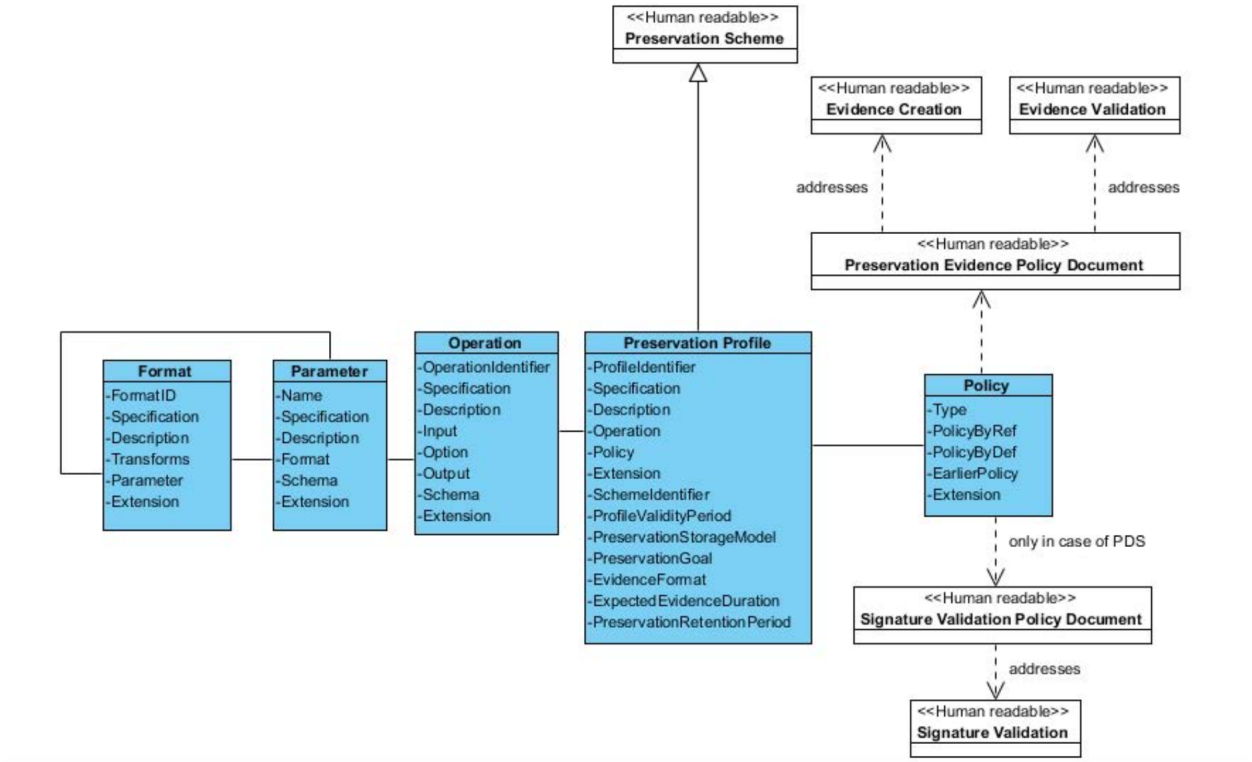



Figura 12: Relação entre Esquema de Preservação, Perfil e Política (Fonte: ETSI TS 119 512)

### 2.4.4 *Técnicas de preservação para a criação de evidências de preservação*

As evidências de preservação são produzidas pelo serviço de preservação e podem ser usadas para demonstrar que um determinado objetivo de preservação foi alcançado.

Um serviço de preservação pode trabalhar tendo em vista vários objetivos. São distinguidos os seguintes objetivos de preservação: (1) fornecimento de provas de integridade ao longo do tempo de dados assinados; (2) a preservação por longos períodos de tempo da capacidade de validar uma assinatura eletrónica, manter o seu estado de validade ou fornecer provas de existência; (3) estender evidências de preservação submetidas ao serviço de preservação.

De acordo com os documentos ETSI SR 019 510, ETSI TS 119 511 e ETSI TS 119 512, a preservação por longos períodos de tempo da capacidade de validar uma assinatura eletrónica mantendo o seu estado de validade ou, simplesmente fornecer provas de existência, é conseguida garantindo que todos os dados de validação necessários são recolhidos, validados e protegidos também, usando técnicas como as seguintes:

- Selos temporais qualificados

  Os selos temporais são dados em formato eletrónico que vinculam outros dados, também em formato eletrónico, a uma hora específica, criando uma prova de que esses outros dados existiam pelo menos a essa hora indicada. Têm também que satisfazer os requisitos estabelecidos no artigo 42º do Regulamento eIDAS. Recorrendo a esta técnica, pode ser construído um *Archive Time-Stamp* de acordo com os documentos ETSI EN 319 122-1 e ETSI EN 319 132-1.

  Contudo, o selo temporal qualificado, por si só, não consegue alcançar o objetivo de preservação. Mas é um complemento imprescindível para as técnicas seguintes.

- Evidence Record Syntax

  *Evidence Record Syntax*, ou em português, Sintaxe de Registo de Evidências, codificado em *Abstract Syntax Notation One (ASN.1)*, de acordo com o documento IETF RFC 4998, ou codificado em *Extensible Markup Language (XML)*, de acordo com o documento IETF RFC 6283, permite a preservação de vários documentos eletrónicos em paralelo ou outro tipo de dados, como assinaturas ou selos qualificados. Para isto, uma árvore de Merkel é construída para cada folha correspondente aos valores de hash de cada documento. Inicialmente, a raiz da árvore é protegida com um selo temporal. A estrutura de um ERS permite a combinação de toda a informação necessária para fornecer provas de integridade e provas de existência.

- Assinaturas Eletrónicas

  De acordo com o documento ETSI SR 019 510, as assinaturas avançadas (AdES) fornecem mecanismos internos para que a assinatura se mantenha verificável por longos períodos de tempo. Por definição, as assinaturas eletrónicas qualificadas também usufruem da mesma característica.

  No ciclo de vida de uma assinatura avançada, existem quatro fases principais:

  1. *Assinatura básica:* apenas pode ser validada se o certificado da assinatura não estiver expirado ou revogado;
  2. *Assinatura com tempo:* contém prova de que foi produzida antes de um certo tempo. Esta prova é criada recorrendo a selos temporais. Pode ser usada para validar a assinatura quando o seu certificado já tenha sido revogado depois da criação da mesma;
  3. *Assinatura com dados de validação de longo prazo:* fornece disponibilidade de longo prazo dos dados de validação incorporando esses dados, ou referências aos mesmos, necessários para proceder à validação, como CRL e OCSP;
  4. *Assinatura que fornece disponibilidade e integridade a longo prazo dos dados de validação:* ajudam a validar assinaturas para além de acontecimentos que limitam o seu

período de vida. Visa a disponibilidade a longo prazo, a integridade do material de validação das assinaturas e pode ajudar a validar a assinatura independentemente de acontecimentos que possam limitar a sua validade (por exemplo, a revogação ou expiração dos certificados e, também, quando os algoritmos usados se tornam questionáveis ou o tamanho das chaves já não é o aconselhado).

Estes quatro níveis de assinatura foram especificados pelo ETSI em normas como o documento ETSI TS 119 102-1. Para uma descrição pormenorizada do ciclo de vida de uma assinatura avançada, podemos consultar o documento ETSI TS 119 102-1.

A classe de assinaturas avançadas exposta no ponto (4), é o ideal para que um serviço de preservação consiga produzir evidências de preservação fidedignas para atingir o objetivo de preservação, ou seja, a preservação por longos períodos de tempo da capacidade de validar uma assinatura eletrónica, manter o seu estado de validade ou fornecer provas de existência.

- ASiC Containers

  Ao criar uma assinatura eletrónica, o signatário deve escolher entre diferentes elementos de empacotamento, nomeadamente *enveloping* (quando a assinatura se aplica aos dados que rodeiam o resto do documento), *enveloped* (quando os dados assinados formam um sub-elemento da própria assinatura, por exemplo objetos em XML) ou *detached* (quando a assinatura diz respeito a recursos externos separados do mesmo).

  Esta escolha não é óbvia, porque no primeiro e segundo casos a assinatura irá alterar o documento assinado e no terceiro caso é possível perder a associação entre o documento assinado e a sua assinatura. É aí que o documento *ETSI EN 319 162 Associated Signature Containers (ASiC)* Part 1: Building blocks and ASiC baseline containers oferece uma utilização normalizada de contentores para estabelecer uma forma comum de associação de objectos de dados com assinaturas.

  Resumidamente, a estrutura do *ASiC Container* vincula vários objetos assinados (como assinaturas e dados de validação) com uma assinatura eletrónica avançada, criando um contentor baseado em *ZIP* (cf. ETSI TS 102 918 *Associated Signature Containers (ASiC)*).

  O formato da assinatura eletrónica avançada usada pelo contentor pode ser *XAdES* ou *CAdES*. Mais informação sobre estes formatos pode ser encontrada na secção 2.6.2.

  Simplificando, um *ASiC* é um contentor de dados que contém um grupo de objectos e as suas assinaturas/e ou selos temporais associados, utilizando o formato *ZIP*.

  A estrutura interna deste contentor inclui:

  – Um directório de raiz que contém todo o conteúdo do contentor, que pode incluir pastas que reflectem a estrutura do conteúdo;

- Um diretório *"META-INF"*, dentro do diretório raiz, que contém ficheiros com metadados sobre o conteúdo, o que inclui os ficheiros de assinatura e/ou de selos temporais associados.

Os ficheiros contidos no diretório *"META-INF"* são aplicados de forma a que a integridade dos dados não seja comprometida quando são extraídos do contentor *ZIP*. Quando colocados em armazenamento, estes ficheiros podem ser verificados em relação aos seus ficheiros associados (*e.g.* assinatura avançada).

Independentemente das técnicas escolhidas pelo serviço de preservação qualificado, o serviço deve monitorizar a força das funções de hash e dos algoritmos criptográficos usados. Isto para, se for necessário, proceder ao mecanismo interno de aumento das evidências de preservação. Este aumento pode ser feito com renovações de hash, renovações de selos temporais ou voltar a assinar recorrendo à ultima classe das assinaturas avançadas. Isto tudo com os algoritmos adequados para o efeito, que podem ser encontrados em ETSI TS 119 312.

### 2.4.5 *Duração Expectável das Evidências e Período de Preservação*

A duração expectável das evidências é um conceito aplicável aos serviços de preservação qualificado com o modelo de armazenamento temporário e sem armazenamento.

É um conceito que expressa a duração que o serviço de preservação prevê para que as evidências de preservação possam ser usadas a fim de atingir os objetivos de preservação, significando que as evidências ainda podem ser verificadas.

Para as evidências de preservação geradas usando técnicas de assinaturas, como assinaturas eletrónicas e selos temporais, devem ser tomadas em linha de conta as seguintes durações:

1. o período de validade da chave privada, ou seja, o período definido previamente no qual a chave privada pode ser utilizada para gerar evidências, como a última classe de assinaturas avançadas e selos temporais qualificados. Isto se o certificado a ela associado não tiver sido revogado;
2. o período de validade dos certificados das chaves;
3. o período no qual as informações de revogação estão disponíveis, normalmente só durante o período de validade, previamente definido, dos certificados;
4. o período no qual as funções de hash, se utilizadas, são resistentes a ataques de colisão;
5. o período no qual as chaves públicas, correspondentes às chaves privadas, são resistentes a ataques criptográficos.

Com a entrada em vigor do Regulamento eIDAS, as informações de revogação dos certificados, usadas para as assinaturas qualificadas, estão sempre disponíveis. Isto, porque, como já foi referido anteriormente, as assinaturas eletrónicas qualificadas têm associado um certificado qualificado de assinatura eletrónica.

"No que respeita ao disposto no nº 3, os prestadores qualificados de serviços de confiança que emitam certificados qualificados fornecem a qualquer utilizador informações sobre a validade ou a revogação dos certificados qualificados por eles emitidos. Estas informações são fornecidas pelo menos para cada certificado, em qualquer altura e mesmo após o termo do prazo de validade do certificado, de uma maneira automática que seja fiável, gratuita e eficaz." (*sic* nº4 do Artigo 24º do Regulamento eIDAS (2014) ).

Logo, as informações de revogação dos certificados qualificados irão estar sempre disponíveis, mesmo que o prazo de validade tenha expirado.

Resumindo, a duração expectável das evidências reflecte uma estimativa calculada tanto com base nos algoritmos de assinatura como nos algoritmos criptográficos usados nos dados de validação. Segundo o ETSI TS 119 511, a duração expectável das evidências deve basear-se na estimativa da adequação dos algoritmos criptográficos.

No caso de serviços de preservação com armazenamento, o período de preservação é a duração durante o qual o serviço de preservação armazena e preserva os dados do utilizador, assim como os objetos para preservação, os objetos preservados e as evidências de preservação geradas. Durante este período, o serviço de preservação cria e estende as evidências de preservação as vezes necessárias para atingir os objetivos de preservação.

Quer a duração expectável, quer o período de preservação, assim como os objetivos de preservação, depois de calculados pelo serviço e escolhidos pelo utilizador, respetivamente, são expostos na política, que por sua vez, estará no perfil de preservação selecionado.

## 2.5 Normas de alguns estados membros da UE

Esta secção expõe o trabalho desenvolvido por alguns Estados-Membros na elaboração de normas que ajudam na implementação de um sistema de preservação qualificado.

### 2.5.1 *França - AFNOR NF Z 42-020*

A *Association Française de Normalisation*, sediada na França, trabalhou na elaboração de normas que ajudam na implementação de um sistema de preservação qualificado. O sistema por eles desenvolvido é apelidado de *Digital Vault Component*, ou, em português, componente caixa-forte digital. A norma AFNOR NF Z40-020 define especificações funcionais para o armazenamento de informações, quer sejam dados para preservar, quer sejam dados

preservados ou evidências de preservação. Este documento tem como objetivo a definição de condições necessárias para garantir a integridade dos dados ao longo do tempo. No documento AFNOR NF Z40-020 são identificados um conjunto de atores, entre eles: o *Admnistrador Geral*, o *Admnistrador Funcional* e o *Utilizador Simples*. Esta separação de atores é definida para diferenciar adequadamente as ações administrativas e o acesso aos dados.

Neste documento técnico é também definido um conjunto de funções que devem ser implementadas. Entre elas, as funções de:

1. *Deposit*: corresponde ao acto de inserção de dados no sistema caixa-forte;
2. *Read*: corresponde à recuperação de dados do sistema;
3. *Delete*: corresponde ao acto de apagar dados do sistema;
4. *Metadata Read*: corresponde à recuperação de dados associados a objetos preservados;
5. *Data Object Control*: possivelmente a função mais importante deste sistema. Permite verificar se determinados dados se encontram no sistema, assim como se estes não foram modificados desde a operação de depósito;
6. *Audit Trail Access*: função que permite ao utilizador requerer e consultar um registo com acontecimentos relacionados com os seus dados;
7. *List Data Object*: permite ao utilizador receber uma lista com os dados, por ele inseridos na operação de depósito;
8. *Count Data Objects*: função que retorna o número de objectos, inseridos pelo utilizador na operação de depósito.

Cada função é descrita pelo seu papel no sistema, pelo seu *input* e pelo seu *output*. O documento AFNOR NF Z40-020 define também medidas de segurança para evitar acessos não autorizados e regras para a implementação/desenvolvimento do sistema.

### 2.5.2 *Alemanha - BSI TR-03125*

A Agência Federal de Segurança da Informação Alemã (BSI) fornece um guia, BSI Technical Guideline 03125, que descreve como os dados e os documentos assinados podem ser armazenados de forma confiável no sentido de preservação de evidências por longos períodos de tempo. Este guião técnico é principalmente destinado às autoridades públicas, contendo recomendações técnicas. Isto porque a necessidade de preservação legal de evidências de documentos criptograficamente assinados está a ganhar cada vez mais importância em quase todos os setores públicos e privados. Documentos eletrónicos, como no setor da saúde, documentos digitalizados, faturas e recibos eletrónicos nas transações comerciais

diárias, registos civis e muitas outras áreas exigem soluções adequadas para a preservação de evidências a longo prazo. Mesmo sendo poucos os exemplos, estes mostram a grande relevância da preservação de evidências de documentos eletrónicos.

A diretiva BSI Technical Guideline 03125, é baseada no Regulanto eIDAS (2014), em normas de preservação ETSI, como os documentos ETSI SR 019 510, ETSI TS 119 511 e ETSI TS 119 512 , em normas do OAIS, como o documento ISO 14721:2012, e em *Evidence Record Syntaxe (ERS)*, como o documento IETF RFC 4998 e o documento IETF RFC 6283.

A arquitetura proposta para o BSI Technical Guideline 03125 não deve ser entendida como um substituto para um sistema de arquivo, mas sim como um *middleware* que descreve uma possível execução dos requisitos para a preservação legalmente válida de evidências de documentos assinados durante o período de retenção estipulado. Para tal, os seguintes tópicos são abordados no BSI Technical Guideline 03125:

1. recomendações de formatos para os dados;
2. recomendações de formatos para a troca de dados entre sistema e o utilizador;
3. recomendações para a arquitetura do sistema;
4. requisitos para as componentes inseridas na arquitetura do sistema;
5. fornecimento de ferramentas de teste.

A arquitectura recomendada está representada na Figura 13 e consiste principalmente nas seguintes componentes:

- Componentes e sistemas externos:
  1. Um *ECM/Long Term* para o armazenamento dos dados. Isto inclui tanto o armazenamento dos objectos de dados arquivados como todos os metadados criados e geridos pelo *Middleware* para garantir o não-repúdio;
  2. pode recorrer a prestadores de serviços de confiança qualificados para assinaturas, selos e selos temporais qualificados.
- Componentes *TR-ESOR-Middleware*:
  1. *ArchiSafe-Module*: componente que é responsável pela dissociação, assim como pelo acesso, do sistema ao *ECM/Long-Term Storage*;
  2. *Cryptographic-Module*: componente que torna todas as funções disponíveis, para que se consiga criar valores de hash, para a validação de assinaturas, selos e selos temporais, para o *Middleware*;
  3. *ArchiSig-Module*: fornece funções necessárias para a criação de assinaturas, selos, selos temporais e para a criação de evidências, por exemplo, recorrendo a ERS de acordo com o IETF RFC 4998 e o IETF RFC 6283;

4. *Upload/Download-Module*: é uma componente opcional que permite a atualização e a recuperação em alta performance, respetivamente, de dados presentes no *ECM/Long-Term Storage*.

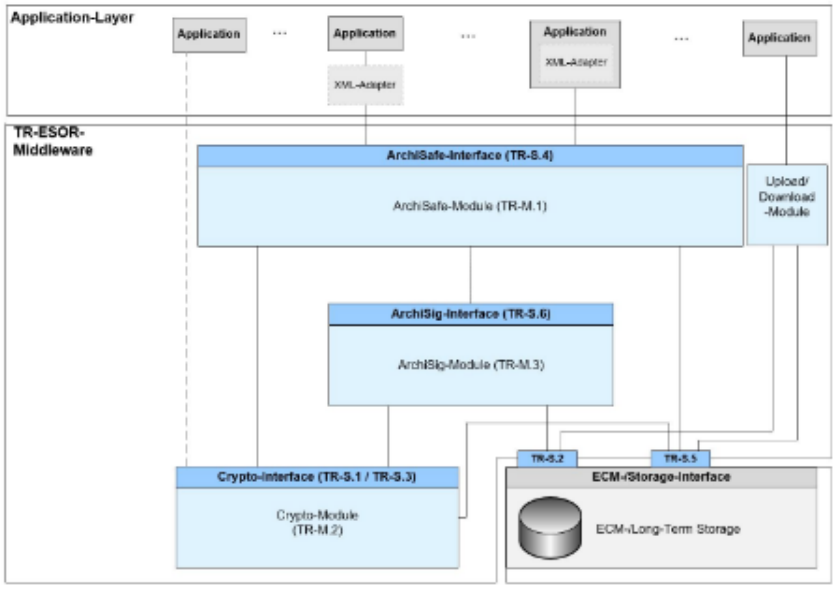



Figura 13: Visão geral da arquitetura do BSI Technical Guideline 03125 (Fonte: BSI Technical Guideline 03125)

## 2.6 PROJETOS

No contexto do Regulamento eIDAS, os projetos apresentados nesta secção visam apoiar a implementação prática do Regulamento na Europa.

Para este fim, os projectos abordam a necessidade de soluções globalmente interoperáveis através de investigação básica no que diz respeito aos fundamentos da confiança e da fiabilidade, apoiar activamente o processo de normalização em áreas relevantes, e fornecer componentes de software *Open Source* e serviços de confiança que facilitarão a utilização da tecnologia de assinatura electrónica em aplicações do mundo real.

### 2.6.1 *FutureTrust*

O FutureTrust[1] é um projeto europeu, cujo objetivo central é apoiar a implementação prática do Regulamento eIDAS de modo a facilitar a utilização e proliferação de tecnologias confiáveis de assinaturas eletrónicas na Europa e fora da Europa, a fim de permitir transações eletrónicas confiáveis em todo o mundo.

Em coordenação com o trabalho de normalização ainda em curso no ETSI, o projeto FutureTrust está a desenvolver uma implementação de referência de um serviço de preservação escalável de acordo com o ETSI SR 019 510, o ETSI TS 119 511 e o ETSI TS 119 512, que pode facilitar consideravelmente a implementação de serviços de preservação qualificados por toda a Europa e promover a interoperabilidade entre diferentes implementações. Contudo ainda não se encontra disponível uma implementação deste projeto.

Depois de uma análise ao documento FutureTrust - Scalable Preservation Service, é de constatar que a arquitectura do sistema FutureTrust (Figura 14) é baseada e inspirada nas normas e na arquitetura do ETSI. As interações com o utilizador são realizadas através da *Preservation API*. A gestão do sistema de preservação é feita através da *Admnistration Interface* e utiliza serviços de validação (*ValS)* e autoridades de criação de selos temporais externos (*TSA*). Este sistema, para poder preservar assinaturas e selos qualificados e para poder estar de acordo com o Regulamento eIDAS, precisa de garantir que estes serviços de confiança externos são serviços de confiança qualificados e que estão presentes na lista de confiança europeia.

1 https://cordis.europa.eu/project/id/700542

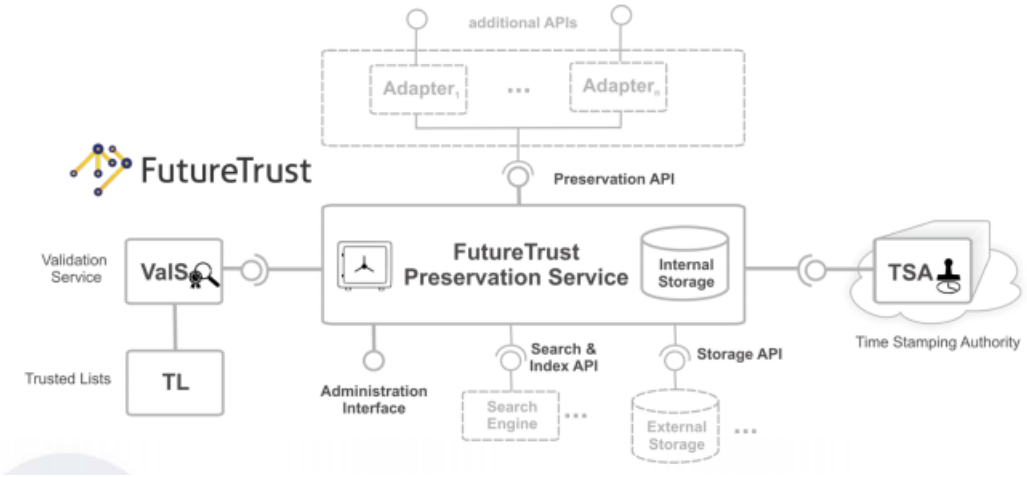



Figura 14: Visão geral da arquitetura do sistema de preservação FutureTrust (Fonte: FutureTrust - Scalable Preservation Service)

### 2.6.2 *Digital Signature Service*

O Digital Signature Service[2] é um projeto *open source*[3] criado pela empresa *Nowina Solutions*, a pedido da UE e vai de encontro com o Regulamento eIDAS (2014) e com as normas associadas às assinaturas eletrónicas[4].

No projeto DSS, três operações principais são identificadas: (1) a criação de assinaturas eletrónicas; (2) a validação de assinaturas eletrónicas; (3) extensão de assinaturas eletrónicas.

Para estas operações, para além da *DSS Demonstration WebApp*[5], foi desenvolvido e disponibilizado uma API[6] em Java, garantindo a portabilidade em numerosas plataformas.

Este projeto suporta tanto as assinaturas electrónicas como os selos electrónicos e apoia as normas da UE sobre: formatos de assinatura e métodos de empacotamento; procedimentos de validação da assinatura.

Neste projeto, a validação é feita com base nas listas de confiança dos Estados Membros.

Apenas a criação de assinaturas eletrónicas avançadas (AdES) é possível.

Como foi mencionado e explicado na secção 2.4.4, quatro níveis de assinaturas *baseline* foram definidos pelas normas ETSI para as assinaturas avançadas (AdES), sendo eles o:

- nível **Baseline-B** *Basic Signature*;
- nível **Baseline-T** *Signature with Time*;
- nível **Baseline-LT** *Signature with Long-Term Validation Material*;

2 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS
3 https://github.com/esig/
4 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+standards
5 https://ec.europa.eu/cefdigital/DSS/webapp-demo/home
6 https://ec.europa.eu/cefdigital/DSS/webapp-demo/apidocs/index.html

- nível **Baseline-LTA** *Signature providing Long Term Availability and Integrity of Validation Material*;

Estes níveis foram implementados, pelo projeto DSS, em vários formatos das assinaturas avançadas, isto é, nos formatos **XAdES**, **CAdES** e **PAdES**.

Para cada um destes formatos de assinaturas, o *DSS* respeita e segue as seguintes normas ETSI, que estão em conformidade com o Regulamento eIDAS:

- **XAdES** *XML Advanced Electronic Signatures*

  - ETSI EN 319 132 XML Advanced Electronic Signatures (XAdES)

  Part1: Building blocks and XAdES baseline signatures

  Part2: Extended XAdES signatures

- **CAdES** *CMS Advanced Electronic Signature*

  - ETSI EN 319 122 CMS Advanced Electronic Signatures (CAdES)

  Part1: Building blocks and CAdES baseline signatures

  Part2: Extended CAdES signatures

- **PAdES** *PDF Advanced Eletronic Signature*

  - ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES)

  Part1: Building blocks and PAdES baseline signatures

  Part2: Additional PAdES signatures profiles

- **ASiC** *Associated Signature Container*

  - ETSI EN 319 162 Associated Signature Containers (ASiC)

  Part 1: Building blocks and ASiC baseline containers

  Part 2: Additional ASiC containers

O formato de assinatura a ser usado depende do documento ou objeto a assinar. Caso seja necessário assinar múltiplos documentos, o DSS implementou também *ASiC Associated Signature Container* para o efeito.

O projeto Digital Signature Service também oferece um bloco de validação de assinaturas eletrónicas, selos eletrónicos e selos temporais. Mas nesta função, para além de conseguir validar assinaturas avançadas, selos avançados e selos temporais avançados, também consegue proceder à validação do seu equivalente qualificado.

O algoritmo de validação de assinaturas eletrónicas qualificadas é composto por três partes principais, baseadas nos artigos 32º e 40º do Regulamento eIDAS: determinar se o certificado de assinatura é um certificado qualificado de assinatura ou selo eletrónico válido

no momento da sua emissão; determinar se o certificado de assinatura é um certificado qualificado de assinatura ou selo eletrónico relacionado com um dispositivo de criação de assinatura qualificado e válido no momento da assinatura; determinar se a assinatura é Assinatura Eletrónica Avançada. (*cf.* CEF eSigntare DSS(2018)).

Ou seja, o bloco de validação do DSS tem a finalidade de validar as assinaturas electrónicas e indicar se são Assinaturas Electrónicas Avançadas (AdES), AdES suportadas por um Certificado Qualificado (AdES/QC) ou uma Assinatura Electrónica Qualificada (QES). Todos os certificados e suas cadeias relacionadas que suportam as assinaturas são validados com base nas Listas de Confiança dos Estados-Membros da UE (isto inclui o certificado do signatário e os certificados utilizados para validar o de estado de validade dos certificados, isto é, CRL, OCSP, e os selos temporais).

O processo de validação do DSS cria quatro tipos de relatórios de validação para expor todo o processo, sendo eles o *simple report*,o *detailed report*, a *diagnostic data* e por último, um *esti report*. A diferença e o conteúdo destes relatórios será abordada na secção 3.5 na parte do Serviço de Validação.

O DSS pode ser reutilizado numa solução informática para assinaturas electrónicas para assegurar que as assinaturas, bem como os selos, sejam criados e validados em conformidade com o Regulamento eIDAS.

Resumindo, trata-se de uma boa referência, com as devidas alterações, para uma implementação de um serviço de preservação qualificado de assinaturas e selos qualificados.

### 2.6.3 *E-ARK*

Existem projetos, relacionados com o serviço de arquivo eletrónico, que disponibilizam normas e aplicações que podem ser úteis à implementação de um serviço de preservação qualificado. Projetos como o E-ARK[7] apresentam tecnologias capazes de ajudar, por exemplo, na implementação de um serviço de preservação qualificado com armazenamento.

O E-ARK foi um grande projecto multinacional de investigação que melhorou os métodos e tecnologias de arquivo digital, a fim de alcançar consistência a uma escala europeia.

Enfrentando uma série de problemas associados a tecnologias, sistemas e práticas de manutenção de registos independentes, o E-ARK beneficiou o desenvolvimento de arquivos acessíveis internacionalmente através: do fornecimento de especificações e ferramentas técnicas, do desenvolvimento de uma infra-estrutura de arquivo, que manterão registos e bases de dados autênticos e utilizáveis ao longo do tempo.

"O RODA é um repositório digital capaz de incorporar, preservar e dar acesso a todo o tipo de material digital produzido por grandes organizações públicas ou privadas. O seu rol de funcionalidades cobre a totalidade das unidades funcionais do modelo de referência

7 https://www.eark-project.com/

OAIS, permitindo que a informação incorporada permaneça autêntica e acessível ao longo do tempo. O RODA permite gerir informação segundo uma abordagem baseada na análise de risco. O sistema monitoriza permanentemente a informação que detém e alerta o responsável para potenciais riscos que poderão colocar em causa a sua longevidade ou dificultar o seu acesso. Sendo baseado em standards (OAIS, *Encoded Archival Description (EAD)*, *Metadata Encoding and Transmission Standard (METS)* e *PREservation Metadata – Implementation Strategies (PREMIS)*), este sistema é a ferramenta ideal para criar um repositório certificado segundo a norma ISO 16363:2012." (*cf.* RODA White Paper)

Entre 2014 e 2016, o projeto RODA recebeu apoios financeiros e técnicos do projeto E-ARK (cofinanciado pela KEEP SOLUTIONS e pelo Programa de Frameworks de Inovação e Competitividade da Comissão Europeia, acordo de subvenção n.º 620998), acabando por resultar num projeto que está em conformidade como os requisitos técnicos do arquivo eletrónico.

Um serviço de preservação, que tenha ativo o modelo de preservação com armazenamento, pode fazer uso de um repositório digital como o RODA para armazenar as evidências de preservação.

Este repositório, que está em conformidade com o modelo de referência OAIS abordado na secção 2.3.1, disponibiliza uma aplicação que pode ser instalada pelo serviço de preservação. Esta aplicação contém uma *REST API* para que possa ser feita a integração e a comunicação com o sistema de preservação. Oferece também uma interface, apelativa e fácil de usar, para que o admnistrador do serviço de arquivo consiga monitorizar as evidências e realizar ações manualmente.

Para cada evidência de preservação enviada para o serviço de arquivo, é devolvido ao sistema de preservação um *AIP-ID* (identificador único do *Archival Information Package (AIP)*) criado pelo sistema do RODA, para a dita evidência. Este identificador serve para que se consiga fazer uma gestão e monitorização do conteúdo do repositório.

# 3

# PROVA DE CONCEITO DE UM SERVIÇO DE PRESERVAÇÃO

Neste capitulo serão abordadas e explicadas todas as tomadas de decisão para a construção da Prova de Conceito de um Serviço de Preservação de assinaturas e selos eletrónicos qualificados.

## 3.1 OBJETIVOS E VISÃO GERAL DO SISTEMA

O objectivo de um Serviço de Preservação é assegurar que as assinaturas electrónicas e os selos electrónicos possam ser validados durante longos períodos de tempo e não percam o seu valor probatório, independentemente de futuras mudanças tecnológicas. Tais mudanças podem incluir em particular o aumento do poder computacional, a melhoria dos ataques existentes ou mesmo a descoberta de ataques completamente novos, o que pode implicar que os algoritmos criptográficos aplicados se tornem fracos e não forneçam protecção suficiente numa perspectiva de longo prazo. O objectivo do Serviço de Preservação é fornecer meios para provas de integridade e provas de existência dos Objectos para Preservação fornecidos e também fornecer meios de preservação adicionais, se for caso disso, tais como a manutenção do estatuto de validade de uma assinatura e da disponibilidade dos dados preservados.

Uma das maneiras de cumprir o objetivo de fornecer meios para provas de integridade e provas de existência, tal como foi abordado na secção 2.3.1, é fazer uso de técnicas de assinaturas digitais na criação de evidências de preservação, como assinaturas eletrónicas e selos temporais.

Tudo aquilo que está bem desenvolvido, implementado e bem documentado deve ser utilizado. Com base nesta afirmação, ficou decidido aproveitar ferramentas criadas pelo projeto DSS, como o bloco de criação de assinaturas, mencionado na secção 2.6.2, para a criação das evidências de preservação. Este bloco de criação de assinaturas faz uso de técnicas de assinaturas digitais, como assinaturas eletrónicas avançadas (e qualificadas) e selos temporais. O projeto DSS rege-se por directrizes europeias e normas internacionais, como mencionado na secção 2.6.2.

Contudo, recorrer apenas a estas técnicas não satisfaz os objetivos de preservação adicionais, como a manutenção do estatuto de validade de uma assinatura ou da disponibilidade dos dados preservados.

O primeiro, dos objetivos de preservação adicionais, apenas é cumprido se for realizado um constante trabalho de monitorização às evidências de preservação criadas (*i.e.* monitorização dos algoritmos usados e do material de validação, como caminhos de certificação e material de revogação), e para tal, as evidências de preservação devem ser geridas e armazenadas pelo sistema do serviço de preservação. O mesmo acontece com o segundo objetivo de preservação adicional, a disponibilidade dos dados preservados só consegue ser garantida se as evidências de preservação forem geridas e armazenadas pelo sistema do serviço de preservação.

Posto isto, para atingir estes objetivos de preservação adicionais foi decidido implementar um sistema "híbrido" para desenvolver um Serviço de Preservação com um perfil de preservação com armazenamento, fazendo uso do repositório digital RODA[1] como serviço de arquivo, mencionado na secção 2.6.3.

O conceito de "híbrido" nasce aqui, com a ideia de criar um sistema que (1) se rege por normas de preservação assim como por normas de arquivo que vão de encontro às directrizes europeias e normas internacionais, nomeadamente, o Regulamento eIDAS e normas publicadas pelo ETSI, e que (2) oferece um modelo com armazenamento ao utilizador, que utiliza tecnologias que estão em conformidade com normas relativas ao Serviço de Arquivo, como o modelo de referência OAIS.

1 https://github.com/keeps/roda

## 3.2 REQUISITOS

| *ETSI TS 119 511 - Policy and Security requirements for Trust Service Providers providing long term preservation* | | |
|---|---|---|
| **[R1]** Um serviço de preservação deve suportar pelo menos um perfil de preservação. (OVR-6.4-01) | ✓ | |
| **[R2]** Para um serviço de preservação sem armazenamento, o perfil de preservação deve conter a duração expectável das evidências. (OVR-6.4-06) | ✓ | |
| **[R3] A** duração expectável das evidências deve basear-se na estimativa da adequação dos algoritmos criptográficos. (OVR-6.4-07) | ✓ | |
| **[R4]** O serviço de preservação deve implementar ficheiros log para estabelecer as informações necessárias para provas posteriores. (OVR-7.10-02) | ✓ | |
| **[R5]** Para cada perfil de preservação activo, o serviço deve monitorizar a força de cada algoritmo criptográfico que foi utilizado com este perfil. (OVR-7.14-01) | ✓ | |
| **[R6]** Para a avaliação dos algoritmos criptográficos em [R5], o *ETSI TS 119 312 Cryptographic Suites* deve ser considerado. (OVR-7.14-03) | ✓ | |
| **[R7]** Durante o período de preservação, o serviço de preservação deve certificar-se de que as evidências de preservação podem ser utilizadas para atingir o objectivo de preservação correspondente. (OVR-7.15-01) | ✓ | |
| **[R8]** Um serviço de preservação com armazenamento deve permitir a recuperação de evidências e/ou de submissões originais. (PRP-8.1-10) | ✓ | |
| **[R9]** Um serviço de preservação com armazenamento deve permitir a eliminação de evidências armazenadas. No caso da eliminação da evidência de preservação, a submissão original correspondente deve ser igualmente eliminada. (PRP-8.1-11) | ✓ | |
| **[R10]** O serviço de preservação deve assegurar que as evidências armazenadas só possam ser eliminadas antes do fim do período de preservação, quando o pedido de eliminação for apresentado tem que vir acompanhado de uma justificação. Qualquer justificação apresentada deve ser registada em log juntamente com a informação do pedido de eliminação. (PRP-8.1-12) | ✓ | |
| **[R11]** Um serviço de preservação com armazenamento pode permitir ao utilizador fornecer uma nova versão da submissão original já submetido. (PRP-8.1-14) | ✓ | |
| **[R12]** Um serviço de preservação sem armazenamento não deve armazenar os objetos a serem preservados após a criação das evidências. (OVR-9.1-01) | ✓ | |
| **[R13]** Se os dados de validação não forem submetidos pelo cliente de preservação, o serviço de preservação fará os seus melhores esforços para recolher e verificar os dados de validação de acordo com a política de validação de assinaturas apoiada pelo perfil de preservação. (OVR-9.3-01) | ✓ | |
| **[R14]** Para estender a capacidade de validação de uma assinatura e de manter o seu estatuto de validade, o serviço de preservação deve, no mínimo, fornecer uma prova da existência da assinatura e dos dados de validação necessários para validar a assinatura utilizando técnicas de assinatura digital (assinaturas digitais, selos temporais, Evidence Records). (OVR-9.3-03) | ✓ | |
| **[R15]** O serviço de preservação deve preservar toda a informação necessária para verificar o estado de qualificação da assinatura ou selo electrónica, que não estaria disponível ao público até ao fim do período de preservação. (OVR-A-02) | ✓ | |
| **[R16]** Os selos temporais utilizados nas evidências de preservação devem ser fornecidos por um serviço de confiança qualificado, que emita selos temporais qualificados. (OVR-A-03) | ✓ | |

Figura 15: Requisitos expostos no ETSI TS 119 511

Nesta secção é feita uma comparação entre alguns dos requisitos mais importantes propostos pelo ETSI e que se decidiu que seriam cumpridos pela Prova de Conceito.

O cumprimento do requisito **[R1]** e do **[R2]**, pode ser observado na secção 3.3 e nos apêndices D e K, respetivamente. O sistema da prova de conceito, depois de ter criado as evidências devolve ao utilizador uma estimativa da duração expectável das mesmas.

Como foi mencionado na secção 3.1, as evidências de preservação são criadas através do recurso ao bloco de criação de assinaturas do projeto DSS.

Posto isto, o conceito de duração expectável das evidências nesta prova de conceito, é baseado na validade criptográfica e matemática das assinaturas geradas para servirem de evidências de preservação, ficando assim o **[R3]** cumprido.

No que toca ao requisito **[R6]**, tanto o projecto DSS como o sistema da Prova de Conceito tomam em atenção o documento de algoritmos criptográficos recomendados. Para a criação das evidências nesta Prova de Conceito, os seguintes algoritmos foram utilizados.

```
<BasicSignature>
    <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
    <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
    <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
    <SignatureIntact>true</SignatureIntact>
    <SignatureValid>true</SignatureValid>
</BasicSignature>
```

Figura 16: Algoritmos usados na criação das evidências de preservação.

Relativamente ao requisito **[R5]**, o projeto DSS disponibiliza dois métodos capazes de ajudar na monitorização das evidências. Tratam-se dos métodos *getSignatureExtensionPeriodMin(*signatureId*)* e do *getSignatureExtensionPeriodMax(*signatureId*)*, que devolvem uma data, estimada na validade criptográfica, de quando as assinaturas devem ser estendidas. Este mínimo e máximo delimita o período no qual as evidências devem ser estendidas, isto sem contar com nenhum evento que obrigue a extensão antecipada, como revogação de certificados ou a perda de confiança num algoritmo. Um exemplo da duração expectável da evidência de preservação pode ser visto na Figura 47 do apêndice D.

No caso do perfil de preservação com armazenamento, uma constante monitorização às evidências de preservação e uma eventual extensão das mesmas é feita de maneira a cumprir o requisito **[R7]**.

Ao ser escolhido o perfil de preservação sem armazenamento, o serviço da Prova de Conceito não armazena nenhum objeto, seja a submissão original ou a respetiva evidência de preservação, ficando cumprido o requisito **[R12]**. Tal como exemplifica o caso de uso nº1 da secção 3.7.2.

Em relação ao requisito **[R13]**, o sistema da Prova de Conceito faz uso da API[2] do DSS para a construção do bloco de validação do serviço de preservação. Recolhendo e verificando os dados de validação da assinatura eletrónica.

2 https://ec.europa.eu/cefdigital/DSS/webapp-demo/apidocs/index.html

No que diz respeito ao **[R15]**, no decorrer da elaboração desta Prova de Conceito, ficou evidente que para validar a estatuto de qualificação de uma assinatura basta confirmar se o emissor do certificado é um serviço de confiança qualificado presente na lista de confiança de um Estado Membro, como visto na secção 2.2.1.

Relativamente ao cumprimento dos restantes requisitos, será abordado ao longo deste capítulo.

### 3.2.1 *Mapeamento dos Requisitos do Regulamento eIDAS*

Neste ponto encontra-se uma tabela que demonstra alguns dos requisitos desta Prova de Conceito que cobrem os requisitos expostos no Regulamento eIDAS referentes ao Serviço de Preservação Qualificado de assinaturas e selos eletrónicos qualificados.

| **Regulamento (UE) No 919/2014** | **Requisitos cumpridos pela Prova de Conceito** |
|---|---|
| **Artigo 24°(2).h** Registam e mantêm acessíveis durante um prazo adequado, incluindo depois de o prestador qualificado de serviços de confiança ter deixado de prestar esses serviços, todas as informações pertinentes relativas aos dados emitidos e recebidos pelo prestador qualificado de serviços de confiança, em particular para efeitos de apresentação de provas em processos judiciais e para garantir a continuidade do serviço. Esse registo poderá ser feito eletronicamente; | [R4] |
| Artigos, mencionado na secção 2.2.1, referentes aos Prestadores de Serviços Qualificados | Fora do âmbito desta Prova de Conceito |
| **Artigo 34° (1)** Os serviços de preservação de assinaturas eletrónicas qualificadas só podem ser prestados por prestadores qualificados de serviços de confiança que utilizem procedimentos e tecnologias capazes de prolongar a fiabilidade das assinaturas eletrónicas qualificadas para além do prazo de validade tecnológica. | [R5], [R6], [R13], [R14], [R15], [R16] |

Figura 17: Mapeamento dos Requisitos do Regulamento eIDAS

Alguns dos requisitos, presentes no Regulamento, que se dirigem para o Prestador de Serviços de Confiança no geral, não foram tidos em conta, visto que não foram considerados como estando enquadrados no âmbito desta Prova de Conceito.

Para a preservação qualificada de selos electrónicos qualificados, é aplicável o Artigo 40º do Regulamento eIDAS, como foi visto na secção 2.2.1, onde os requisitos são os mesmos (*mutatis mutandis*) para a preservação de assinaturas eletrónicas qualificadas. Ao longo deste documento sempre que se falou e/ou falar em assinaturas eletrónicas qualificadas, também se reporta ao conceito de selos eletrónicos qualificado.

## 3.3 Esquema de preservação, perfis de preservação e políticas de preservação

Como foi visto na secção 2.4.3, um Esquema de Preservação é suportado por um ou mais Perfis de Preservação. No âmbito desta Prova de Conceito foi implementado um esquema de preservação que é suportado por dois perfis de preservação.

O esquema de preservação desta Prova de Conceito tem como objetivos de preservação:

1. estender por longos períodos de tempo o estado de validade de uma assinatura;
2. estender evidências de preservação recorrendo a técnicas de assinaturas digitais, nomeadamente assinaturas eletrónicas e selos temporais.

Para tal, foram implementados nesta Prova de Conceito dois Perfis de Preservação.

O primeiro perfil possui um modelo **com** armazenamento, onde as evidências de preservação são criadas e armazenadas como exposto na secção 2.4.2.

Este perfil de preservação permite ao utilizador a realização de operações de depósito, de recuperar, de apagar e de substituir a submissão original, tal como expostas na secção 2.4.2. O fluxo de eventos destas operações no sistema da Prova de Conceito pode ser observado na secção 3.7.2, nos casos de uso 2, 3, 4 e 5, ficando cumpridos os requisitos [R8], [R9], [R10] e [R11].

No que toca à monitorização das evidências de preservação armazenadas no sistema de arquivo, a Prova de Conceito tem como referência a data calculada com base nos algoritmos criptográficos usados na criação da evidência, como referido na secção 3.2.

A Prova de Conceito faz uma constante validação das evidências presentes no sistema de arquivo esperando o resultado *TOTAL-PASSED*, como exposto na secção 3.5. Durante o período de tempo iniciado pela criação da evidência de preservação e terminado pela data calculada com base nos algoritmos criptográficos usados na criação da evidência, caso o resultado da validação das evidências seja sempre positivo, o sistema da Prova de Conceito não procede à extensão da evidencia de preservação. Caso o resultado da validação não seja positivo ou caso tenha terminado o período de tempo, o sistema da Prova de Conceito procede à extensão da evidência de preservação.

O segundo perfil possui um modelo **sem** armazenamento, onde as evidências de preservação são criadas como exposto na secção 2.4.2. A informação da duração expectável das evidências, como abordado na secção 3.2, é calculada com base nos algoritmos criptográficos usados na criação da evidência e é devolvida ao utilizador após a criação da evidência de preservação. O fluxo de eventos com este perfil pode ser observado na secção 3.7.2 no caso de uso 1.

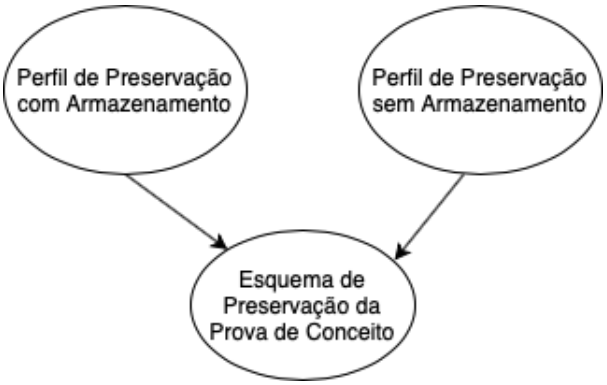



Figura 18: Esquema e Perfis de Preservação

Em relação às politicas elaboradas, como se trata de uma Prova de Conceito, não foi elaborada um documento de política para o sistema da Prova de Conceito.

Contudo, caso fosse elaborada uma política para um serviço de preservação, como esta Prova de conceito, deveria conter as políticas mencionadas na secção 2.4.3.

A política essencial no âmbito desta Prova de Conceito seria a política de evidências de preservação, que conteria informação relativa à sua criação, assim como informações sobre como poderiam ser validadas.

Posto isto, a política de evidências de preservação desta Prova de Conceito deveria conter informação sobre a criação da evidência segundo a política de criação de assinaturas do projeto DSS e informação de como poderiam ser validadas segundo a política de validação do projeto DSS.

No âmbito da Prova de Conceito foi desenvolvido um ficheiro de políticas fictício que se encontra em `https://www.devisefutures.com/pdf/preservacao/PoliticaPreservacao.pdf` e foi implementada uma classe em *Java* que cria um ficheiro em *XML* que representa o perfil de preservação escolhido por cada Utilizador. Este ficheiro inclui o modelo de armazenamento escolhido, o objetivo de preservação, o conteudo da evidência de preservação criada, a duração expectável da evidência de preservação e um apontamento para onde encontrar a política do serviço de preservação que é esta Prova de Conceito. Um exemplo deste ficheiro pode ser observado no apêndice K.

```
<Policy>
    <Id>https://www.devisefutures.com/pdf/preservacao/PoliticaPreservacao.pdf</Id>
    <Url>https://www.devisefutures.com/pdf/preservacao/PoliticaPreservacao.pdf</Url>
    <ZeroHash>false</ZeroHash>
    <DigestAlgoAndValue>
        <DigestMethod>SHA256</DigestMethod>
        <DigestValue>YEHjO7Zw+Is8mZtQpUbebzaRaaPhCp3HaoTJthiRrPo=</DigestValue>
    </DigestAlgoAndValue>
    <Asn1Processable>false</Asn1Processable>
    <Identified>true</Identified>
    <Status>true</Status>
    <DigestAlgorithmsEqual>true</DigestAlgorithmsEqual>
</Policy>
```

Figura 19: Inclusão da política

Tendo desenvolvido um ficheiro com a política, a informação sobre a mesma vai explicita na evidência de preservação, uma vez que está exposta, nos parâmetros da assinatura que forma a evidência de preservação, onde pode ser encontrada (tal como se pode observar na Figura 19).

## 3.4 Arquitetura do Sistema

Esta secção descreve as decisões tomadas para a conceção da arquitetura da Prova de Conceito.

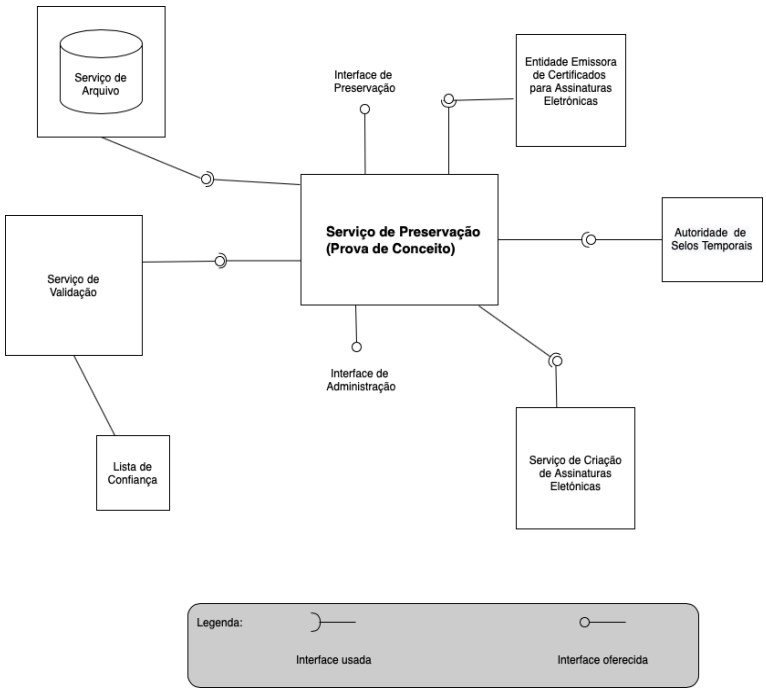



Figura 20: Arquitetura da Prova de Conceito

Após um estudo detalhado das normas e requisitos impostos aos serviços de preservação qualificados, a arquitetura desta Prova de Conceito foi concebida com base na arquitetura proposta pelo ETSI e abordada na secção 2.4.1, como pode ser observado numa comparação entre a Figura 11, da secção 2.4.1, e a Figura 20.

Na arquitetura da Prova de Conceito, a *Interface de Preservação* é onde o utilizador pode submeter documentos contendo assinaturas eletrónicas para o sistema da Prova de Conceito com a finalidade de serem protegidos e preservados pelo serviço de confiança.

Como foi abordado na secção 2.4.3, dependendo do perfil de preservação (com/sem armazenamento) escolhido pelo utilizador, é devolvido um identificador único que representa as evidências de preservação do mesmo. Na Prova de Conceito é na *Interface de Preservação* que o utilizador pode realizar as operações mencionadas na secção 3.3. A comunicação entre o utilizador e o sistema da Prova de Conceito é realizada através da *Interface de Preservação*.

Tal como apresentado pela arquitetura ETSI, um serviço de preservação, opcionalmente pode incluir no seu sistema serviços externos, como *Validation Service - ValS* ou *Time Stamping Authority - TSA*.

Para a arquitetura da Prova de Conceito, ficou decidido que faz sentido haver uma componente de validação, a componente do *Serviço de Validação*. Isto para proceder à validação das assinaturas submetidas ao sistema da Prova de Conceito, reunindo material de validação.

Ficou também decidido fazer uso de um *Serviço de Criação de Assinaturas Eletrónicas*, como componente da arquitetura da Prova de Conceito, para a criação de assinaturas avançadas *-LTA* e de contentores *ASIC* (mencionados na secção 2.4.4) como evidências de preservação. Mas, para tal, componentes adicionais são necessárias. Para a criação de assinaturas *-LTA*, o sistema da Prova de Conceito necessita de um certificado de chave para a assinatura, assim como de informações de revogação do mesmo. Para isso, o sistema da Prova de Conceito tem na sua arquitetura a componente *Entidade Emissora de Certificados para Assinaturas Eletrónicas* que é responsável pela emissão do certificado e da informação de revogação.

O nível *-LTA* de uma assinatura avançada só é atingido se a assinatura contiver informação de revogação assim como selos temporais. Posto isto, outra componente essencial para a Prova de Conceito é a *Autoridade de Selos Temporais*.

Como mencionado na secção 3.3, a Prova de Conceito oferece dois perfis de preservação, um com armazenamento e outro sem. E tal como demonstra a arquitetura ETSI exposta na Figura 11, a arquitetura da Prova de Conceito poderia fazer uso de armazenamento interno ou de um serviço externo controlado pelo sistema da Prova de Conceito. Posto isto, a arquitetura da Prova de Conceito faz uso da componente *Serviço de Arquivo* como armazenamento externo controlado pelo sistema da Prova de Conceito.

Por fim, a arquitetura da Prova de Conceito contém uma *Interface de Administração* que é onde o Administrador gere o sistema da Prova de Conceito.

O conceito de sistema "híbrido", mencionado na secção 3.1, aplica-se ao sistema da Prova de Conceito, uma vez que a sua arquitetura faz uso de componentes que se regem por normas de preservação assim como por normas de arquivo, nomeadamente o Regulamento eIDAS, as normas publicadas pelo ETSI e o modelo de referência OAIS. Componentes como o *Serviço de Validação*, o *Serviço de Criação de Assinaturas Eletrónicas* e a *Autoridade de Selos Temporais* estão em conformidade com o Regulamento eIDAS e com as normas publicadas pelo ETSI.

O que faz este sistema ser intitulado de "híbrido" é o facto de fazer uso da componente de *Serviço de Arquivo* que está em conformidade com o modelo de referência OAIS, conforme retratado na Figura 10.

É de mencionar que as operações de ingestão marcadas a vermelho na Figura 10, como a operação de *Deposit*, *Update* e *Delete*, assim como as operações de acesso marcadas a amarelo, como a operação *Retrieve* são realizadas através da *Interface de Preservação*, como pode ser observado na Figura 21.

O serviço de arquivo OAIS exposto na Figura 9, está representado na arquitetura da Prova de Conceito como sendo a componente de "Serviço de Arquivo".

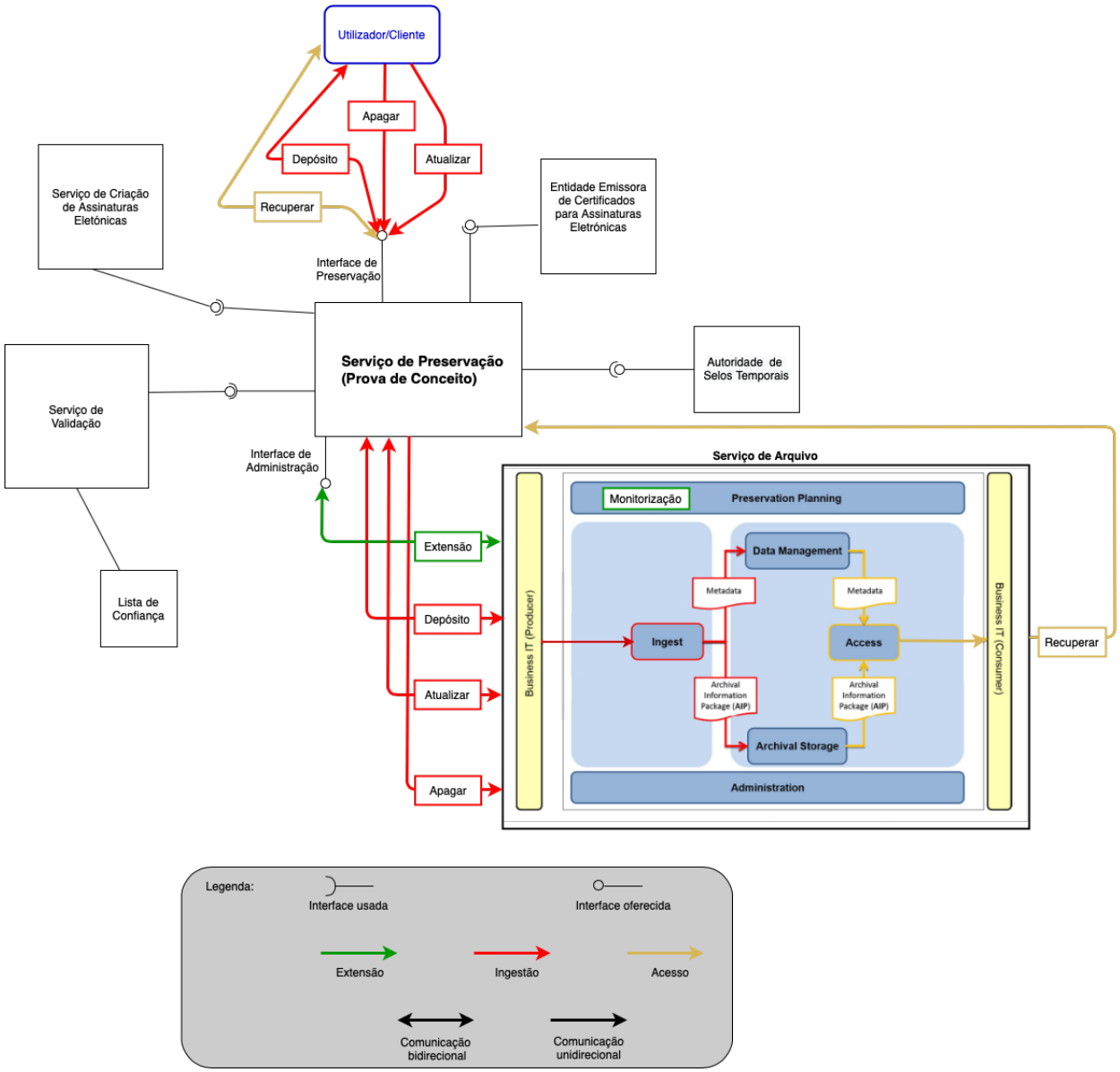



Figura 21: Fluxo das componentes da arquitetura da Prova de Conceito com o serviço de arquivo

A Figura 21 representa o fluxo de atividades entre as componentes da Prova de Conceito que sustentam o conceito de sistema "híbrido". Isto é, entre o sistema do serviço de preservação da Prova de Conceito e a componente de serviço de arquivo.

Consoante os pedidos de ingestão e/ou acesso por parte do utilizador, o sistema da Prova de Conceito acede ao serviço de arquivo que está sob seu controlo.

Por exemplo, na operação de depósito, o utilizador submete o documento contendo a assinatura a preservar ao sistema da Prova de Conceito, posto isto, o sistema da Prova de Conceito procede à ingestão do mesmo. Dependendo do modelo de armazenamento escolhido pelo o utilizador, o sistema da Prova de Conceito ou (1) devolve as evidências de

preservação criadas, no caso do perfil de preservação sem armazenamento, (2) ou envia as evidências de preservação para a componente do serviço de arquivo, que depois da ingestão e da criação de um AIP, devolve o AIP-ID (identificador único do AIP) do mesmo (tal como referido na secção 2.6.3) ao sistema da Prova de Conceito, que por sua vez devolve um identificador único ao utilizador, que representa as suas evidências de preservação, no caso do perfil de presevação com armazenamento.

## 3.5 COMPONENTES DO SISTEMA

O sistema desta Prova de Conceito é baseado na arquitetura ETSI, mencionada na secção 2.4.1.

Como já foi mencionado, nessa mesma secção, o serviço de preservação pode fazer uso de serviços de confiança qualificados externos, que se encontram identificados na lista de confiança de cada Estado Membro.

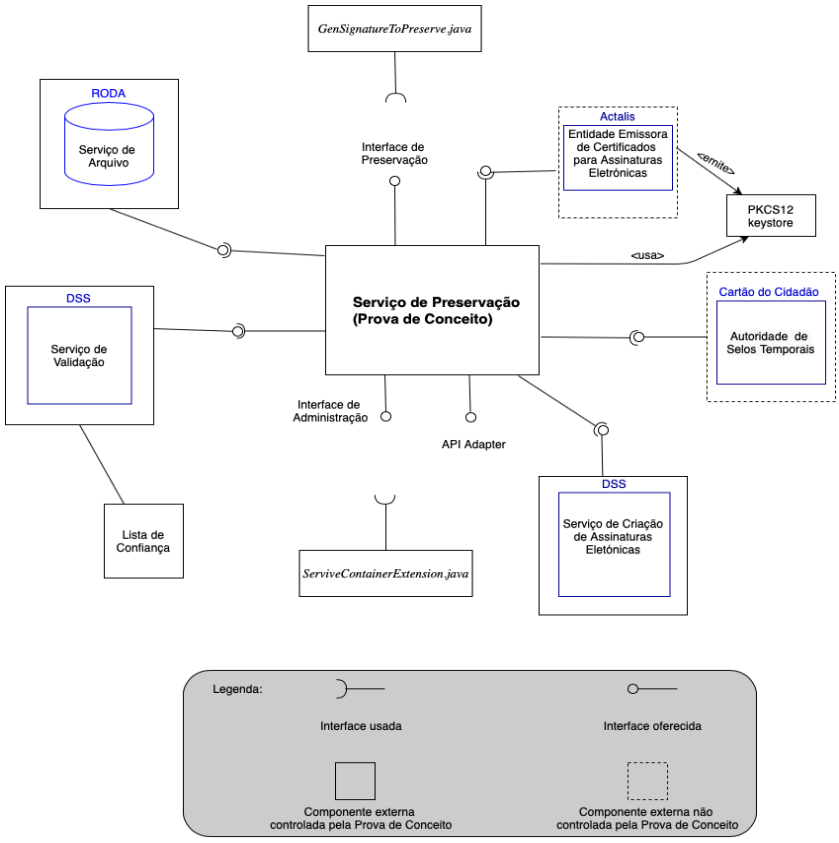



Figura 22: Componentes da Arquitetura da Prova de Conceito

A arquitetura da Prova de Conceito é constituída por vários componentes externos. Alguns destes componentes externos não são controlados pela Prova de Conceito. Isto é,

estas componentes externas são entidades reais, como a componente *Autoridade de Selos Temporais* e a *Entidade Emissora de Certificados para Assinaturas Eletrónicas*.

As várias componentes do serviço desenvolvido nesta Prova de Conceito são as seguintes (*cf.* Figura 22):

- **Serviço de Validação**

  No contexto desta Prova de Conceito foi decidido desenvolver o serviço de validação, em conformidade com o Regulamento eIDAS, fazendo uso do bloco de validação do projeto DSS abordado na secção 2.6.2.

  A validação de assinaturas e selos qualificados e avançados baseia-se nas normas ETSI. Apesar de só existir um *draft* do documento Draft ETSI TS 119 172-4, que tem por objectivo criar normas para as políticas de validação de assinaturas e selos eletrónicos qualificados, utiliza-se o bloco de validação do DSS que faz a sua interpretação dos requisitos para a validação de assinaturas e selos qualificados do regulamento eIDAS e de documentos como ETSI TS 119 102-1, resultando no documento onde é explicado o algoritmo usado para a validação de assinaturas eletrónicas qualificadas.

  O algoritmo de validação de assinaturas eletrónicas qualificadas do DSS foca-se em três aspetos:

  – em primeiro lugar verifica se o certificado é qualificado;

  – depois identifica o tipo do certificado;

  – por último confirma se a chave privada correspondente é protegida por um dispositivo de criação de assinaturas qualificado.

    (*cf.* CEF eSigntare DSS(2018))

  Geralmente, o processo de validação termina num dos três estados seguintes: *TOTAL-FAILED*, *TOTAL-PASSED* ou *INDETERMINATE*. Uma resposta *TOTAL-PASSED* indica que a assinatura passou na verificação e está em conformidade com a política de validação de assinaturas. Uma resposta *TOTAL-FAILED* indica que o formato da assinatura está incorrecto ou que o valor da assinatura falhou a verificação. Uma resposta de validação *INDETERMINATE* indica que o formato e as verificações da assinatura não falharam, mas há informação insuficiente para determinar se a assinatura electrónica é válida.

  Como foi mencionado na secção 2.6.2, o processo de validação do DSS cria quatro tipos de relatórios de validação para expor todo o processo. Todos estes relatórios são devolvidos em *XML*, o que permite ao serviço manipular e extrair facilmente informação para análise posterior.

– **Simple Report**

O resultado do processo de validação é baseado em regras muito complexas. O objectivo deste relatório é tornar a informação tão simples quanto possível, mantendo ao mesmo tempo os elementos mais importantes. Assim, o utilizador final pode ter uma visão sintética da validação.

– **Detailed Report**

Este relatório é um documento mais detalhado, a sua estrutura é construída em torno de *Basic Building Blocks*, dados de validação, dados de validação de selos temporais e dados de validação dos níveis de assinatura AdES, abordados na secção 2.4.4.

Ao abrigo do Regulamento eIDAS, uma nova dimensão foi acrescentada à validação clássica de uma assinatura electrónica: a determinação do seu nível de qualificação.

É por isso que o bloco de assinaturas é composto por dois tipos de sub-blocos:

* Os primeiros sub-blocos que resumem o resultado dos "processos clássicos de validação de assinaturas electrónicas" (*cf.* ETSI TS 119 102-1).
* O último sub-bloco com informação detalhada sobre o nível de qualificação da assinatura (*cf.* Draft ETSI TS 119 172-4).

Cada sub-bloco aborda um processo de validação específico, e contém informação extensiva sobre o mesmo, tal como verificações criptográficas e de conformidade de formato, enquanto os blocos de *Trusted Lists* fornecem a informação utilizada para a aceitação ou rejeição de uma Lista de Confiança.

– **Diagnostic Data**

Trata-se de um conjunto de dados construído a partir da informação contida na própria assinatura, mas também da informação recuperada dinamicamente, (como dados de revogação e, informação extrapolada como a validade matemática de uma assinatura).

– **ETSI Validation Report**

O Relatório de Validação do ETSI representa uma implementação do ETSI TS 119 102-2. O relatório contém um resultado padronizado de uma validação de assinatura ASiC. Inclui os dados originais de entrada de validação, a política de validação aplicada, bem como o resultado da validação de uma ou mais assinaturas e as suas restrições.

(*cf.* Digital Signature Service)

Um exemplo de um *Simple Report* pode ser encontrado no apêndice E, juntamente com direções para encontrar exemplos dos restantes relatórios. Estes exemplos de relatórios não foram colocados nesta dissertação porque são muito extensos.

Este componente externo foi desenvolvido no âmbito desta tese, recorrendo à API[3] do DSS, e é controlado e gerido pelo sistema da Prova de Conceito.

- **Serviço de Criação de Assinaturas Eletrónicas**

  Atualmente não existe nenhuma implementação ativa de um projeto relativo à preservação de assinaturas eletrónicas. Com isto, para a criação de evidências de preservação, foi decidido fazer uso de algo que está bem desenvolvido, implementado e documentado.

  Como foi mencionado na secção 2.4.4, uma das técnicas para a criação de evidências de preservação é fazer uso do último nível de uma assinatura eletrónica , ou seja, assinatura que fornece disponibilidade e integridade a longo prazo dos dados de validação (*AdES -LTA*), ou fazer uso de contentores ASiC com uma assinatura avançada *-LTA* associada, para preservar mais que um documento.

  Para tal, foi usado mais uma vez o projeto DSS, ou melhor dizendo, o bloco de criação de assinaturas do DSS para a criação de evidências de preservação por parte da Prova de Conceito.

  Quando o serviço é instanciado quer para a criação de uma assinatura AdES ou de um contentor ASiC, é definido um verificador de certificados. Este objecto é utilizado para fornecer quatro fontes de informação diferentes:

  – a fonte de certificados de confiança (baseada na(s) lista(s) de confiança específica(s) do contexto);

  – a fonte de certificados intermediários utilizada para construir a cadeia de certificados até à âncora de confiança.

  – a fonte de OCSP;

  – a fonte de CRL.

  Para mais informações sofre o perfil de assinaturas do DSS, consultar `https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#_signature_profile_guide`.

  Este componente externo foi desenvolvido no âmbito desta tese, recorrendo à API[4] do DSS, e é controlado e gerido pelo sistema da Prova de Conceito.

3 `https://ec.europa.eu/cefdigital/DSS/webapp-demo/apidocs/index.html`
4 `https://ec.europa.eu/cefdigital/DSS/webapp-demo/apidocs/index.html`

- **Entidade Emissora de Certificados para Assinaturas Eletrónicas**

  Como é sabido, para assinar electronicamente um objeto, é necessário um certificado de assinatura (que prove a identidade do signatário) e o acesso à sua chave privada associada. E como foi mencionado na secção 3.4, para a construção do nível *-LTA* de uma assinatura, é necessário informação de revogação.

  Para esta Prova de Conceito foi decidido fazer uso de um certificado não qualificado emitido pela empresa italiana *Actalis*[5], que emite certificados para a criação de assinaturas não qualificados, mas com informação de revogação. A informação de revogação tem de estar sempre presente para a construção do último nível de assinatura (*AdES -LTA*), quer seja a informação dos certificados, quer seja a informação dos certificados dos selos temporais.

  Para esta Prova de Conceito foi também decidido não proteger a chave privada, usada pelo serviço de preservação para criar as evidências de preservação, com um dispositivo de criação de assinaturas qualificado, já que o certificado emitido pela *Actalis* é não qualificado, como referido anteriormente.

  Este facto pode ser observado no excerto do relatório de validação da evidência de preservação criada pela Prova de Conceito, nomeadamente nos avisos que são apresentados.

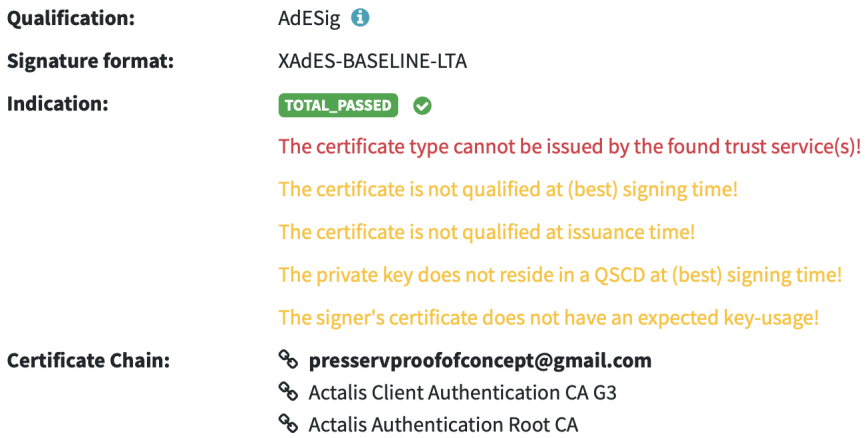



Figura 23: Excerto do relatório de validação da evidência de preservação

A *Actalis* forneceu uma *PKCS12 keystore* que fica à inteira responsabilidade do serviço da Prova de Conceito, continuando a providenciar informação de revogação sobre os certificados presentes na mesma (*e.g.* o certificado de assinatura e os certificados pertencentes à cadeia de certificação).

5 https://www.actalis.it

No âmbito desta Prova de Conceito, foi desenvolvida uma classe em Java (*cf.* Pkcs12.java) capaz de fazer a gestão e tratar do acesso à *keystore* sempre que for necessário ao serviço da Prova de Conceito (para a criação de evidências de preservação, por exemplo).

- **Autoridade Emissora de Selos Temporais**

  Como mencionado na secção 3.4, para a construção do nível *-LTA* de uma assinatura, é necessário uma fonte de selos temporais qualificados. Neste contexto, esta prova de conceito faz uso de um selo temporal qualificado disponibilizado pelo Cartão de Cidadão. Ou seja, este protótipo recorre a um prestador de serviços qualificados externo para a criação de selos temporais qualificados. (*cf.* Selo Temporal Cartão de Cidadão (2010)).

  Fica, assim, cumprido o requisito [R16], exposto na secção 3.2.

- **Serviço de Arquivo**

  Como foi exposto na secção 3.3, esta Prova de Conceito suporta dois perfis de preservação distintos, um recorrendo ao modelo com armazenamento e outro sem armazenamento.

  Tal como descrito na secção 3.1, a Prova de Conceito faz uso do repositório digital Roda, que está em conformidade com o modelo de referência OAIS, como serviço de arquivo externo para armazenar as evidências de preservação.

  Este componente externo é controlado, gerido e está integrado com o sistema da Prova de Conceito e goza das seguintes características:

  – compatibilidade com normativos como o EAD e *Dublin Core (DC)* para metadados de descrição, PREMIS para metadados de preservação, METS para metadados estruturais e várias normas ao nível dos metadados técnicos (*e.g* ANSI/NISO Z39.87).

  – 100% suportado por tecnologias *open-source*, sem licenças associadas, permitindo a qualquer instituição assumir responsabilidade pela manutenção do sistema sem depender de um fornecedor específico. Do ponto de vista dos utilizadores, estes apenas necessitam de um *browser* com suporte para *Javascript* para que possam tirar partido de todas as funcionalidades do sistema.

  – as ações de preservação e gestão no interior do RODA são desempenhadas por um módulo de execução de tarefas. As ações de preservação incluem conversões de formatos, verificações de integridade, comunicação, despiste de vírus, etc.

  – todas as ações realizadas por utilizadores ou por processos automáticos ficam registadas para auditoria futura.

  (*cf.* RODA White Paper)

- **Interface de Preservação e Interface de Administração**

  Esta prova de conceito oferece os seus serviços ao utilizador através da Interface de Preservação, sendo gerida pelo administrador recorrendo à Interface de Administração. Ambas as interfaces foram desenvolvidas no âmbito desta tese.

- **Comunicação entre o Sistema de Preservação e o Serviço de Arquivo**

  A componente de serviço de arquivo utilizada pela Prova de Conceito disponibiliza uma *API*[6] para que se possa comunicar com ele através de pedidos *REST*. Para a Prova de Conceito deste serviço de preservação, o serviço de arquivo RODA foi alojado num servidor distinto daquele onde se encontra o serviço de Preservação. Foi desenvolvida uma classe em Java que trata da comunicação entre estes dois serviços, recorrendo à tal API.

  Tal como foi exposto na secção 2.4.2, um serviço de preservação com armazenamento tem que devolver ao utilizador um identificador único referente à evidência de preservação gerada para o mesmo, para futura gestão da mesma.

  Como foi mencionado anteriormente, na secção 2.6.3, sempre que o serviço de preservação submete uma evidência de preservação para o serviço de arquivo, o RODA cria um novo AIP e devolve ao sistema o AIP-ID.

  Inicialmente houve a ideia de devolver este AIP-ID ao utilizador como identificador único das suas evidências. Mas algumas questões surgiram. Se o utilizador quisesse fazer uma atualização ao objeto originalmente submetido, o serviço de preservação iria criar novas evidências de preservação e em seguida armazenava-as no repositório, que por sua vez iria devolver um novo AIP-ID, que teria que ser devolvido ao utilizador, tendo o serviço de preservação de manter todas as versões recebidas.

  Outra questão, no caso do serviço de preservação com armazenamento, é a extensão interna das evidências de preservação. O serviço de preservação recupera as evidências a estender do repositório, aplica os mecanismos de extensão e volta a submeter no repositório, que por sua vez gera um novo AIP-ID.

  O problema destas situações é entrar em contacto com o titular das evidências para lhe dar o novo identificador único.

  Posto isto, a solução encontrada para esta Prova de Conceito foi fazer uso da classe *Universally Unique Identifier (UUID)* do Java, associando um utilizador a um UUID, e assim, todos os AIP-IDs daquele utilizador, estão associados a um único UUID, que será o identificador devolvido ao utilizador.

  Foi utilizada uma estrutura *Map<Key,Value>*, em que a *Key* representa o UUID, gerado pelo serviço de preservação para identificar o utilizador, e em que o *Value* retrata uma

6 https://demo.roda-community.org/api-docs/

Lista com todos os AIP-IDS relativos àquele utilizador, sendo que o último identificador da lista faz referência à versão mais recente da evidência de preservação.

A utilização deste serviço pela Prova de Conceito pode ser observada nos apêndices.

- **Criação das Evidências de Preservação**

  Como foi mencionado na secção 2.4.4, uma das técnicas para a criação de evidências de preservação é fazer uso do último nível de uma assinatura eletrónica, ou seja, assinatura que fornece disponibilidade e integridade a longo prazo dos dados de validação. Dependendo do tipo de certificado e do dispositivo usado na criação da assinatura, se é qualificado ou não, é que se vai determinar se a assinatura é qualificada ou apenas avançada.

  Tal como foi exposto no ponto da Entidade Emissora de Certificados, o certificado usado para criar as evidências de preservação não tem o estatuto de qualificado. Posto isto, as assinaturas criadas por esta Prova de Conceito são assinaturas eletrónicas avançadas (AdES).

  Para a criação das evidências de preservação, esta prova de conceito faz uso dos blocos de validação e de criação de assinaturas do DSS, mencionados nesta secção e obedece ao seguinte processo:

  1. usa a componente do serviço de validação, gerando os relatórios mencionados nesta secção;
  2. dependendo do tipo de assinatura da submissão original, o serviço cria uma assinatura avançada utilizando o respectivo tipo, *XadES*, *CadES* ou *PadES*, com o nível *LTA*;
  3. o serviço faz uso de um *ASiC LTA* para vincular os objetos dos pontos anteriores, juntamente com um ficheiro onde expõe as políticas usadas, com uma assinatura eletrónica avançada (*XadES LTA*), criando um contentor baseado em *ZIP*. Este *ASiC LTA* é constituído por um directório de raiz que contém todo o conteúdo do contentor, ou seja, os objetos mencionados anteriormente. E contém também um diretório *"META-INF"*, dentro do diretório raiz, que engloba ficheiros com metadados sobre o seu conteúdo, o que inclui os ficheiros de assinatura e/ou de selos temporais associados;
  4. este *ASiC LTA* resultante é a evidência de preservação criada pela Prova de Conceito.

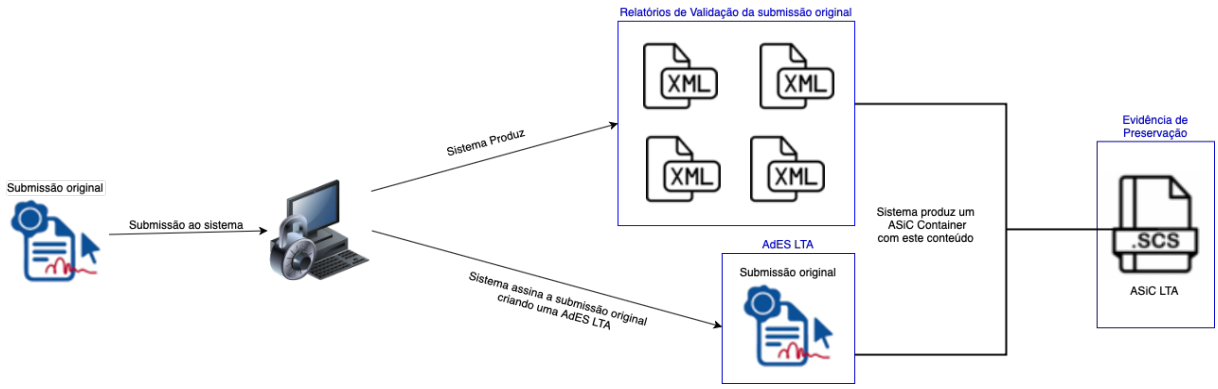



Figura 24: Criação das evidências de Preservação

Fica, assim, cumprido o requisito [R14], da secção 3.2.

Para mais informações sobre a criação destes contentores, consultar `https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#_asic_signature_containers`.

- **Extensão das Evidências de Preservação**

  Os níveis *-T/-LT/-LTA*, mencionados na secção 2.6.2, acrescentam propriedades à assinatura. Isto significa que as propriedades destes níveis poderiam ser adicionadas posteriormente a qualquer assinatura *AdES*. Esta adição ajuda a tornar a assinatura mais resistente a ataques criptográficos durante um período de tempo mais longo. A extensão da assinatura é incremental, ou seja, quando se pretende estender a assinatura ao nível *-LTA*, o nível inferior *(-LT)* também será adicionado.

  Contudo, não é esta extensão incremental que a Prova de Conceito necessita, visto que todas as evidências criadas já se encontram no último nível *(LTA)*.

  Uma assinatura *AdES -LTA* pode ser estendida com mais um nível *-LTA*. Ao fazer isto, os seguintes passos serão realizados:

  – Um novo nível *-LT* será acrescentado à assinatura, com material de validação adicional necessário para a validação do último *Archive TimeStamp* incorporado (nível *-LTA* anterior);

  – Um novo nível *-LTA* será acrescentado com um novo *Archive TimeStamp*.

  A figura seguinte representa o comportamento descrito.

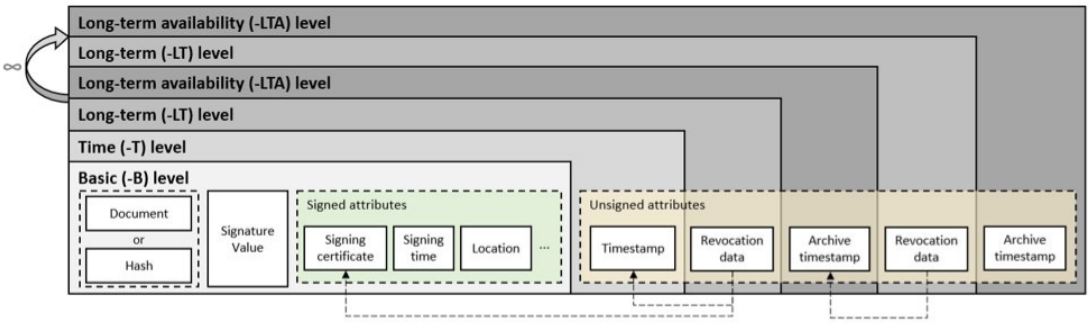



Figura 25: Processo de extensão (Fonte:https://ec.europa.eu/cefdigital/tracker/browse/DSS-2289)

Em geral, pode ser necessário um novo nível *-LTA*, no caso do último certificado de selo temporal expirar em breve, a fim de prolongar a validade da assinatura. Este processo de extensão pode ser realizado inúmeras vezes.

No âmbito desta Prova de Conceito, foi implementada a classe *ServiceContainerExtension.java* que, faz uso das ferramentas de extensão do DSS, é usada para a extensão de todas as evidências armazenadas no serviço de arquivo ou apenas uma específica.

Por último, e com o intuito de realizar testes ao sistema da Prova de Conceito, foi desenvolvida a classe *GenSignatureToPreserve.java* capaz da criação de assinaturas avançadas *-LTA* nos formatos *XadES*, *CadES* e *PadES*.

## 3.6 TECNOLOGIAS USADAS

As principais tecnologias presentes na concretização da Prova de Conceito estão destacadas nos seguintes pontos:

- **Java**

  Como foi visto na secção 2.2.6, a API disponibilizada pelo DSS está desenvolvida em Java.

  Posto isto, todo o *backend* desta Prova de Conceito foi desenvolvido recorrendo à linguagem de programação Java. Incluindo as classes referentes ao serviço de validação e ao serviço de criação de assinaturas eletrónicas.

- **Java Swing**

  De modo a elaborar uma interface de fácil utilização e intuitiva para o utilizador, foi usado *Java Swing*, que se trata de um *widget toolkit* para o Java. Esta interface de utilização pode ser observada nos apêndices.

- **MongoDB**

  Para armazenar a estrutura, mencionada na *comunicação entre o Sistema de Preservação e o serviço de arquivo* presente na secção 3.5, é utilizado uma base de dados não relacional, o Mongodb.

- **Maven**

  Para facilitar o uso do projeto DSS assim como de outras ferramentas, foi usada a ferramenta de automação de compilação Maven.

## 3.7 Funcionalidades do Sistema de Preservação

Como foi exposto na secção 2.3, duas abordagens são reconhecidas de maneira a assegurar a preservação de assinaturas eletrónicas qualificadas. A primeira, resume-se a uma abordagem sistemática baseada na proteção, em termos de integridade do sistema de arquivo eletrónico onde as assinaturas serão preservadas. Pelo contrário, a segunda é uma abordagem específica baseada na proteção em termos de integridade, de forma unitária, de cada assinatura que seja objeto de preservação, através da extensão regular da assinatura ou da recolha regular dos dados de validação da mesma.

O sistema da Prova de Conceito é um sistema híbrido constituído pela combinação de um serviço de preservação com um serviço de arquivo e, a abordagem escolhida para o seu funcionamento engloba as duas abordagens referidas anteriormente. A primeira que vai de encontro com normas para o serviço de arquivo, como o modelo referência OAIS, e a segunda abordagem que vai de encontro com normas ETSI. Com a abordagem escolhida, a preservação de assinaturas electrónicas qualificadas significa:

1. a recolha de todos os dados de validação necessários para validar a assinatura ou o selo;

2. validar a assinatura e o selo, recorrendo, ou não, a serviços de confiança qualificados de validação externos;

3. recolher as evidências usadas na validação, e protegê-las em conjunto com a assinatura ou o selo, usando provas de existência, como por exemplo, selos temporais qualificados, de maneira a que seja possível provar o estado de validade de uma assinatura ou de um selo no momento em que a prova foi criada. Estas provas são denominadas por evidências de preservação;

4. como armazenamento, para as evidências de preservação resultantes da escolha do perfil de preservação com armazenamento, é usado um serviço de arquivo e é feita uma constante monitorização.

Ficou então decidido que o *workflow* desta prova de conceito seria o seguinte:

1. o serviço de preservação recebe o documento que contém a assinatura ou selo para preservar (Figura 22 Interface de Preservação);
2. o serviço de preservação procede à validação da mesma usando o bloco de validação do DSS abordado na secção 3.5, reunindo provas da validação (Figura 22 Serviço de Validação);
3. o serviço de preservação procede à criação das evidências de preservação, como exposto na secção 3.5 (Figura 22 Serviço de Criação de Assinaturas Eletrónicas);
4. dependendo do modelo de armazenamento escolhido pelo utilizador, o serviço de preservação ou armazena (Figura 22 Serviço de Arquivo) ou devolve (Figura 22 Interface de Preservação) as evidências de preservação;
5. o serviço de preservação tem que permitir ao utilizador que escolheu o modelo com armazenamento a realização das operações mencionadas na secção 3.3 (Figura 22 Interface de Preservação);
6. o serviço de preservação tem que realizar um constante trabalho de monitorização das evidências de preservação armazenadas, caso seja necessária a sua extensão (Figura 22 Interface de Administração).

Todas as ações que ocorrem nesta Prova de Conceito, quer sejam realizadas por parte do utilizador, quer sejam operações internas no sistema, são registadas e controladas pelo serviço de preservação num ficheiro de *log*, cumprido com o requisito [R4], exposto na secção 3.2.

Um excerto do ficheiro de *log* desta prova de conceito pode ser observado no apêndice J.

### 3.7.1 *Modelo de Casos de Uso*

O Modelo de Caso de uso serve para agrupar as funções que o sistema deve ter, especificadas entre o utilizador e o serviço de preservação.

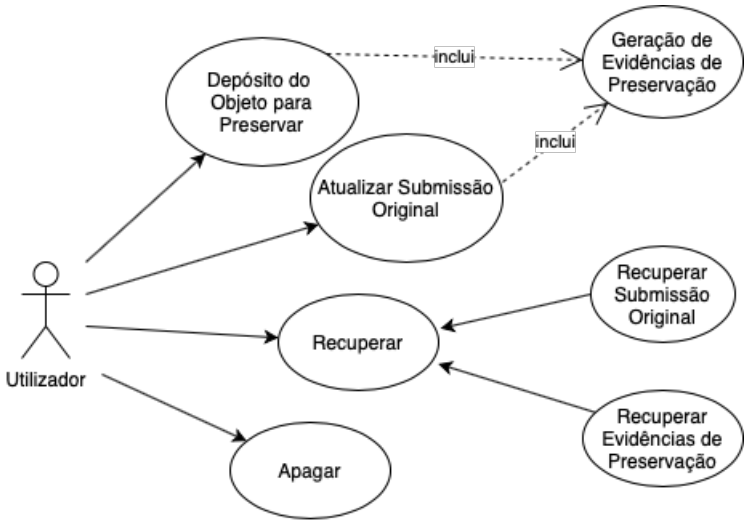



Figura 26: Caso de Uso Utilizador

No que diz respeito aos casos de uso, pode-se distinguir entre o serviço de preservação com e sem armazenamento.

Os casos de uso do serviço de preservação com armazenamento incluem as seguintes funções para os Utilizadores do Serviço de Preservação:

- Depósito (do Objeto para Preservar);
- Atualizar (a Submissão Original);
- Recuperar (a Submissão Original ou as Evidências de Preservação);
- Apagar (tudo submetido e criado pelo Serviço de Preservação);

Estas operações são recebidas pelo sistema da Prova de Conceito (Figura 21 Interface de Preservação) e aplicadas ao serviço de arquivo (Figura 21 Serviço de Arquivo).

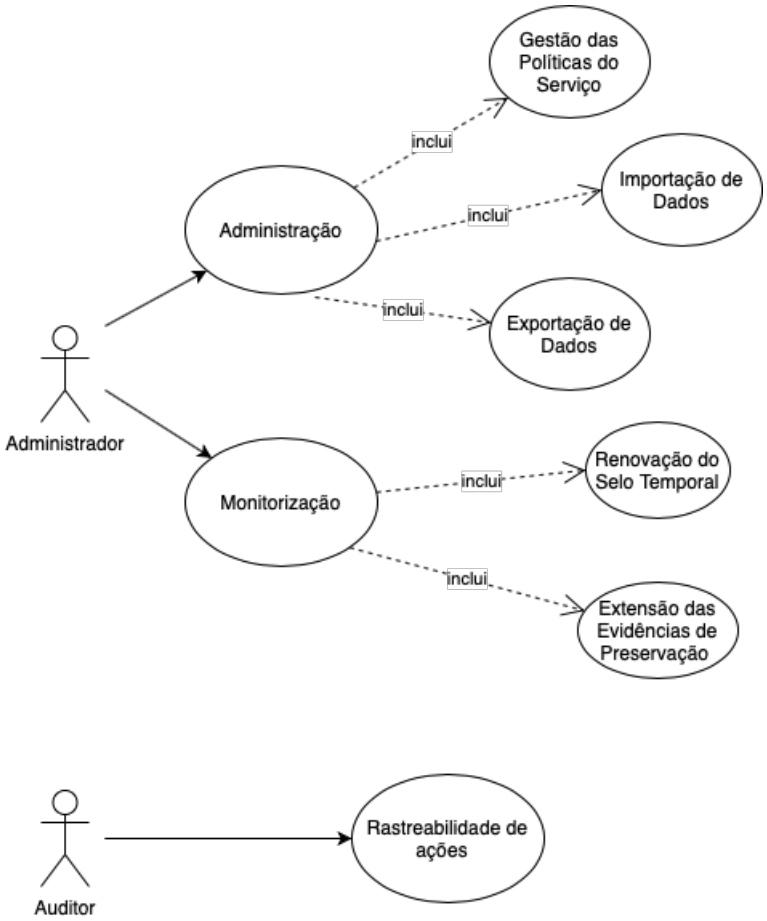



Figura 27: Caso de Uso Administrador e Auditor

O Administrador pode aceder à funcionalidade de Administração, que inclui em particular a gestão das políticas de preservação aplicáveis para um utilizador específico e a funcionalidade de exportar e importar o conjunto completo de dados internos, disponibilizados pelo serviço de arquivo. Podem ser encontrados alguns exemplos no apêndice C.

Além disso, o Administrador tem acesso à função de Monitorização interna, que supervisiona a adequação dos algoritmos criptográficos implementados, o que pode levar à extensão das evidências de preservação.

Por último, se necessário, um Auditor é capaz de recuperar registos auditáveis, como por exemplo ficheitos de log, o que permite provar a conformidade do funcionamento do Serviço de Preservação no que diz respeito a requisitos políticos específicos.

### 3.7.2 *Casos de Uso*

Esta secção captura o modelo das funções implementadas no sistema e do seu ambiente.

No sistema desta Prova de Conceito são destingidos 3 atores diferentes, o Utilizador, o Administrador e um possível Auditor.

- **UC.1 Nome do caso de uso: Preservação sem Armazenamento**

  1. Breve descrição

     Este caso de uso descreve como um Utilizador faz uso do serviço escolhendo o perfil de preservação sem armazenamento, que cumpre com o requisito [R12] indicado na secção 3.2. Na secção 3.1 são abordados aspetos sobre perfis de armazenamento oferecidos pela Prova de Conceito.

     Este caso de uso está ilustrado no apêndice D.

  2. Atores
     - Utilizador
  3. Pré-condições
     - A assinatura ou selo presente no documento submetido ao sistema deve ser de um destes formatos: *XadES, PadES, CadES*.
  4. Pós-condições
     - O Utilizador recebe a evidência de preservação assim como dados de validação da mesma e da submissão original, mencionados na secção 3.5.
  5. Fluxo de eventos

     a) O caso de uso inicia quando o Utilizador abre a aplicação acedendo à *Interface de Preservação*.

     b) O Utilizador solicita a preservação pressionando o botão "ESig and ESeal Long-Term Preservation" (*cf.* Figura 41 do apêndice D).

     c) O Utilizador escolhe o modelo de armazenamento pressionando o botão "Without Storage" (*cf.* Figura 42 do apêndice D).

     d) O Utilizador faz o *upload* do documento que contem a assinatura para o sistema da Prova de Conceito (*cf.* Figura 44 do apêndice D).

     e) O Sistema da Prova de Conceito valida o formato da assinatura confirmando o sucesso do *upload* (*cf.* Figura 45 do apêndice D).

     f) O Sistema da Prova de Conceito começa o processo de criação das evidências de preservação, tal como descrito na secção 3.5.

     g) O Sistema da Prova de Conceito devolve ao utilizador uma estimativa da duração expectável da evidência de preservação (*cf.* Figura 47 do apêndice D).

h) O Sistema da Prova de Conceito devolve ao Utilizador as evidências geradas assim como algum material de validação relativo à submissão original e às evidências criadas. Sendo as evidências de preservação os contentores *ASiC* e o material de validação os relatórios mencionados na secção 3.5 (*cf.* Figura 48 do apêndice D).

i) O Sistema da Prova de Conceito devolve ao Utilizador um ficheiro que representa o perfil de preservação por si escolhido (*cf.* apêndice K).

j) O Sistema da Prova de Conceito regista no ficheiro de *log* a ação de preservação sem armazenamento e o nome submissão original.

- **UC.2 Nome do caso de uso: Preservação com Armazenamento**

  1. Breve descrição

     Este caso de uso descreve como um Utilizador faz uso do serviço escolhendo o perfil de preservação com armazenamento.

     Este caso de uso está ilustrado no apêndice B.

  2. Atores
     - Utilizador.
  3. Pré-condições
     - A assinatura ou selo presente no documento submetido ao sistema deve ser de um destes formatos: *XadES, PadES, CadES*.
  4. Pós-condições
     - O Utilizador recebe um identificador único referente à evidência de preservação criada. Este identificador é de total responsabilidade do Utilizador. Sem ele não poderão ser efetuadas nenhumas operações subsequentes (*cf.* casos de uso 3, 4 e 5).
  5. Fluxo de eventos

     a) O caso de uso inicia quando o Utilizador abre a aplicação acedendo à *Interface de Preservação*.

     b) O Utilizador solicita a preservação pressionando o botão "ESig and ESeal Long-Term Preservation" (*cf.* Figura 30 do apêndice B).

     c) O Utilizador escolhe o modelo de armazenamento pressionando o botão "With Storage" (*cf.* Figura 31 do apêndice B).

     d) O Utilizador faz o *upload* do documento que contem a assinatura para o sistema da Prova de Conceito (*cf.* Figura 33 do apêndice B).

e) O Sistema da Prova de Conceito valida o formato da assinatura confirmando o sucesso do *upload* (*cf.* Figura 34 do apêndice B).

f) O Sistema da Prova de Conceito começa o processo de criação das evidências de preservação, tal como descrito na secção 3.5.

g) O Sistema da Prova de Conceito envia a evidência para o serviço de arquivo, recebendo um AIP-ID, tal como mencionado nas secções 2.6.3 e 3.5.

h) Como abordado na secção 3.5, o Sistema gera um identificador único e associa-o ao AIP-ID gerado pelo serviço de arquivo.

i) O Sistema da Prova de Conceito atualiza a base de dados com esses identificadores associados.

j) O Sistema da Prova de Conceito devolve ao Utilizador o identificador único por si gerado, como explicado na secção 3.5 (*cf.* Figura 35 do apêndice B).

k) O Sistema regista no ficheiro de *log* a ação de preservação sem armazenamento e o identificador único atribuído ao utilizador.

- **UC.3 Nome do caso de uso: Operação de Recuperar**

1. Breve descrição

   Este caso de uso descreve como um Utilizador recupera as evidências de preservação associadas ao seu identificador assim como a submissão original e outros objetos como material de validação, em conformidade com o requisito [R8] indicado na secção 3.2. Esta operação apenas pode ser efetuada dentro do perfil de preservação com armazenamento.

   Este caso de uso está ilustrado no apêndice F.

2. Atores
   - Utilizador.
3. Pré-condições
   - O identificador único, recebido aquando do caso de uso 2, submetido pelo Utilizador tem que ser válido.
4. Pós-condições
   - O Utilizador recebe a evidência de preservação e a submissão original assim como dados de validação das mesmas, mencionados na secção 3.5.
5. Fluxo de eventos

a) O caso de uso inicia quando o Utilizador abre a aplicação acedendo à *Interface de Preservação*.

b) O Utilizador dirige-se para a área de gestão pressionando o botão "Manage" (*cf.* Figura 50 do apêndice F).

c) O Utilizador escolhe a ação desejada pressionando o botão "Get Preservation Evidence and Others" (cf. Figura 51 do apêndice F).

d) O Utilizador insere e submete o identificador único (*cf.* Figura 52 do apêndice F).

e) O Sistema da Prova de Conceito confirma a validade do identificador.

f) O Sistema da Prova de Conceito vai à sua base de dados buscar o AIP-ID mais recente associado ao identificador recebido, como mencionado na secção 3.5.

g) O Sistema da Prova de Conceito extrai da componente de sistema de arquivo as evidências associadas ao AIP-ID.

h) O Sistema da Prova de Conceito devolve ao Utilizador as evidências de preservação e a submissão original assim como algum material de validação relativo às mesmas. Sendo as evidências de preservação os contentores *ASiC* e o material de validação os relatórios mencionados na secção 3.5 (*cf.* Figura 53 do apêndice F).

i) O Sistema da Prova de Conceito regista no ficheiro de *log* o identificador único que realizou a ação de recuperar.

- **UC.4 Nome do caso de uso: Operação de Atualizar a Submissão Original**

1. Breve descrição

   Este caso de uso descreve como um Utilizador consegue substituir a submissão original ao Sistema da Prova de Conceito, em conformidade com o requisito [R11] na secção 3.2. Esta operação apenas pode ser efetuada dentro do perfil de preservação com armazenamento.

   Este caso de uso está ilustrado no apêndice G.

2. Atores
   - Utilizador.

3. Pré-condições

   a) O identificador único, recebido aquando do caso de uso 2, submetido pelo Utilizador tem que ser válido.

b) A assinatura ou selo presente no novo documento submetido ao sistema deve ser de um destes formatos: *XadES, PadES, CadES*. (Não necessita de ser do mesmo formato da submissão original)

4. Pós-condições
   a) O Utilizador recebe um aviso a informar o sucesso da operação.
   b) Todas as evidências de preservação associadas àquele identificador são guardadas.
5. Fluxo de eventos
   a) O caso de uso inicia quando o Utilizador abre a aplicação acedendo à *Interface de Preservação*.
   b) O Utilizador dirige-se para a área de gestão pressionando o botão "Manage" (*cf.* Figura 55 do apêndice G).
   c) O Utilizador escolhe a ação desejada pressionando o botão "Update Original Submission" (*cf.* Figura 56 do apêndice G).
   d) O Utilizador insere e submete o identificador único (*cf.* Figura 57 do apêndice G).
   e) O Sistema da Prova de Conceito confirma a validade do identificador.
   f) O Utilizador faz o *upload* do novo documento que contem a nova assinatura para o sistema da Prova de Conceito (*cf.* Figura 57 do apêndice G).
   g) O Sistema da Prova de Conceito valida o formato da assinatura confirmando o sucesso do *upload* (*cf.* Figura 58 do apêndice G).
   h) O Sistema da Prova de Conceito começa o processo de criação das evidências de preservação, tal como descrito na secção 3.5.
   i) O Sistema da Prova de Conceito envia a evidência de preservação para a componente de serviço de arquivo, recebendo um AIP-ID, tal como mencionado na secção 3.5.
   j) O Sistema da Prova de Conceito atualiza a base de dados associando ao identificador do Utilizador este AIP-ID recebido, como versão mais recente.
   k) O Sistema da Prova de conceito guarda todas as evidências de preservação antigas.
   l) O Utilizador quando realizar uma operação de recuperar evidências (*cf.* caso de uso 3), irá receber informação relativa à submissão mais recente.
   m) O Utilizador quando realizar uma operação de apagar (*cf.* caso de uso 5), todas as evidências de preservação, relacionadas com o identificador único do utilizador, são removidas do Sistema da Prova de Conceito.

n) O Sistema da Prova de Conceito regista no ficheiro de *log* a ação realizada e o nome da nova submissão.

- **UC.5 Nome do caso de uso: Operação de Remoção**

1. Breve descrição

   Este caso de uso descreve como um Utilizador consegue apagar todas as evidências de preservação associadas ao identificador único a ele atribuído. Esta operação apenas pode ser efetuada dentro do perfil de preservação com armazenamento.

   Este caso de uso está ilustrado no apêndice H.

2. Atores
   - Utilizador.
3. Pré-condições
   a) O identificador único, recebido aquando o acontecimento do caso de uso 2, submetido pelo Utilizador tem que ser válido.
   b) O Utilizador tem que fornecer uma justificação.
4. Pós-condições
   a) O Utilizador recebe um aviso a informar o sucesso da operação.
   b) Todas as evidências associadas ao identificador são apagadas.
5. Fluxo de eventos
   a) O caso de uso inicia quando o Utilizador abre a aplicação acedendo à *Interface de Preservação*.
   b) O Utilizador dirige-se para a área de gestão pressionando o botão "Manage" (*cf.* Figura 61 do apêndice H).
   c) O Utilizador escolhe a ação desejada pressionando o botão "Delete Preservation Evidence and Others" (*cf.* Figura 62 do apêndice H).
   d) O Utilizador insere e submete o identificador único com a justificação (*cf.* Figura 63 do apêndice H).
   e) O Sistema da Prova de Conceito confirma a validade do identificador.
   f) O Sistema da Prova de Conceito vai à sua base de dados e, para todos os AIP-IDs associados ao identificador recebido, apaga as evidências de preservação presentes na componente de serviço de arquivo assim como qualquer dado a elas associado.

g) O Sistema da Prova de Conceito apaga todas as entradas na sua base de dados com aquele identificador.

h) O Sistema da Prova de Conceito regista no ficheiro de *log* a ação realizada, a justificação e o identificador único do utilizador.

- **UC.6 Nome do caso de uso: Administração**

1. Breve descrição

   Este caso de uso descreve como um Administrador faz a gestão do seu sistema e está ilustrado no apêndice C.

2. Atores

   – Administrador.

3. Pré-condições

   – Acesso a um *browser*.

4. Fluxo de eventos

   a) O caso de uso inicia quando o Administrador abre o *browser* e se dirige ao endereço, onde instalou a componente de serviço de arquivo, na porta *8080*, acedendo à *Interface de Administração*.

   b) O Administrador faz o *login* com as credenciais *admin roda*.

   c) O Administrador tem acesso a uma catálogo com todas as evidências de preservação submetidas à componente de serviço de arquivo

   d) O Administrador tem acesso a informação complementar, como os metadados abordados na secção 3.5 (serviço de arquivo), fornecida pela componente de serviço de arquivo para cada uma das evidências de preservação (*cf.* Figura 38 do apêndice C).

   e) O Administrador tem acesso a funções manuais de remoção e submissão para a componente de serviço de arquivo.

- **UC.7 Nome do caso de uso: Monitorização**

1. Breve descrição

   Este caso de uso descreve como um Administrador faz a monitorização de aspetos relevantes para o sistema.

2. Atores

- Administrador.

3. Fluxo de eventos

   a) O Administrador monitoriza a força dos algoritmos criptográficos usados pelo bloco de criação de assinaturas do projeto DSS, assim como os parâmetros de segurança como tamanho de chaves. Com base no documento referido no requisito [R6] da secção 3.2;

   b) O Administrador monitoriza o estado de validade dos certificados usados, quer para a criação das evidências de preservação, quer para a emissão de selos temporais, recorrendo ao bloco de validação do projeto DSS.

   c) Sendo necessário, o Administrador aplica o mecanismo de extensão, mencionado na secção 3.5, a uma ou mais evidências.

# 4

# CONCLUSÃO

Este capítulo apresenta as conclusões que podem ser extraídas deste trabalho, as principais contribuições que proporciona ao campo da preservação e uma descrição do trabalho futuro.

No decorrer da elaboração desta tese começou a pandemia que marcou o ano de *2020*. Trata-se de mais um fator que leva à necessidade da transformação acelerada para uma economia cada vez mais digital e com cada vez menos interação face-a-face.

Com o aumento do uso de documentos eletrónicos na desmaterialização de processos, na preservação do património documental e na digitalização da economia, o uso de assinaturas eletrónicas qualificadas é cada vez mais comum para as garantias de integridade e de não-repúdio. O crescimento do uso de assinaturas eletrónicas qualificadas é sustentado pelo número de serviços qualificados de emissão de certificados qualificados de assinaturas e selos eletrónicos (*cf.* Figura 28).


Figura 28: Serviços de Confiança Qualificados (Fonte: https://webgate.ec.europa.eu/tl-browser/#/)

Como se pode ver na figura 28, o serviço qualificado de validação e o serviço qualificado de preservação são os serviços de confiança com menos entidades em produção. *Mas porque será?* Será que tem a ver com o modelo de negócios? Será que tem a ver com os requisitos altamente técnicos? Ou será que tem a ver com dificuldades na utilização de um serviço qualificado de preservação face aos sistemas OAIS? Na minha opinião nenhuma destas razões é o motivo principal. A justificação que eu encontro assenta na **necessidade**. Isto é, o facto das assinaturas eletrónicas qualificadas estarem a começar a ser usadas em massa vai levar ao crescimento inevitável do uso dos serviços de validação e de preservação. Até porque o serviço qualificado de validação é essencial para testar a validade de uma assinatura eletrónica qualificada e o serviço qualificado de preservação de assinaturas e selos qualificados terá grande impacto no futuro, visto que um dos objetivos deste serviço de confiança é manter o estado de validade da assinatura de um documento ao longo do tempo.

A realização deste trabalho levou-me à conclusão de que a importância da preservação no mundo digital é cada vez mais crescente, visto que os serviços de arquivo eletrónico apenas se focam na integridade do documento eletrónico e não tomam em linha de conta aspetos que influenciam o estado de validade de uma assinatura eletrónica usada nos documentos eletrónicos arquivados (*e.g.* revogação de certificados). Garantir a integridade de um documento, mas não garantir simultaneamente o seu não-repúdio, pode levar a disputas jurídicas no longo prazo, sendo que o serviço de preservação qualificado foca simultâneamente a integridade e o não-repúdio.

Segundo o documento eIDAS: Overview on the implementation and uptake of Trust Services, um dos principais fatores que travam a aceitação e o crescimento dos serviços de preservação qualificados é a forte necessidade da preservação de documentos electrónicos a longo prazo em sistemas de preservação digital em conformidade com o modelo OAIS.

É exactamente nesse âmbito que decorre o trabalho desta tese, e se distingue de outros serviços de preservação eletrónica, apresentando uma possível solução para um sistema "híbrido" constituído por um serviço de preservação que engloba um serviço de arquivo que está em conformidade com o modelo de referência OAIS. Este sistema não só toma em conta a integridade do documento eletrónico como também garante o seu não-repúdio.

Como foi abordado ao longo desta dissertação, o sistema do serviço de preservação desta tese não passa de uma Prova de Conceito, ficando entendido que muitos dos requisitos gerais estavam fora do seu âmbito. Tem, portanto, requisitos que devem ser tomados em linha de conta e componentes que necessitam de ser alterados para que esta Prova de Conceito possa ser transformada num serviço de confiança qualificado em produção.

Tal como foi mencionado na secção 2.2.1, os prestadores de serviços de confiança, que queiram obter o estatuto de qualificado, necessitam de passar por uma avaliação por parte de um organismo de avaliação de conformidade. Esse organismo irá determinar e avaliar se

estão em conformidade com os requisitos previstos no Regulamento eIDAS e expostos na secção 2.2.1. Serão também avaliadas as normas e requisitos impostos aos prestadores de serviços de confiança pelo documento ETSI EN 319 401, nomeadamente as constantes dos capítulos 5, 6 e 7, onde são expostos controlos de conformidade para que possam atingir o título de qualificado. O organismo de avaliação de conformidade produzirá um relatório de avaliação de conformidade, indicando se os requisitos foram cumpridos e é entregue à entidade supervisora do Estado Membro onde o serviço se encontra.

Falando agora, em específico, dos serviços de preservação qualificados, requisitos aplicáveis presentes no documento ETSI TS 119 511 também serão alvo de avaliação. Na secção 3.2 pode ser observado a conformidade da Prova de Conceito com alguns dos requisitos deste documento.

Relativamente às componentes que constituem o sistema da Prova de Conceito, algumas delas não estão em conformidade com as normas aplicáveis, sendo, portanto, necessária a sua alteração.

Um dos aspetos a ser alterado é a utilização de um tipo de certificado de chaves diferente para a criação das evidências de preservação, isto é, atualmente o sistema da Prova de Conceito faz uso de um certificado não qualificado, podendo ser feito o uso de um certificado qualificado providenciado por um serviço de confiança qualificado presente na lista de confiança da União Europeia.

Outro aspeto a ser alterado é a localização da chave privada e dos certificados associados, fazendo uso de um dispositivo de criação de assinaturas qualificado.

Não esquecendo que a utilização de um serviço de confiança qualificado de validação de assinaturas e selos eletrónicos como componente de serviço de validação é aconselhado pelas normas, criando outro ponto a ser alterado.

Parte III

# APÊNDICES

# A

# PROVA DE CONCEITO: DOCUMENTAÇÃO DE UTILIZAÇÃO

Esta secção consiste num manual de instruções, permitindo que o utilizador tenha um acesso facilitado a todas as informações necessárias para o uso da Prova de Conceito, aumentando assim as probabilidades de existir um uso correto da mesma.

### A.0.1 *Pré Requisitos de Instalação e de Utilização*

- Java 13 ou superior;
- Maven 3.6 ou superior;
- MongoDB instalado e a correr;
- RODA instalado numa máquina à escolha e a correr.

  Para a instalação e *deployment* do ambiente de teste do repositório digital RODA, consultar `https://github.com/eark-project/roda/blob/master/documentation/Installation_Testing_Environments.md`.

### A.0.2 *Onde Encontrar e Instalação*

Esta Prova de Conceito está disponível para clonagem no repositório `https://github.com/fernandesjm/PreservationServiceProofOfConcept`.

O próximo passo não é para ter em consideração caso a instalação do serviço de arquivo RODA tenha sido feita na mesma máquina onde foi feito o clone do repositório.

Após a clonagem do repositório e da instalação do RODA, aceda à diretoria `Preservation-Service/src/main/java/com/devisefutures/projeto/` para fazer uma alteração no ficheiro *Roda.java*, responsável pela comunicação com o repositório RODA.

```
public class Roda{
    // Username and password credentials
    byte[] credentials = Base64.encodeBase64(("admin" + ":" + "roda").getBytes(StandardCharsets.UTF_8));
    // Base Url
    String baseUrl = "http://localhost:8080/api/v1/";
```

Figura 29: URL Base do repositório

Na *String baseUrl*, onde se encontra *localhost*, como exposto na Figura 29, deve ser substituído pelo endereço onde o repositório RODA se encontra instalado. Caso esteja instalado na mesma máquina que o resto do sistema da Prova de Conceito, "*localhost*"deverá ser utilizado.

Em seguida deve ser feita a execução dos seguintes comandos onde se encontra o clone do repositório:

- apagar todos os ficheiros e recursos anteriormente compilados no projeto.

```
mvn clean -f PreservationServiceProofOfConcept/projeto/pom.xml; mvn clean -f
    PreservationServiceProofOfConcept/projeto/Preservation-Service/pom.xml
```

- compilar e testar o projeto, e criar um ficheiro executável *.jar*.

```
mvn install -f PreservationServiceProofOfConcept/projeto/pom.xml; mvn install -f
    PreservationServiceProofOfConcept/projeto/Preservation-Service/pom.xml
```

### A.0.3 *Modo de Utilização*

Uma vez que os pré requisitos sejam cumpridos e a instalação esteja feita, o seguinte comando deve ser executado para o *deploy* da Interface de Preservação:

```
java -jar PreservationServiceProofOfConcept/projeto/Preservation-Service/target/df-Preservation
    -Service-1.0-SNAPSHOT-jar-with-dependencies.jar
```

- Utilizador (Cliente)

  O Cliente pode fazer uso da Prova de Conceito tal como descrito nos casos de uso 1, 2, 3, 4 e 5 da secção 3.7.2. Após efetuar os casos de uso, pode realizar a validação da evidência de preservação na *webapp* do projeto DSS (em `https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation`).

- Administrador

  O Administrador abre o seu *browser* de eleição e dirige-se ao endereço onde instalou o repositório na porta *8080*, acedendo à *Interface de Administração* (`https://localhost:8080` caso o serviço de arquivo esteja na mesma máquina). Faz o *login* com as credenciais *admin roda*, tal como indicado na secção 3.7.2 no caso de uso nº6.

### A.0.4 *Demo*

Para a realização de uma *demo* desta Prova de Conceito foram pedidos dois certificados para assinatura à *Actalis*, sendo devolvido duas *keystores* tal como abordado na secção 3.5:

- um delas para o Serviço de Preservação usar para criar as evidências, com o certificado em nome de "*presservproofofconcept@gmail.com*";
- a outra *keystore* foi para um *Mock Client*, para a criação de assinaturas teste, para a submissão ao sistema de preservação, com o certificado em nome de "*mock.user.sign@gmail.com*".

Para a criação das evidências de preservação, precisamos ainda de especificar onde a chave privada pode ser encontrada.

Posto isto, como foi mencionado na secção 3.5, foi desenvolvida uma classe em Java *Pkc12.java* que faz a gestão e trata do acesso à *keystore* sempre que for necessário ao serviço da Prova de Conceito.

Nesta Prova de Conceito todos os dados utilizados para a criação de evidências, como chaves e certificados, estão localizados em `Preservation-Service/src/main/resources/keystore`. Diferentes *keystores* podem ser usadas, tendo em conta que no âmbito desta tese apenas foi implementada a gestão e o acesso a *PKCS12 keystores*.

Com o intuito da concretização de testes, foi desenvolvida uma classe Java *GenSignatureToPreserve.java* onde é possível a criação de assinaturas eletrónicas avançadas de todos os formatos (XadES, CadES e PadES), recorrendo à *keystore* do *Mock Client*.

Para a criação destas assinaturas de teste é necessária a execução do seguinte comando:

```
cd PreservationServiceProofOfConcept/projeto/Preservation-Service; mvn exec:java -Dexec.
    mainClass=com.devisefutures.projeto.GenSignatureToPreserve
```

Por defeito, são criadas três assinaturas avançadas, uma *XadES -LTA*, uma *PadES -LTA* e uma *CadES -LTA* em volta de documentos exemplo que se encontram em `Preservation-Service/src/main/resources/toSign`.

#### *Máquina Virtual*

Com o objetivo de facilitar o teste ao serviço de preservação desta Prova de Conceito, foi desenvolvida uma máquina virtual, tendo já instalado todo o sistema envolvente.

Esta máquina virtual, com *123456* como *password* do utilizador *root*, pode ser usada recorrendo ao importador de aplicações do software *VirtualBox*[1]. O ficheiro de virtualização está disponível em `https://vm4.devisefutures.com/`.

Para o correto uso do serviço da Prova de Conceito, os comandos presentes no ficheiro `comands.txt`, localizado no *Desktop* da máquina virtual, devem ser lidos e executados no terminal a partir do *Desktop* da máquina virtual, consoante a necessidade.

No *browser* presente na máquina virtual foram guardados dois *websites*, no qual o primeiro é `https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation`, onde o utilizador pode validar a evidência de preservação criada pelo serviço da Prova de Conceito. O segundo *website* é `https://localhost:8080`, que permite aceder à Interface de Administração do serviço de arquivo do serviço da Prova de Conceito.

1 `https://www.virtualbox.org`

# B

## PROVA DE CONCEITO: PRESERVAÇÃO COM ARMAZENAMENTO

Este apêndice contém os passos essenciais para o uso do perfil de preservação com armazenamento, recorrendo ao serviço de arquivo, o repositório digital RODA, que está apresentado no apêndice C e relaciona-se com o caso de uso 2 exposto na secção 3.7.2.


Figura 30: Interface Inicial do Serviço de Preservação

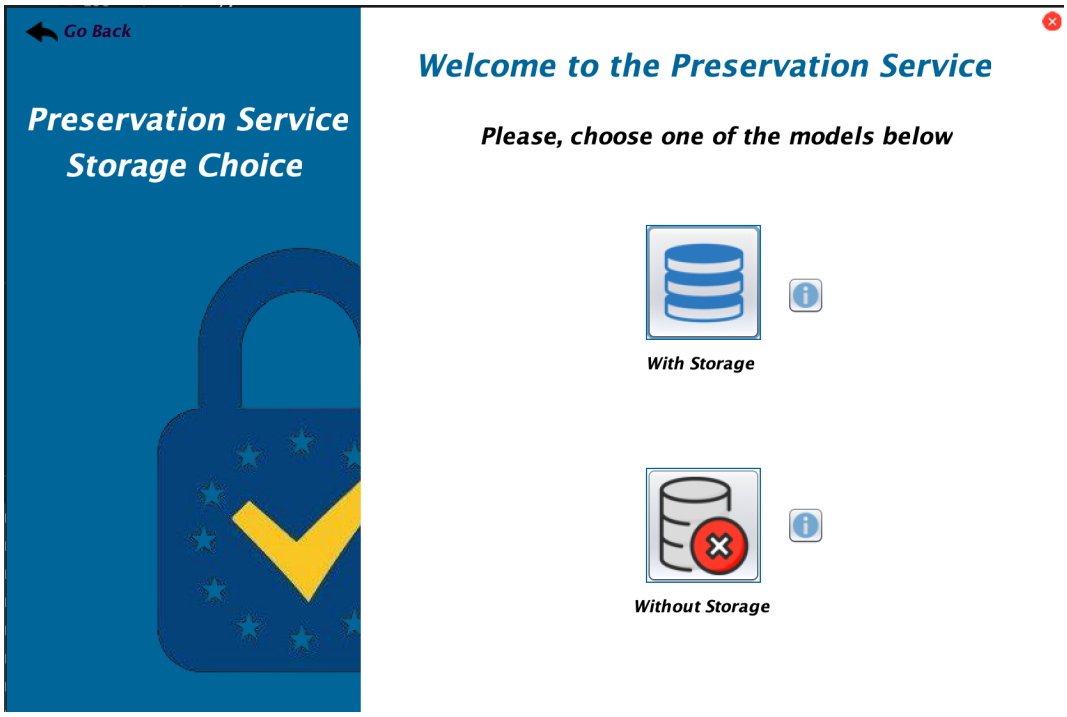



Figura 31: Escolha do modelo de armazenamento

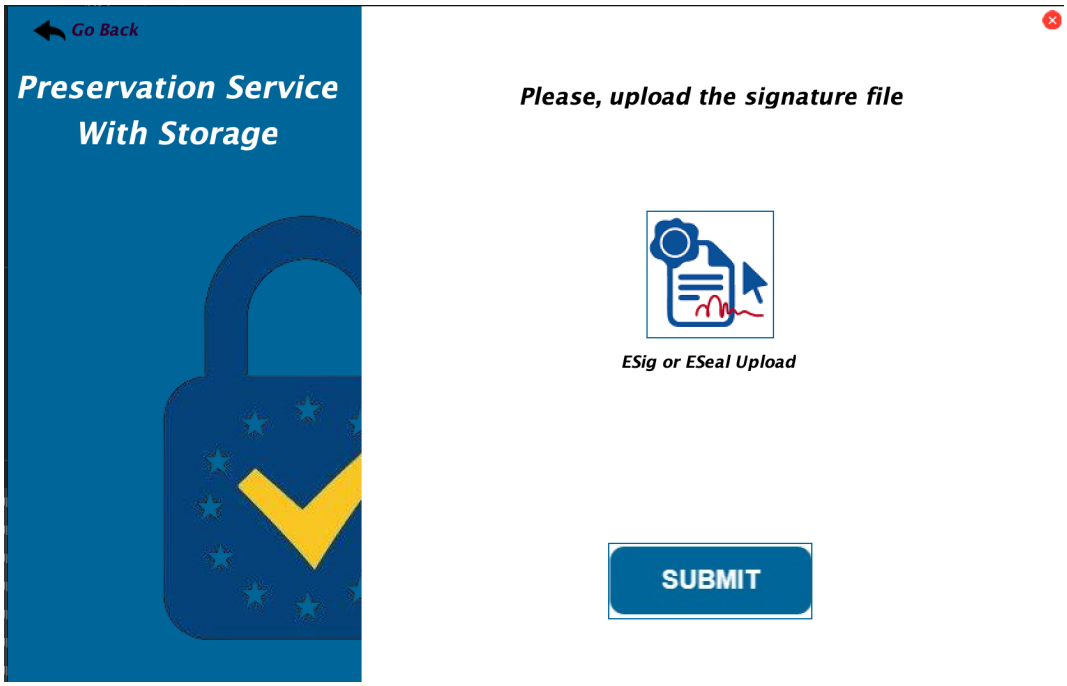



Figura 32: Serviço de Preservação com Armazenamento

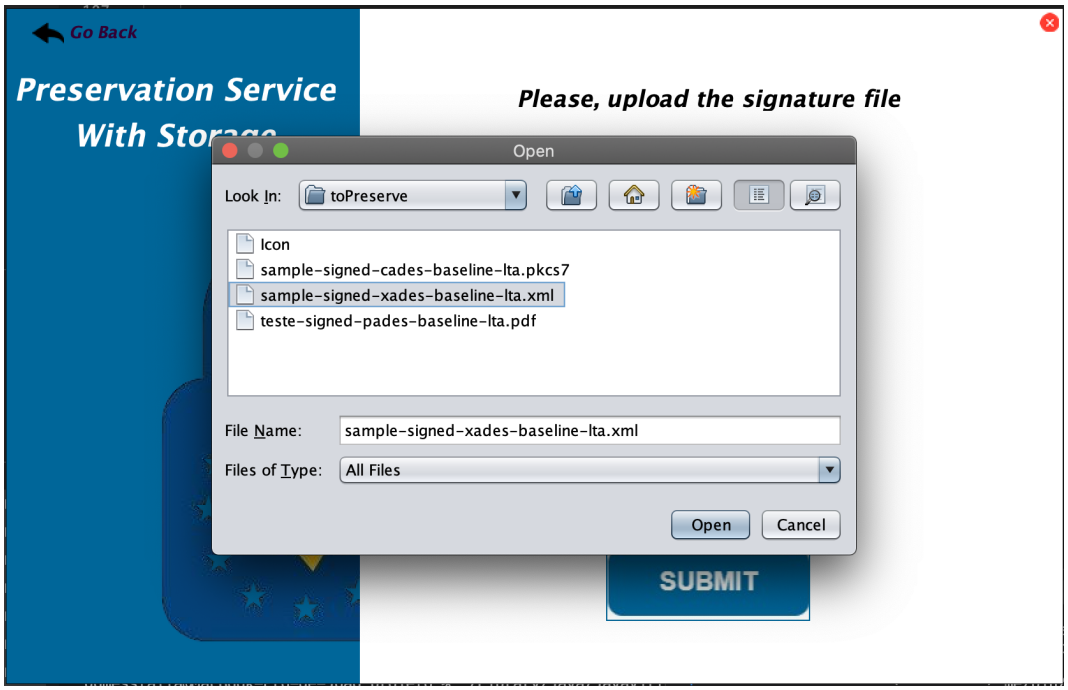



Figura 33: Upload da assinatura para o Serviço de Preservação

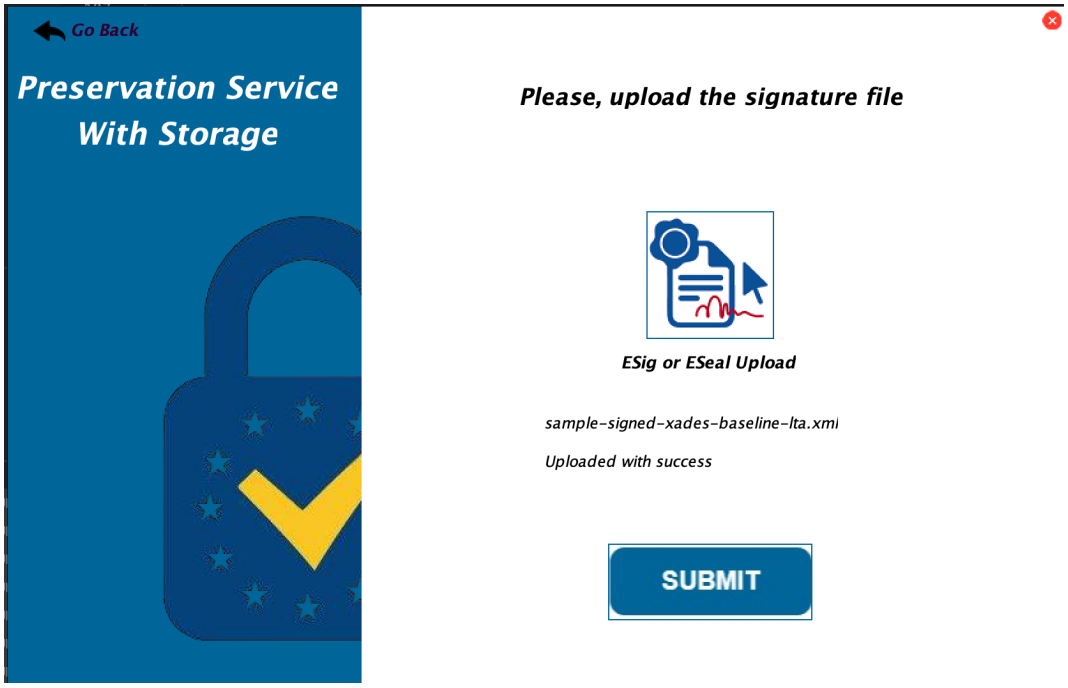



Figura 34: Upload da assinatura realizado com sucesso

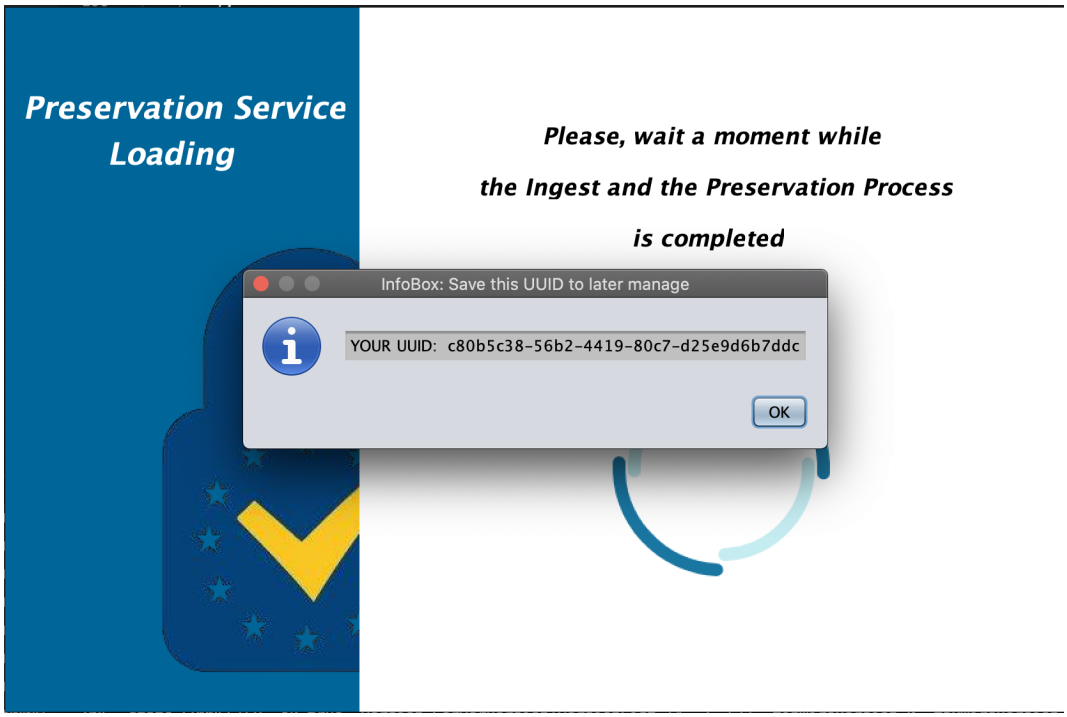



Figura 35: Resposta com o identificador único do utilizador

# C

# PROVA DE CONCEITO: REPOSITÓRIO DIGITAL

Aqui encontra-se o "antes"e o "depois"do repositório digital RODA, após a acção exposta no apêndice B.

Este apêndice relaciona-se com o caso de uso 6 exposto na secção 3.7.2.


Figura 36: RODA: Repositório Digital

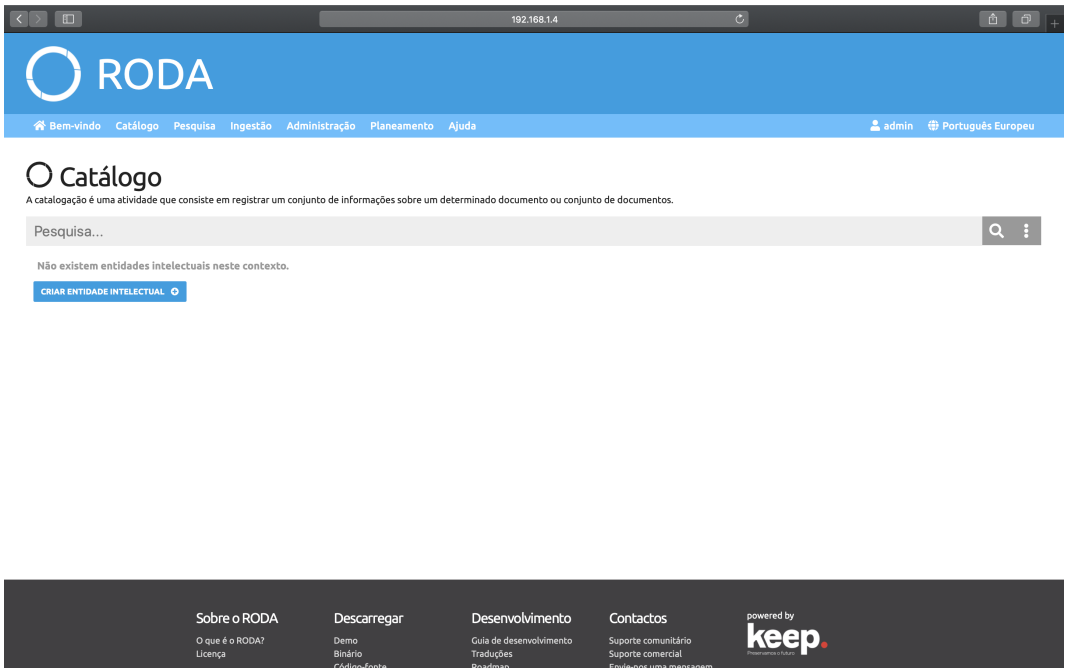



Figura 37: RODA: Repositório Vazio

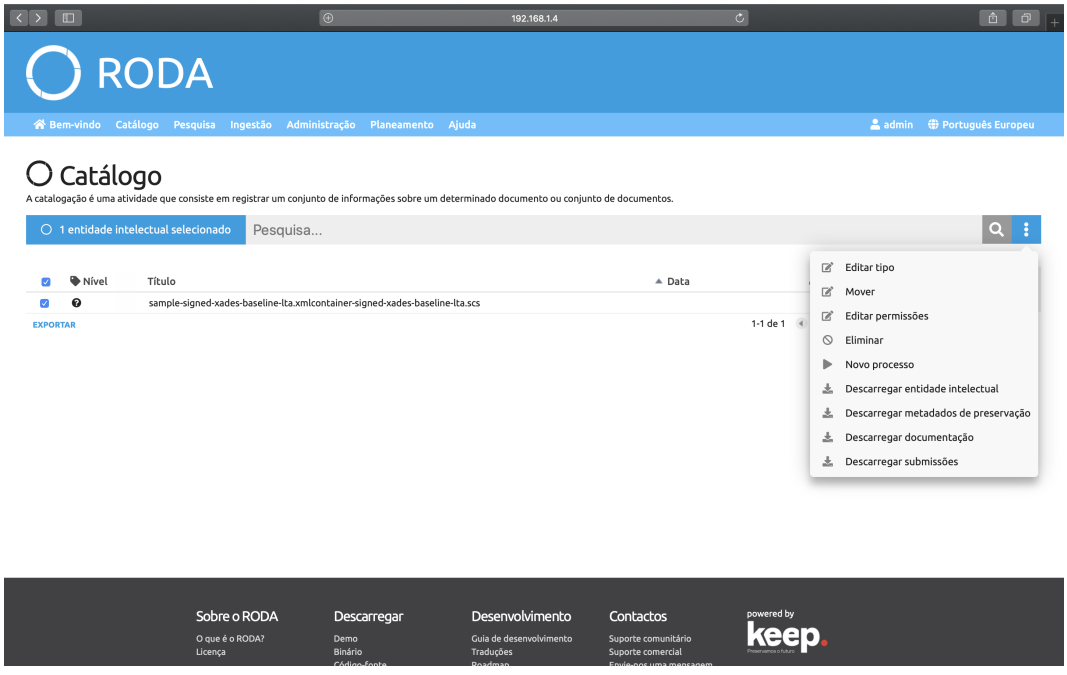



Figura 38: RODA: Repositório com a evidência de preservação criada

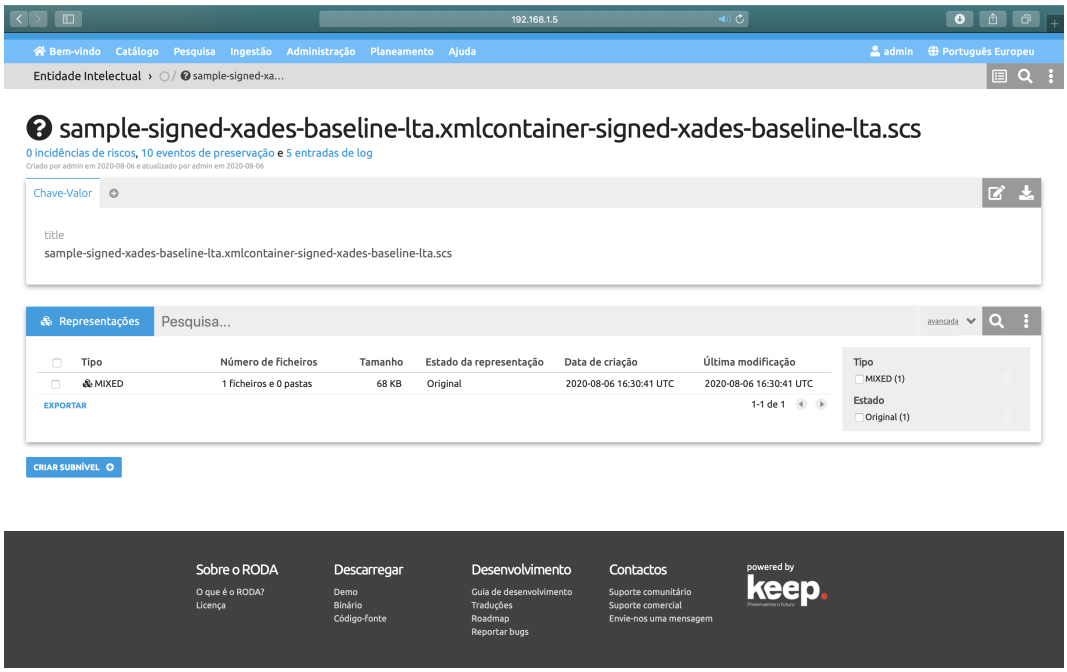



Figura 39: RODA: Archival Information Package

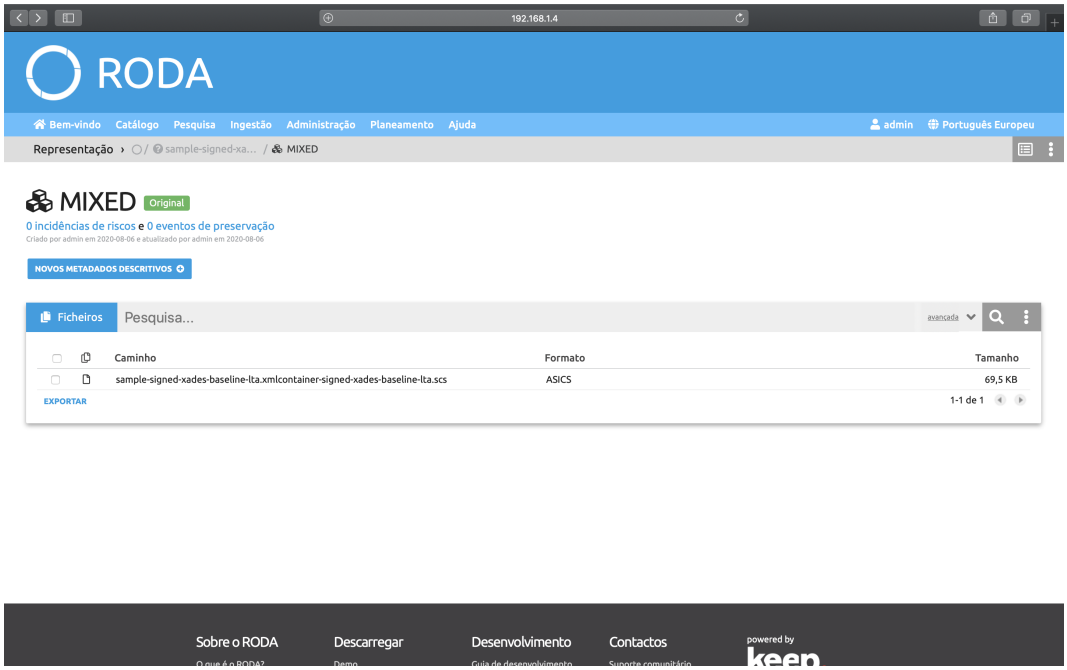



Figura 40: RODA: tipo da submissão

# D

## PROVA DE CONCEITO: PRESERVAÇÃO SEM ARMAZENAMENTO

Este apêndice contém os passos essenciais para o uso do perfil de preservação sem armazenamento e relaciona-se com o caso de uso 1 exposto na secção 3.7.2.


Figura 41: Interface Inicial do Serviço de Preservação

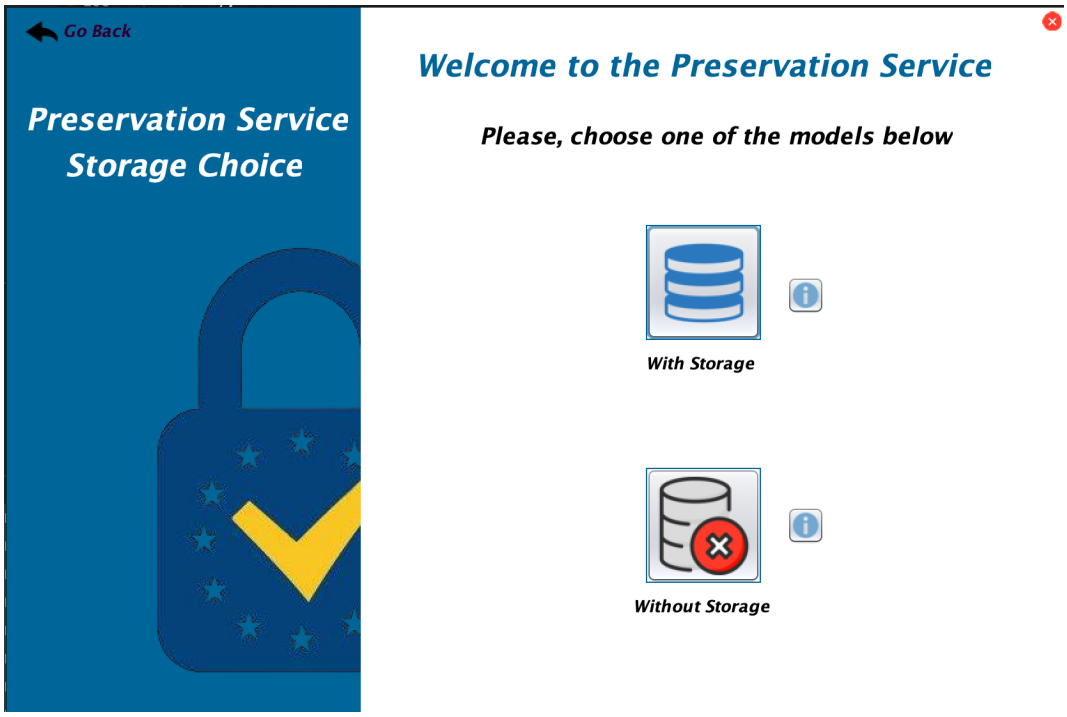



Figura 42: Escolha do modelo de armazenamento

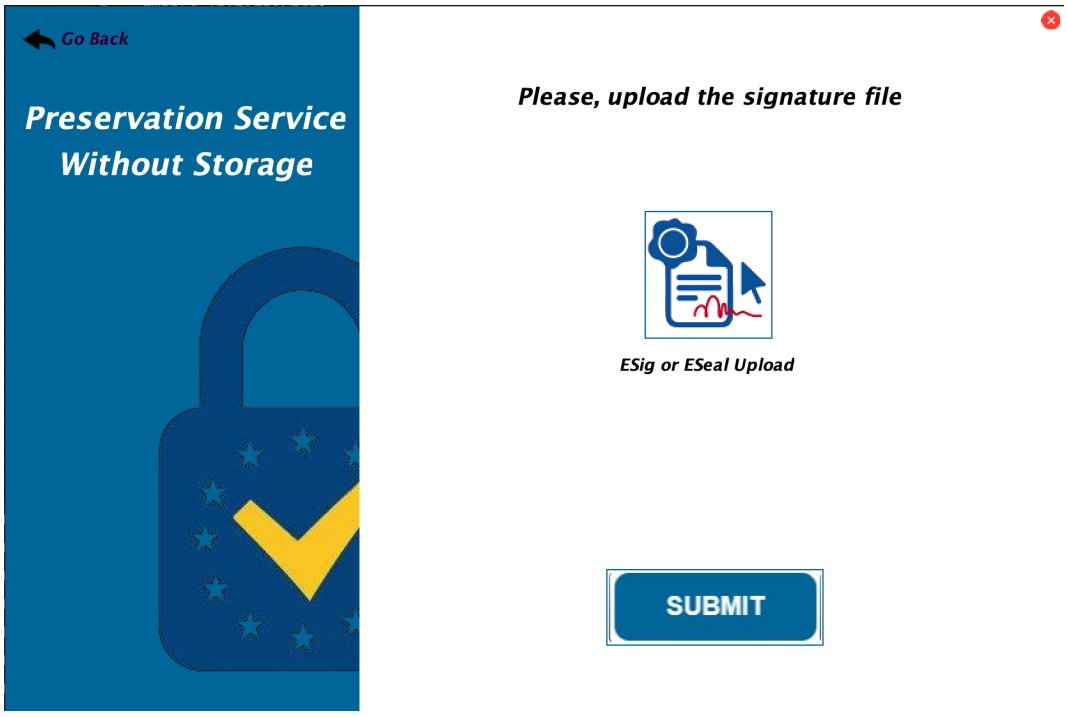



Figura 43: Serviço de Preservação sem Armazenamento

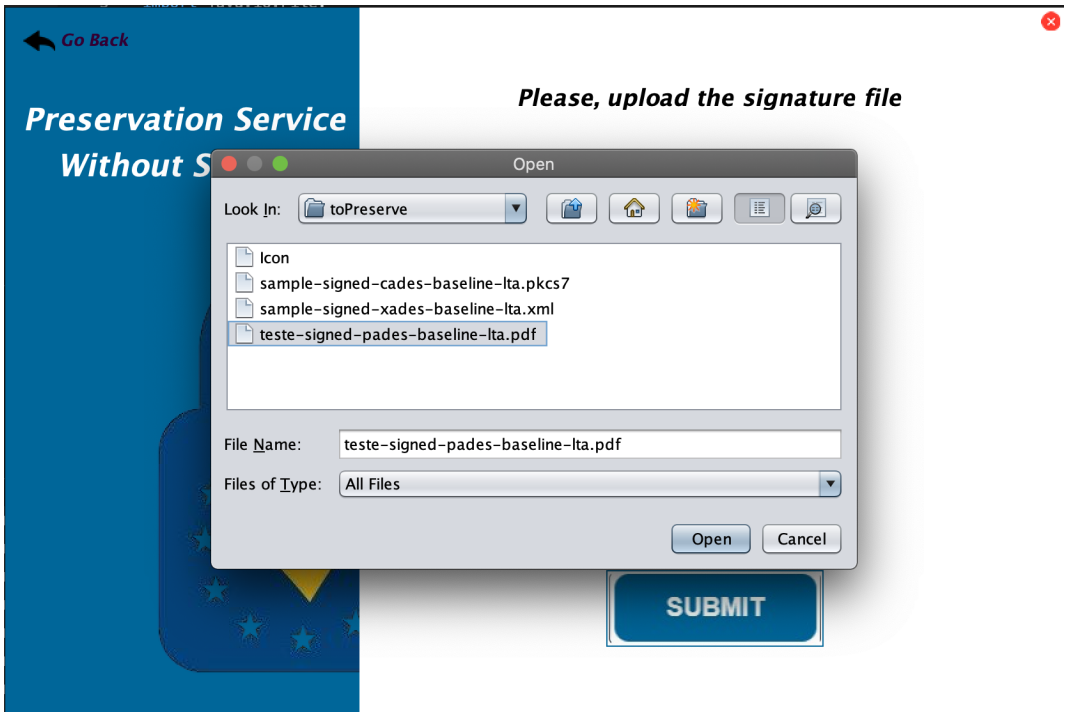



Figura 44: Upload da assinatura para o serviço de preservação

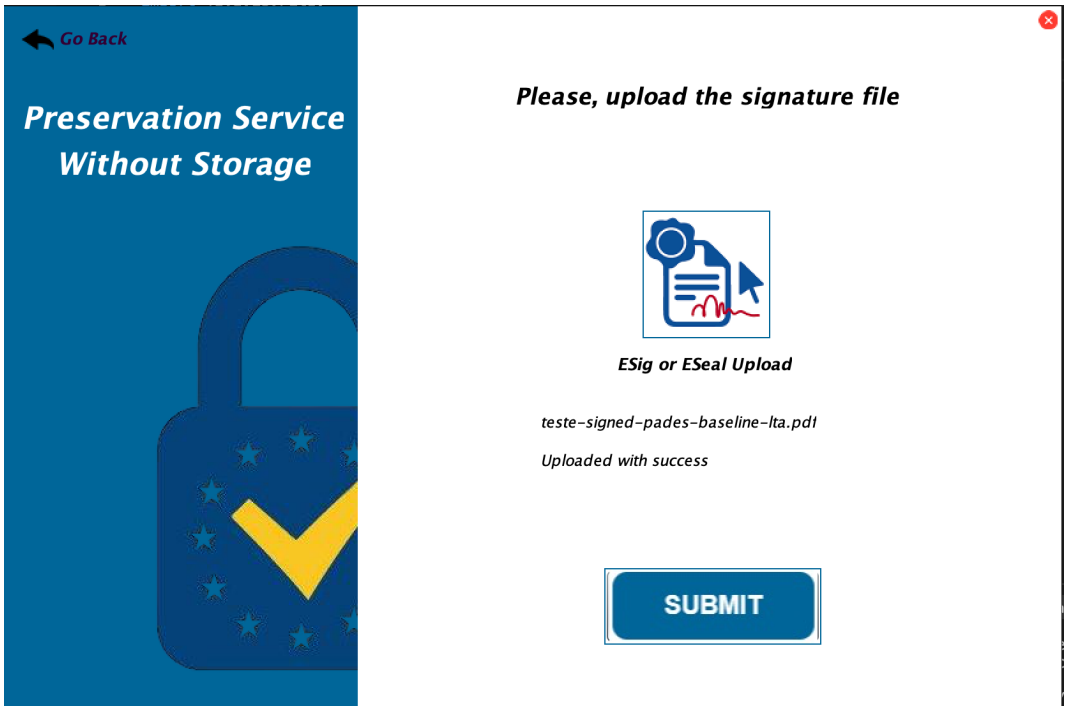



Figura 45: Upload da assinatura realizado com sucesso

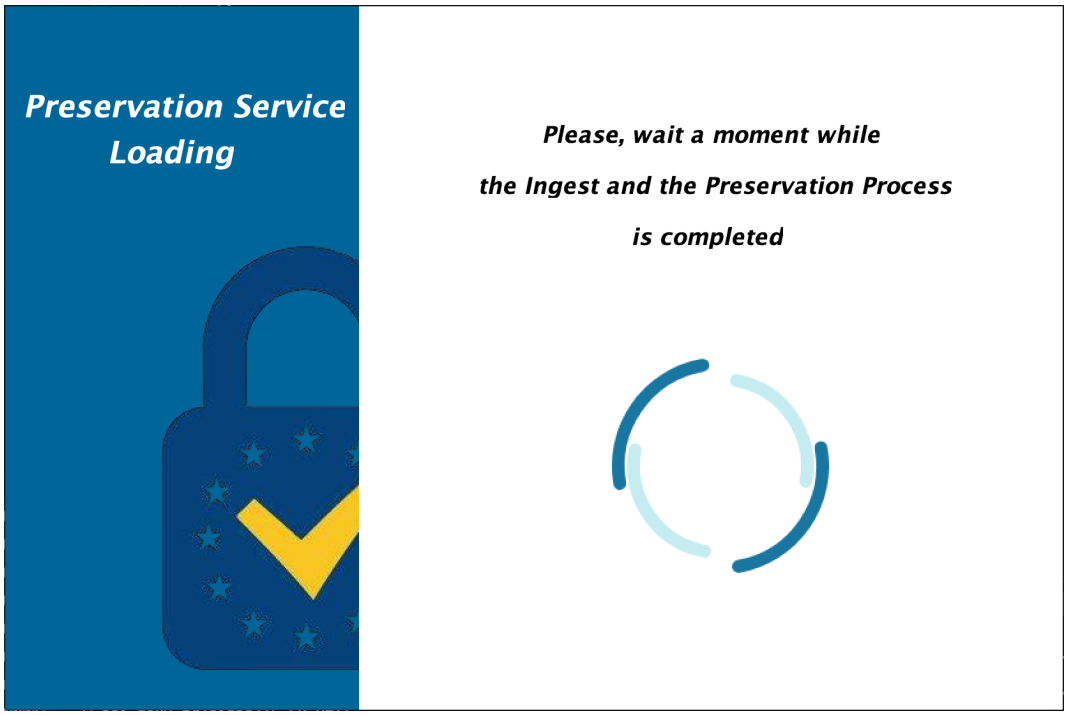



Figura 46: Loading menu

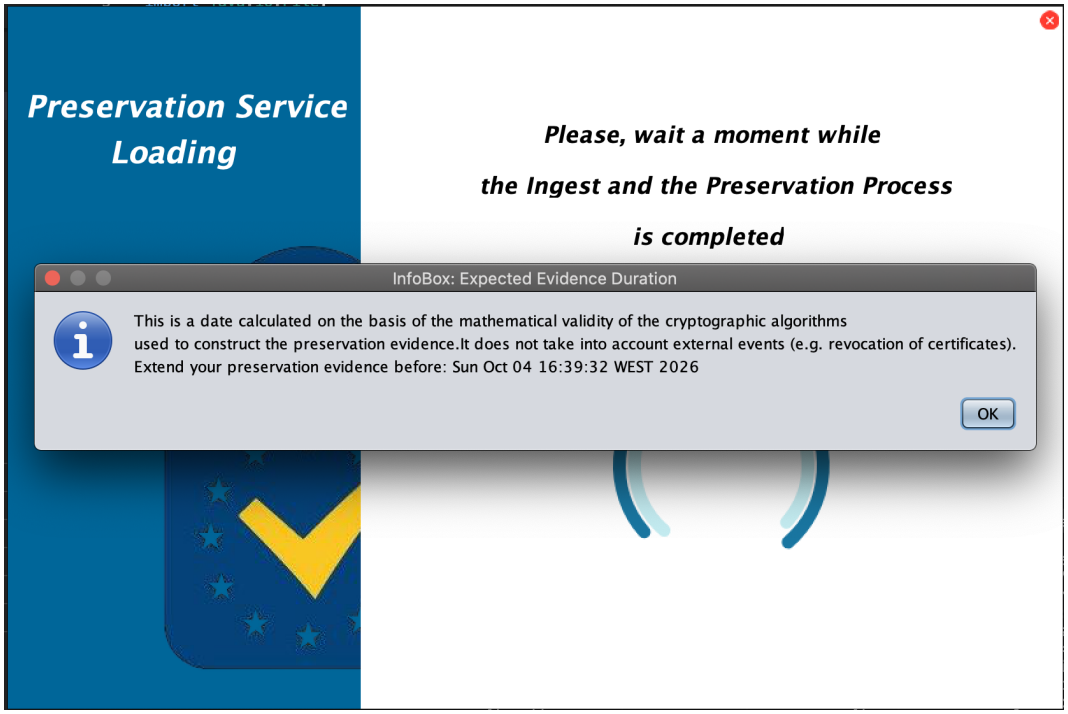



Figura 47: Duração expectável da evidência de preservação

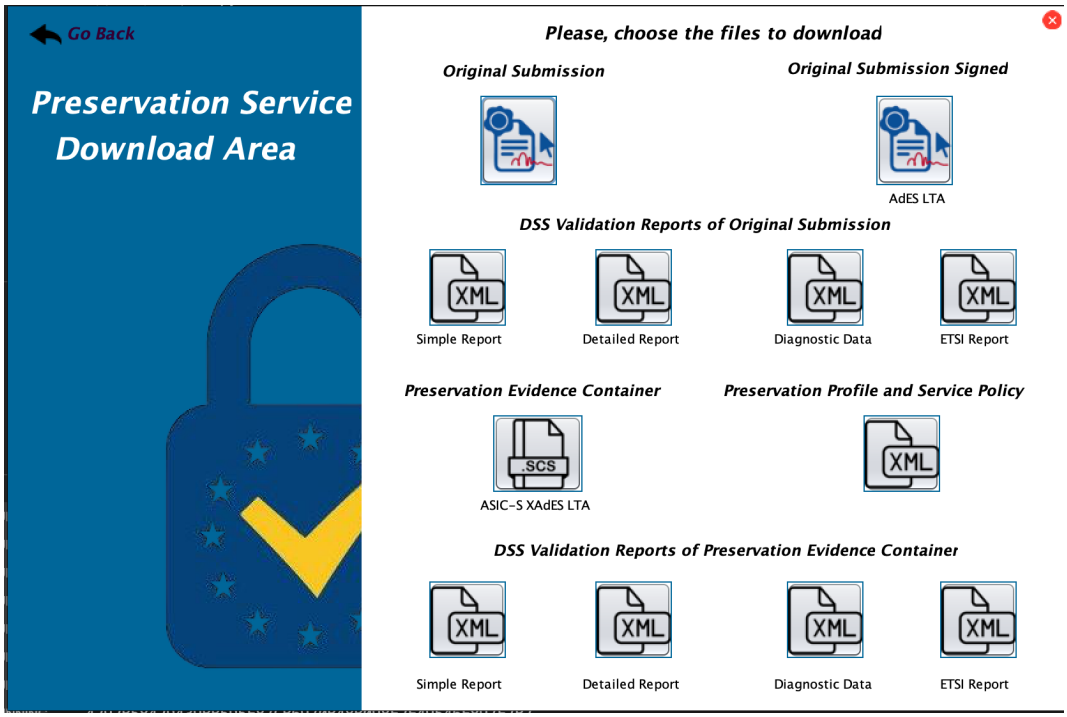



Figura 48: Área de Download

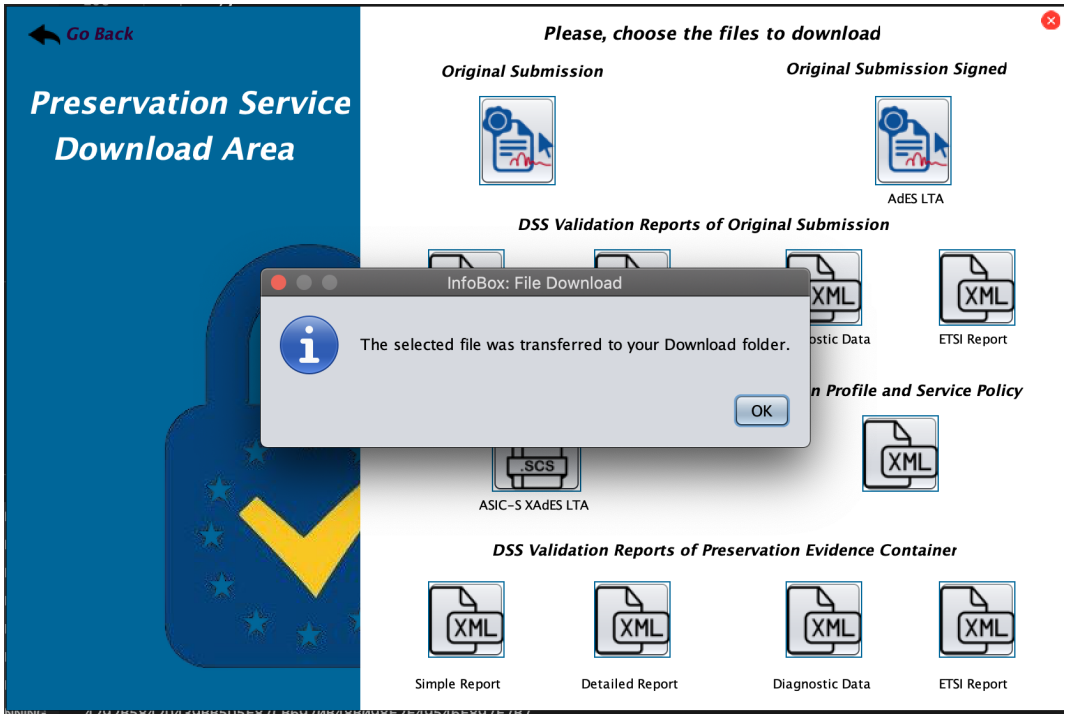



Figura 49: Informação do Download

# E

## PROVA DE CONCEITO: RELATÓRIOS DE VALIDAÇÃO DO DSS

Neste apêndice encontra-se um dos quatro diferentes tipos de relatório de validação produzidos pelo DSS. Estes relatórios são referentes à validação da assinatura recebida pelo sistema de preservação no apêndice B. O resto dos relatórios podem ser encontrados no repositório[1].

Neste repositório do *Git*, serão encontrados os relatórios de validação da submissão original, a evidência de preservação criada, assim como os relatórios de validação da evidência para verificar o conteúdo da mesma.

De referir ainda que a API do DSS, mencionada na secção 2.6.3 disponibiliza funções que são capazes de dizer se tudo correu bem com a criação dos relatórios, assim como identificar qualquer erro.

```
<!--Generated by DSS v.5.7--><div class="card" xmlns:dss="http://dss.esig.europa.eu/validation/simple-report">
   <div class="card-header bg-primary" data-target="#collapsePolicy" data-toggle="collapse">
       Validation Policy : QES AdESQC TL based</div>
   <div class="card-body collapse in" id="collapsePolicy">Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a
   Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes
   signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).
  </div>
</div><div class="card mt-3">
   <div class="card-header bg-primary" data-target="#collapseSigS-28DA936FAB815DCAFF5E9286B1A4481BF8E7BC268655CBD3735876E09AE5F982" data-toggle="collapse">
       Signature
      S-28DA936FAB815DCAFF5E9286B1A4481BF8E7BC268655CBD3735876E09AE5F982</div>
   <div class="card-body collapse in" id="collapseSigS-28DA936FAB815DCAFF5E9286B1A4481BF8E7BC268655CBD3735876E09AE5F982">
      <dl class="row mb-0">
```

1 https://github.com/fernandesjm/PreservationServiceProofOfConcept/tree/main/projeto/Preservation-Service/src/main/resources/out

```
14          <dt class="col-sm-3">
15
16                Qualification:
17              </dt>
18          <dd class="col-sm-9">
19             AdESig<i class="fa fa-info-circle text-info ml-2" data-toggle="tooltip" data-
                   placement="right" title="Advanced Electronic Signature"></i>
20          </dd>
21       </dl>
22       <dl class="row mb-0">
23          <dt class="col-sm-3">
24
25                Signature format:
26              </dt>
27          <dd class="col-sm-9">XAdES-BASELINE-LTA</dd>
28       </dl>
29       <dl class="row mb-0">
30          <dt class="col-sm-3">
31              Indication:
32         </dt>
33          <dd class="col-sm-9 text-success">
34             <div class="badge mr-2 badge-success">TOTAL_PASSED</div>
35             <i class="fa fa-check-circle align-middle"></i>
36          </dd>
37       </dl>
38       <dl class="row mb-0">
39          <dt class="col-sm-3"></dt>
40          <dd class="col-sm-9 text-danger">The certificate type cannot be issued by the found
                trust service(s)!</dd>
41       </dl>
42       <dl class="row mb-0">
43          <dt class="col-sm-3"></dt>
44          <dd class="col-sm-9 text-warning">The trusted list is not well signed!</dd>
45       </dl>
46       <dl class="row mb-0">
47          <dt class="col-sm-3"></dt>
48          <dd class="col-sm-9 text-warning">The certificate is not qualified at (best) signing
                 time!</dd>
49       </dl>
50       <dl class="row mb-0">
51          <dt class="col-sm-3"></dt>
52          <dd class="col-sm-9 text-warning">The certificate is not qualified at issuance time!<
                /dd>
53       </dl>
54       <dl class="row mb-0">
55          <dt class="col-sm-3"></dt>
```

```
56          <dd class="col-sm-9 text-warning">The private key does not reside in a QSCD at (best)
                signing time!</dd>
57       </dl>
58       <dl class="row mb-0">
59          <dt class="col-sm-3"></dt>
60          <dd class="col-sm-9 text-warning">The signer's certificate does not have an expected
                key-usage!</dd>
61       </dl>
62       <dl class="row mb-0">
63          <dt class="col-sm-3">
64
65             Certificate Chain:
66           </dt>
67          <dd class="col-sm-9">
68             <ul class="list-unstyled mb-0">
69                <li>
70                   <i class="fa fa-link mr-2"></i><b>mock.user.sign@gmail.com</b>
71                </li>
72                <li>
73                   <i class="fa fa-link mr-2"></i>Actalis Client Authentication CA G3
74                </li>
75                <li>
76                   <i class="fa fa-link mr-2"></i>Actalis Authentication Root CA
77                </li>
78             </ul>
79          </dd>
80       </dl>
81       <dl class="row mb-0">
82          <dt class="col-sm-3">
83
84              On claimed time:
85             </dt>
86          <dd class="col-sm-9">2020-11-12T15:54:24</dd>
87       </dl>
88       <dl class="row mb-0">
89          <dt class="col-sm-3">
90
91                Best signature time:
92              </dt>
93          <dd class="col-sm-9">
94             2020-11-12T15:54:56<i class="fa fa-info-circle text-info ml-2" data-toggle="
                   tooltip" data-placement="right" title="
95              Lowest time at which there exists a proof of existence for the signature
96             "></i>
97          </dd>
98       </dl>
99       <dl class="row mb-0">
```

```
100          <dt class="col-sm-3">
101
102              Signature position:
103             </dt>
104          <dd class="col-sm-9">1 out of 1</dd>
105       </dl>
106       <dl class="row mb-0">
107          <dt class="col-sm-3">
108
109                Signature scope:
110              </dt>
111          <dd class="col-sm-9">
112             Full XML File (FULL)
113             <br>
114             The full XML file with transformations.
115          </dd>
116       </dl>
117    </div>
118 </div><div class="card mt-3">
119    <div class="card-header bg-primary" data-target="#collapseInfo" data-toggle="collapse">
120        Document Information
121        </div>
122    <div class="card-body collapse in" id="collapseInfo">
123       <dl class="row mb-0">
124          <dt class="col-sm-3">
125
126             Signatures status:
127           </dt>
128          <dd class="col-sm-9 text-success">1 valid signatures, out of 1</dd>
129       </dl>
130       <dl class="row mb-0">
131          <dt class="col-sm-3">
132
133             Document name:
134           </dt>
135          <dd class="col-sm-9">sample-signed-xades-baseline-lta.xml</dd>
136       </dl>
137    </div>
138 </div>
```

Listing E.1: Simple Report DSS

# F

## PROVA DE CONCEITO: OPERAÇÃO DE RECUPERAR

Este apêndice contém os passos essenciais para a realização da acção de recuperar evidências de preservação e outros objetos por parte do utilizador e relaciona-se com o caso de uso 3 exposto na secção 3.7.2.


Figura 50: Interface Inicial do Serviço de Preservação

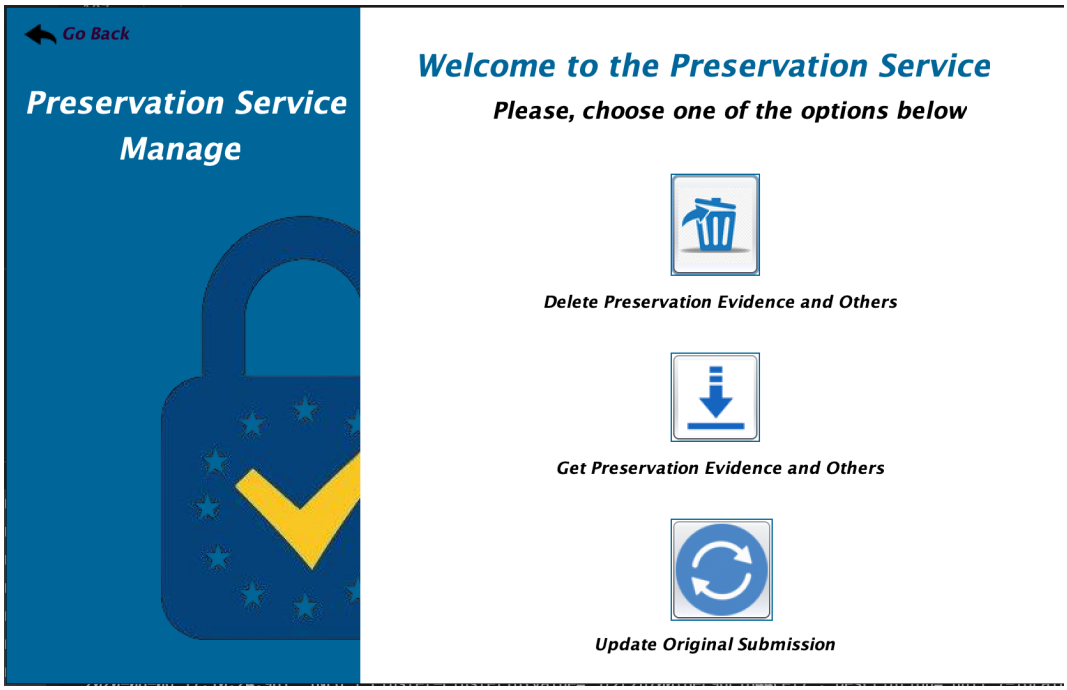



Figura 51: Menu de gestão

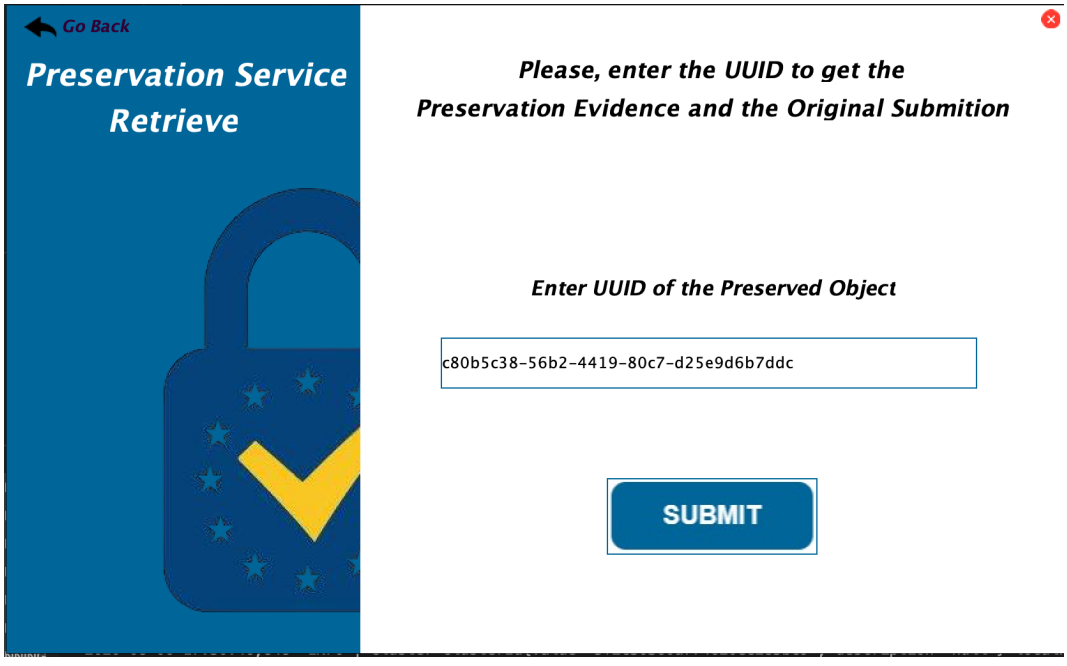



Figura 52: Inserção do identificador único

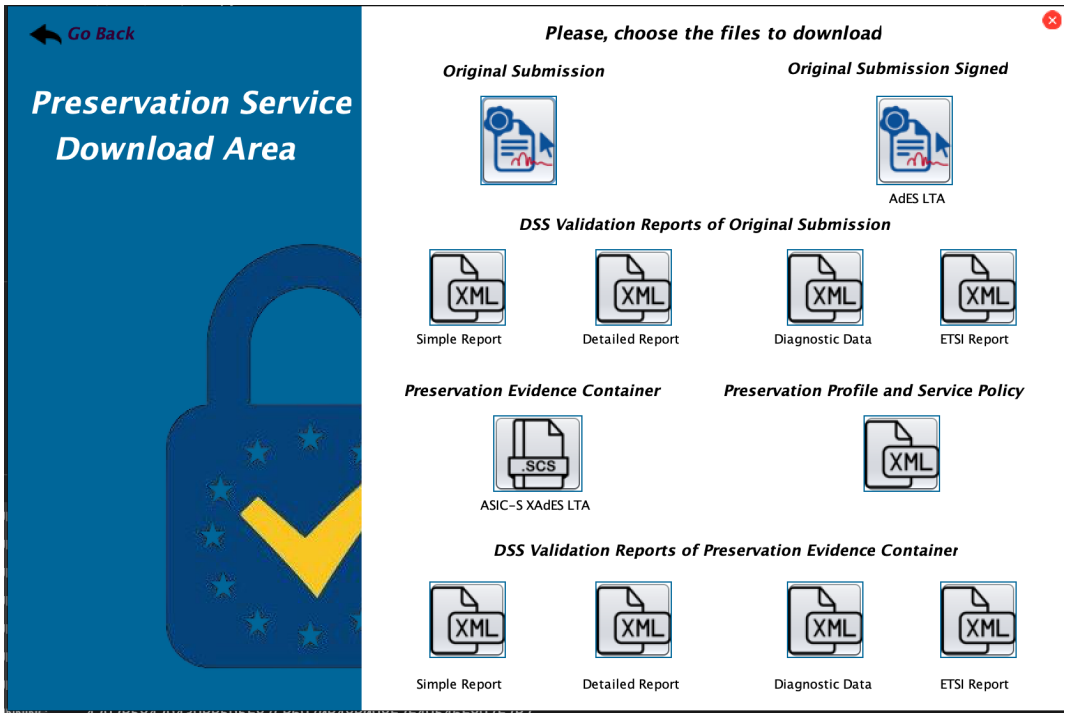



Figura 53: Área de Download

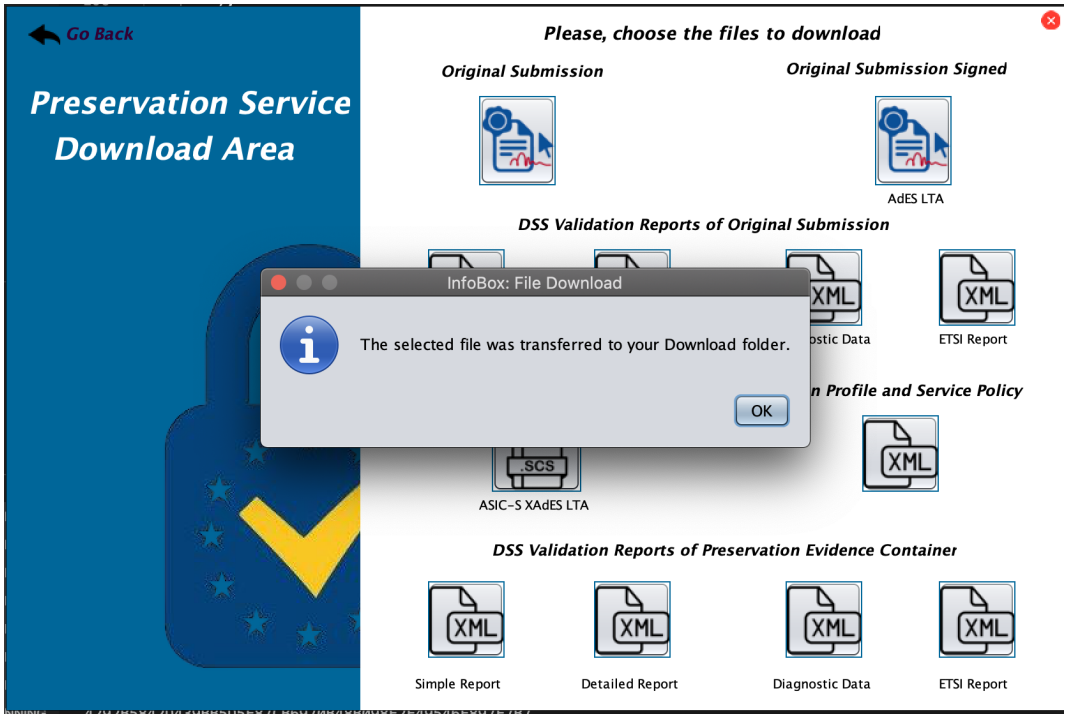



Figura 54: Informação do Download

# G

## PROVA DE CONCEITO: OPERAÇÃO DE ATUALIZAR A SUBMISSÃO ORIGINAL

Este apêndice contém os passos essenciais para a realização da acção de atualizar a submissão original por parte do utilizador e relaciona-se com o caso de uso 4 exposto na secção 3.7.2.


Figura 55: Interface Inicial do Serviço de Preservação

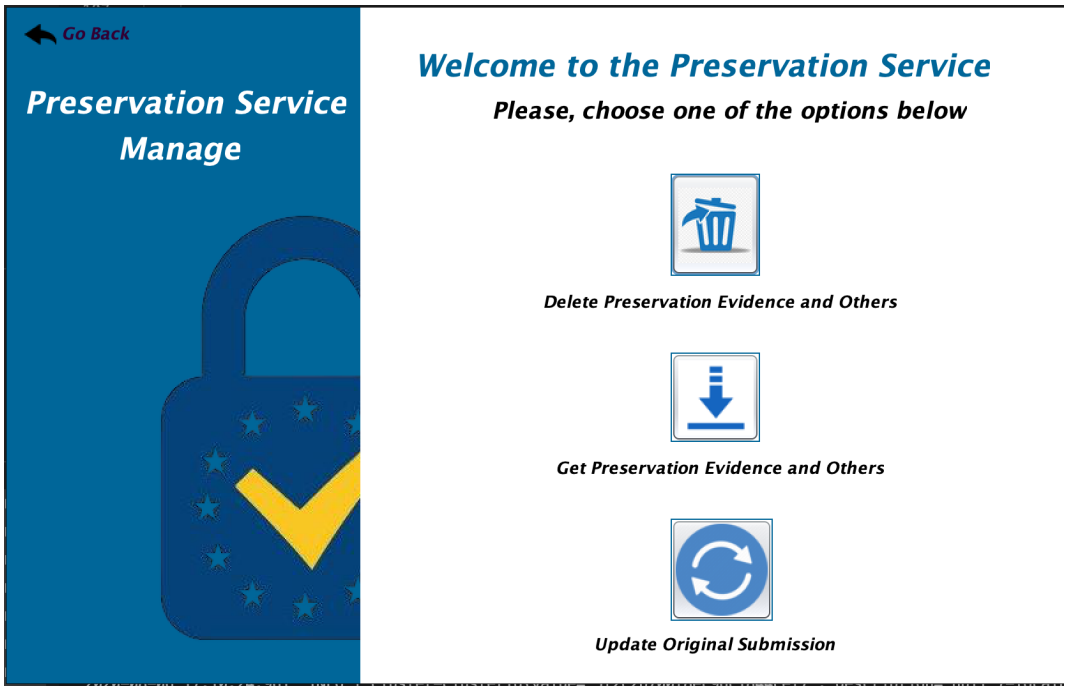



Figura 56: Menu de gestão

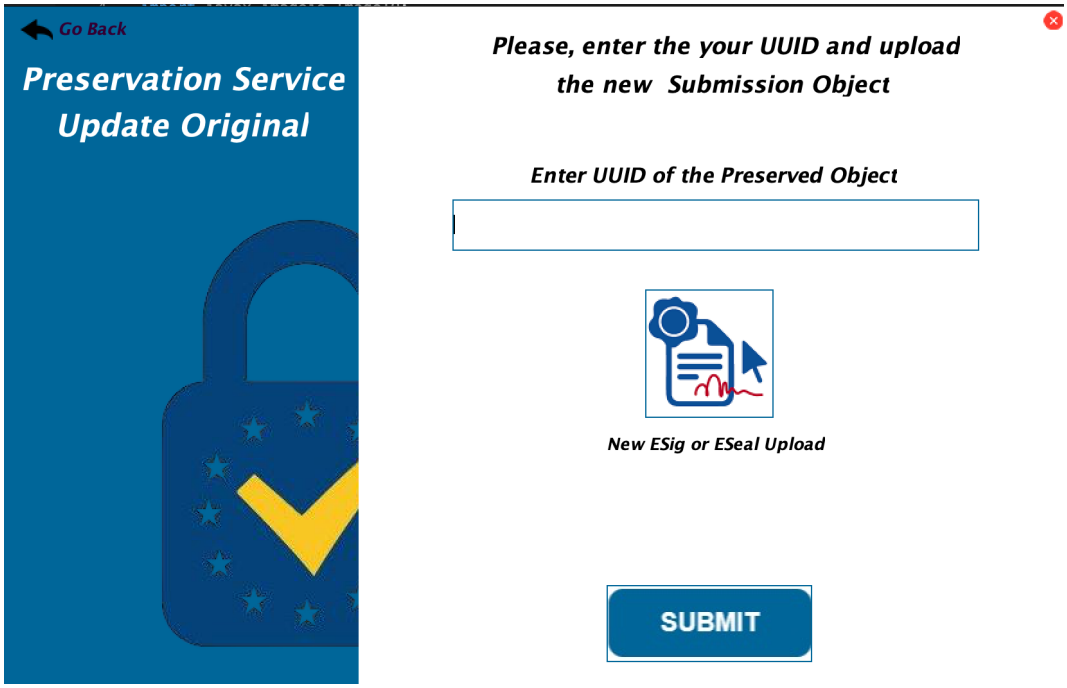



Figura 57: Upload da nova assinatura para o serviço de preservação e do uuid do utilizador

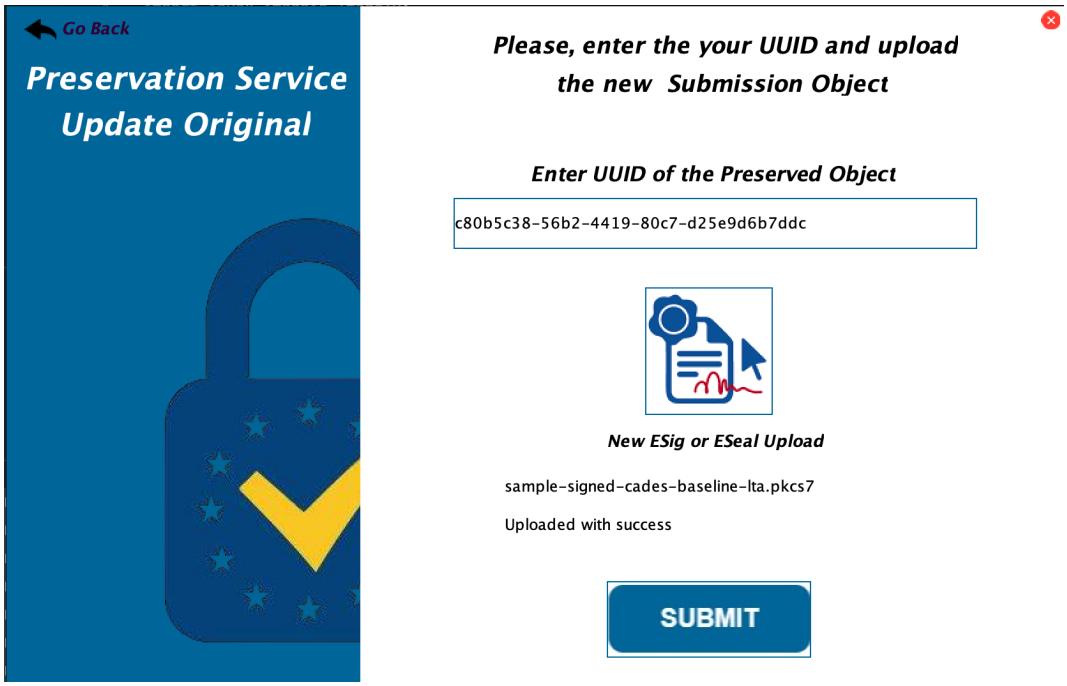



Figura 58: Upload da nova assinatura realizado com sucesso

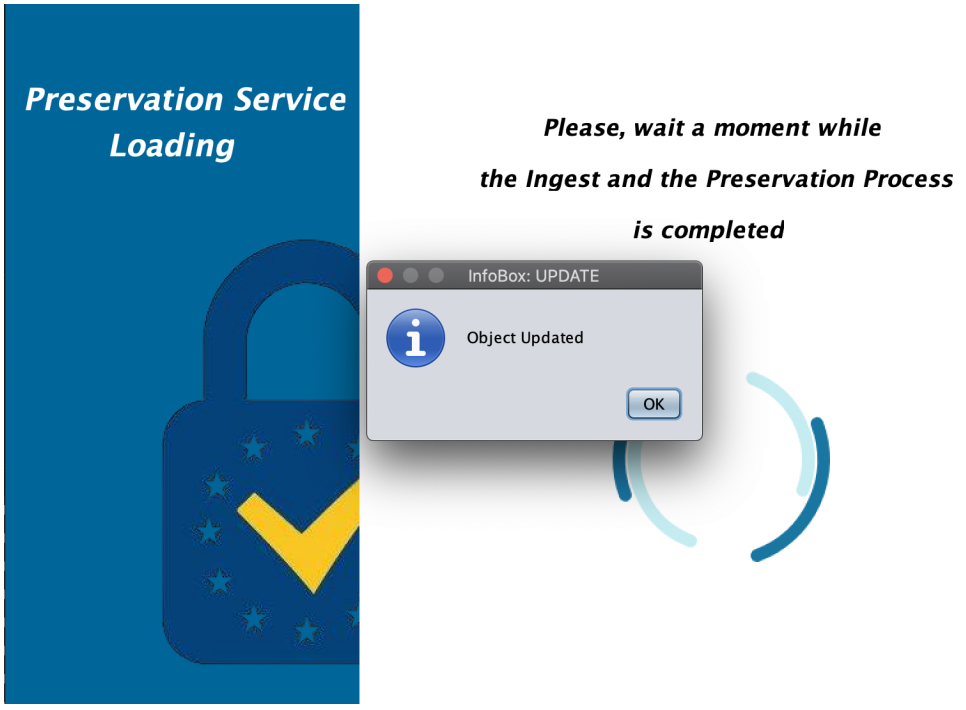



Figura 59: Atualização realizada com sucesso

Com este processo, novas evidências de preservação são criadas pelo serviço de preservação. As evidências antigas são guardadas pelo serviço de preservação.

O utilizador quando realizar uma operação de recuperar evidências, irá receber informação relativa à submissão mais recente. Aquando da realização da operação de apagar, todas as evidências de preservação, relacionadas com o identificador único do utilizador, são removidas do serviço de preservação.

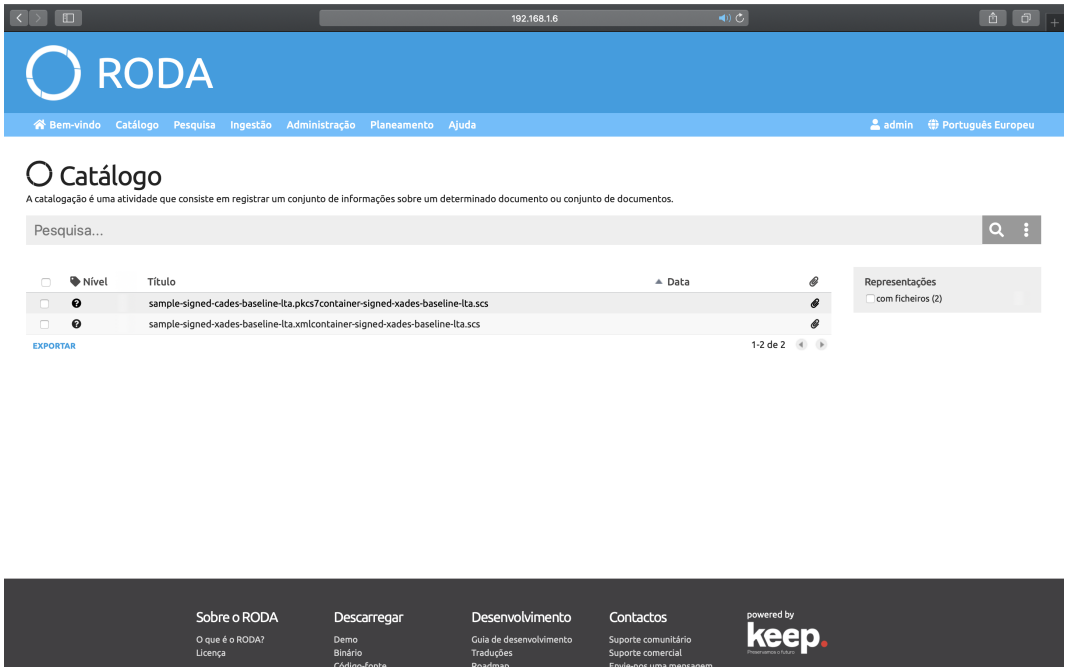



Figura 60: Armazenamento de todas as versões no repositório

# H

## PROVA DE CONCEITO: OPERAÇÃO DE REMOÇÃO

Este apêndice contém os passos essenciais para a realização da acção de remoção por parte do utilizador e relaciona-se com o caso de uso 5 exposto na secção 3.7.2.


Figura 61: Interface Inicial do Serviço de Preservação

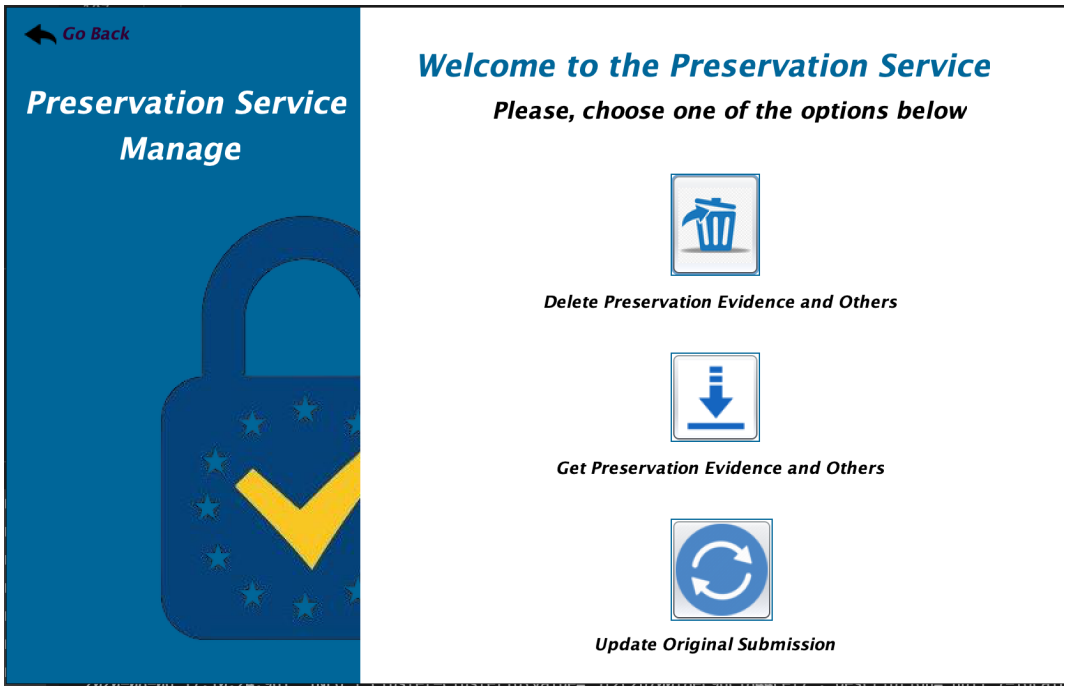



Figura 62: Menu de gestão

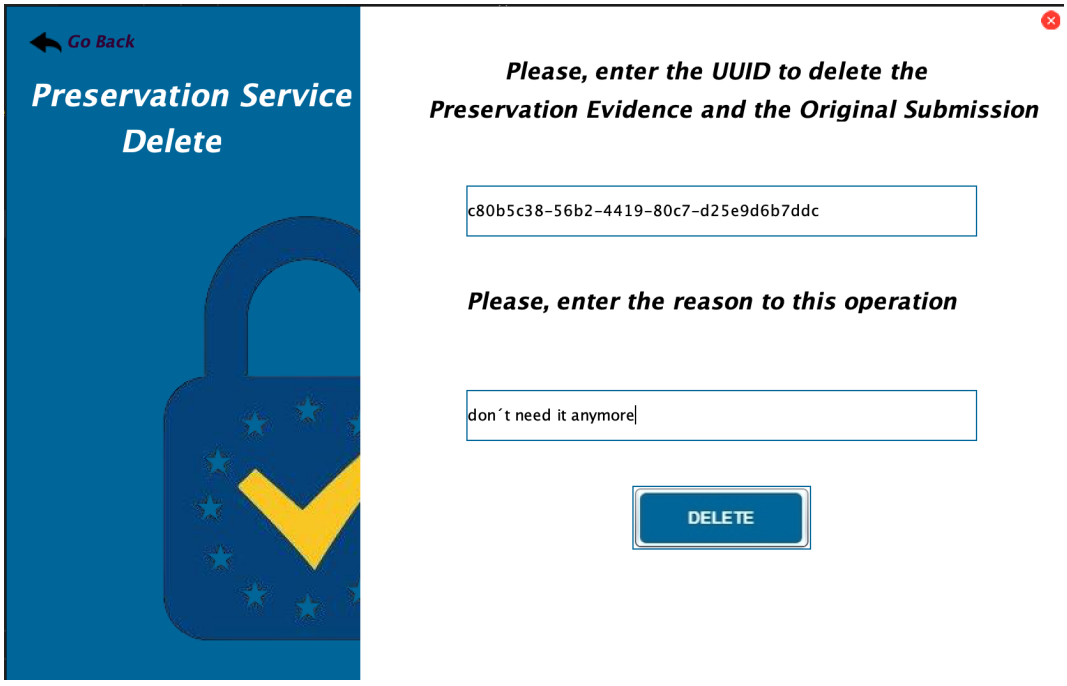



Figura 63: Inserção do identificador único

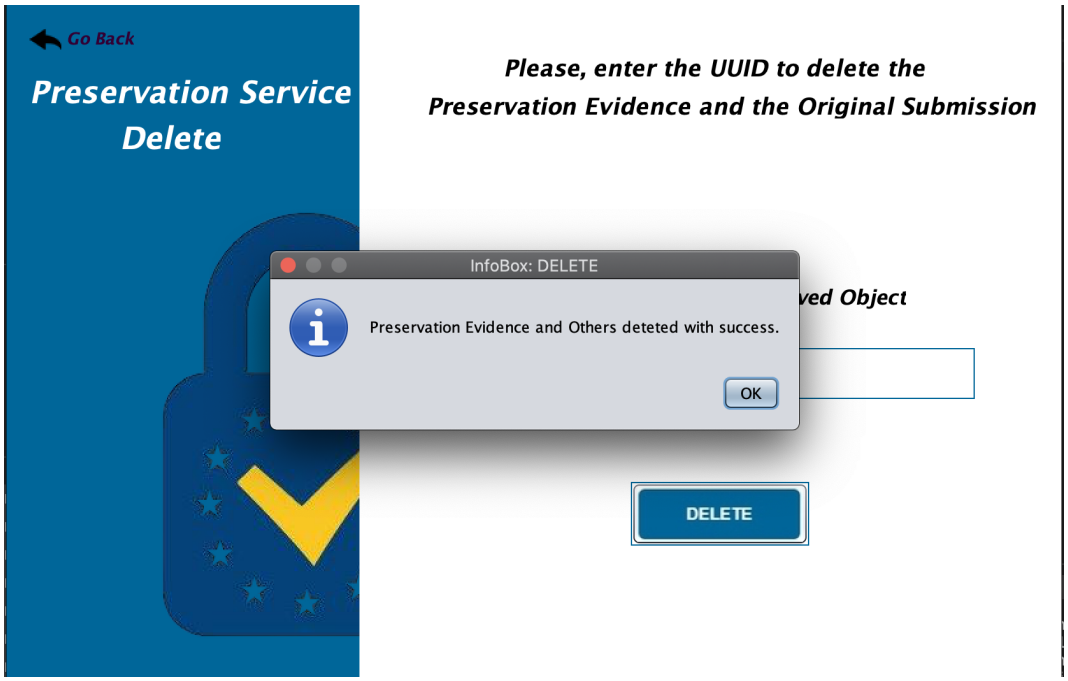



Figura 64: Operação de remoção realizada com sucesso

# I

## PROVA DE CONCEITO: RELATÓRIO DE VALIDAÇÃO DA EVIDÊNCIA DE PRESERVAÇÃO, ASIC CONTAINER LTA

Neste apêndice encontra-se um dos quatro diferentes tipos de relatório de validação da evidência de preservação produzidos no âmbito do serviço de preservação. Estes relatórios referem-se à validação do ASIC Container LTA produzido pelo sistema de preservação no apêndice B. Estes relatórios de validação são gerados pelo sistema quando o utilizador realiza a acção de recuperar evidências, ou quando o utilizador opta pelo perfil de preservação sem armazenamento.

É de notar a indicação *TOTAL-PASSED* na validação e no *signature scope* do contentor, que indica o conteúdo abrangido pela evidência de Preservação. O resto dos relatórios podem ser encontrados no repositório[1].

```
<!--Generated by DSS v.5.7--><div class="card" xmlns:dss="http://dss.esig.europa.eu/validation/simple-report">
   <div class="card-header bg-primary" data-target="#collapsePolicy" data-toggle="collapse">
       Validation Policy : QES AdESQC TL based</div>
   <div class="card-body collapse in" id="collapsePolicy">Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a
   Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes
   signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).
 </div>
</div><div class="card mt-3">
   <div class="card-header bg-primary" data-target="#collapseSigS-2865D4F0D66C08D310B58A12967C07D74218BF1CEBAAD91FC85930811DC051C0" data-toggle="collapse">
       Signature
      S-2865D4F0D66C08D310B58A12967C07D74218BF1CEBAAD91FC85930811DC051C0</div>
   <div class="card-body collapse in" id="collapseSigS-2865D4F0D66C08D310B58A12967C07D74218BF1CEBAAD91FC85930811DC051C0">
      <dl class="row mb-0">
        <dt class="col-sm-3">
```

1 https://github.com/fernandesjm/PreservationServiceProofOfConcept/tree/main/projeto/Preservation-Service/src/main/resources/out

```
15
16                Signature filename:
17               </dt>
18          <dd class="col-sm-9">META-INF/signatures.xml</dd>
19       </dl>
20       <dl class="row mb-0">
21          <dt class="col-sm-3">
22
23                Qualification:
24              </dt>
25          <dd class="col-sm-9">
26             AdESig<i class="fa fa-info-circle text-info ml-2" data-toggle="tooltip" data-
                   placement="right" title="Advanced Electronic Signature"></i>
27          </dd>
28       </dl>
29       <dl class="row mb-0">
30          <dt class="col-sm-3">
31
32                Signature format:
33              </dt>
34          <dd class="col-sm-9">XAdES-BASELINE-LTA</dd>
35       </dl>
36       <dl class="row mb-0">
37          <dt class="col-sm-3">
38              Indication:
39           </dt>
40          <dd class="col-sm-9 text-success">
41             <div class="badge mr-2 badge-success">TOTAL_PASSED</div>
42             <i class="fa fa-check-circle align-middle"></i>
43          </dd>
44       </dl>
45       <dl class="row mb-0">
46          <dt class="col-sm-3"></dt>
47          <dd class="col-sm-9 text-danger">The certificate type cannot be issued by the found
                trust service(s)!</dd>
48       </dl>
49       <dl class="row mb-0">
50          <dt class="col-sm-3"></dt>
51          <dd class="col-sm-9 text-warning">The trusted list is not well signed!</dd>
52       </dl>
53       <dl class="row mb-0">
54          <dt class="col-sm-3"></dt>
55          <dd class="col-sm-9 text-warning">The certificate is not qualified at (best) signing
                 time!</dd>
56       </dl>
57       <dl class="row mb-0">
58          <dt class="col-sm-3"></dt>
```

```
59          <dd class="col-sm-9 text-warning">The certificate is not qualified at issuance time!<
                /dd>
60       </dl>
61       <dl class="row mb-0">
62          <dt class="col-sm-3"></dt>
63          <dd class="col-sm-9 text-warning">The private key does not reside in a QSCD at (best)
                 signing time!</dd>
64       </dl>
65       <dl class="row mb-0">
66          <dt class="col-sm-3"></dt>
67          <dd class="col-sm-9 text-warning">The signer’s certificate does not have an expected
                 key-usage!</dd>
68       </dl>
69       <dl class="row mb-0">
70          <dt class="col-sm-3">
71
72             Certificate Chain:
73           </dt>
74          <dd class="col-sm-9">
75             <ul class="list-unstyled mb-0">
76                <li>
77                   <i class="fa fa-link mr-2"></i><b>presservproofofconcept@gmail.com</b>
78                </li>
79                <li>
80                   <i class="fa fa-link mr-2"></i>Actalis Client Authentication CA G3
81                </li>
82                <li>
83                   <i class="fa fa-link mr-2"></i>Actalis Authentication Root CA
84                </li>
85             </ul>
86          </dd>
87       </dl>
88       <dl class="row mb-0">
89          <dt class="col-sm-3">
90
91                On claimed time:
92             </dt>
93          <dd class="col-sm-9">2020-11-12T17:46:16</dd>
94       </dl>
95       <dl class="row mb-0">
96          <dt class="col-sm-3">
97
98                Best signature time:
99             </dt>
100         <dd class="col-sm-9">
101            2020-11-12T17:46:23<i class="fa fa-info-circle text-info ml-2" data-toggle="
                   tooltip" data-placement="right" title="
```

```
102                Lowest time at which there exists a proof of existence for the signature
103              "></i>
104           </dd>
105        </dl>
106        <dl class="row mb-0">
107           <dt class="col-sm-3">
108
109                Signature position:
110              </dt>
111           <dd class="col-sm-9">1 out of 1</dd>
112        </dl>
113        <dl class="row mb-0">
114           <dt class="col-sm-3">
115
116                  Signature scope:
117               </dt>
118           <dd class="col-sm-9">
119              package.zip (FULL)
120              <br>
121              ASiCS archive
122           </dd>
123        </dl>
124        <dl class="row mb-0">
125           <dt class="col-sm-3">
126
127                  Signature scope:
128               </dt>
129           <dd class="col-sm-9">
130              sample-signed-xades-baseline-lta-signed-xades-baseline-lta.xml (ARCHIVED)
131              <br>
132              ASiCS archive content
133           </dd>
134        </dl>
135        <dl class="row mb-0">
136           <dt class="col-sm-3">
137
138                  Signature scope:
139               </dt>
140           <dd class="col-sm-9">
141              sample-signed-xades-baseline-lta.xml (ARCHIVED)
142              <br>
143              ASiCS archive content
144           </dd>
145        </dl>
146        <dl class="row mb-0">
147           <dt class="col-sm-3">
148
```

```
149                Signature scope:
150               </dt>
151            <dd class="col-sm-9">
152               VAL-SimpleReport.xml (ARCHIVED)
153               <br>
154               ASiCS archive content
155            </dd>
156         </dl>
157         <dl class="row mb-0">
158            <dt class="col-sm-3">
159
160                Signature scope:
161               </dt>
162            <dd class="col-sm-9">
163               VAL-DetailedReport.xml (ARCHIVED)
164               <br>
165               ASiCS archive content
166            </dd>
167         </dl>
168         <dl class="row mb-0">
169            <dt class="col-sm-3">
170
171                Signature scope:
172               </dt>
173            <dd class="col-sm-9">
174               VAL-DiagnosticData.xml (ARCHIVED)
175               <br>
176               ASiCS archive content
177            </dd>
178         </dl>
179         <dl class="row mb-0">
180            <dt class="col-sm-3">
181
182                Signature scope:
183               </dt>
184            <dd class="col-sm-9">
185               VAL-ETSIReport.xml (ARCHIVED)
186               <br>
187               ASiCS archive content
188            </dd>
189         </dl>
190      </div>
191   </div><div class="card mt-3">
192      <div class="card-header bg-primary" data-target="#collapseInfo" data-toggle="collapse">
193          Document Information
194          </div>
195      <div class="card-body collapse in" id="collapseInfo">
```

```
196       <dl class="row mb-0">
197          <dt class="col-sm-3">
198
199              Container type:
200             </dt>
201          <dd class="col-sm-9">ASiC-S</dd>
202       </dl>
203       <dl class="row mb-0">
204          <dt class="col-sm-3">
205
206             Signatures status:
207           </dt>
208          <dd class="col-sm-9 text-success">1 valid signatures, out of 1</dd>
209       </dl>
210       <dl class="row mb-0">
211          <dt class="col-sm-3">
212
213             Document name:
214           </dt>
215          <dd class="col-sm-9">sample-signed-xades-baseline-lta.xmlcontainer-signed-xades-
                 baseline-lta.scs</dd>
216       </dl>
217    </div>
218 </div>
```

Listing I.1: Simple Report DSS da evidência de preservação

# J

## PROVA DE CONCEITO: FICHEIRO DE LOG

No âmbito da Prova de Conceito foi implementado um *Logger* que regista todas as ações que foram referidas ao longo deste documento e que ocorrem no sistema.

Acções essas de preservação e de gestão que são registadas cronologicamente neste ficheiro, para mais tarde poder servir de prova para uma possível auditoria e para rastreabilizar passos dados no sistema.

```
janeiro 18, 2021 5:10:47 DA TARDE com.devisefutures.projeto.LoggerPS logMessage
INFO: Preservation With Storage was choosen to the file: sample-signed-xades-baseline-lta.xml
      PSOutput UUID: c80b5c38-56b2-4419-80c7-d25e9d6b7ddc
janeiro 19, 2021 4:32:17 DA TARDE com.devisefutures.projeto.LoggerPS logMessage
INFO: Preservation Evidences and others requested by UUID: c80b5c38-56b2-4419-80c7-
    d25e9d6b7ddc
janeiro 19, 2021 5:05:39 DA TARDE com.devisefutures.projeto.LoggerPS logMessage
INFO: Preservation Without Storage was choosen to the file: teste-signed-pades-baseline-lta.
    pdf
janeiro 21, 2021 2:52:10 DA TARDE com.devisefutures.projeto.LoggerPS logMessage
INFO: Original Submission Update for UUID: c80b5c38-56b2-4419-80c7-d25e9d6b7ddc New Original
    Submission File: sample-signed-cades-baseline-lta.pkcs7
janeiro 21, 2021 3:12:51 DA TARDE com.devisefutures.projeto.LoggerPS logMessage
INFO: Preservation Evidences and others deleted by UUID: c80b5c38-56b2-4419-80c7-d25e9d6b7ddc
      Reason: dont need it anymore
```

Listing J.1: Ficheiro de Log

# K

## PROVA DE CONCEITO: FICHEIRO DO PERFIL DE PRESERVAÇÃO

No âmbito da Prova de Conceito foi implementada uma classe em *Java* que cria um ficheiro em *XML* que representa o perfil de preservação escolhido por cada Utilizador. Este ficheiro inclui o modelo de armazenamento escolhido, o objetivo de preservação, o conteúdo da evidência de preservação criada, a duração expectável da evidência de preservação e um apontamento para onde encontrar a política do serviço de preservação que é esta Prova de Conceito.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<PreservationSrevice>
   <PreservationProfile>
      <storageModel>WITHOUT_STORAGE</storageModel>
      <preservationGoal>LONG-TERM PRESERVATION</preservationGoal>
      <content id="Preservation Evidence Container Content">
        <point>Original Submission</point>
        <point>Original Submissition Signed with AdES LTA</point>
        <point>Original Submission Validation Reports DSS</point>
      </content>
      <Duration id="Expected Evidence Duration (without storage) and Preservation Period (with
           storage)">
        <max>extend your evidence before: Sun Oct 04 16:39:32 WEST 2026</max>
      </Duration>
      <policy id="Preservation Service Policy available at:">
        <link>https://www.devisefutures.com/pdf/preservacao/PoliticaPreservacao.pdf</link>
     </policy>
  </PreservationProfile>
</PreservationSrevice>
```

Listing K.1: Ficheiro do Perfil de Preservação

# BIBLIOGRAFIA


Afnor nf z40-020: "spécifications fonctionnelles d'un composant coffre-fort numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps", 2012.

Digital signature service. https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.pdf.

Etsi ts 119 102-1,electronic signatures and infrastructures (esi); procedures for creation and validation of ades digital signatures; part 1: Creation and validation. a.

Etsi en 319 122-1 (2016): Electronic signatures and infrastructures (esi); v1.1.1. b.

Etsi en 319 132-1 (2016): Electronic signatures and infrastructures (esi); v1.1.1. c.

Etsi ts 119 312: "electronic signatures and infrastructures (esi); cryptographic suites". d.

Etsi en 319 401, electronic signatures and infrastructures (esi);general policy requirements for trust service providers. e.

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. f.

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. g.

Etsi ts 119 512, electronic signatures and infrastructures (esi); protocols for trust service providers providing long-term data preservation services. h.

Futuretrust - scalable preservation service d.3.4.

Iso 14641-1,electronic archiving—part 1: Specifications concerning the design and the operation of an information system for electronic information preservation. a.

Iso 14721:2012, space data and information transfer systems — open archival information system (oais) — reference model. b.

R. merkle: "protocols for public key cryptosystems", proceedings of the 1980 ieee symposium on security and privacy (oakland, ca, usa), 1980, pages 122-134.

Ietf rfc 4998: "evidence record syntax (ers)". a.

Ietf rfc 6283 (2011): "extensible markup language evidence record syntax (xmlers)". b.

*RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, 2008.

Iso 16363:2012, space data and information transfer systems – audit and certification of trustworthy digital repositories. 2012.

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. 2014.

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.

*Guia de Operacionalização: Processos e/ ou serviços eletrónicos*. AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA.

*Cartão de Cidadão Selo Temporal*. Agência para a Modernização Administrativa, 2010.

*CEF eSignature DSS, Qualified electronic singature (QES) validation algorithm*. Connecting Europe Facility, 2018.

*Portaria nº 380/2017, de 19 de dezembro - Tramitação Eletrónica dos Processos da Jurisdição Administrativa e Fiscal*. Diário da República nº 242/2017, 2017.

*Decreto-Lei nº 28/2019*. Diário da República n.º 33/2019 de 15 de fevereiro, 2019.

*ETSI TS 102 918 Associated Signature Containers (ASiC)*. Electronic Signatures and Infrastructures (ESI), 2013.

*ETSI EN 319 122 CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*. Electronic Signatures and Infrastructures (ESI), 2016a.

*ETSI EN 319 122 CAdES digital signatures; Part 2: Extended CAdES signatures*. Electronic Signatures and Infrastructures (ESI), 2016b.

*ETSI EN 319 132 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures*. Electronic Signatures and Infrastructures (ESI), 2016c.

*ETSI EN 319 132 XAdES digital signatures; Part 2: Extended XAdES signatures*. Electronic Signatures and Infrastructures (ESI), 2016d.

*ETSI EN 319 142 PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures*. Electronic Signatures and Infrastructures (ESI), 2016e.

*ETSI EN 319 142 PAdES digital signatures; Part 2: Additional PAdES signatures profiles*. Electronic Signatures and Infrastructures (ESI), 2016f.

*Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers*. Electronic Signatures and Infrastructures (ESI), 2016g.

*Associated Signature Containers (ASiC); Part 2: Additional ASiC containers*. Electronic Signatures and Infrastructures (ESI), 2016h.

*ETSI TS 119 102 Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report*. Electronic Signatures and Infrastructures (ESI), 2018.

*Draft ETSI TS 119 172-4; Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists*. Electronic Signatures and Infrastructures (ESI), 2019a.

*ETSI TS 119 403-3, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers*. Electronic Signatures and Infrastructures (ESI), 2019b.

*Security guidelines on the appropriate use of qualified electronic signatures*. European Union Agency For Network And Information Security, 2016a.

*Security guidelines on the appropriate use of qualified electronic seals*. European Union Agency For Network And Information Security, 2016b.

*Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards*. European Union Agency For Network And Information Security, 2016c.

*eIDAS: Overview on the implementation and uptake of Trust Services*. European Union Agency For Network And Information Security, 2017.

Tina Hühnlein Mike Prechtl Detlef Hühnlein Florian Otto, Tobias Wich. Towards a standardised preservation service for qualified electronic signatures and qualified electronic seals.

*DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 13 de Dezembro de 1999 relativa a um quadro legal comunitário para as assinaturas electrónicas*. Jornal Oficial das Comunidades Europeias, 2000.

*RODA WHITEPAPER PRESERVAÇÃO DIGITAL DE LONGA-DURAÇÃO CARACTERÍSTICAS E REQUISITOS TÉCNICOS*. Keep Solutions, 2008.

*ANSI/NISO Z39.87-2006 (R2017) Data Dictionary - Technical Metadata for Digital Still Images*. National Information Standards Organization, 2017.

Agence nationale de la sécurité des systèmes d'information. Qualified preservation servicesfor qualified electronic signatures and seals criteria for assessing compliance with the eidas regulation.

A presente dissertação foi proposta pela empresa *DeviseFutures Lda.*