Estudo comparativo entre as aplicações de Assinatura Digital com o Cartão de Cidadão e a Chave Móvel Digital

Mestrado em Cibersegurança e Informática Forense

Cláudia Andrade Pena

Leiria, Dezembro de 2020

Estudo comparativo entre as aplicações de Assinatura Digital com o Cartão de Cidadão e a Chave Móvel Digital

Mestrado em Cibersegurança e Informática Forense

Cláudia Andrade Pena (2182106)

Trabalho de Projeto realizado sob a orientação do Professor Doutor Miguel Monteiro de Sousa Frade.

Leiria, Dezembro de 2020

Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Agradecimentos

Em primeiro lugar, agradeço à minha família que sempre me incentivou e motivou de forma positiva para que desse o melhor de mim ao longo desta jornada. Aos meus amigos um obrigada, pelas conversas de desabafo assim como motivadoras ao longo deste 2º ano do mestrado.

Por fim, agradeço ao Professor Miguel Frade pela sua orientação e disponibilidade durante o desenvolvimento do presente projeto.

Resumo

Se refletirmos acerca da evolução tecnológica e do processamento eletrónico dos documentos, poderemos colocar a seguinte questão “Porque precisamos das assinaturas digitais?” Se imaginarmos um documento que tem um valor legal, este documento pode conter informações importantes como direitos e obrigações, sendo que devemos garantir a autenticidade do mesmo. O presente projeto tem como objetivo principal o estudo comparativo entre aplicações de Assinatura Digital, o que nos leva à compreensão do estado atual das assinaturas digitais. E por sua vez, o projeto STORK que foi dado como concluído com sucesso, transmitindo que o mesmo está a ser utilizado e que quando um documento é assinado em Portugal este é válido num outro país, como por exemplo em Espanha. Ao longo do desenvolvimento do presente projeto foram vistos os formatos de assinatura existentes e projetos europeus e tecnologias usadas para realização da assinatura digital. Assim como avaliar e perceber qual o futuro das assinaturas digitais em Portugal, analisar os formatos de assinatura existentes e projetos europeus, bem como tecnologias usadas para realização da assinatura digital.

Compreende-se que o mundo digital está em continuo desenvolvimento e que as assinaturas digitais apresentam-se como um método eficaz no contexto de realização da assinatura de documentos, podendo este ser realizado à distância. Relativamente às ferramentas, entre os três softwares instalados e analisadas as suas características concluímos que a aplicação aCCinaPDF é a mais completa. Face aos desafios apresentados dada a presente situação de propagação do COVID-19, precisámos de nos adaptar às tecnologias existentes e utilizá-las a nosso favor pelo que realizar a assinatura de documentos de uma forma que não a manuscrita foi uma delas. Mesmo que existente e utilizada, neste ponto a assinatura eletrónica revela-se um instrumento bastante útil para que seja efetuada a assinatura de documentos à distância.

Palavras-chave: Assinatura Digital, Cartão de Cidadão, Segurança, Certificados Digitais, Software de assinatura digital

Abstract

If we reflect on the technology evolution and the electronic processing of documents, we may ask the following question "Why do we need the digital signatures? If we imagine a document that has legal value, this document may contain important information such as rights and obligations, and we must guarantee its authenticity. The main objective of this project is the comparative study between Digital Signature applications, which leads us to understand the current state of digital signatures. And in turn, the STORK project that was given as successfully completed, conveying that it is being used and that when a document is signed in Portugal it is valid in another country, such as Spain. Throughout the development of this project we have seen the existing signature formats and European projects and technologies used to make the digital signature. As well as evaluating and understanding the future of digital signatures in Portugal, analysing the existing signature formats and European projects, as well as technologies used for digital signature.

It is understood that the digital world is in continuous development and that digital signatures present themselves as an effective method in the context of document signing, which can be done from a distance. Regarding the tools, among the three softwares installed and analyzed their characteristics we concluded that the aCCinaPDF application is the most complete. Given the challenges presented by the present situation of propagation of COVID-19, we needed to adapt to existing technologies and use them to our advantage so that the signing of documents in a way other than manuscript was one of them. Even if existing and used, at this point the electronic signature proves to be a very useful tool for signing documents from a distance.

Keywords: Digital Signature, Citizen Card, Security, Digital Certificates, Digital Signature Software

Índice

Lista de Figuras

Lista de Tabelas

Lista de Gráficos

Lista de Siglas e Acrónimos

AMA	Agência para a Modernização Administrativa
CA	Certificate Authority
CAdES	CMS Advanced Electronic Signatures
CC	Cartão de Cidadão
CMD	Chave Móvel Digital
e-ID	Identificação Eletrónica
EC	Entidades Certificadoras
ECC	Criptografia de Curva Elíptica
ESTG	Escola Superior de Tecnologia e Gestão
IdP	Identity Provider
LTV	Long Term Validation
PDF	Portable Document Format
PEPS	PEPS Pan-European Proxy Service
PGP	Pretty Good Privacy
PIN	National Identification Number
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
S/ MIME	Secure / Multipurpose Internet Mail Extensions
SP	Service Provider
STORK	Secure idenTity acrOss boRders linked
TAS	Trusted Archival Services
TI	Tecnologias de Informação
TSA	TimeStamp Authority
XAdES	XML Advanced Electronic Signatures
XML	Extensible Markup Language
XML-DSIG	XML Digital Signatures

1. Introdução

O presente projeto tem como matéria de estudo as assinaturas eletrónicas, mais precisamente as assinaturas digitais e as assinaturas qualificadas assim como a identificação eletrónica. Consistindo desta forma, investigar diferentes formatos existentes de assinaturas bem como perceber qual o ponto de situação na utilização da identificação eletrónica bem como a pesquisa acerca dos desenvolvimentos em países europeus e ferramentas e/ou tecnologias que são utilizadas para o efeito. Este tema encontra-se inserido na área da segurança informática com o papel de assegurar a qualidade da informação digital.

Se pensarmos na evolução tecnológica e no processamento eletrónico dos documentos, poderemos colocar a seguinte questão "Porque precisamos das assinaturas digitais?" se imaginarmos um documento que tem um valor legal, este documento pode conter determinadas informações importantes sobre direitos e obrigações, sendo que nesse caso devemos garantir a autenticidade do mesmo. Dado que nestas circunstâncias não queremos que as pessoas neguem os compromissos que assinaram. Para além disso, este documento provavelmente deve ser enviado por correio, visualizado e armazenado/guardado por diferentes partes. Seguindo por diferentes sítios no fluxo de trabalho, em certos e determinados momentos este pode ser alterado seja de forma voluntária como por exemplo, adicionar uma assinatura extra ou involuntária devido a um erro de transmissão ou realizada de forma deliberada, em que alguém quer criar uma falsificação do documento original (Lowagie, 2012).

Tendo como base o artigo de (Blythe, 2005), ao celebrarmos um contrato online são possíveis quatro graus de segurança, em que o primeiro nível existiria se uma parte aceitasse uma oferta tendo apenas clicado no botão "Concordo", ou mais conhecido "*I agree*" no ecrã de um computador. O segundo nível de segurança seria incidido se informação que não deve ser divulgada fosse partilhada entre duas partes contratantes, por exemplo, uso de uma palavra-passe ou número de cartão de crédito para verificar a intenção de um cliente de que determinados serviços seriam adquiridos. O terceiro nível é alcançado com a biometria, em que esses métodos envolvem um atributo físico único da parte contratante e estes são extremamente difíceis de replicar por um pretenso ciberataque. O quarto nível são as Assinaturas digitais com tecnologia PKI, em que a assinatura digital é considerada o quarto

nível de segurança dado que é mais complexa que a biometria. Sendo por muitas vezes assumida por leigos de que esta é meramente uma versão digitalizada da assinatura manuscrita. Este não é o caso, a assinatura digital engloba todo o documento em que a tecnologia utilizada com a mesma é conhecida como Public Key Infrastructure ou "PKI".

Para além de mais vantajoso, os serviços de segurança sendo eles a confidencialidade, integridade e disponibilidade são de grande relevância relativamente à segurança e partilha de informação. Em que, todos nós somos responsáveis pela segurança da informação e por sua vez também temos a responsabilidade de proteger os nossos dados assim como os que nos são confiados. A confidencialidade passa por assegurar que a informação é acessível somente por pessoas devidamente autorizadas, sendo o acesso a essa mesma informação restrito a utilizadores legítimos. A integridade garante a veracidade e corroboração da informação, em que o conteúdo da informação não pode ser modificado de forma inesperada. A disponibilidade é caracterizada por assegurar o acesso à informação e bens associados por alguém devidamente autorizado. No serviço de segurança designado de disponibilidade consta a autenticação e o não repúdio, em que estes incluem o controlo de acesso, autenticação de entidades, autenticação de mensagens tendo por sua vez como mecanismo de segurança associado a assinatura digital em que esta depende da integridade e certificação. De forma a que se incuta a responsabilidade pela segurança da informação que se pretende partilhar com outro individuo e/ou entidade para que não exista a possibilidade de que a informação seja alvo de qualquer alteração inesperada.

A criação do Cartão de Cidadão, documento de identificação português foi desenvolvido no âmbito do projeto de Modernização da Administração Pública, tendo este projeto proporcionado novas informações e funcionalidades relativas ao cidadão (Barbosa A. , 2010) (Rito, 2018). Com o desenvolvimento deste projeto, proporciona-se ao cidadão comum a possibilidade de realização da assinatura digital qualificada em documentos através da utilização do seu documento de identificação. A possibilidade de assinar documentos digitalmente trouxe consigo o crescente desenvolvimento de aplicações que permitem assinar e/ou validar a assinatura digital, como por exemplo: Acrobat Reader, aCCinaPDF e a Autenticação.GOV sendo estes os softwares que optei por comparar. A utilização das assinaturas digitais com o cartão de cidadão ajuda a resolver muitos dos problemas associados à gestão documental, ainda que possa existir falta de conhecimento sobre a sua correta utilização pelos utilizadores.

Pelo que, desta forma a relevância da realização deste estudo passa por compreender as potencialidades da assinatura digital, tecnologias e ferramentas existentes que englobam o mundo das assinaturas eletrónicas bem como a comparação dessas mesmas ferramentas e aspetos das assinaturas. Dado que por sua vez, ao se analisar e perceber quais as iniciativas que foram realizadas noutros países da união europeia podemos compreender se existe um crescimento na sua utilização bem como na autenticidade da informação partilhada. Desta forma, estes poderão promover a progressão e a exponente utilização das assinaturas digitais bem como da identificação eletrónica. Revela-se também importante perceber qual a situação atual e futura das assinaturas digitais de forma a analisar possíveis vulnerabilidades e riscos no ponto de vista de segurança. Sabendo que é imprescindível que toda a informação digital seja devidamente protegida e tenha o seu valor de confiança, dado que o mundo digital está em crescimento e faz parte do nosso dia-a-dia.

1.1. Objetivos

O objetivo principal deste projeto consiste no estudo comparativo entre aplicações de Assinatura Digital e respetivas assinaturas. Sendo que desta forma, dividimos este grande objetivo nos seguintes:

- Compreender quais os dados que estão a ser utilizados na realização da assinatura digital;
- Estudar as assinaturas eletrónicas e a autenticação com eID;
- Conhecer o funcionamento dos mecanismos que verificam a integridade das assinaturas digitais;
- Analisar os formatos de assinatura existentes e projetos europeus bem como tecnologias usadas para realização da assinatura digital;
- Comparar ferramentas de assinatura digital e aspetos de assinatura;
- Avaliar e perceber qual o futuro das assinaturas digitais em Portugal;

1.2. Metodologia do trabalho

O desenvolvimento do presente projeto corresponde essencialmente a um trabalho de investigação tendo sido elaborada com recurso a pesquisa bibliográfica tendo por sua vez recorrido à legislação referente às assinaturas eletrónicas abordadas. A parte prática relativa

ao estudo comparativo corresponde à instalação de três softwares (autenticação.gov, aCCinaPDF e Abode Reader) e realizar uma comparação relativa às suas funcionalidades e características aquando se efetua digitalmente a assinatura de um documento.

Numa fase de termos técnicos era importante abordar determinados conceitos como o funcionamento das chaves públicas/ gestão da chave e do certificado, certificados digitais bem como a criptografia e tipos de algoritmos criptográficos, entre outros. Sendo o nosso caso de estudo a assinatura digital também é necessário compreender e investigar qual a legislação existente e que se aplica neste contexto e no do cartão de cidadão. Numa fase posterior, realização de pesquisa de forma a compreender qual o investimento em e-ID que têm sido realizados noutros países da Europa bem como qual o estado do projeto STORK, sendo a Estónia o país que apresenta um maior desenvolvimento no contexto da identificação eletrónica. Numa fase final, instalar três softwares que permitem assinar digitalmente documentos e compreender quais as suas diferenças realizando a comparação aquando realizamos o processo de assinatura do documento. Concluindo com uma discussão sobre qual o ponto atual e futuro das assinaturas digitais em Portugal.

1.3.Estrutura do trabalho

O presente projeto encontra-se organizado da seguinte forma:

No capítulo dois é apresentada uma introdução às assinaturas eletrónicas dando a conhecer as diferentes modalidades de assinatura, referindo principalmente o caso da assinatura digital e assinatura eletrónica qualificada.

No capítulo três são descritos os formatos das assinaturas em documentos e apresentada a identificação eletrónica bem como o projeto STORK.

No capítulo quatro refere-se o caso de Portugal e a assinatura digital, analisando o Cartão de Cidadão e a Chave Móvel Digital.

No capítulo cinco são apresentadas três ferramentas de assinatura digital, a aplicação autenticação.gov, o aCCinaPDF e o Adobe Reader realizando uma comparação às funcionalidades dos mesmos.

No capítulo seis é realizada a discussão sobre o ponto atual e futuro das assinaturas digitais em Portugal.

Por último, no capítulo sete são apresentadas as respetivas conclusões do presente projeto.

2. Introdução às Assinaturas eletrónicas

Em 1999, com a aprovação do Decreto-Lei n. º 290-D/99, de 2 de Agosto, "dá-se, em Portugal, o primeiro passo no sentido da consagração legal das assinaturas electrónicas, acolhendo-se, designadamente, as soluções avançadas no quadro da União Europeia, na proposta de diretiva do Parlamento Europeu e do Conselho, relativa a um quadro legal comunitário para as assinaturas electrónicas." Sendo referenciado no mesmo decreto que "As redes electrónicas abertas, como a Internet, têm assumido uma importância crescente na vida quotidiana dos cidadãos e dos agentes económicos, proporcionando uma teia de relações comerciais globais. Para aproveitar da melhor forma estas oportunidades, urge criar um ambiente seguro para a autenticação electrónica. Na realidade, as comunicações e o comércio electrónicos exigem assinaturas electrónicas e serviços a elas associados que permitam a autenticação electrónica dos dados. As assinaturas electrónicas possibilitam ao utente de dados enviados electronicamente que verifique a sua origem (autenticação), bem como se os dados foram alterados (integridade). Em matéria de assinatura electrónica, o presente diploma assenta no modelo tecnológico ora prevalecente: a assinatura digital produzida através de técnicas criptográficas. Como se depreende dos estudos disponíveis sobre tecnologias de assinaturas digitais baseadas na criptografia de chaves públicas, a assinatura digital constitui, neste momento, a técnica mais reconhecida de assinatura electrónica, apresentando o mais elevado grau de segurança para as trocas de dados em redes abertas. E é esta constatação do estado da tecnologia que tem levado as experiências legislativas estrangeiras a privilegiar esta forma de assinatura electrónica."

Numa fase inicial de contextualização e de forma a que possamos compreender que tipos de assinaturas existem e o que as caracterizam, podemos guiarmo-nos pelo Decreto-Lei n.º 62/2003 de 3 de Abril. O presente decreto-lei visa compatibilizar o regime jurídico da assinatura digital estabelecido no Decreto-Lei n.º 290-D/99, de 2 de Agosto, com a Diretiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas eletrónicas. Este decreto-lei por sua vez estabelece e apresenta ao leitor o tipo de assinaturas existentes, sendo por sua vez apresentadas as seguintes modalidades de assinaturas eletrónicas como se pode observar na figura 1: a assinatura eletrónica, a assinatura eletrónica avançada, assinatura digital e a

assinatura eletrónica qualificada, sendo que estas correspondem a diferentes graus de segurança e fiabilidade.

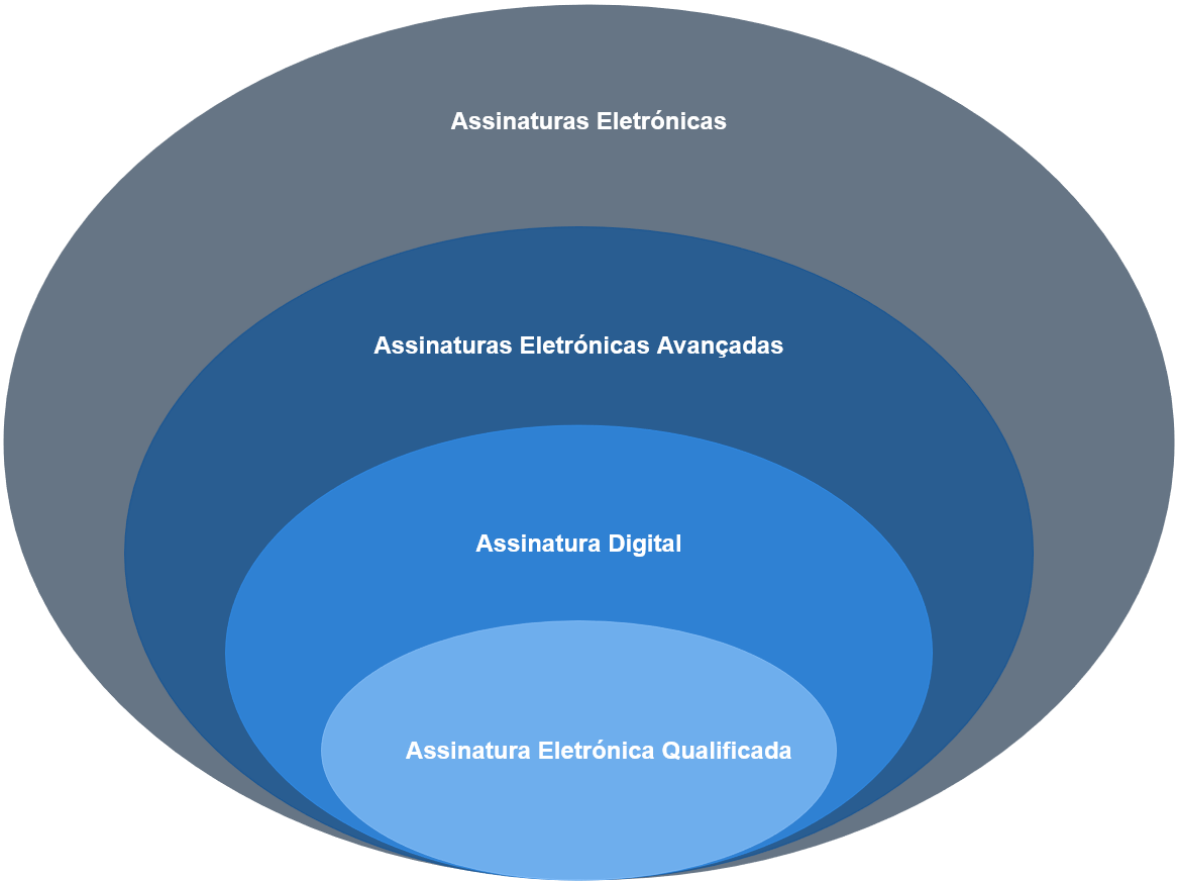


Figura 1 - Modalidades de assinaturas eletrónicas

Baseado no Artigo 2º decreto anteriormente referenciado, conseguimos ter uma base para definição e compreensão do que é uma assinatura eletrónica e quais os tipos de assinatura bem como o que as diferencia. Inicialmente e de forma mais abrangente são nos apresentadas as assinaturas eletrónicas, que correspondem "ao resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico;" Sendo esta uma assinatura simples que consiste numa assinatura constituída pelo nosso nome como forma de nos identificar, como no caso de uma assinatura de e-mail onde colocamos o nosso nome para que o destinatário saiba que fomos nós a enviar a mensagem.

Em segundo e de forma a identificar essas mesmas diferenças compreende-se que a assinatura eletrónica avançada corresponde à assinatura eletrónica que preenche determinados requisitos, sendo esses requisitos os seguintes:

- "Identifica de forma unívoca o titular como autor do documento;
- A sua aposição ao documento depende apenas da vontade do titular;
- É criada com meios que o titular pode manter sob seu controlo exclusivo;
- A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste;"

Começando a especificar as características e respetivas distinções para que possamos chegar ao foco do nosso estudo, as assinaturas digitais englobam em si as assinaturas eletrónicas qualificadas. Ou seja, tendo como base de referência as assinaturas eletrónicas desta forma especificando procedimentos em que as mesmas nos conduzem às assinaturas digitais e qualificadas que nos permitem um grau de segurança diferente para as trocas de informação em redes abertas.

2.1.O caso da Assinatura digital

"A prática de Assinaturas acompanhou a Humanidade, basicamente desde a invenção da escrita, por isso é natural que queiramos transpor o mesmo conceito para o novo mundo digital. A esse novo conceito de assinatura, deu-se o nome de Assinatura Digital" (Gomes, 2015). A assinatura digital é uma "modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura".

As assinaturas digitais são ferramentas muito importantes para implementar sinais seguros e corretos, dado que hoje em dia a assinatura manuscrita está de certa forma ultrapassada. À medida que o comércio eletrónico aumenta, por sua vez também aumenta a necessidade de um grau superior de autenticação. Pensemos no seguinte exemplo, a assinatura da Alice num contrato que têm com o Bruno. O Bruno não só tem que saber que a Alice é a outra assinante e que realmente está a assinar o contrato, como ele também deve ser capaz de provar a um terceiro (chamado de juiz) que a Alice o assinou e que o contrato que ele apresenta não foi alterado desde que a Alice assinou o mesmo. Esta construção é designada de assinatura

digital que autentica tanto a origem assim como o conteúdo de uma determinada mensagem de forma que esta é provada a um terceiro (Bishop, 2004).

Como referido anteriormente no Artigo 2º do Decreto-lei 62/2003 podemos analisar as definições dadas para os diferentes tipos de assinaturas eletrónicas, sendo que "a assinatura digital é baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes." O desenvolvimento mais importante do trabalho realizado sobre a criptografia de chave pública é a assinatura digital. A assinatura digital disponibiliza um conjunto de recursos de segurança que seriam difíceis de implementar de qualquer outra maneira (Stallings, 2017). Podendo desta forma completar essa informação adquirida com os objetivos da mesma. O objetivo das assinaturas digitais passa pela garantia de assegurar a autoria de uma mensagem perante terceiros, de forma que aquando uma mensagem for assinada digitalmente esta deverá ser associada a uma e uma só entidade e a assinatura deverá poder ser validada universalmente (Zuquete, 2013).

Ainda tendo como referência o artigo 2º do Decreto-Lei n.º 62/2003, é-nos possível identificar os elementos que fazem parte do regime de uma assinatura digital, sendo eles:

- A existência de um par de chaves criptográficas, pública e privada;
- A utilização da chave privada para geração da assinatura digital;
- A correspondência necessária da chave privada à chave pública;
- A emissão de um Certificado que contenha a chave pública;
- A emissão de um Certificado que contenha a chave pública, por uma entidade certificadora credenciada nos termos do diploma;
- A validade do Certificado, quer quanto à sua emissão, quer por não estar suspenso, nem revogado, nem caduco.

Distribuição/gestão da chave pública e do certificado

A base da infraestrutura da chave pública assenta na criptografia assimétrica com um par de chaves, pública e privada. A chave pública é normalmente distribuída sob a forma de certificado, enquanto que a chave privada é um item separado com uma estrutura própria e distinta que deve ser protegida de ser revelada a terceiros não autorizados quando nela é transportada, utilizada e armazenada (Mason, 2017). Com base no Decreto-Lei N.º 290-D/99 de 2 de Agosto, regime jurídico dos documentos eletrónicos e da assinatura eletrónica, sob

consulta do Capitulo I mais precisamente do Artigo 2º podemos ter em conta as seguintes caraterísticas e definições para chave privada como "elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública;". Sendo a chave pública caracterizada como o "elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves." Por sua vez e assim que uma pessoa subscreve uma assinatura digital, uma série de questões que são referidas como gestão do ciclo de vida, entre outros termos, devem ser abordadas. Independentemente do nome dado ao processo, devem existir procedimentos para criar o certificado e o par de chaves, verificar a identidade do requerente, distribuir o certificado e cancelar o certificado no final do seu período de validade ou antes, caso este seja comprometido. A qualidade do software, a conceção da rede e a gestão do sistema de segurança afetam a forma como as chaves e o certificado são geridos e armazenados. Isto é importante, porque uma assinatura digital não é computorizada pelo utilizador, mas sim pelo software. O software de um computador irá executar a tarefa segundo as instruções de um utilizador, mas o software não está em condições de identificar se as instruções vêm de um utilizador legítimo ou por outro lado se os sinais vêm de um software malicioso não autorizado que se tenha incorporado com sucesso no computador desse mesmo utilizador (Mason, 2017).

Relativamente ao certificado, quando a autoridade certificadora tiver verificado a identidade do indivíduo ou entidade a seu contento, eles emitirão um certificado. Este é um registo de software que afirma a ligação de uma chave pública a uma pessoa ou entidade empresarial identificada. Não se segue que uma autoridade de certificação irá realizar esta tarefa. Há uma série de razões para isso. Primeiro, o custo de desenvolver uma infraestrutura administrativa adequada com a experiência relevante será caro. Pode, portanto, não ser possível justificar o custo em termos comerciais. Em segundo lugar, há uma série de organizações que já possuem a perícia relevante, tais como bancos e agências de referência de crédito. Embora a base de dados que estas organizações utilizam possa ser imperfeita, no entanto, faz todo o sentido económico não replicar um serviço existente. Isto geralmente significa que existe uma camada adicional de contato onde uma autoridade de certificação emite um certificado. Em primeiro lugar, a autoridade de registo tomará medidas para verificar a identidade da pessoa ou entidade legal que procura um certificado. Após a confirmação da identidade pela autoridade de registo, a autoridade de certificação emitirá então um certificado. Assim, um

nível adicional de complexidade é adicionado à mistura que envolve a ligação entre a pessoa ou entidade legal que procura um certificado e a subsequente concessão do certificado. O próximo ponto a ponderar é a entidade que gera a chave da autoridade de registo. Quem gera a chave da autoridade de registo também estará envolvido na matriz contratual. Com toda probabilidade, existirá uma relação contratual entre a autoridade de certificação e a autoridade de registo, e o contrato preverá a responsabilidade e as garantias entre cada entidade. Onde a responsabilidade falhará em caso de disputa dependerá das circunstâncias particulares do caso (Mason, 2017).

Tem por base (Zuquete, 2013) refere as infraestruturas de gestão das chaves públicas sendo que ao conjunto das Entidades Certificadoras existentes num dado contexto, à sua interligação com cadeias de certificação e ao conjunto de políticas e de mecanismos de software e hardware usados para gerir os certificados, é vulgar associar a sigla PKI (*Public Key Infrastructure*). Uma PKI tem diversas tarefas a seu cargo, as seguintes:

- Definir políticas de criação de pares de chaves assimétricas de pessoas ou serviços;
- Definir políticas de emissão de certificados de chaves públicas;
- Definir políticas de emissão de certificados de revogação de chaves públicas;
- Definir cadeias de certificação;
- Criar pares de chaves assimétricas se tal for imposto por uma política e de acordo com as regras impostas pela mesma;
- Emitir certificados de chaves públicas de entidades, após prova adequada de associação entre as chaves e as entidades;
- Distribuir publicamente certificados de chaves públicas emitidos;
- Distribuir publicamente certificados de revogação de chaves públicas;

As Entidades Certificadoras são a principal componente operacional das PKI, sendo que por essa razão, muitas vezes usa-se a sigla PKI para indicar o conjunto de tecnologias de software e hardware utilizadas para concretizar uma Entidade Certificadora.

Para distribuição das chaves-publicas são-nos disponibilizados dois tipos de distribuição, o centralizado baseado em certificados digitais, sendo que neste contexto apresenta-se uma maior relevância relativa aos certificados X509 e o tipo descentralizado associado e caracterizado pelo OpenPGP. No caso das assinaturas digitais, o mais relevante é a

centralização dado que é tipo que referencia os certificados digitais e estes são relevantes neste contexto.

Distribuição centralizada – Os certificados X509

A recomendação X.509 da ITU-T faz parte da série X.500 de recomendações que definem um serviço de diretório. O diretório é, na verdade, um servidor ou conjunto distribuído de servidores que mantém uma base de dados de informações sobre os utilizadores. As informações incluem um mapeamento do nome do utilizador para o endereço da rede, bem como outros atributos e informações sobre os utilizadores. X.509 define uma estrutura para o fornecimento de serviços de autenticação pelo diretório X.500 para os seus utilizadores, este mesmo diretório pode servir como um repositório de certificados de chave pública do tipo anúncio público, diretório disponível publicamente, autoridade de chave pública e certificados de chave pública. Cada certificado contém a chave pública de um utilizador e é assinado com a chave privada de uma autoridade de certificação de confiança. Além disso, o X.509 define protocolos alternativos de autenticação baseados no uso de certificados de chave pública. O X.509 é um padrão importante porque a estrutura do certificado e os protocolos de autenticação definidos no X.509 são utilizados em vários contextos. Por exemplo, o formato de certificado X.509 é utilizado em S/MIME, Segurança IP e SSL/TLS. O X.509 foi inicialmente emitido em 1988, a norma foi subsequentemente revista em 1993 para abordar algumas das preocupações de segurança documentadas em [IANS90] e [MITC90]. A norma encontra-se atualmente na versão 7, emitida em 2012. X.509 é baseado no uso de criptografia de chave pública e assinaturas digitais. O padrão não dita o uso de um algoritmo específico de assinatura digital nem uma função específica de hash. A figura 2 ilustra o esquema geral do X.509 para que seja gerado um certificado de chave pública. O certificado para a chave pública do Bob inclui informação de identificação única para Bob, a chave pública do Bob, e informação de identificação sobre a CA, mais outras informações como explicado posteriormente. Esta informação é então assinada através da computação de um valor *hash* da informação e da geração de uma assinatura digital usando o valor *hash* e a chave privada da Autoridade de Certificação. X.509 indica que a assinatura é formada pela criptografia do valor de *hash*. Isto sugere o algoritmo criptográfico assimétrico. No entanto, a versão atual do X.509 não dita um algoritmo específico de assinatura digital. Se o esquema NIST DSA (Algoritmo de assinatura digital NIST) ou ECDSA (Algoritmo de assinatura

digital *Elliptic Curve*) for utilizado, então o valor *hash* não é encriptado, mas serve como entrada para um algoritmo de geração de assinatura digital.

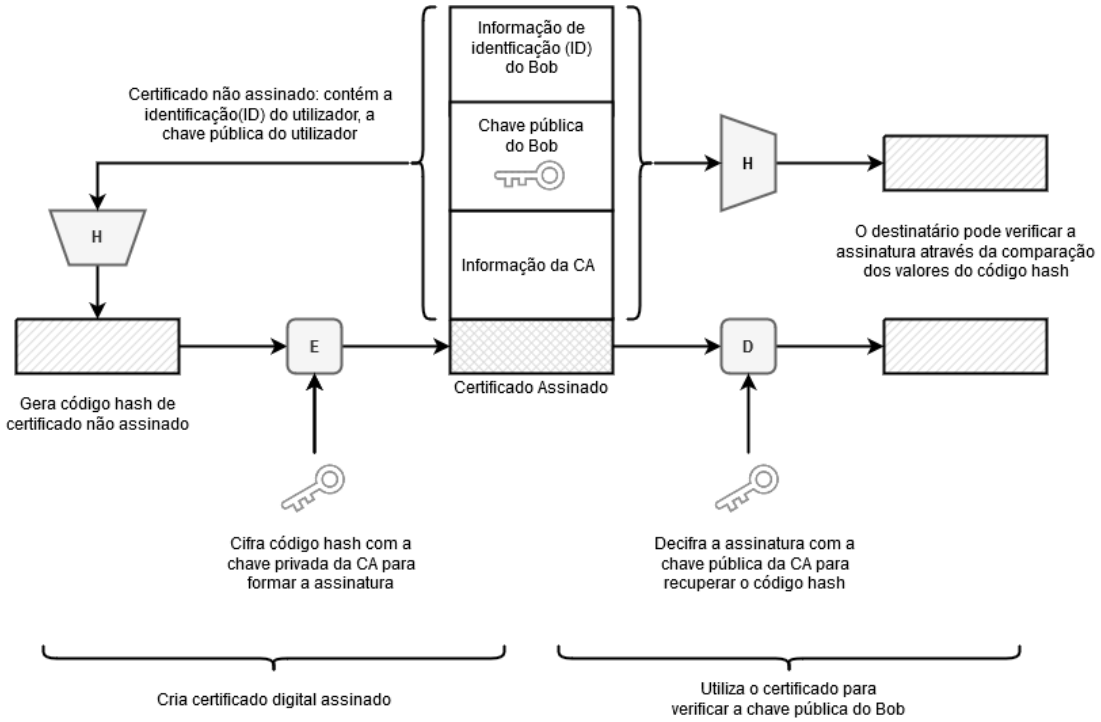


Figura 2 - Certificado de chave pública X.509 (Stallings, 2017)

Segundo (Stallings, 2017), o coração do esquema X.509 é o certificado de chave pública associado a cada utilizador. Estes certificados de utilizadores são assumidos como criados por alguma autoridade de certificação (CA) confiável e colocados no diretório pela CA ou pelo próprio utilizador. O servidor de diretório em si não é responsável pela criação de chaves públicas ou pela função de certificação, apenas fornece um local de fácil acesso para os utilizadores obterem certificados.

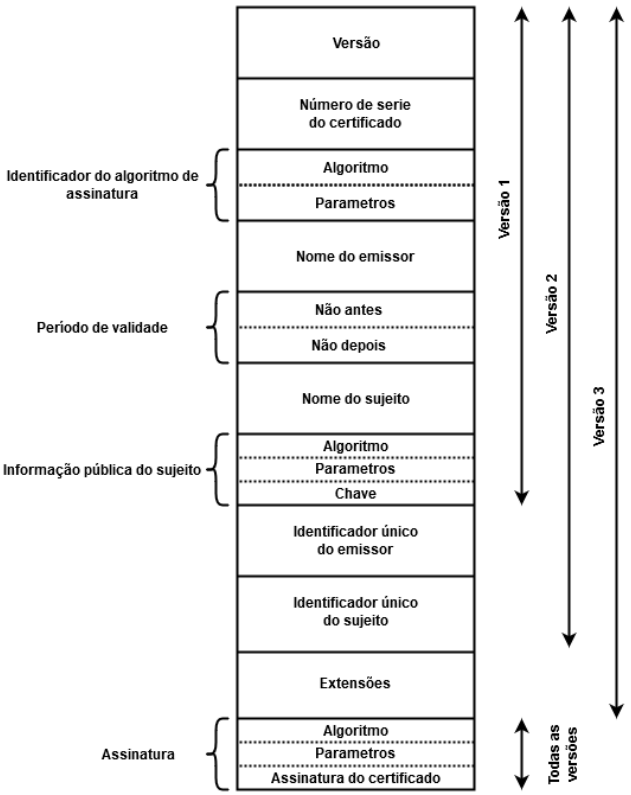


Figura 3 - Formato Certificado X509 (Stallings, 2017)

A figura 3 apresenta o formato geral do certificado, sendo que este inclui os seguintes elementos descritos em baixo tendo como constante referência a descrição e o trabalho realizado por (Stallings, 2017) :

- **Versão (*Version*):** Diferencia entre as sucessivas versões do formato do certificado; o padrão é a versão 1. Se o identificador único do emissor ou o identificador único do sujeito estiverem presentes, o valor deve ser a versão 2. Se uma ou mais extensões estiverem presentes, a versão tem de ser a versão 3. Embora a especificação X.509 esteja atualmente na versão 7, não foram feitas alterações aos campos que compõem o certificado desde a versão 3;
- **Número de série (*Serial Number*):** Um valor inteiro único dentro da Autoridade de Certificação emissora que está inequivocamente associado a este certificado;
- **Identificador do algoritmo de assinatura (*Signature algorithm identifier*):** O algoritmo utilizado para assinar o certificado juntamente com quaisquer parâmetros associados. Como esta informação é repetida no campo assinatura no final do certificado, este campo tem pouca, ou nenhuma, utilidade;

- **Nome do emissor (*Issuer Name*):** X.500 nome da Autoridade de Certificação que criou e assinou este certificado;
- **Período de validade (*Period of validity*):** Consiste em duas datas: a primeira e a última em que o certificado é válido;
- **Nome do sujeito (*Subject name*):** O nome do utilizador a quem se refere este certificado. Ou seja, este certificado certifica a chave pública do sujeito que possui a chave privada correspondente;
- **Informação pública do sujeito (*Subject's public-key information*):** A chave pública do sujeito, mais um identificador do algoritmo para o qual esta chave deve ser usada, juntamente com quaisquer parâmetros associados;
- **Identificador único do emissor (*Issuer unique identifier*):** Um campo opcional de cadeia de bits utilizado para identificar de forma exclusiva a Autoridade de Certificação emissora no caso de o nome X.500 ter sido reutilizado para diferentes entidades;
- **Identificador único do sujeito (*Subject unique identifier*):** Um campo opcional de *string* de bits utilizado para identificar de forma única o assunto no caso de o nome X.500 ter sido reutilizado para diferentes entidades;
- **Extensões (*Extensions*):** Um conjunto de um ou mais campos de extensão. As extensões foram adicionadas na versão 3 e são discutidas mais adiante nesta seção;
- **Assinatura (*Signature*):** Cobre todos os outros campos do certificado. Um componente deste campo é a assinatura digital aplicada aos outros campos do certificado. Este campo inclui o identificador do algoritmo de assinatura.

Distribuição Descentralizada – OpenPGP

O PGP (*Certificate Signature Chains*) é um programa de incentivo amplamente utilizado para fornecer privacidade para o correio eletrónico através da Internet, e para assinar ficheiros digitalmente. Utiliza uma infraestrutura de gestão de chaves públicas dos utilizadores baseada em certificados. Um certificado OpenPGP é composto de pacotes, em que um pacote é um registo com uma etiqueta descrevendo qual é o seu propósito. Um certificado contém um pacote de chave pública seguido por pacotes com zero ou mais assinaturas como refere (Bishop, 2004).

OpenPGP não inclui a chave pública do remetente com cada mensagem, portanto é necessário que os destinatários das mensagens OpenPGP obtenham separadamente a chave

pública do remetente a fim de verificar a mensagem. Muitas organizações disponibilizam chaves OpenPGP em *websites* protegidos por TLS, as pessoas que desejam verificar assinaturas digitais ou enviar mensagens criptografadas para essas organizações precisam de descarregar manualmente essas chaves e adicioná-las aos seus clientes do OpenPGP. As chaves também podem ser registadas nos servidores de chaves públicas OpenPGP, que são servidores que mantêm uma base de dados de chaves públicas PGP organizada por endereço de e-mail. Qualquer pessoa pode colocar uma chave pública nos servidores de chaves OpenPGP, e essa chave pública pode conter qualquer endereço de e-mail. Não há verificação das chaves OpenPGP, portanto os utilizadores devem usar a *Web-of-Trust* para decidir se confiam em uma determinada chave pública (Stallings, 2017).

O certificado PGP difere dos certificados X.509 de várias formas importantes. Ao contrário do X.509, uma única chave pode ter várias assinaturas enquanto que todas as chaves PGP Versão 4 são assinadas pelo proprietário, isto é chamado de "*self-signing*". Também ao contrário do X.509, uma noção de "confiança" é incorporada em cada assinatura, e as assinaturas de uma única chave podem ter diferentes níveis de confiança. Os utilizadores dos certificados podem determinar o nível de confiança para cada assinatura e agir em conformidade.

Devemo-nos lembrar de que um indivíduo pode gerar o seu próprio par de chaves públicas e privadas, utilizando software no seu computador. O indivíduo então disponibiliza à autoridade de certificação provas de sua identidade. O tipo de prova e o grau de prova dependerá da natureza do tipo de certificado exigido. Em qualquer caso, a identidade da pessoa e/ou entidade deve estar vinculada à chave pública. Ao confirmar a identidade de uma pessoa e/ou entidade jurídica, uma autoridade de certificação tenderá a cumprir os requisitos de um organismo reconhecido (Mason, 2017).

Criptografia e tipos de algoritmos criptográficos

Tendo como base a leitura (Mason, 2017), a criptografia é um método para ocultação do conteúdo de uma mensagem usado desde os tempos antigos até ao presente. e também é definida como um processo pelo qual uma mensagem de texto ou texto sem formatação é "disfarçada" suficientemente de forma a ocultar o seu conteúdo. Assim como um texto comum, uma mensagem de texto simples pode ser um fluxo de dígitos binários, um ficheiro de texto, um *bitmap*, um som gravado em formato digital, áudio de um vídeo ou filme bem

como qualquer outra informação formada em bits digitais. Quando uma mensagem é encriptada, ela é conhecida como cifrada. O procedimento oposto, ou seja, transformar o texto cifrado novamente em texto normal é designado de decifração. Em síntese, os sistemas criptográficos contemporâneos alteram um conjunto de símbolos que têm significado num segundo conjunto que não tem significado, por meio de um processo matemático.

Um princípio criptográfico é fundamental na autenticação, autorização e não-repudio na assinatura digital. O objetivo da assinatura digital passa por fornecer meios para a entidade vincular a sua identidade a uma informação. O processo de assinatura implica transformar a mensagem e algumas "informações secretas" detidas pela entidade numa marca designada de assinatura (A.J. Menezes, 1996).

A autenticação por si só tem pouco significado além de transmitir a ideia de que alguns meios foram fornecidos para garantir que as entidades são quem afirmam ser, ou que a informação não foi manipulada por partes não autorizadas. A autenticação é específica para o objetivo de segurança que se está a tentar alcançar. Exemplos de objetivos específicos incluem o controlo de acesso, autenticação de entidades, autenticação de mensagens, integridade de dados, não repúdio e autenticação chave (A.J. Menezes, 1996).

Como foi referido anteriormente, a criptografia é necessária para realizar várias funções, das quais a mais importante é a autenticidade sendo que existem outras que procuram assegurar uma comunicação segura (Mason, 2017) :

- **Autenticidade**: a chave pública do emissor é obtida a partir de um certificado digital, que a associa à identidade do seu titular. Esta associação é garantida pela assinatura digital de uma entidade certificadora. É com esta chave que depois se decifra o conteúdo. Se a comparação tiver sucesso, então só a chave privada correspondente à chave pública pode ter sido usada para cifrar o sumário do emissor (logo, confirma-se que foi este que produziu a assinatura). A autenticidade deve existir ao enviar ou receber informações ou até mesmo ao fazer um pedido, ambas as partes precisam de ter a certeza da origem da mensagem que estão a receber, o objetivo é corroborar a identidade do software que enviou os dados. A identidade de uma pessoa não pode ser confirmada, porque esta não faz parte do processo de comunicação, dado que o processo apenas envolve comunicações entre software;

- **Integridade**: através da utilização de uma função de síntese (*hash function* ou *digest function*) que é uma função matemática não invertível, que produz uma síntese de tamanho pré-definido a partir de um conjunto de dados de tamanho arbitrário. A probabilidade de haver dois conjuntos de dados iguais com a mesma síntese é muitíssimo reduzida. A comparação final das sínteses confirma que o conjunto não foi modificado, sendo útil para demonstrar a integridade da mensagem porque é importante saber se o conteúdo da mensagem foi adulterado;
- **Confidencialidade**: outros dos objetivos passa por providenciar a confidencialidade de um documento. No ambiente digital, a criptografia é usada como um substituto para a assinatura manuscrita e assim sendo é muitas vezes descrita como uma assinatura digital.
- **Não-repúdio** (de criação ou origem): quando se estabelece a autenticação do emissor através da relação da chave pública com a privada, este não pode negar a autoria dos dados (ou pelo menos o seu conhecimento, no momento de assinar), partindo do princípio que só ele tem acesso à sua chave privada. Também é importante garantir que determinada chave pública pertence realmente ao emissor (para depois se poder determinar a posse da chave privada). É esse o papel do certificado digital, sendo fundamental a confiança depositada na entidade certificadora que o emite. Fornece-nos uma garantia, na medida do tecnicamente possível, que demonstre que o software emana de uma fonte conhecida. O objetivo é uma tentativa de vincular os utilizadores a ações específicas para que de tal forma, se eles negarem a tomar a ação ou demonstrarem a intenção de enganar ou de que por sua vez foram negligentes ao não assegurar adequadamente o uso da sua chave privada. No livro de (Mason, 2017) o autor utiliza a palavra honestidade, no entanto esta não é a melhor palavra para descrever o que se pretende e do ponto de vista técnico o termo correto é "não-repudio", tendo sido assim designada a função anteriormente descrita.

Existem diferentes tipos de não-repudio: não-repudio de origem que impede que a entidade que enviou mensagem ou documento negue que a enviou e não-repudio de recebimento quando uma entidade não pode negar não ter recebido uma mensagem ou documento. Outros tipos de não-repudio incluem não-repudio de criação, não-repudio de entrega e não repudio de aprovação (Mason, 2017).

Na leitura (Ponka), para possibilitar o não-repúdio no ambiente digital, todas as partes devem poder se autenticar. As assinaturas digitais são uma das principais tecnologias propostas para isso e o não repúdio é um requisito essencial.

Existe uma distinção definitiva entre o uso legal e técnico do termo "não-repudio". No contexto técnico, significa que nem o remetente nem o destinatário podem negar uma mensagem transmitida, neste caso temos o não-repudio da origem e entrega. A assinatura digital oferece o "não-repudio", ou seja, o signatário não pode alegar mais tarde que não criou a assinatura, dado que é o único que tem acesso à chave privada e a assinatura não pode ser criada sem a mesma, portanto ele deve ter realizado a assinatura.

No sentido legal, um suposto signatário sempre pode repudiar uma assinatura que lhe foi atribuída. Os detalhes variam de país para país, mas em geral a base para um repúdio inclui pelo menos o seguinte: falsificação, conduta imprópria (por exemplo, intimidação, engano) da outra parte, fraude por terceiros. Por exemplo, se um contrato ou assinatura é uma falsificação, não há de todo contrato feito. Noutros casos há um contrato, mas este é inválido e, por sua vez não é eficaz. Em alguns casos, o contrato pode até ser válido, se a outra parte não tiver conhecimento e não deve estar ciente de fraude ou influência indevida por terceiros. Além disso, o erro de uma parte nem sempre torna possível o repúdio (contrato inválido), a menos que o erro possa ser atribuído à outra parte. O caso mais interessante é a alegada falsificação, em que o suposto signatário alega que ele não assinou o documento. Em outros casos, a assinatura em si não é repudiada, mas a sua eficácia.

De forma a garantir a autoria de uma mensagem por parte de terceiros, uma mensagem que seja assinada digitalmente deve ser associada a uma e uma só entidade. Assim sendo a criptografia assimétrica é a que melhor se adequa a este fim, uma vez que os pares de chaves pertencem apenas a uma entidade.

As leituras de (Zuquete, 2013) referem que os pares de chaves assimétricas são associados a pessoas, serviços ou servidores pelo que a componente privada só deve ser conhecida e usada pela entidade a que se encontra associada. Enquanto que a componente pública pode e deve ser ampla e publicamente divulgada para poder ser usada por qualquer entidade.

Suponhamos que o Bob quer enviar uma mensagem à Alice. Embora não seja de todo importante que a mensagem seja mantida em segredo, ele quer que a Alice tenha a certeza de que a mensagem é de facto dele. Para tal, Bob usa uma função de *hash* segura, como

SHA-512, para gerar um valor de *hash* para a mensagem que pretende enviar. Esse valor de *hash* juntamente com a chave privada do Bob serve como entrada para um algoritmo de geração de assinatura digital, que produz um bloco pequeno que funciona como uma assinatura digital. E então, Bob envia a mensagem com a assinatura anexada. Quando a Alice recebe a mensagem mais a assinatura ela (1) calcula um valor hash para a mensagem; (2) disponibiliza o valor de *hash* e a chave pública do Bob como entradas para um algoritmo de verificação de assinatura digital. Se o algoritmo retornar o resultado de que a assinatura é válida, a Alice tem a certeza de que a mensagem deve ter sido assinada pelo Bob.

Como ninguém tem a chave privada do Bob e, portanto, ninguém mais poderia ter criado uma assinatura que pudesse ser verificada para esta mensagem com a chave publica do Bob. Para além disso, é impossível alterar a mensagem sem acesso à chave privada do Bob, por isso a mensagem é autenticada tanto em termos de fonte como em termos de integridade dos dados (Stallings, 2017).

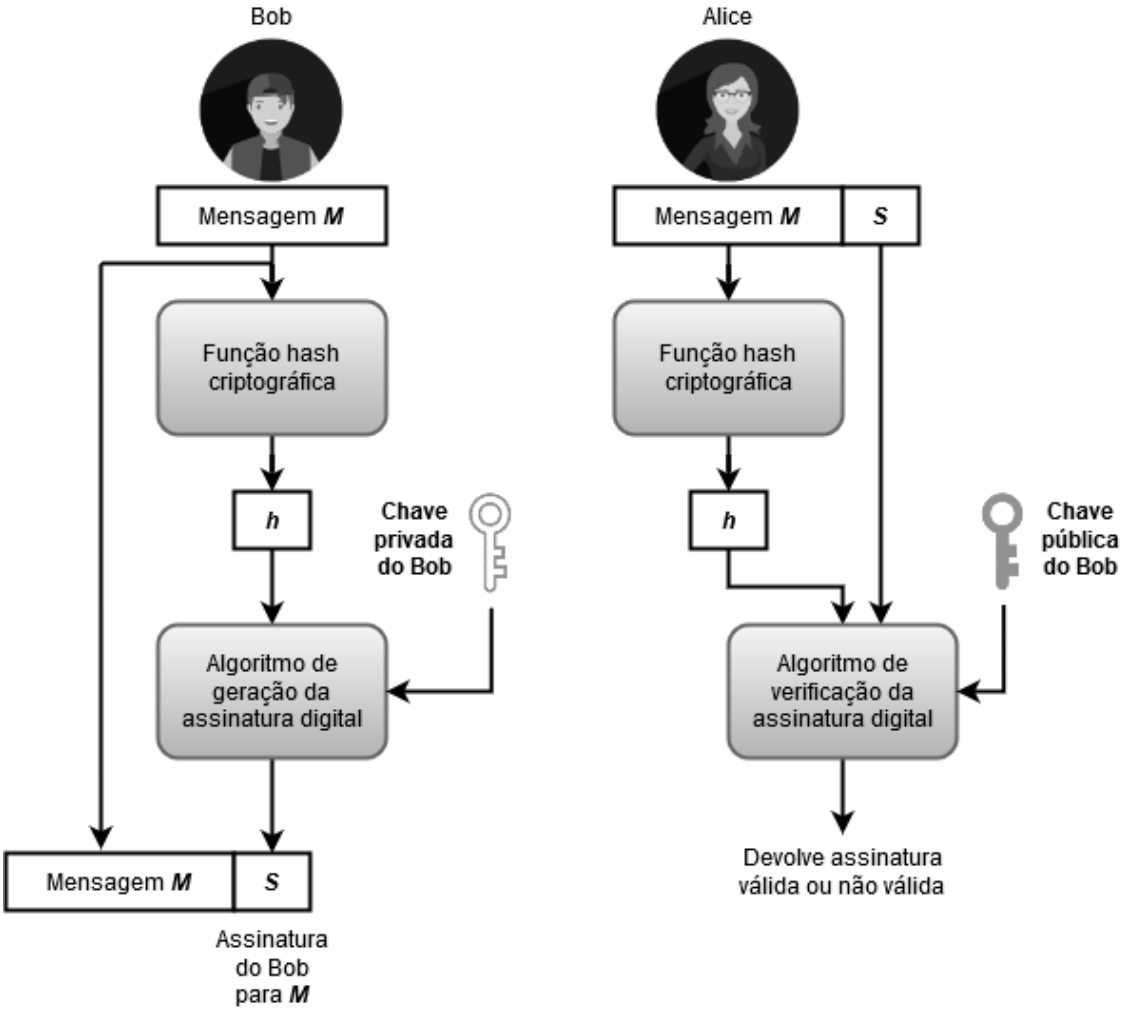


Figura 4 - Representação simplificada dos elementos essenciais do processo de assinatura digital (Stallings, 2017)

Na anterior figura 4 é apresentado um modelo genérico do processo de construção e utilização de assinaturas digitais.

Outro exemplo com base em (Bishop, 2004), de forma a perceber quando se trata ou não de uma assinatura digital. Seja ***m*** uma mensagem. Suponhamos que a Alice e o Bob partilham uma chave secreta **k**. A Alice envia ao Bob **m || { m }k** , ou seja, a mensagem e a sua codificação sob **k**. Primeiro, a Alice autenticou o conteúdo da mensagem, porque o bob decifra **{ m }k** e pode verificar se a mensagem corresponde à decifrada. Dado que só o Bob e a Alice sabem **k**, e o Bob sabe que não enviou a mensagem, então ele conclui que a mensagem veio da Alice. Ele autenticou a origem e a integridade da mensagem. No entanto, apenas com base na matemática o Bob não pode provar que não criou a mensagem visto que ele conhece a chave utilizada para criá-la. Portanto, este exemplo não é um caso de uma assinatura digital. A criptografia de chave pública veio resolver esta questão. Respetivamente temos que, ***dAlice*** e ***eAlice*** são as chaves privada e pública da Alice. A Alice envia a mensagem ao Bob **m || { m }*dAlice***. Antes o Bob pode autenticar a origem e o conteúdo de **m**, mas nesta situação um juiz é que deve determina que a Alice assinou a mensagem, dado que é ela que conhece a chave privada com a qual a mensagem foi assinada. O juiz apenas obtém ***eAlice*** e calcula **{{ m }*dAlice* } *eAlice***. Se o resultado for **m**, significa que a Alice a assinou. Ou seja, esta situação representa de facto uma assinatura digital. Uma assinatura digital disponibiliza o serviço de não-repúdio, para este exemplo consideramos o serviço de não-repúdio como sendo a incapacidade de negar que a chave criptográfica de alguém foi utilizada para produzir a assinatura digital.

Usar um sistema criptográfico simétrico com um grande número de utilizadores é difícil. As chaves não podem ser distribuídas através da rede de comunicações aberta, por isso têm de ser distribuídas de outras formas. Quando um membro deixa o grupo, todos os outros membros têm de redistribuir novas chaves. Assim, assumindo que uma chave separada é usada para cada par em um grupo, e se houver 10 pessoas membros do grupo, 45 chaves diferentes serão necessárias. O desenvolvimento do sistema criptográfico assimétrico, ou chave pública, ajuda a resolver este problema. Com este sistema, as chaves têm apenas um propósito: uma chave para encriptar e uma chave para decifrar. Dada uma chave suficientemente grande, a chave de decifração não pode ser calculada a partir da chave de criptografia dentro de um período de tempo útil (talvez vários séculos). Os algoritmos utilizados no sistema são normalmente chamados de 'chave pública' porque a chave de

encriptação é normalmente tornada pública. Qualquer pessoa pode usar a chave de encriptação para encriptar uma mensagem em texto simples, mas apenas a pessoa com a chave de desencriptação correspondente à chave de encriptação pode desencriptar a mensagem. A chave de encriptação é chamada de chave pública ou chave de encriptação pública, e a chave de desencriptação é chamada de chave privada, chave secreta ou chave de desencriptação privada. O sistema pode funcionar de duas maneiras (Mason, 2017).

As cifras assimétricas em termos operacionais apresentam como principal vantagem o facto de serem necessárias menos chaves para efetuar interações seguras, isto porque permitem uma relação de muitos para um. Ou seja, para realizar qualquer troca de dados confidencial entre qualquer par de N interlocutores só é preciso usar N chaves publicas dos interlocutores. Ainda assim têm como desvantagens o facto de serem pouco eficientes visto que se baseiam em operações matemáticas complexas. Relativamente a termos administrativos as situações associadas à utilização de criptografia assimétrica são: o confinamento rigoroso das chaves privadas aos seus legítimos detentores, a distribuição fidedigna de chaves públicas aos que as pretendem usar assim como a gestão do tempo de vida dos pares de chaves (Zuquete, 2013). Como exemplo de cifras assimétricas temos os algoritmos RSA e Elliptic Curve.

O trabalho pioneiro de Diffie e Hellman [DIFF76b] introduziu uma nova abordagem à criptografia e, na verdade, desafiou a criação de um algoritmo criptográfico que atendesse aos requisitos dos sistemas de chaves públicas. Vários algoritmos foram propostos para a criptografia de chaves públicas. Alguns destes, embora inicialmente promissores, revelaram-se quebráveis. Uma das primeiras respostas de sucesso ao desafio foi desenvolvida em 1977 por Ron Rivest, Adi Shamir e Len Adleman no MIT e publicada pela primeira vez em 1978 [RIVE78]. O esquema Rivest-Shamir-Adleman (RSA) tem sido desde então a abordagem de propósito geral mais amplamente aceite e implementada para a criptografia de chave pública. O esquema de RSA é uma cifra na qual o texto cifrado e o texto integral são inteiros entre 0 e n - 1 para alguns n. Um tamanho típico para n é 1024 bits, ou 309 dígitos decimais. Ou seja, n é inferior a 2^{1024}. RSA [756] é uma cifra de exponenciação. Exemplo, escolha dois grandes números primos p e q, e deixe n = pq. O *totient* φ(n) de n é o número de números inferior a n, sem fatores em comum com n. Para além de confidencialidade, a RSA pode fornecer dados e autenticação de origem. Se Alice cifra a sua mensagem utilizando a sua chave privada, qualquer um pode lê-la, mas se alguém a altera, o texto cifrado (alterado) não pode ser decifrado corretamente. A utilização de um sistema de chave pública proporciona

um tipo técnico de não-repúdio de origem. A mensagem é decifrada utilizando a chave pública de Alice. Como a chave pública é o inverso da chave privada, apenas a chave privada poderia ter decifrado a mensagem. Como Alice é a única que conhece esta chave privada, só ela poderia ter decifrado a mensagem. O pressuposto subjacente é que a chave privada da Alice não foi comprometida e que a chave pública com o seu nome realmente lhe pertence. Na prática, ninguém usaria blocos do tamanho aqui apresentado. A questão é que, mesmo que n seja muito grande, se um carácter por bloco for cifrado, a RSA pode ser quebrada usando as técnicas usadas para quebrar as clássicas cifras de substituição. Além disso, embora nenhum bloco individual possa ser alterado sem deteção (porque presumivelmente o atacante não tem acesso à chave privada), um atacante pode arranjar forma de reajustar blocos e alterar o significado da mensagem (Bishop, 2004) (Stallings, 2017).

A versão 2009 da FIPS 186 inclui uma nova técnica de assinatura digital baseada na criptografia de curvas elípticas, conhecida como ECDSA (Elliptic Curve Digital Signature Algorithm). A ECDSA está a desfrutar de uma aceitação crescente devido à vantagem de eficiência da criptografia de curvas elípticas, que proporciona uma segurança comparável à de outros esquemas com um comprimento de bits chave menor (Stallings, 2017).

Em primeiro, num ponto de visão geral do processo envolvido na ECDSA. Em essência, apresentam-se quatro elementos envolvidos.

1. Todos os participantes no esquema de assinatura digital utilizam os mesmos parâmetros globais de domínio, que definem uma curva elíptica e um ponto de origem na curva.
2. Um assinante deve primeiro gerar um par de chaves públicas e privadas. Para a chave privada, o assinante seleciona um número aleatório ou pseudoaleatório. Usando esse número aleatório e o ponto de origem, o assinante calcula outro ponto na curva elíptica. Esta é a chave pública do assinante.
3. Um valor *hash* é gerado para que a mensagem seja assinada. Usando a chave privada, os parâmetros de domínio e o valor de hash, é gerada uma assinatura. A assinatura consiste em dois inteiros, r e s.
4. Para verificar a assinatura, o verificador usa como entrada a chave pública do assinante, os parâmetros de domínio e os inteiros s. A saída é um valor v que é comparado com r. A assinatura é verificada se v = r.

A maioria dos produtos e normas que utilizam criptografia de chave pública para criptografia e assinaturas digitais utilizam RSA. Como (Stallings, 2017) refere, o comprimento da chave para uso seguro de RSA aumentou nos últimos anos, o que colocou uma maior carga de processamento em aplicações que utilizam RSA. Esta carga tem ramificações, especialmente para sites de comércio eletrônico que realizam um grande número de transações seguras. Um sistema concorrente que desafia a RSA: a criptografia de curva elíptica (ECC). O ECC está a aparecer nos esforços de padronização, incluindo o Padrão IEEE P1363 para Criptografia de Chave Pública. A principal atração do ECC, em comparação com a RSA, é que ele parece oferecer segurança igual para um tamanho de chave bem menor, reduzindo assim as despesas gerais de processamento. O ECC é fundamentalmente mais difícil de explicar do que a RSA ou Diffie- Hellman, e como escreve o autor, uma descrição matemática completa está além da abrangência do livro. Uma curva elíptica é definida por uma equação em duas variáveis com coeficientes. Para a criptografia, as variáveis e coeficientes são restritos a elementos em um campo finito, o que resulta na definição de um grupo finito abeliano. As curvas elípticas não são elipses. Elas são assim designadas porque são descritas por equações cúbicas, semelhantes às utilizadas para calcular a circunferência de uma elipse. Desta forma, este tipo de criptografia faz uso de curvas elípticas em que as variáveis e coeficientes são todos restritos a elementos de um campo finito.

Em comparação às assinaturas convencionais, pode referir-se que uma assinatura simples e a assinatura digital de um documento têm algumas semelhanças no sentido em que associa o autor ao documento e permite que tal associação seja validável perante terceiros. Sendo que, a assinatura digital garante a correção do documento, isto é, que o conteúdo presente no documento se mantém tal e qual quando o documento foi assinado anteriormente, o que com uma assinatura convencional não acontece.

Apresenta-se de seguida o processo de assinatura digital, o processo de Verificação da Assinatura Digital bem como um exemplo prático (SUBRAMANYA S.R., 2016) (Barbosa A. , 2010) (Guedes, 2008) (Carvalho, 2003) (Gomes, 2015) .

O Processo de Assinatura Digital consiste nas seguintes etapas apresentadas e encontra-se esquematizado na seguinte figura 5:

1. “O primeiro passo para a utilização de uma assinatura digital consiste na geração de um resumo do documento usando uma função de “Hash”. Estas funções matemáticas

geram uma mensagem de tamanho pré-definido, designado por valor de resumo, calculada com base no documento e têm a propriedade de, para uma mudança mínima no documento, gerarem mensagens muito diferentes. Para além disso, a probabilidade de documentos diferentes gerarem mensagens iguais é remota.

2. De seguida esse valor de resumo (que não passa de uma cadeia de caracteres), é encriptada usando a chave privada da entidade assinante.
3. O valor de resumo encriptado é associada à mensagem original, produzindo um novo documento: o documento assinado digitalmente."

Figura 5 - Criação da assinatura digital (SUBRAMANYA S.R., 2016)

"O Processo de Verificação da Assinatura Digital consiste em dois processos distintos em paralelo aquando a realização de uma assinatura digital, como podem ser observados na figura 6:

Processo A: Gerar o valor de resumo do documento recebido.

Processo B: Decifrar do valor de resumo da assinatura, usando a chave pública da entidade que assinou o documento.

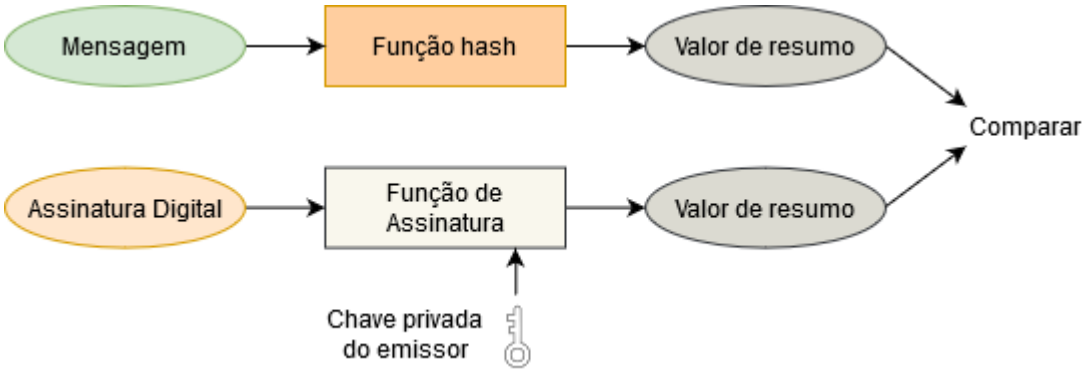


Figura 6 - Verificação da Assinatura digital (SUBRAMANYA S.R., 2016)

Comparação dos dois valores de resumo:

- Se forem iguais o documento encontra-se íntegro;
- Se forem diferentes o documento foi modificado desde o momento de assinatura.

Em ambos os casos o autor da assinatura é passível de ser identificado."

A assinatura digital é um elemento responsável que através de mecanismos e propriedades características permitem que esta seja considerada uma medida de segurança, o que no sentido do mundo digital e eletrónico ajuda-nos na proteção e combate a ataques tais como os seguintes:

- Personificação ("*Masquerading*"): Uma entidade fazer-se passar por outra, perante terceiros aquando da troca de mensagens.
- Alteração de Dados ("*Data Tampering*"): Modificação de alguns ou de todos os dados transmitidos numa sessão de comunicação entre entidades credíveis.

Como exemplo prático para compreensão do conceito das assinaturas baseada na explicação de (Lowagie, 2012) , de forma que será analisado um ficheiro pdf e identificar possíveis problemas relacionados à integridade do documento. É apresentado um simples documento pdf que contem apenas as palavras "Hello World" apresentado na figura 7 e o conteúdo foi posteriormente alterado, tanto as dimensões e os metadados do documento.

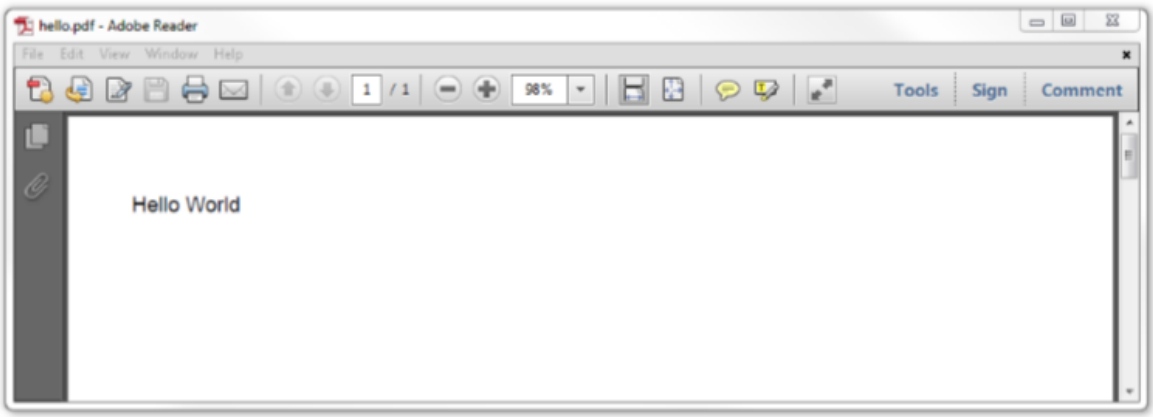


Figura 7 - Um simples ficheiro Hello World (Lowagie, 2012)

Foi substituído manualmente a palavra "World" por "Bruno" e as dimensões da página bem como o número da versão, como podemos ver na seguinte figura 8. Alterar um pdf manualmente irá comprometer o ficheiro em 99.9% dos casos. (Lowagie, 2012) realizou isto para provar que embora o pdf seja um formato de processamento de texto, não se destina à edição de um documento mesmo podendo fazê-lo não é recomendado. Com a introdução da assinatura digital pretendemos evitar exatamente a realização dessa alteração no documento.

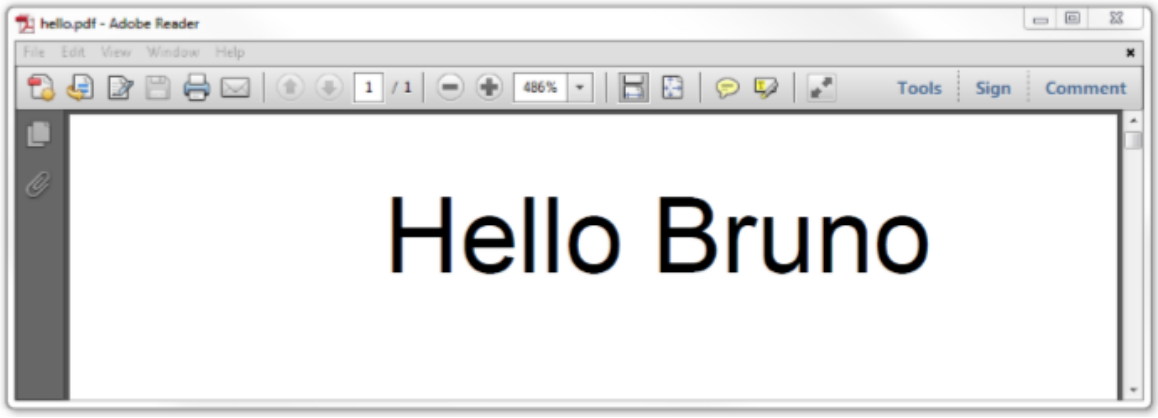


Figura 8 - Ficheiro Hello World alterado (Lowagie, 2012)

A figura 9 apresenta o documento Hello World que foi assinado digitalmente. A faixa azul indica-nos que o documento é "assinado e todas as assinaturas são válidas". O painel informa que o ficheiro foi "Assinado por Bruno Specimen" e mostra mais detalhes da assinatura. A marca verde de seleção significa que o documento não foi modificado desde que a assinatura foi aplicada e que a identidade do assinante é válida. Ou seja, documento assinado digital assinado digitalmente, com assinatura válida e documento intacto.

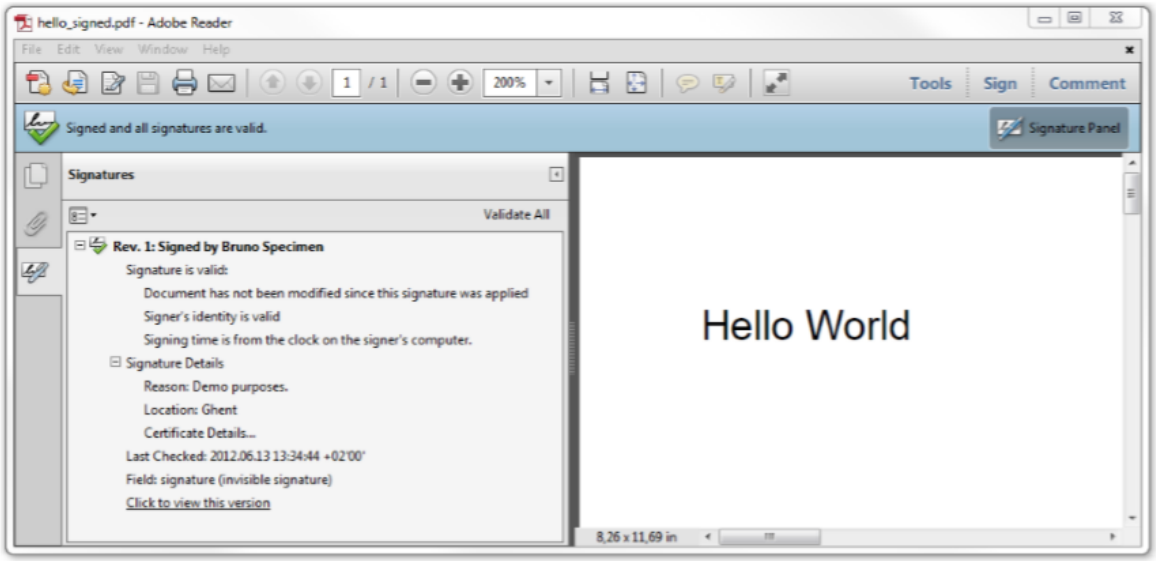


Figura 9 - Documento Hello World assinado (Lowagie, 2012)

Agora tendo sido alterados um dos bytes dentro do intervalo de bytes e tornando a assinatura inválida, o Adobe Reader mostra a cruz vermelha em vez da marca verde. A figura 10 apresenta-nos o que acontece ao substituir manualmente "World" por "Bruno". Neste caso com base nos detalhes sabemos que a identidade do assinante é válida, mas que o "Documento foi alterado ou corrompido desde que foi assinado." Ou seja, documento assinado digitalmente com a assinatura válida, mas modificado no seu código fonte.

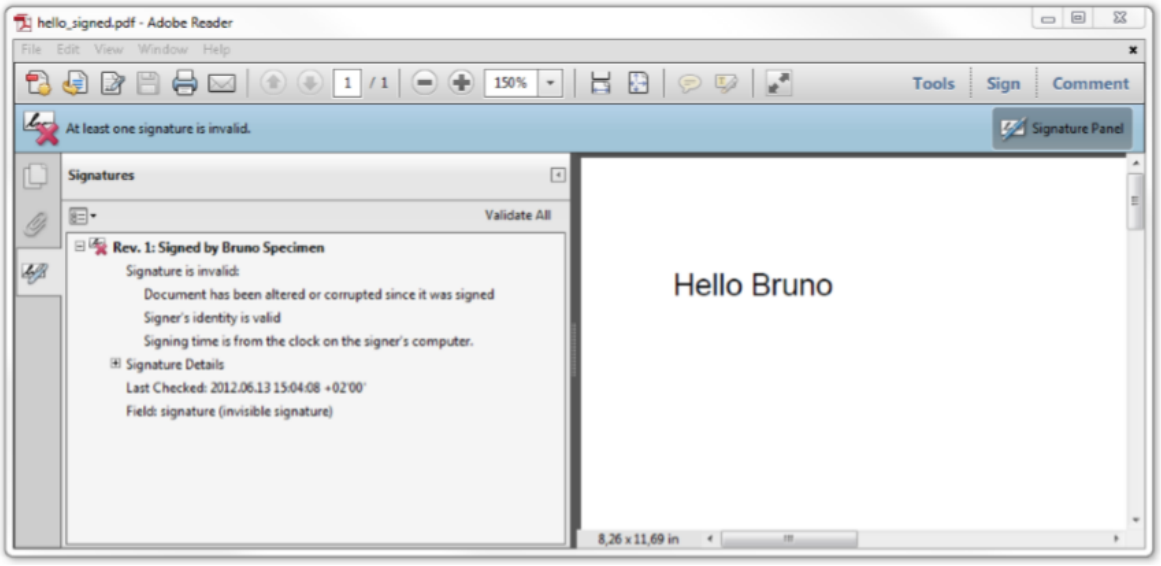


Figura 10 - Assinatura do documento invalidada (Lowagie, 2012)

2.2.Assinatura Eletrónica Qualificada

"Assinatura electrónica qualificada: assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura;"

Uma assinatura eletrónica qualificada é uma assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça a exigência de segurança idênticas às da assinatura digital, sendo a assinatura eletrónica qualificada baseada num certificado qualificado e criada através de um dispositivo seguro de criação de assinatura. Aspetos importantes a considerar neste tipo de assinatura são o facto de a mesma ser certificada por uma entidade, o que por sua vez traz uma maior garantia da segurança na utilização pelo seu utilizador ou cidadão, sendo que preserva a autenticidade e veracidade.

Tendo como perceção o funcionamento da assinatura eletrónica qualificada, o artigo 7.º do Decreto-Lei n. º 62/2003 de 3 de Abril descreve que:

1. A aposição de uma assinatura electrónica qualificada a um documento electrónico equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:

a) A pessoa que apôs a assinatura electrónica qualificada é o titular desta ou é representante, com poderes bastantes, da pessoa colectiva titular da assinatura electrónica qualificada;
b) A assinatura electrónica qualificada foi aposta com a intenção de assinar o documento electrónico;
c) O documento electrónico não sofreu alteração desde que lhe foi aposta a assinatura electrónica qualificada.

2. A assinatura electrónica qualificada deve referir-se inequivocamente a uma só pessoa singular ou colectiva e ao documento ao qual é aposta.
3. A aposição de assinatura electrónica qualificada substitui, para todos os efeitos legais, a aposição de selos, carimbos, marcas ou outros sinais identificadores do seu titular.
4. A aposição de assinatura electrónica qualificada que conste de certificado que esteja revogado, caduco ou suspenso na data da aposição ou não respeite as condições dele constantes equivale à falta de assinatura.

Com base na consulta do Decreto-Lei n. º 62/2003 de 3 de Abril, um certificado é um documento eletrónico que liga dados de verificação de assinatura ao seu titular e confirma a identidade desse mesmo titular. Dado que a assinatura qualificada é baseada num certificado qualificado, isto significa que, este certificado deve conter os elementos referidos do artigo 29. º do decreto-lei referenciado anteriormente e é emitido por uma entidade certificadora que reúne os requisitos definidos no artigo 24.º.

Para que o certificado seja caracterizado como qualificado, este deve conter as seguintes informações:

a) Nome e assinatura eletrónica qualificada da entidade certificadora, bem como a indicação do país onde se encontra estabelecida;
b) Dados de verificação de assinatura correspondentes aos dados de criação de assinatura detidos pelo titular;
c) Identificadores de algoritmos utilizados na verificação de assinaturas do titular e da entidade certificadora;
d) Limitações convencionais da responsabilidade da entidade certificadora;
e) Indicação de que é emitido como certificado qualificado.

A entidade certificadora é "uma entidade ou pessoa singular ou colectiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respectiva publicidade e presta outros serviços relativos a assinaturas electrónicas. E que por sua vez deve reunir os seguintes requisitos:

a) Estar dotada dos requisitos patrimoniais, ou seja, as entidades certificadoras privadas que sejam pessoas colectivas, devem estar dotadas de capital social no valor mínimo de 200000€ ou, não sendo sociedades, do substrato patrimonial equivalente;
b) Oferecer garantias de absoluta integridade e independência no exercício da actividade de certificação;
c) Demonstrar a fiabilidade necessária para o exercício da actividade de certificação;
d) Manter um contrato de seguro válido para a cobertura adequada da responsabilidade civil emergente da actividade de certificação, nos termos previstos no artigo 16.º;
e) Dispor de recursos técnicos e humanos que satisfaçam os padrões de segurança e eficácia, nos termos do diploma regulamentar;
f) Utilizar sistemas e produtos fiáveis protegidos contra qualquer modificação e que garantam a segurança técnica dos processos para os quais estejam previstos;
g) Adoptar medidas adequadas para impedir a falsificação ou alteração dos dados constantes dos certificados e, nos casos em que a entidade certificadora gere dados de criação de assinaturas, garantir a sua confidencialidade durante o processo de criação;
h) Utilizar sistemas fiáveis de conservação dos certificados, de forma que:
    a. Os certificados só possam ser consultados pelo público nos casos em que tenha sido obtido o consentimento do seu titular;
    b. Apenas as pessoas autorizadas possam inserir dados e alterações aos certificados;
    c. A autenticidade das informações possa ser verificada; e
    d. Quaisquer alterações de carácter técnico susceptíveis de afectar os requisitos de segurança sejam imediatamente detectáveis;
i) Verificar rigorosamente a identidade dos requerentes titulares dos certificados e, tratando-se de representantes de pessoas colectivas, os respectivos poderes de representação, bem como, quando aplicável, as qualidades específicas a que se refere a alínea i) do n.º 1 do artigo 29.º;

j) Conservar os elementos que comprovem a verdadeira identidade dos requerentes titulares de certificados com pseudónimo;
l) Informar os requerentes, por forma escrita, de modo completo e claro, sobre o processo de emissão de certificados qualificados e os termos e condições exactos de utilização do certificado qualificado, incluindo eventuais restrições à sua utilização;
m) [Anterior alínea e) do artigo 25.º]
n) Não armazenar ou copiar dados de criação de assinaturas do titular a quem a entidade certificadora tenha oferecido serviços de gestão de chaves;
o) Assegurar o funcionamento de um serviço que:
    a. Permita a consulta, de forma célere e segura, do registo informático dos certificados emitidos, revogados, suspensos ou caducados; e
    b. Garanta, de forma imediata e segura, a revogação, suspensão ou caducidade dos certificados;"

Com a publicação do Decreto-Lei n.º 116-A/2006, de 16 de Junho, a Autoridade Nacional de Segurança (ANS) foi designada como entidade competente para a credenciação e a fiscalização das Entidades Certificadoras (EC) estabelecidas em Portugal, funções e competências até então cometidas ao Instituto das Tecnologias da Informação da Justiça (ITIJ).

Como foi referido anteriormente para se criar uma assinatura eletrónica qualificada é necessário um dispositivo seguro, este dispositivo seguro consiste num dispositivo de criação de assinatura que assegure através de meios técnicos e processuais adequados que:

1. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada;
2. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis;
3. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros;

4. Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura;

Neste contexto, os dados de criação de uma assinatura correspondem a um conjunto único de dados, como chaves privadas, utilizado pelo titular (pessoa singular ou coletiva identificada num certificado como detentora de um dispositivo de criação de assinatura) para criação de uma assinatura eletrónica.

Tendo como base o Decreto-Lei n.º 116-A/2006, Criação do Sistema de Certificação Electrónica do Estado - Infra-Estrutura de Chaves Públicas e designa a Autoridade Nacional de Segurança como autoridade credenciadora nacional. O artigo 8º diz-nos que "a autoridade credenciadora é a autoridade competente para o registo, credenciação e fiscalização das entidades certificadoras compreendidas no SCEE, bem como das que emitam certificados qualificados no âmbito do regime jurídico dos documentos eletrónicos e da assinatura digital, é a Autoridade Nacional de Segurança".

Sendo que, o conselho técnico de credenciação é um órgão consultivo da autoridade credenciadora, competindo-lhe pronunciar-se sobre todas as questões que a autoridade credenciadora lhe submeta. Pode ainda por sua iniciativa, emitir pareceres ou recomendações à autoridade credenciadora. O conselho técnico de credenciação é composto:

a) Pela Autoridade Nacional de Segurança, que preside;
b) Por duas personalidades designadas pelo Primeiro-Ministro;
c) Por uma personalidade designada pelo Ministro da Administração Interna;
d) Por uma personalidade designada pelo Ministro da Justiça;
e) Por uma personalidade designada pelo Ministro da Ciência, Tecnologia e Ensino Superior;
f) Por um representante do ICP - ANACOM.

O Gabinete Nacional de Segurança assegura o apoio logístico e administrativo ao conselho técnico de credenciação, suportando também os encargos inerentes ao seu funcionamento. A AC pode, no exercício das competências que lhe estão cometidas pelo presente decreto-lei, solicitar a outras entidades públicas ou privadas toda a colaboração que julgar necessária. Segundo (Rito, 2018), "Como instrumento de melhoria para o funcionamento por via eletrónica na Administração Pública, dando destaque à medida implementada no processo das Compras Eletrónicas, através da Contratação Pública Eletrónica, surgiu a necessidade

de adotar medidas de segurança e de criar condições legislativas de forma a introduzir as assinaturas eletrónicas nos serviços públicos facilitando, ao mesmo tempo, a participação dos cidadãos. Embora se trate de uma matéria relativamente recente, a Assinatura Digital Qualificada já se encontra explanada na doutrina e na legislação de forma a possibilitar uma evolução eficaz e rápida, com o objetivo de conferir validade jurídica aos documentos eletrónicos e torná-los seguros."

A Certificação Digital Qualificada é uma exigência do **DL 143-A/2008** e da **Portaria 701-G/2008**. Esta Portaria entrou em vigor no dia 1 de janeiro de 2009 e obriga à utilização de assinaturas eletrónicas qualificadas e selos temporais, para uso em plataformas eletrónicas de contratação.

O **DL 143-A/2008** descreve que toda esta mudança de um sistema baseado no papel para um sistema baseado nas tecnologias de informação e de comunicação não se limita a uma opção de política legislativa mas atende, também, à efectiva situação no que tange às tecnologias disponíveis que, por sua vez, devem estar, na sua utilização, submetidas a dois grandes princípios, a disponibilidade e a interoperabilidade das tecnologias. A permanente evolução e desenvolvimento das tecnologias determinam a sua rápida desactualização, impondo a correlativa necessidade de actualização das tecnologias existentes às novas funcionalidades, capacidades, aparelhos e dispositivos. Pelo que estabelece os princípios gerais a que devem obedecer as comunicações, trocas e envio de dados e informações, em particular na disponibilização das peças do procedimento bem como envio e receção dos documentos que constituem as candidaturas, propostas e soluções.

A presente **Portaria 701-G/2008** "não pretende esgotar todo o espectro dos serviços a prestar pelas plataformas electrónicas, a qual deve estar associada a um manual e não ao presente documento. Pretende-se, através desta portaria, estabelecer as normas aplicáveis aos procedimentos a implementar nas plataformas cuja uniformização é desejável. Não obstante, para além dos referidos serviços de base exigíveis às plataformas electrónicas, que correspondem às funcionalidades essenciais que permitam o desenvolvimento total e completo dos procedimentos pré-contratuais públicos, podem as mesmas oferecer toda uma gama de serviços complementares, no âmbito do normal funcionamento do mercado e da concorrência. As plataformas electrónicas constituem uma infraestrutura informática que serve de suporte aos procedimentos de contratação pública, desenrolando-se os vários passos sob o comando directo da entidade adjudicante e dos interessados ou concorrentes, nos

termos e dentro dos limites previamente estabelecidos. Não cabe, por isso, às plataformas electrónicas uma intervenção própria e autónoma em cada procedimento específico, mas exclusivamente um papel de base automática disponibilizada aos utilizadores e detentora de uma série de aplicações informáticas que consubstanciam os serviços que prestam".

O Artigo 27.º apresenta o sentido de obrigatoriedade do uso de certificados digitais qualificados para assinar todos os documentos carregados nas plataformas, podendo observar os pontos que caracterizam o mesmo.

- Todos os documentos carregados nas plataformas electrónicas deverão ser assinados electronicamente mediante a utilização de certificados de assinatura electrónica qualificada.
- Para efeitos da assinatura electrónica, as entidades que devam utilizar assinaturas eletrónicas emitidas por entidades certificadoras integradas no Sistema de Certificação Eletrónica do Estado devem utilizar certificados digitais emitidos por uma mesma entidade certificadora do Sistema de Certificação Electrónica do Estado. Em que, o nível de segurança exigido é o que consta do **Decreto-Lei n.º 116 -A/2006, de 16 de Junho.**
    - A arquitectura do SCEE constitui, assim, uma hierarquia de confiança que garante a segurança electrónica do Estado e a autenticação digital forte das transacções electrónicas entre os vários serviços e organismos da Administração Pública e entre o Estado e os cidadãos e as empresas.
- Nos casos em que o certificado digital não possa relacionar directamente o assinante com a sua função e poder de assinatura, deve a entidade interessada submeter à plataforma um documento electrónico oficial indicando o poder de representação e assinatura do assinante.

Relativamente à utilização de plataformas, na realização e operações relacionadas com obras urbanísticas a **Lei n.º 60/2007** estabelece o regime jurídico da urbanização e edificação, tornado obrigatório que a realização de comunicações por via eletrónica sejam instruídos com assinatura digital qualificada.

Segundo o Artigo 8.º-A, o método de procedimento previstos é realizado informaticamente com recurso a um sistema informático próprio o que permita:

a) A entrega de requerimentos e comunicações;

b) A consulta pelos interessados do estado dos procedimentos;
c) A submissão dos procedimentos a consulta por entidades externas ao município;
d) Disponibilizar informação relativa aos procedimentos de comunicação prévia admitida para efeitos de registo predial e matricial.

Sendo que o sistema informático previsto no presente artigo é objeto de portaria conjunta dos membros do Governo responsáveis pela justiça, pela administração local e pelo ordenamento do território. De forma que tanto a apresentação de requerimento como outros elementos e a realização de comunicações através de via eletrónica devem ser instruídos com assinatura digital qualificada.

Os procedimentos previstos no presente diploma iniciam-se através de requerimento ou comunicação apresentados com recurso a meios eletrónicos através do sistema previsto que foi referido no Artigo 8.º-A. Estes serão dirigidos ao presidente da câmara municipal, dos quais deverá constar a identificação do requerente ou comunicante como refere o Artigo 9.º, sendo que devem incluir o domicílio ou sede bem como a identificação da qualidade de titular de qualquer direito que lhe confira a faculdade de realizar a operação urbanística. Com a apresentação de requerimento ou comunicação por via eletrónica por sua vez é emitido recibo entregue por via eletrónica.

Assim como refere o Artigo 10.º, "o requerimento ou comunicação é sempre instruído com declaração dos autores dos projectos, da qual conste que foram observadas na elaboração dos mesmos as normas legais e regulamentares aplicáveis, designadamente as normas técnicas de construção em vigor, e do coordenador dos projectos, que ateste a compatibilidade entre os mesmos".

A **Lei n.º 25/2008**, de 5 de Junho, "ao estabelecer medidas de natureza preventiva e repressiva de combate ao branqueamento de vantagens de proveniência ilícita e ao financiamento do terrorismo, fixa, entre outros, um conjunto de deveres que impendem sobre entidades que se dediquem ao exercício das actividades de mediação imobiliária e de compra e revenda de imóveis, bem como entidades construtoras que procedam à venda directa de imóveis, correntemente designadas de promotoras imobiliárias".

Segundo o artigo 34º , as pessoas singulares ou colectivas que exerçam a actividade de mediação imobiliária, bem como a actividade de compra, venda, compra para revenda ou permuta de imóveis, e a actividade de, directa ou indirectamente, decidir, impulsionar,

programar, dirigir e financiar, com recursos próprios ou alheios, obras de construção de edifícios, com vista à sua posterior transmissão ou cedência, seja a que título for, devem proceder, junto do Instituto da Construção e do Imobiliário, I. P.:

a) À comunicação, nos termos legalmente previstos, da data de início da actividade de mediação imobiliária, da actividade de compra, venda, compra para revenda ou permuta de imóveis, ou da actividade de, directa ou indirectamente, decidir, impulsionar, programar, dirigir e financiar, com recursos próprios ou alheios, obras de construção de edifícios, com vista à sua posterior transmissão ou cedência, seja a que título for, acompanhada do código de acesso à certidão permanente do registo comercial, no prazo máximo de 60 dias a contar da data de verificação de qualquer dessas situações;
b) Ao envio semestral, em modelo próprio, dos seguintes elementos sobre cada transacção efectuada:
    - Identificação clara dos intervenientes;
    - Montante global do negócio jurídico;
    - Menção dos respectivos títulos representativos;
    - Meio de pagamento utilizado;
    - Identificação do imóvel.

Pelo que a transmissão electrónica passa a ser a única via admitida para efectuar as comunicações, isto justifica-se pelas seguintes razões:

- Procede à completa desmaterialização dos procedimentos respeitantes às comunicações obrigatórias
- Promove a diminuição de encargos para os administrados, facultando um meio de registo mais eficaz e menos dispendioso para cumprimento dos deveres a que estão obrigados;
- Agiliza o acesso à informação por parte da Procuradoria-Geral da República e da Unidade de Informação Financeira da Polícia Judiciária;
- Assegura a qualidade dos dados inscritos nas comunicações e garante a autenticação da entidade declarante, conferindo a esta maior segurança na sua actuação.

Visando-se assegurar a eficácia das medidas de prevenção e repressão de combate ao branqueamento de vantagens de proveniência ilícita e do financiamento do terrorismo,

garantindo a qualidade e a integridade dos dados constantes das comunicações, bem como a consequente responsabilização do declarante, considera-se que tais objetivos só podem ser alcançados através da autenticação das entidades declarantes, com recurso a certificados digitais qualificados, para além do registo no portal do InCI, I. P.

Desta forma e de modo a que haja cumprimento relativo ao envio de documentos, as comunicações obrigatórias devem ser autenticadas electronicamente através da utilização de certificado digital qualificado, nos termos previstos no regime jurídico dos documentos electrónicos e da assinatura electrónica. Sendo que, para o caso de as comunicações obrigatórias necessitarem de ser instruídas com documentos, os mesmos devem ser correctamente digitalizados e integralmente apreensíveis e remetidos através dos mecanismos existentes nos formulários electrónicos previstos. Segundo o nº 2 do artigo 2.º que complementa as questões relacionadas com os mecanismos existentes nos mesmos formulários, as comunicações obrigatórias efectuam-se exclusivamente por transmissão electrónica de dados para o InCI, I. P. através do sítio na Internet com o endereço www.inci.pt, mediante a utilização dos formulários com as características e estrutura disponibilizadas nas respectivas áreas restritas, tendo-se como não efectuadas as comunicações apresentadas por qualquer outra via.

Como apresenta o Artigo 5º, as Comunicações Obrigatórias só são consideradas validamente submetidas após a emissão de um comprovativo electrónico que indique a data e a hora em que a comunicação foi concluída.

Um dos aspetos importantes são a confidencialidade e a segurança dos dados, que têm vindo a ser abordados ao longo do presente projeto. Como é apresentado no Artigo 6.º, os titulares da assinatura electrónica qualificada devem proceder no sentido de não permitir a sua utilização por terceiros, definir expressamente, quando for caso disso, quais as pessoas autorizadas a elaborar e enviar os dados contidos nas comunicações obrigatórias, bem como agir diligentemente e praticar todos os actos necessários para assegurar a manutenção da respectiva confidencialidade e restrição da sua utilização. Pelo que, o InCI, I. P. assegurará a utilização de mecanismos de cópia e salvaguarda da informação associada às comunicações efectuadas pelos utilizadores, garantindo a protecção da informação na sua vertente de confidencialidade e impossibilitando o acesso indevido à mesma, bem como a preservação digital dos documentos e dos certificados digitais, através de mecanismos tecnológicos adequados de armazenamento, de indexação e de recuperação de arquivos.

Relativamente à comunicação de transacções, o envio de elementos sobre transacções imobiliárias deve ser efectuado nos seguintes prazos: os elementos sobre transacções efectuadas no primeiro semestre de cada ano, devem ser comunicados até 31 de Agosto do mesmo ano enquanto que os elementos sobre transacções efectuadas no segundo semestre de cada ano, devem ser comunicados até 28 de Fevereiro do ano seguinte.

O **Decreto- Lei n.º 13/93**, de 15 de Janeiro, que regula a criação e fiscalização das unidades privadas de saúde, regulamentado pelo Decreto Regulamentar n.º 63/94, de 2 de Novembro, que estabelece os requisitos relativos a instalações, organização e funcionamento das unidades privadas de saúde, teve como objetivo garantir que a prestação de cuidados de saúde pelo sector privado se realizava com respeito pelos parâmetros mínimos de qualidade, quer no plano das instalações, quer no que diz respeito aos recursos técnicos e humanos utilizados.

Tendo-se verificado a difícil implementação por força das regras estabelecidas dado a serem demasiado burocráticos e complexos, tornou-se inevitável construir um novo modelo de licenciamento de unidades privadas de serviços de saúde que, permita efetivamente garantir que se verificam os requisitos mínimos necessários para que seja assegurada a qualidade dos serviços prestados no sector privado, com ou sem fins lucrativos. Pretende-se que cumpra objetivos, um sector privado de prestação de serviços de saúde complementar ao Serviço Nacional de Saúde, que garanta qualidade e segurança.

Desta forma, para funcionamento das unidades privadas de serviços de saúde e para cumprimento dos requisitos deve cumprir requisitos de higiene, segurança e salvaguarda da saúde pública e as unidades privadas de serviços de saúde devem funcionar de acordo com as regras de qualidade e segurança definidas pelos códigos científicos e técnicos aplicáveis, como nos informa o Artigo 9.º.

Para além disso segundo o Artigo 10.º, as unidades privadas de serviços de saúde devem afixar nas suas instalações, em local bem visível, para os utentes e visitantes, a identificação dos serviços prestados e a licença.

As taxas e o sistema existente segundo o Artigo 12.º, estão disponíveis para a tramitação dos procedimentos previstos no presente decreto-lei que é realizada informaticamente, com recurso a um sistema informático próprio, o qual permite, nomeadamente:

- A entrega de requerimentos e comunicações;
- O pagamento de taxas;
- A consulta pelos interessados do estado dos procedimentos;
- A disponibilização de informação relativa aos procedimentos de licença.

Segundo o nº2 do Artigo 12.º, a apresentação de requerimentos, de outros elementos e a realização de comunicações por via electrónica devem ser instruídos com assinatura digital qualificada.

A importância da utilização da assinatura digital qualificada é que, desta forma poderão assegurar a autenticidade de qualquer comunicação realizada eletronicamente entre o serviço de saúde e o utente, bem como de que aquela informação referente ao utente é integra. Promovendo uma maior garantia de segurança e que por sua vez preserva a autenticidade e veracidade.

Como referido anteriormente o presente regulamento apresenta-nos diversas definições que ajudam na compreensão no mesmo. Por sua vez, é apresentada como definição a

No capítulo II do regulamento podemos identificar matérias relativas à identificação eletrónica tais como o reconhecimento mútuo, a elegibilidade para notificação dos sistemas de identificação eletrónica bem como os níveis de garantia dos sistemas de identificação eletrónica, entre outros. Estes aspetos característicos da identificação eletrónica serão abordados posteriormente e de forma mais alongada.

2.3. Validação a longo termo de assinaturas digitais (LTV) e validação cronológica (*timestamping*)

Comecemos por um breve exemplo, o Bruno empresta 5000€ à Alice e por sua vez ela assina digitalmente uma nota promissória em que afirma que deve esses 5000€ ao Bruno. É do interesse do Bruno que a assinatura digital seja suficiente para convencer um juiz de que a Alice realmente lhe deve dinheiro. No entanto, pode ocorrer uma disputa no tribunal muito depois da assinatura da nota promissória. Isto porque o certificado de chave pública da Alice pode ter revogado ou expirado, ou seja, deixado de ter efeito e por sua vez ser inválida. Pelo que, é necessário garantir que os documentos eletrónicos mantenham a sua autenticidade comprovada durante um longo período de tempo depois da sua criação.

Os documentos em formato digital são cada vez mais um meio comum para uma grande abrangência dos vários tipos de informação, tais como registo de transações, livros, trabalhos científicos, contratos e até mesmo decretos governamentais. Em vários casos, estes documentos devem ser preservados por longos períodos de tempo, como por exemplo para efeitos de controlo e contabilidade futuros, por razões probatórias ou para a proteção de interesses de uma determinada entidade e/ou pessoa. O valor dos documentos arquivados depende da existência de uma assinatura digital, que é a principal expressão da intenção de um autor, ao mesmo tempo que esta garante a integridade do documento. Desta forma, existe uma diferença entre a potencial durabilidade de um documento digital e a durabilidade da sua assinatura digital depende de múltiplos fatores, que têm um tempo de vida pequeno. Pelo que vejamos os seguintes apresentados baseados em (Lekkas & Gritzalis, 2004):

- As chaves utilizadas para a criação e verificação da assinatura digital devem ter um tempo de vida limitado a fim de evitar uma longa exposição a criptanalistas e outras possíveis ameaças. Uma prática comum das autoridades de certificação é impor um limite de um ou dois anos na duração de vida dos certificados emitidos que se baseiam num par de chaves RSA, sendo que o CC atualmente utiliza chaves RSA de 2048 bits;
- As chaves de assinatura podem ser comprometidas antes da conclusão da sua vida útil ou os algoritmos utilizados para a criação da assinatura podem ser quebrados, tornando a assinatura de um documento vulnerável a ataques de modificação à informação que este contém;
- As informações necessárias para a verificação de uma assinatura digital, tais como cadeias de certificados digitais e o estado de revogação de certificados, podem não estar disponíveis passado um determinado tempo;

A assinatura digital é um mecanismo fundamental nos serviços de segurança, como a autenticação e a não-repúdio. Em que um par de chaves privadas e públicas são utilizadas para gerar as assinaturas e verificação, respetivamente (Lekkas & Gritzalis, 2004). Foram propostos diversos esquemas de assinatura eletrónica, sendo que o procedimento principal é o mais comum e baseia-se na criptografia de chave pública, tendo esta sido referida anteriormente no presente documento. Os algoritmos *hash* trouxeram uma solução para a eficiência computacional das assinaturas, os certificados digitais e as chaves forneceram os meios para a identificação eficaz do assinante, as arquiteturas de infraestruturas de chaves

públicas (PKI) construíram as relações de confiança necessárias e, finalmente, os esquemas de *timestamping* e autenticação tornaram uma assinatura digital ainda mais forte.

O *timestamp* e a autenticação foram utilizados para prolongar a vida útil de uma assinatura digital, indicando que uma assinatura foi criada num momento anterior a um compromisso subsequente, bem como transferindo a confiança contra os dados assinados para uma nova entidade, o notário. No entanto, os carimbos temporais e as autenticações consistem em assinaturas digitais e, portanto, poderão ser invalidados a partir de um período de tempo.

Um carimbo de tempo digital é um atestado gerado por uma Autoridade de Validação Cronológica (Time Stamping Authority - TSA), um serviço de confiança, de que um item de dados existia num determinado momento. Os carimbos de tempos são tipicamente utilizados para registar eventos, em que num registo cada evento é marcado com um carimbo temporal. Nos sistemas de ficheiros, os carimbos temporais podem referir-se à data/hora armazenada da criação ou modificação do ficheiro. O carimbo temporal de confiança é o processo de manter um registo seguro da hora de criação e modificação de um documento. O TSA de confiança pode ser utilizado para provar a consistência e integridade das provas digitais em cada fase da sua existência (Brzica, Herceg, & Stančić, 2013). Na figura 11 podemos ver uma representação de diferentes situações relativamente aos diversos formatos de assinatura (ETSI, 2009).

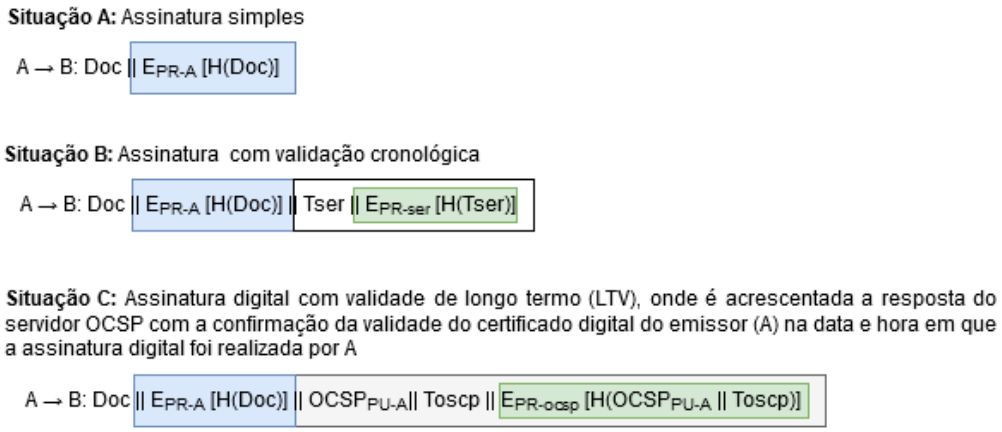


Figura 11 - Diversos tipos de assinaturas digitais

Relativamente à validade das assinaturas digitais, os requisitos de segurança sobre assinaturas digitais são diferentes quando são utilizados em serviços de autenticação e não-repúdio, respetivamente. Enquanto os serviços de autenticação protegem contra possíveis equívocos, os serviços de não-repúdio fornecem provas que permitem a resolução de divergências. Nos serviços de autenticação, o verificador da assinatura apenas necessita

certificar-se de que tanto a assinatura como o certificado de chave pública são válidas no tempo de verificação, e dessa forma não se preocupa com a sua validade após isso. Nos serviços de não repúdio, contudo, a validade de uma assinatura aceite anteriormente deve ser verificada no momento da resolução de controvérsias, mesmo que o certificado de chave pública correspondente tenha expirado ou sido revogado. Na figura 12 apresenta-se uma visão mais clara sobre esta situação, sendo de seguida apresentado um exemplo para que melhor se possa compreender a validade das assinaturas.

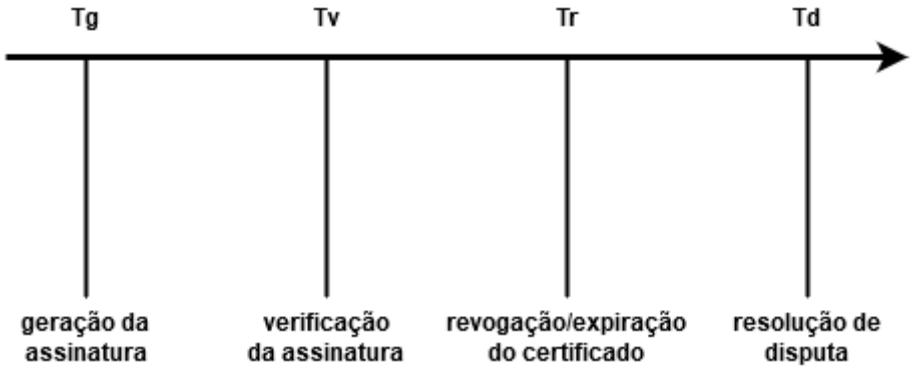


Figura 12 - Validade das Assinaturas Digitais (Zhou, Bao, & Deng, 2003)

Suponhamos que é gerada uma assinatura no momento Tg. O serviço de autenticação termina no momento da Tv, em que a validade da assinatura é verificada. O sucesso da autenticação se a assinatura e o certificado de chave pública correspondente são válidos na Tv. A Revogação do prazo de validade do certificado Tr, em que Tr >T v, não tem efeito no serviço de autenticação. Suponha que a resolução de disputas tem lugar na Td, onde Td >T r. Obviamente, o certificado é inválido na Td. Por outro lado, a assinatura foi aceite como prova de não repúdio na Td, onde Tv <T r. Se a assinatura for tratada como inválida na Td por causa da revogação do certificado ou expiração do mesmo, qualquer parte pode gerar uma assinatura e mais tarde negá-la, revogando o certificado. Por conseguinte, é fundamental assegurar que uma vez aceite uma assinatura como prova válida, esta permanece válida mesmo se o certificado correspondente for revogado ou expirar mais tarde.

A preservação a longo prazo apresenta-se como uma parte importante uma vez que as assinaturas digitais avançadas e certificados digitais qualificados estão a ser cada vez mais acrescentados ou associados a documentos e registos originários digitalmente. Sendo que, os arquivistas digitais devem decidir o que fazer com elas, tendo em mente que as assinaturas digitais, do ponto de vista arquivístico, têm um curto período de validade e que as assinaturas digitais associadas podem ser revogadas a qualquer momento. Tudo isto acrescenta incerteza

ao processo de arquivação e impede a possibilidade de verificar a autenticidade, integridade e não-repúdio de um registo após um certo período. Para tornar as coisas ainda mais difíceis, não só os arquivos digitais estão a enfrentar o dilema de preservar ou não registos assinados digitalmente, mas eles próprios estão a utilizar assinaturas digitais. Os repositórios de preservação utilizam as assinaturas digitais de três formas principais (Stančić, 2016):

1. para submissão ao repositório, um Agente (o autor) pode assinar um objeto para afirmar que é realmente o autor do mesmo;
2. para disseminação a partir do repositório, o repositório pode assinar um objeto para afirmar que é verdadeiramente a fonte da disseminação;
3. para armazenamento de arquivos, um repositório pode querer arquivar objetos assinados de modo a que seja possível confirmar a origem e integridade dos dados.

A primeira e a segunda utilização são comuns, uma vez que as assinaturas digitais são utilizadas na transmissão de documentos comerciais e outros dados. Normalmente, a validação tem lugar pouco depois da assinatura e não há necessidade de preservar a própria assinatura ao longo do tempo. No primeiro caso, o repositório pode registar o ato de validação como um evento, e guardar a informação relacionada necessária para demonstrar a proveniência no detalhe do evento. No segundo caso, o repositório pode também registar a assinatura como um evento, mas a utilização da assinatura é da responsabilidade do recetor. Apenas no terceiro caso, em que as assinaturas digitais são utilizadas pelo repositório como ferramenta para confirmar a autenticidade dos seus objetos digitais armazenados ao longo do tempo, a própria assinatura e as informações necessárias para validar a assinatura devem ser preservadas. Tendo em conta o ponto de vista dos arquivos e baseado em (Stančić, 2016) (Jean-François, 2006), existem as seguintes soluções possíveis:

- Preservar as assinaturas digitais: pressupõe a utilização de meios consideráveis para preservar os mecanismos necessários à validação das assinaturas, e não responde à necessidade de preservar simultaneamente a inteligibilidade dos documentos;
- Eliminar as assinaturas: requer a menor adaptação da instituição arquivística, mas empobrece a descrição do documento, pois elimina a assinatura como um elemento técnico utilizado para assegurar a autenticidade dos documentos;
- Registar os vestígios das assinaturas como metadados: requer poucos meios técnicos, e regista tanto a existência da assinatura como o resultado da sua verificação. No

> entanto, as assinaturas digitais perdem o seu estatuto especial como a principal forma de prova a partir da qual se pode inferir a autenticidade do documento.

A fim de preservar as assinaturas digitais juntamente com os registos, os arquivos devem ter a possibilidade de validar a assinatura em qualquer momento no futuro. Devido ao facto de as assinaturas digitais e certificados associados serem válidos apenas por um determinado período de tempo e de os certificados poderem ser revogados, esta opção parece bastante improvável de funcionar a longo prazo, a menos que se encontrem reunidas certas condições prévias. Dumortier e Van den Eynde referem que a única solução eficaz (na sua opinião) para o problema da durabilidade da assinatura passa pelo arquivo da representação binária original do documento (Stančić, 2016). Tendo esta solução sido proposta pela European Electronic Signature Standardization Initiative (EESSI) no relatório de estudo Trusted Archival Services (TAS). A TAS deve garantir que ainda será possível validar documentos arquivados anos após a data inicial do arquivo, mesmo que as aplicações que foram utilizadas na altura da criação da assinatura já não estejam a ser utilizadas. Por outras palavras, a TAS deve manter um conjunto de aplicações juntamente com as plataformas correspondentes (hardware, sistemas operativos) ou pelo menos um emulador de tais aplicações e/ou ambiente, a fim de garantir que a assinatura do documento ainda possa ser validada anos mais tarde. É claro que esta opção exigiria muitas competências técnicas e conhecimentos dos arquivos, para não citar as implicações financeiras. A segunda opção é tecnicamente a menos desafiante no contexto da preservação a longo prazo, mas na realidade não é uma opção para arquivar os registos que precisam de ser preservados como autênticos. Portanto, para a preservação a longo prazo de registos assinados digitalmente autênticos, a terceira opção é a mais realista (Stančić, 2016).

A questão da preservação a longo prazo de documentos e registos assinados digitalmente é uma questão relevante para a ciência e prática arquivista. Por um lado, facilitam os negócios, as transações e atividades digitais podem ser tornadas fiáveis e seguras. Por outro lado, a confiança nas assinaturas digitais depende da infraestrutura de informação e da hierarquia de certificados interligados. Além disso, a validade das assinaturas e certificados digitais é limitada no tempo e esta validade pode ser revogada a qualquer momento. Um conjunto separado de problemas está ligado aos métodos de preservação digital - conversão de formatos de ficheiro mais antigos para mais recentes, migração de suportes mais antigos para mais recentes, emulação, virtualização, etc. Estes procedimentos são necessários no contexto

da preservação a longo prazo, para que os registos digitais se mantenham legíveis e acessíveis. Contudo, cada um destes procedimentos pode influenciar substancialmente a autenticidade, integridade, fiabilidade, usabilidade, e não-repúdio dos registos. Assim, (Stančić, 2016) salienta, a informação de validade adicionada aos metadados torna-se a prova primária quando, eventualmente, a integridade do bit é quebrada e as ferramentas criptográficas já não são válidas após uma transformação. Por este motivo, a verificação e validação de material assinado digitalmente é também muito importante para fornecer provas de validade prévia de assinaturas digitais.

3. Trabalho relacionado

O conceito de assinatura digital tendo em conta as tecnologias e mesmo os conceitos de apoio à confiança em registos eletrónicos, em que o conceito de assinatura eletrónica pode ser visto como base para o desenvolvimento consequente de outras tecnologias. Podemos compreender de seguida os formatos de assinaturas eletrónicas XMLDSig, XAdES, CAdES e PAdES.

3.1.1. XMLDSig

A assinatura XML (Extensible Markup Language) é definida pela recomendação do W3C, sendo referida como XMLDSig, XML-DSig ou XML-Sig. A Recomendação do W3C afirma que as assinaturas XML podem ser aplicadas a qualquer conteúdo digital (objeto de dados), incluindo XML. Referindo também que uma assinatura em XML pode ser aplicada ao conteúdo de um ou mais recursos". Pelo que, desta forma é possível diferenciar a assinatura num documento XML entre (Guedes, 2008) (Brzica, Herceg, & Stančić, 2013):

- *Detached signature* (assinatura destacada) - uma assinatura XML utilizada para assinar um recurso fora dele que contém um documento XML, a assinatura alude a dados externos ao ficheiro onde se encontra. Ou seja, a assinatura está sobre o conteúdo externo ao elemento S*ignature*;
- *Enveloped signature* (assinatura envolta) – a assinatura é utilizada para assinar alguma parte do documento que a contém, ou seja, a assinatura é sobre o conteúdo encontrado dentro de um elemento *Object* da própria assinatura;
- *Enveloping signature* (assinatura envolvente) – a assinatura contém os dados assinados dentro de si mesmo, ou seja, a assinatura é sobre o conteúdo XML que contém a assinatura como um elemento. O conteúdo fornece o elemento de documento XML de raiz. Obviamente, as *enveloped signatures* (assinatura envolta) devem ter o cuidado de não incluir o seu próprio valor no cálculo do *SignatureValue* (valor da assinatura).

As assinaturas XML são aplicadas a conteúdos digitais arbitrários (objetos de dados) por meio de um indireto. Os objetos de dados são assimilados, o valor de resumo é colocado num elemento (com outras informações) e esse elemento é depois assimilado e assinado criptograficamente.

3.1.2. XAdES (*XML Advanced Electronic Signature*)

XAdES alarga a especificação XMLDSig ao domínio de não-repudio definindo desta forma formatos XML para assinaturas eletrónicas avançadas que permanecem válidas durante longos períodos e se encontram em conformidade com a Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas. Incorporam também informações uteis adicionais em casos de utilizações comuns. Isto inclui provas quanto à sua validade, mesmo que o signatário ou parte verificadora tente posteriormente negar, ou seja, mesmo que este tente repudiar a validade da assinatura. Uma assinatura eletrónica avançada alinhada com a especificação XAdES pode consequentemente, ser utilizada para arbitragem em caso de disputa entre o signatário e o verificador, o que pode ocorrer num momento posterior, mesmo anos mais tarde. Relativamente ao XMLDig, a especificação XAdES acrescenta seis níveis adicionais sendo os seguintes apresentados (Brzica, Herceg, & Stančić, 2013) (Guedes, 2008):

1. **XAdES** igualmente referido como **XAdES-BES** – forma básica definindo elementos para autenticação e proteção da integridade dos registos, mas não fornecendo a não repudiação da sua existência;
2. **XAdES-T (*Time-stamped*)** – a adição do *timestamp* assegura a não repudiação, que se apresenta como um fator importante uma vez que pretendemos que uma assinatura permaneça válida durante meses ou até mesmo anos;
3. **XAdES-C (*Complete*)** – baseia-se no XAdES-T por acrescentar referências ao conjunto de dados e toda a informação necessária que suportam a validação da assinatura eletrónica, ou seja, as referências às cadeias de certificação e a informação associada ao estado de revogação. Este formulário é útil para as situações em que tal informação é arquivada por uma fonte externa, como por exemplo, um fornecedor de serviços de confiança;
4. **XAdES-X (*eXtended*)** – baseia-se em XAdES-C, acrescentando carimbos temporais, por sua vez alargando as capacidades de validação a longo prazo da assinatura, de forma a proteger contra o risco de que quaisquer chaves utilizadas no certificado ou no estado de revogação possa ser comprometida a informação sobre a cadeia;
5. **XAdES-X-L (*eXtended Long-term*) –** baseia-se no XAdES-X adicionando os dados de validação, ou seja, acrescentando certificados e valores de revogação para as situações em que os dados de validação não são armazenados noutro local para longo prazo;

6. **XAdES-A (*Archival*)** – arquivamento de dados de validação, baseia-se em XAdES-X-L em que este nível acrescenta à assinatura carimbos de tempo para o arquivamento de assinaturas. Ou seja, desta forma protege a assinatura a longo prazo contra futuros algoritmos de segurança que se venham a tornar-se frágeis.

Podemos também observar na figura 13 e verificar a estrutura dos níveis de especificação XAdES apresentados anteriormente.

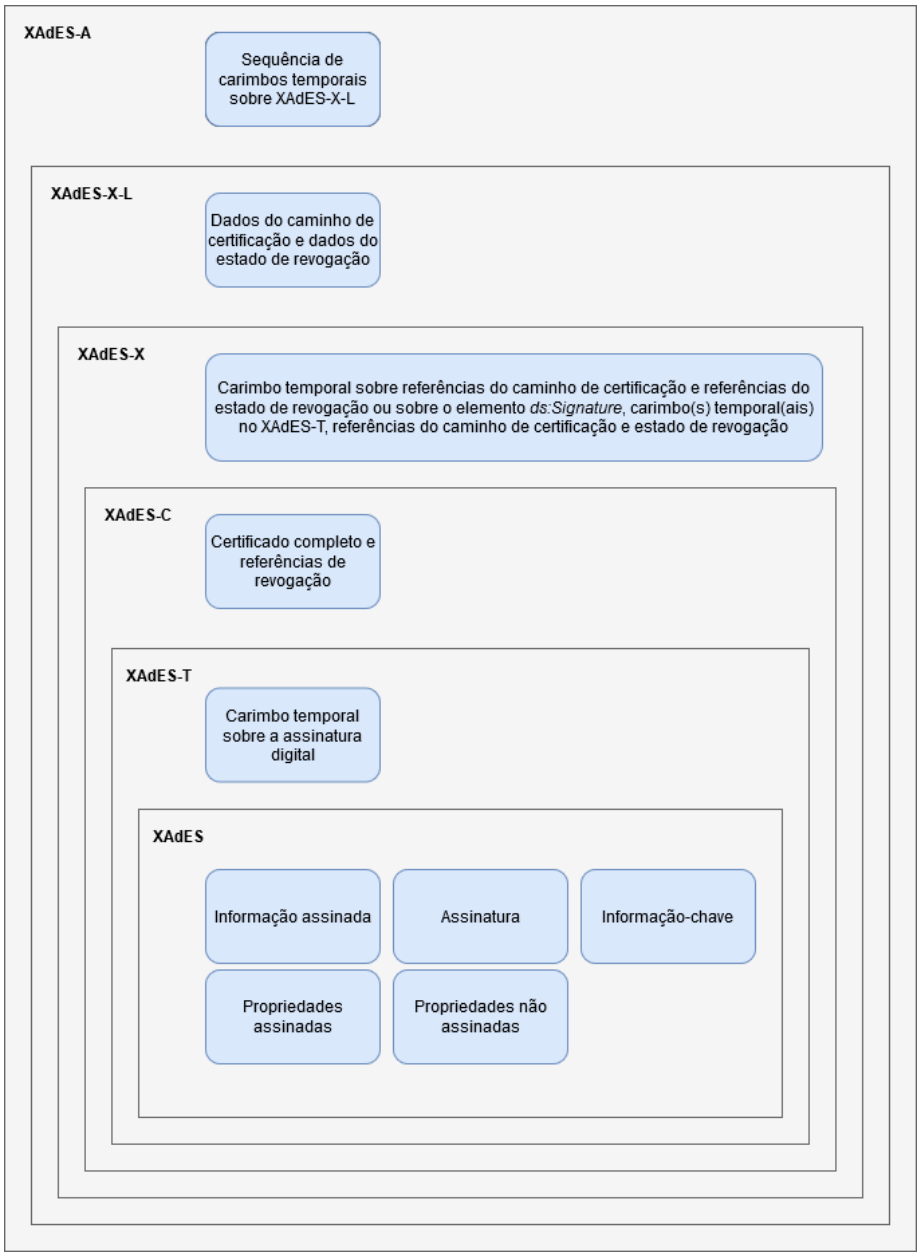


Figura 13 - Estrutura dos formulários de especificação XAdES (Brzica, Herceg, & Stančić, 2013)

Independentemente dos diferentes níveis referidos, a existência de um determinado nível não obriga à existência das características especificas dos outros níveis anteriores. Na seguinte tabela 1 são apresentas as dependências entre os níveis apresentados. Sendo interpretada da seguinte forma, o nível associado obriga à existência das propriedades especificas dos níveis das colunas assinaladas. Por exemplo, observando a tabela: o nível XAdES-X-L obriga a presença das propriedades especificas dos níveis XAdES, XAdES-C, XAdES-X e XAdES-X-L.

Tabela 1 - Dependências dos níveis XAdES (Guedes, 2008)

Níveis	XAdES	XAdES-T	XAdES-C	XAdES-X	XAdES-X-L	XAdES-A
XAdES	x					
XAdES-T	x					
XAdES-C	x	x	x			
XAdES-X	x		x	x		
XAdES-X-L	x		x	x	x	
XAdES-A	x				x	x

3.1.3. CAdES (*CMS Advanced Electronic Signatures*)

CAdES é um conjunto de extensões a dados assinados CMS (*Cryptographic Message Syntax*), que define uma série de formatos de assinatura eletrónica, incluindo assinaturas eletrónicas que podem permanecer válidas durante longos períodos. Incluindo provas quanto à sua validade, mesmo que o signatário ou parte verificadora tente posteriormente repudiar a validade da assinatura eletrónica. Semelhante a XAdES, a especificação CAdES define seis perfis, cada um a desenvolver-se em relação ao anterior: CAdES – forma básica, CAdES-T (*Timestamp*), CAdES-C (*Complete*), CAdES-X (*eXtended*), CAdES-X-L (*eXtended Longterm*) e CAdES-A (*Archival*). A distinção que existe entre as duas especificações é que, enquanto a CAdES torna a assinatura como dados binários, a XAdES fornece uma solução XML (Brzica, Herceg, & Stančić, 2013).

3.1.4. PAdES (*PDF Advanced Electronic Signature*)

PAdES detém das mesmas capacidades apresentadas em CAdES e XAdES, sendo que este difere na medida em que se aplica apenas a documentos PDF e define os requisitos que o software de visualização e edição de PDF deve seguir ao utilizar assinaturas digitais em

documentos PDF. O PDF também define como uma assinatura pode ser exibida com uma assinatura de tinta em papel numa determinada posição numa determinada página e como as assinaturas digitais podem ser integradas com as características de preenchimento de formulários do PDF. Este pode ser considerado um fator chave que distingue CAdES e XAdES, que são mais adequados para aplicações que podem não envolver documentos legíveis. A especificação PAdES é realizada em seis partes: PAdES Overview, PAdES Basic, PAdES Enhanced, PAdES Long Term, PAdES for XML Content e Visual Representations of Electronic Signatures (Brzica, Herceg, & Stančić, 2013).

Na seguinte tabela 2, podemos observar uma comparação dos formatos das assinaturas eletrónicas.

Tabela 2 - Comparação de XAdES, CAdES e PAdES (Brzica, Herceg, & Stančić, 2013)

XAdES	CAdES	PAdES

• Fornece uma solução XML completa:
  ○ assina quaisquer dados incluindo PDF e binário;
  ○ suporta pacotes XML ou ficheiros separados;
• Requer frequentemente a personalização de aplicações ou assinatura genérica fora da aplicação;
• Suporta múltiplas assinaturas aplicadas em paralelo, em série através de assinatura repetida;
	• Permite a assinatura de quaisquer dados, incluindo PDF;
	• Apoia dois métodos de assinatura:
	  ○ *detached* - os dados assinados são separados da assinatura (dados e assinatura podem ser empacotados juntos);
	  ○ *encapsulated* - os dados são envolvidos dentro da estrutura de assinatura;
		• Contém assinaturas dentro do PDF;
		• Suporte de dados XML;
		• Incluído na norma ISO PDF;
		• Inclui assinatura e verificação em software PDF (sem necessidade de programação customizada);
		• Suporta fluxos de trabalho em série a partir do preenchimento e assinaturas para aprovação;
		• Suporta um aspeto de assinatura visual no documento;

• Apoiar uma assinatura visual, dependendo da aplicação; • Proporciona validade a longo prazo.	• Torna a assinatura como dados binários; • Requer frequentemente a personalização de aplicações ou assinatura genérica fora da aplicação; • Suporta múltiplas assinaturas aplicadas em paralelo, em série através de assinatura repetida; • Proporciona validade a longo prazo.	• Proporciona validade a longo prazo.

3.2. Identificação eletrónica (e-ID)

Os sistemas de identificação eletrónica e-ID geram uma variedade de benefícios para indivíduos, empresas assim como para o governo sendo que inclusivamente facilitam o comércio na economia digital, possibilitando desta forma serviços de *e-Government* na melhoria da segurança das transações online (Castro, 2011) .

Entende-se por identificação eletrónica, “o processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva". A identidade única de uma pessoa no processo tradicional “analógico” manifesta-se através de posse de determinados documentos tais como certificados de nascimento, bilhetes de identidade, passaportes e entre outros, ligados à aparência física da pessoa como um meio adicional para verificar a identidade correta da pessoa. Digitalmente, no domínio da identidade eletrónica, nenhum mecanismo deste tipo é viável. A identificação "tradicional" através de bilhetes de identidade e aparência física não pode ser realizada no mundo virtual da Internet pelo que desta forma, existe uma necessidade do equivalente funcional da identificação pública para o mundo virtual.

Um identificador único geralmente significa um atributo ou um conjunto de atributos de uma entidade que identifica de forma única a entidade dentro de um determinado contexto. Os identificadores digitais primários diretamente ligados a uma pessoa incluem, por exemplo, nome, morada, número de telemóvel, palavra-passe ou assinatura eletrónica. Estes identificadores são armazenados numa forma codificada, assim sendo, uma pessoa pode definitivamente ser identificada através do número de cidadão ou cliente que a ele ou ela esteja atribuída (Lentner, 2016).

Desta forma podemos compreender a definição de uma identificação eletrónica sob consulta do Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 que é um regulamento relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE. Sendo que este tem como objetivo assegurar o correto funcionamento do mercado interno e alcançar um nível adequado de segurança dos meios de identificação eletrónica e dos serviços de confiança. Conforme o Artigo 1º do capítulo 1, o presente regulamento:

a) Estabelece as condições em que os Estados-Membros reconhecem e aceitam os meios de identificação eletrónica para identificar pessoas singulares e coletivas no quadro de um sistema de identificação eletrónica notificado de outro Estado-Membro;
b) Estabelece normas aplicáveis aos serviços de confiança, nomeadamente às transações eletrónicas; e
c) Institui um quadro legal para as assinaturas eletrónicas, os selos eletrónicos, os selos temporais, os documentos eletrónicos, os serviços de envio registado eletrónico e os serviços de certificados para autenticação de sítios web.

Atualmente, a identificação e-ID é geralmente definida com três formas de funcionalidade de segurança de informação (Arora, 2008):

Identificação(I) em que um individuo/entidade A pode provar a B que ele é a A mas que outra pessoa não pode provar a um individuo/entidade B que ele é a A;

Autenticação(A) em que um individuo/entidade A pode provar a B que ele é a A mas o individuo/entidade B não pode provar a outra pessoa que ele é a A;

Assinatura(S) em que um individuo/entidade A pode provar a B que ele é a A mas o individuo/entidade B não pode provar para si mesmo que ele é a A.

Sendo mais conhecido como a funcionalidade I-A-S, em que uma das primeiras referencias ao I-A-S foi realizada na conferencia CRYPTO '86, onde Fiat e Shamir ilustraram as limitações da não utilização da tecnologia e-ID. Naquela altura eles apresentaram que os passaportes podiam ser fotocopiados por governos hostis, os números de cartão de crédito podiam ser copiados e também que as palavras-passe seriam vulneráveis a hackers.

Os principais *drivers* dos cartões e-ID surgiram de três ângulos:

- ***E-Passports,*** pressões políticas e legais levam à possibilidade de implementar passaportes eletrónicos que são considerados os passaportes da próxima geração.
- **Diretiva da UE relativa às assinaturas eletrónicas,**
- **Alargar os esquemas de cartões de identificação nacional para suportar novas funções,** um exemplo clássico é a adição de um *chip smartcar*d a um cartão de identidade já existente.

Os atuais cartões e-ID são usualmente elaborados por vários ministérios nacionais do governo. Em geral o *design* funcional tem tido uma participação limitada do setor privado. Apesar de, por exemplo, o uso de um recurso de digital ter uma utilização valiosa no setor privado, em que os atuais cartões e-ID apoiam muitas das vezes tais cenários.

3.2.1. Cartões e-ID e a privacidade

Relativamente à privacidade os cartões e-ID, do ponto de vista da gestão da identidade a privacidade pode ser vista como uma abordagem a quatro características, definidas na norma ISO 15408 e debatidas por (Pfitzmann & Hansen, 2006), sendo as seguintes:

1. **Anonimato** - Assegura que um utilizador pode utilizar um recurso ou serviço sem revelar a identidade desse mesmo utilizador.
2. **Inexistência de ligações** - Garante que um utilizador pode fazer múltiplas utilizações de recursos ou serviços sem que outros possam ligar essas utilizações em conjunto.
3. **Inobservabilidade** - Assegura que um utilizador pode utilizar um recurso ou serviço sem que outros, especialmente terceiros, sejam capazes de observar que o recurso ou serviço está a ser utilizado.

4. **Pseudónimo (“Nome falso”)** - Assegura que um utilizador pode utilizar um recurso ou serviço sem revelar a sua identidade de utilizador, mas pode ainda assim ser responsável por essa utilização.

3.2.2. Identidade, nacionalidade e cidadania

A definição da identidade de uma pessoa ou aplicações é hoje mais complexa e importante do que nunca, sendo que descreve a unidade essencial de uma pessoa. Atualmente, a natureza da identidade social está a mudar e a expandir-se e no mundo digital as identidades estão ligadas a direitos, obrigações, filiações e títulos. A identidade é definida como a totalidade das características, as características de uma pessoa, mas também de um objeto. As características físicas podem ser complementadas pela posse de objetos de legitimação, tais como cartões de identificação, tais como palavras-passe, PINs, entre outros. Cada identidade deve poder ser comprovada com dados significativos que permitam verificar se essa identidade é legítima e válida. Em suma, deve ser possível provar de forma credível que o proprietário de uma legitimação é também quem afirma ser (Fiebig, 2020).

Vale a pena darmos um passo atrás para definir o que se entende por identificação das pessoas, visto que isso nos auxilia a associar melhor a sua representação sob forma eletrónica. Como por exemplo, num cartão de identidade eletrónica. “A identificação humana é a associação de dados com um determinado ser humano”, é uma definição apresentada por (Clarke, 1994). Sabemos que estes dados podem assumir diferentes formas, mas geralmente incluem aspetos como os seguintes representados na tabela 3:

Tabela 3 - Identificação das pessoas sob representação eletrónica (Arora, 2008)

Meios de Identificação	**Definição de Clarke**	**exemplos**
Aparência	O aspeto da pessoa	Utilização de fotografias em documentos de identidade, biometria facial
Comportamento social	Como a pessoa interage com outros	Registos escolares, registos telefónicos, extratos de cartões de crédito, dados de videovigilância

Nomes/Códigos	O que a pessoa é chamada por outras pessoas ou por uma organização	Nome inscrita no registo nacional, em passaportes, certidões de nascimento, números de bilhetes de identidade, número da segurança social, etc.
Conhecimento	O que a pessoa sabe	Palavras-passe, PINs
Fichas(“*tokens*”)	O que a pessoa tem	Smartcards, cartões de identificação seguros
Biodinâmica	O que a pessoa faz ou é	A maioria das formas de biometria: impressão digital, íris, retina, etc.
Características físicas	O que a pessoa é agora	Peso, altura

O bilhete de identidade nacional procura representar as formas de identificação acima referidas para além de atributos como a nacionalidade associada ao cartão.

Na época romana, a lei definia os termos da cidadania, que acabaram por definir a quem o individuo pagava os seus impostos. A cidadania podia ser obtida por estrangeiros inimigos através da deserção e da colaboração. Com os direitos de cidadania, surgiram certos deveres para além do pagamento de impostos, sobretudo o serviço militar. Na altura, a recusa de participar no serviço significaria a revogação da cidadania. Do mesmo modo que, os romanos perderiam automaticamente a sua cidadania se se tornassem prisioneiros de guerra. Hoje em dia, as identidades eletrónicas podem ser revogadas de forma semelhante, como por exemplo, através da publicação de listas de revogação de certificados de identidade, embora a sua motivação tenda a ser devida a uma alteração do estatuto do cartão ou do seu conteúdo, por oposição a uma revogação da cidadania (Arora, 2008).

Ao contrário da cidadania, o conceito de nacionalidade é um conceito mais moderno. Este termo teve origem na teoria revolucionária de que pessoas com uma língua e cultura comuns formam uma nação e, de tal modo, devem ter direito a autogoverno como Estado.

A passagem do tempo fundiu e confundiu de certa forma as ideias de filiação, nacionalidade e cidadania, sublinhou Lloyd. Esta fusão e confusão aumenta ainda mais quando se incorporam os conceitos de e-ID e cartões e-ID, especialmente quando se trata de cartões e-ID nacionais, que implicam a nacionalidade, mas não necessariamente a cidadania.

3.2.3. Aplicações e utilizadores do cartão e-ID

Dependendo do tipo de aplicação em que um cartão e-ID venha a ser utilizado, existem diferentes utilizadores que interagem com o cartão. Os principais tipos de utilizadores de cartões de identidade eletrónica são os seguintes apresentados:

- **Identidade do provedor e emissor** - Geralmente uma agência governamental (ou terceiros de confiança) que verifica e recolhe as credenciais necessárias para a emissão de um cartão e-ID. Para além da emissão do cartão, o fornecedor da identidade também detém alguma forma de responsabilidade e segurança no que diz respeito à autenticidade/validade da identidade. Na Europa, isto incluiu ministérios do Interior e tipografias estatais.
- **Funcionário público** - Pessoal do Governo/funcionários públicos que trabalham com o cartão e-ID para vários fins.
- **Cidadãos particulares/privados** – São o titular principal, utilizador do cartão e-ID. O cartão de identidade eletrónica é geralmente emitido no seu nome.
- **Representantes empresariais** - Identidades que não são cidadãos privados, mas que representam entidades jurídicas, tais como as empresas.

Quase todas as áreas de aplicação dos atuais e-IDs giram em torno dos serviços governamentais. Esses serviços têm sido a habilitação de aplicações de governo eletrônico. As que parecem ser consideradas mais eficazes são aquelas que geram alguma forma de renda, tais como as que se encontram relacionadas à cobrança de impostos. Outras aplicações de *e-Government* incluem: verificação da idade, verificação dos dados pessoais (registo nacional), *e-voting* (ensaios já realizados na Estónia) assim como e-mail seguro (na Estónia cada cidadão recebe um endereço de e-mail juntamente com a sua identidade eletrónica). A utilização de cartões de identidade eletrónica em sectores não governamentais na Europa assume duas formas: utilização de cartões e-ID como SSCD para assinatura digital e eletrónica de documentos com validade legal e colaboração com instituições financeiras para partilhar infraestruturas de autenticação (por exemplo, PKI).

Segundo (Arora, 2008) algumas utilizações futuras das aplicações do cartão e-ID incluiriam:

- Acesso a LANs/Metronets sem fios públicos;
- Verificação da idade para serviços como os jogos online;
- Sistemas de credenciais anónimas para resolver problemas de privacidade;
- Criptografia.

Embora a utilização de cartões inteligentes para criptografia seja uma extensão acessível, não se tem visto esta utilização de cartões e-ID pelas seguintes razões:

- Requer um certificado adicional;
- Não existe legislação de mandato;
- Os alternativos convencionais já estão presentes;
- Embora a privacidade esteja a ser tratada, principalmente do ponto de vista da retenção de dados, a cifragem das comunicações não aparece na matéria existente relativamente aos cartões e-ID.

3.2.4. Riscos

Os cartões de identidade eletrónica nacionais são tão vulneráveis a ataques como qualquer outro sistema informático, especialmente quando se considera os cartões de identidade eletrónica e a respetiva infraestrutura como uma forma de infraestrutura nacional crítica. Assim sendo, aspetos como os ataques de negação de serviço tanto no sentido tradicional, como a recusa intencional de aceitação quando um utilizador não deseja que o cartão seja reconhecido, a quebra ou falha da infraestrutura PKI subjacente, ou os ataques físicos aos cartões inteligentes devem ser todos considerados quando se procede a uma avaliação dos riscos dos sistemas nacionais de cartões de identidade eletrónica (Arora, 2008).

Provavelmente, a vulnerabilidade com maior ameaça aos sistemas de cartões de identidade eletrónica é o erro humano. O erro humano pode ocorrer em qualquer fase em que os seres humanos interagem com o sistema. Por exemplo, durante o processamento da matrícula, os dados podem ser introduzidos incorretamente, o que pode gerar confusão após a emissão do bilhete de identidade. Isto é especialmente verdade no caso dos documentos de base cuja validade é menos suscetível de ser questionada como por exemplo as certidões de nascimento. Do mesmo modo, durante o registo, a biometria pode ser mal capturada, conduzindo a um nível mais elevado de falsos indeferimentos.

3.2.5. Investimento na Europa

Grande parte do investimento em e-ID tem sido observado na Europa. A União Europeia impulsionou o desenvolvimento de cartões de identidade nacionais interoperáveis com a criação da norma do Cartão de Cidadão Europeu (CEC). Em 2005, na Conferência Ministerial de Manchester as nações europeias aprovaram unanimemente um plano para criar um programa de identificação eletrónica nos países membros. Como é possível observar na tabela 4, alguns países europeus, incluindo a Bélgica, Finlândia, Suécia e Portugal, criaram programas nacionais de identidade eletrónica. Por exemplo, a Lituânia iniciou a implantação nacional de uma identidade eletrónica nacional biométrica em janeiro de 2009. Embora o principal objetivo do smartcard lituano seja fornecer um bilhete de identidade mais seguro e facilitar o controlo eficiente das fronteiras, o bilhete de identidade também contém um certificado digital que pode ser utilizado por indivíduos num computador com um leitor de cartões para transações online mais seguras, como a autenticação num serviço online ou a assinatura eletrónica de um documento.

A utilização de um eID emitido nacionalmente melhora a segurança digital. Os eID podem, com muito maior certeza, determinar com segurança que a pessoa que acede a um serviço online é quem diz ser. Em vez de inúmeras combinações de login para cada serviço a que acede online, pode utilizar um único eID como método de acesso, a maioria dos eID inclui também uma opção de assinatura, tornando possível aos cidadãos e empresas assinar documentos eletrónicos com o seu eID. O Regulamento 910/2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno torna obrigatório que os serviços públicos europeus aceitem os eID dos estados membros notificados até setembro de 2018. As fronteiras digitais na Europa são removidas e os métodos eID dos estados membros da União Europeia podem ser aceites por outros estados membros. A legislação é também conhecida como "eIDAS". A eID é largamente utilizada no mundo digital europeu, podendo observar na tabela *5* quais os eIDs existentes sendo que os que se encontram apresentados com asterisco (*) indica que não há identificação eletrônica conhecida listada para o seu país. Isso pode ser porque o sistema ainda não foi introduzido (Connectis, 2016).

Tabela 4 - eID no mundo digital europeu (Connectis, 2016)

País	Tem e-ID	Nome do e-ID
Alemanha	Sim	(Neuer) Personalausweiss

Áustria	Sim	Buergerkarte
Bélgica	Sim	eID/.beID
Bulgária	*	*
Chipre	*	*
Croácia	*	*
Dinamarca	Sim	NemID
Eslováquia	Sim	National eID card
Eslovénia	*	*
Espanha	Sim	DNIe
Estónia	Sim	ID-Kaart
Finlândia	Sim	Finnish eID card
França	*	*
Grécia	*	*
Hungria	*	*
Irlanda	Sim	IceKey
Islândia	*	*
Itália	Sim	SPID
Letónia	Sim	eID Card, eParaksts
Lituânia	Sim	National eID card, Bank ID
Luxemburgo	Sim	CTIE
Malta	Sim	Identity Malta
Noruega	Sim	MinID, BankID
Países Baixos	Sim	DigiD, eHerkenning
Polónia	*	*
Portugal	Sim	Cartão de Cidadão, Chave Movel Digital
Reino Unido	Sim	Gov.UK Verify eIDs
República Checa	Sim	MojeID
Roménia	*	*
Suécia	Sim	ank ID, Telia eID
Suíça	Sim	SuisseID
Turquia	Sim	National eID card

3.2.6. Cartões nacionais e-ID na Europa: Áustria, Bélgica, Reino Unido e Estónia

A implementação dos cartões de identidade eletrónica varia consideravelmente em toda a Europa. A Espanha e Portugal deram passos em frente no que diz respeito a uma rápida implantação e utilização da norma definida pelo Comité Europeu de Normalização (CEN) para o Cartão de Cidadão Europeu (CEC), respetivamente. Ainda assim, é seguro dizer que, em toda a Europa, os diferentes países encontram-se em diferentes fases de maturidade no que respeita à implantação, mas também carecem de um conjunto comum de mecanismos de implementação. Mais concretamente, é possível ver as diferentes motivações e implementações técnicas subjacentes em cada país. Por conseguinte, serão analisados mais de perto os seguintes sistemas nacionais de cartões de identidade eletrónica, a fim de demonstrar de forma ilusória a variedade de implementações.

1. **Cartão de Cidadão Austríaco**

A Áustria implantou um sistema baseado em múltiplos cartões diferentes que permitem o acesso aos serviços. O eCard da Bürgerkarte, um cartão de seguro de saúde, é complementado por um cartão de estudante, cartões de serviço e de profissão (funcionários públicos, advogados, notários, farmacêuticos, entre outros). Ao mesmo tempo, a HandySignature, uma alternativa móvel de eID, e a mais popular eID com cerca de 750.000 utilizadores ativos até 2017, também está disponível. Este esquema utiliza um certificado armazenado num dispositivo criptográfico, ao qual é concedido acesso ao assinante do certificado graças à combinação do seu nome de utilizador e palavra-passe. Um extrato da assinatura resultante é então enviado para o telemóvel do cidadão. Após a sua confirmação, a assinatura é enviada para o requerimento solicitante (Comission, 2017).

O cartão austríaco Bu¨rgerkarte apresenta os seguintes aspetos que merecem destaque:

- **Múltiplas tokens (e-IDs)**

A identidade eletrónica austríaca, ao contrário de outras iniciativas na Europa, não está centrada na representação com um único cartão. Por conseguinte, as fichas físicas podem ser encontradas sob a forma de um cartão de identidade emitido pelo governo, mas também todos os cartões multibanco austríacos emitidos por bancos são considerados cartões e-ID (SSCD) legalmente válidos, e mesmo um dos operadores de telecomunicações emite cartões SIM que cumprem a legislação austríaca para servir de "cartão" de identidade eletrónica.

- **Duas formas de identidade eletrónica legalmente aceites**

Enquanto noutros regimes nacionais tende a existir apenas uma identidade única, os austríacos definem legalmente duas formas de identidade aceitável:

Identidade Única - Designação de uma pessoa específica através de uma ou mais características que permitem distinguir inequivocamente a pessoa em causa de todas as outras pessoas em causa.

Identidade recorrente - Designação de uma pessoa específica de uma forma que, embora não garanta uma identidade única, permite que essa pessoa seja reconhecida por referência a um acontecimento anterior. Algumas das vantagens de definir e aceitar legalmente a identidade recorrente incluem: permitir que múltiplas partes possam gerar as suas próprias fichas de identidade eletrónica para a mesma identidade única e a capacidade de integrar as identidades eletrónicas estrangeiras no regime austríaco.

- **Inexistência de ligação**

Não existe um motor legal para impedir a possibilidade de ligação como mecanismo de proteção da privacidade. No entanto, os austríacos fazem questão de salientar este aspeto do cartão deles. A motivação subjacente ao tratamento da característica de não ligação é garantir que, quando um identificador é utilizado por uma organização governamental, por exemplo, um seguro de saúde nacional, outra agência governamental seja obrigada a utilizar um identificador diferente, por exemplo, as autoridades fiscais. Embora, tecnicamente, seja apresentada uma solução, a capacidade dos austríacos para resolver verdadeiramente o problema da falta de ligação falha em dois aspetos:

1. Não há qualquer condutor legal para resolver o problema da falta de ligação. Assim, ao contrário das leis de retenção de dados definidas, esta característica de privacidade carece de qualquer definição legal ou capacidade para garantir a conformidade.
2. A utilização de outros dados para identificar um cidadão (por exemplo, nome e data de nascimento) mostra rapidamente que, para fins práticos, os cidadãos ainda podem ser "relacionados" entre si.

- **Interoperabilidade**

A Áustria implementou um sistema nacional de identidade eletrónica que, através de uma Prova de Conceito (PoC) (Rössler, 2008), tentou ilustrar a interoperabilidade de uma

identidade eletrónica estrangeira com o seu sistema nacional. A capacidade para desempenhar essa função é possível devido à definição austríaca de Identidade Recorrente. Note-se que a utilização da interoperabilidade entre sistemas é prática comum noutros domínios, como a possibilidade de utilizar um cartão ATM em bancos estrangeiros, a autenticação numa rede de telefonia móvel quando se está em roaming ou a utilização de uma carta de condução para provar o direito de operar veículos mesmo quando se está no estrangeiro. Estes exemplos equivalentes de interoperabilidade continuam a não existir entre os sistemas de cartões e-ID.

Em resultado dos objetivos de conceção e da definição legal da identidade eletrónica austríaca, permitiu uma implantação muito mais ampla das identidades eletrónicas nacionais do que noutras partes da Europa. Embora não dispondo de um cartão e-ID único, a legislação austríaca permitiu a emissão de uma identidade eletrónica válida a nível nacional com base em múltiplos fatores formais. Sendo eles, cartão nacional de identidade eletrónica, cartões bancários/ATM, cartões SIM e dispositivos USB.

2. Cartão de Cidadão Belga

O esquema nacional de identidade eletrónica da Bélgica baseia-se no cartão de identidade nacional público, BELPIC. Os nacionais de outros países residentes na Bélgica também têm acesso a um ID estrangeiro com o mesmo elevado nível de garantia. O cartão contém três chaves RSA privadas de 1024 bits, uma das chaves é específica do cartão e as outras duas são específicas do cidadão. A chave específica do cartão (a chamada chave privada básica) é utilizada para realizar uma autenticação mútua entre o cartão de identificação e o Registo Nacional. Isto é necessário, por exemplo, para atualizar os dados do cartão. A chave pública correspondente só está disponível para o Registo Nacional, sendo por isso a única autoridade capaz de verificar as assinaturas criadas por esta chave privada. A primeira chave específica do cidadão é utilizada para a assinatura de documentos eletrónicos, esta chave está ligada a um certificado qualificado que permite a identificação do cidadão. A segunda chave específica do cidadão é utilizada para autenticação em aplicações de *eBusiness* e *eGovernment* e está ligada a um certificado não qualificado. O armazenamento dos dados extraídos do eID numa base de dados deve ser aprovado pela Comissão belga de privacidade (Comission, 2017).

Sendo que os objetivos da BELPIC passam pela realização de funções tais como, a identificação dos cidadãos, recolha de dados, autenticação bem como a assinatura digital e o controlo de acesso, como por exemplo a serviços municipais. A fim de realizar o que se descreveu foi decidido utilizar três pares de chaves para os seguintes fins (Arora, 2008):

1- Autenticação do cidadão - utilizando um certificado de autenticação:
2- Assinatura eletrónica avançada - utilização de um certificado qualificado para produzir assinaturas digitais em conformidade com a Diretiva 1999/93/CE da UE;
3- Autenticação do cartão e-ID - o registo nacional conhece a respetiva chave para uma determinada carteira de identidade eletrónica.

Os dois primeiros casos utilizam cada um certificados X.509 v3 para guardar as chaves no cartão. Embora seja apenas um aspeto de uniformização entre os sistemas de cartões, a utilização do mesmo formato de certificado é um exemplo em que a interoperabilidade entre sistemas de cartões se torna mais fácil de implementar, embora atualmente não o seja (Arora, 2008).

3. Cartão de identidade do Reino Unido

Ao contrário da maioria dos países da Europa, o Reino Unido não dispõe de um sistema de bilhete de identidade nacional emitido pelo governo ou um esquema de cartão de identidade eletrónico. Os cidadãos provam a sua identidade através de documentos de identificação alternativos, tais como passaportes e cartas de condução. Isto é em grande parte atribuído às más conotações que os cartões de identificação emitidos centralmente ainda apresentam: o Reino Unido tinha introduzido sistemas de cartões de identificação nacionais duas vezes antes e durante as duas Guerras Mundiais, onde os cartões de identificação eram utilizados para fins de inscrição. Uma vez que esta utilização era contra os princípios em que os sistemas foram criados, os bilhetes de identidade nacionais eram considerados como meios de monitorização da atividade da população (Tsakalakis, Stalla-Bourdillon, & O'Hara, 2017).

O esquema de identidade digital do Reino Unido para pessoas singulares é o GOV.UK Verify, concebido para permitir aos utilizadores uma forma simples e segura de provar a sua identidade online. Em que, foi lançado para utilização pelo público em geral em maio de 2016. Utiliza parceiros do sector privado (IDPs) para efetuar a prova de identidade dos

utilizadores e a emissão de meios de identificação eletrónica para utilização com os serviços governamentais do Reino Unido. O Government Digital Service (GDS) mantém o GOV.UK Verify Identity Assurance Hub, que liga os IDPs aos serviços do Reino Unido. O serviço de verificação é uma porta de entrada para serviços de identidade bem como tais serviços oferecidos como um produto adicional de outras entidades públicas ou privadas como o Barclays, Correios e Royal Mail (Comission, 2017).

4. Cartão de Identidade Estoniano

A introdução do *e-Government* na Estónia deve ser entendida como parte do investimento geral em alta tecnologia que se seguiu à queda do império soviético e ao restabelecimento da Estónia como Estado independente no final dos anos 90. O *e-Government* foi desenvolvido através de uma estreita cooperação entre interesses privados e públicos, com o sector bancário em particular a liderar o caminho. Há já vários anos que se encontra a Estónia entre os países mais bem classificados do mundo em matéria de digitalização do governo. Os documentos estratégicos do ITC da Estónia são permeados pela visão de uma sociedade completamente digitalizada. A Estónia destina-se a ser "um campeão mundial da vida digital" (Björklund, 2016).

Uma identificação pessoal fiável e segura, bem como a gestão da identidade física e digital, são a base para um processo credível de emissão de documentos de identidade. A Estónia tem uma longa experiência na utilização de autenticação eletrónica e é líder mundial no contexto do governo eletrónico. A Estónia emite o cartão de identificação como o documento primário e obrigatório para a identificação dos seus cidadãos e dos cidadãos da UE que vivem na Estónia. Os proprietários do cartão de identidade têm o direito de ter um portador de identidade digital adicional ou ficha eID como a Digi-ID ou Mobiil-ID. O cartão chip emitido é um documento de identificação física e possui funções eletrónicas avançadas que facilitam uma autenticação segura e uma assinatura. Os primeiros cartões de identificação estonianos foram emitidos em 28/01/2002. O cartão destina-se a ser universal, e as suas funções devem ser utilizadas em qualquer forma de comunicação comercial, governamental ou privada. O objetivo é ajudar as pessoas a tornar as comunicações diárias mais convenientes (Estonia, 2018).

O documento de identidade nacional da Estónia representado na figura 14, contém as seguintes informações na frente do cartão: nome, fotografia, assinatura, número de

identificação pessoal, data de nascimento, sexo, nacionalidade, número do cartão e data de validade do cartão. O verso do cartão contém as seguintes informações: local de nascimento, data de emissão do cartão e informações sobre a autorização de residência, se disponíveis.

Figura 14 - Cartão e-ID da Estónia (frente e verso) (Estonia, 2018)

O cartão contém igualmente as informações não gráficas (ou seja, dados que não incluem a fotografia ou a assinatura) em formato legível por máquina. O *chip* do bilhete de identidade contém dois certificados, um para autenticação eletrónica e outro para assinaturas eletrónicas. A Estónia é um dos poucos países europeus em que a funcionalidade de assinatura eletrónica não é opcional. Os certificados contêm o nome e o número de identificação pessoal do titular do cartão e o certificado de autenticação contém igualmente um endereço de correio eletrónico oficial único para cada titular do cartão. O cartão é obrigatório para os cidadãos com quinze anos ou mais.

O governo eletrónico na Estónia significa concentração de dados pessoais e públicos em bases de dados nacionais, e a digitalização diz respeito aos contactos entre as autoridades de bem-estar e os cidadãos, bem como entre as diferentes autoridades do sector público. As soluções digitais são também praticadas em eleições gerais. A votação eletrónica foi introduzida em 2005 e tem sido utilizada em eleições parlamentares, eleições locais e nas eleições para o Parlamento Europeu da Estónia. Para além do voto eletrónico, as autoridades públicas lançaram websites interativos na Internet para a comunicação com o público sobre iniciativas políticas (Björklund, 2016).

O governo não colocou quaisquer restrições à utilização da identidade eletrónica no sector privado e o mecanismo de autenticação está à disposição de qualquer desenvolvedor externo. Assim, qualquer organização pode construir uma aplicação que utilize a identidade eletrónica para identificação e autenticação. Existem aplicações que utilizam a identidade

eletrónica para autorizar transações bancárias online, assinar contratos e declarações fiscais, autenticar em redes sem fios, aceder a bases de dados governamentais e para o acesso automatizado a edifícios.

O governo também procura utilizar a identidade eletrónica para eliminar o desperdício e melhorar serviços, por exemplo, os cidadãos podem aceder aos serviços de saúde utilizando a sua identidade eletrónica, em vez de precisarem de um cartão de saúde separado. A direção da polícia estónia procurou integrar o bilhete de identidade com uma base de dados de condutores, para que possam verificar o estatuto dos condutores, eliminando a necessidade de os cidadãos possuírem uma carta de condução separada. Nas cidades estónias de Tallinn, Tartu e Harjumaa, o governo implementou um sistema de bilhetes sem papel com bilhetes de identidade eletrónicos de forma a substituir os bilhetes físicos para os transportes públicos. Desta forma, os passageiros poderiam adquirir os bilhetes nos quiosques, na Internet ou por telemóvel e depois utilizar o seu bilhete de identidade nacional como bilhete. Sendo que os passageiros que beneficiam de tarifas reduzidas ou até mesmo gratuitas também podem utilizar o seu bilhete de identidade como bilhete. O sucesso das identidades eletrónicas na Estónia pode ser visto nos números (Castro, 2011).

A Estónia também lançou a "Mobiil-ID", uma identificação eletrónica para telemóveis. O sistema é baseado num cartão SIM móvel especial, que o cliente deve solicitar ao operador do telemóvel. As chaves privadas são armazenadas no cartão SIM móvel, juntamente com uma aplicação que disponibiliza as funções de autenticação e assinatura. Tal como o bilhete de identidade eletrónico, contém certificados que permitem às pessoas identificar-se e assinar documentos digitalmente, tendo a vantagens de não ser necessário utilizar um leitor de cartões. Muitos serviços digitais permitem que as pessoas utilizem o Mobiil-ID em vez do cartão de identificação.

Tendo como base o website e-Estonia Briefing Centre, https://e-estonia.com/, é possível consultar os seguintes números apresentados relativamente aos residentes estónios e se estes utilizam a identificação eletrónica, sendo o seguinte apresentado:

- 99% têm cartão de identificação, sendo que 67% deles utilizam ativamente o cartão de identificação eletrónico;
- 17% têm o Mobiil-ID que também é o seu portador de identidade digital;

- 34% utilizam o Smart-ID, que pode ser utilizado para aceder a serviços financeiros eletrónicos para confirmar transações e acordos.

3.2.7. Benefícios dos sistemas de identificação eletrónica

No mundo digital, as identidades têm a tarefa de restringir o acesso a sistemas e aplicações informáticas a fim de proteger dados sensíveis e controlar a sua utilização. Neste contexto, o termo sistema TI abrange a combinação de diferentes hardwares e softwares, dispositivos e máquinas móveis, com capacidade de rede (smartphone, tablet, dispositivos inteligentes, robots, controlos de máquinas, entre outros), redes, bem como administração e utilizadores. As redes globais permitem a utilização mundial de sistemas TI. A globalização aumenta assim a gama de identidades e torna-as mais difíceis de verificar. O resultado é um ato de equilíbrio entre a utilização flexível dos serviços e a autenticação segura de todos os utilizadores. Por outras palavras, as identidades digitais movem-se num campo de tensão entre uma torrente de serviços globalmente utilizáveis que requerem registo, confidencialidade e conveniência, controlo e segurança, e a eficiência alcançável com as ofertas. Muitas aplicações e serviços digitais exigem identidades digitais. São criadas através da criação de uma conta de utilizador para um serviço digital (Fiebig, 2020).

Os sistemas de identificação eletrónica concebem uma variedade de benefícios para os indivíduos, as empresas e o governo, incluindo a facilitação do comércio na economia digital, permitindo serviços de governo eletrónico e melhorando a segurança das transações online. Muitos tipos de transações de comércio eletrónico tornam-se mais eficientes com um sistema de identificação eletrónica. Estes sistemas permitem aos indivíduos autenticarem-se nos serviços online, comunicarem de forma segura online e criarem assinaturas eletrónicas juridicamente vinculativas, como a assinatura de um contrato ou a inscrição num serviço. As empresas podem utilizar funções de gestão de identidade para interagir com os seus clientes, como a autenticação dos utilizadores em aplicações online. A utilização de e-ID também permite muitos serviços do sector privado que dependem do conhecimento da identidade do indivíduo ou de algo sobre o indivíduo, como a sua idade, que de outra forma é difícil de verificar à distância. Algumas identidades eletrónicas também podem ser utilizadas como carteira digital para fazer compras tanto pessoalmente como online.

A utilização de e-ID também pode facilitar muitos tipos de serviços *e-Government*. A administração pública pode racionalizar muitos serviços, como o fornecimento de benefícios

públicos, que dependem do conhecimento da identidade de um indivíduo. Os governos podem também oferecer serviços inovadores, como a votação online, que exigem autenticação remota. Os cidadãos podem preencher e assinar formulários da administração pública eletronicamente a partir de qualquer lugar com uma ligação à Internet, eliminando desta forma possíveis deslocações a realizar até repartições públicas ou notários públicos. Do mesmo modo, as empresas podem interagir de forma segura com as administrações públicas online para atividades como o pagamento de impostos ou o pedido de autorizações. A utilização de comunicações eletrónicas seguras também elimina a necessidade de transcrever dados de formulários em papel, ajudando a reduzir os erros e o tempo de processamento. A administração pública recebe muitos dos benefícios de uma maior eficiência, por exemplo, eliminando a duplicação de dados e reduzindo os custos associados à burocracia desnecessária, incluindo os custos de impressão, armazenamento, transporte e eliminação.

Por último, a utilização de sistemas de identificação eletrónica pode melhorar a segurança das transações online e ajudar a prevenir a fraude e a usurpação de identidade. Em primeiro lugar, as identidades eletrónicas podem criar mais confiança e responsabilização no ecossistema de identidade. Por exemplo, ao criar registos de auditoria suficientes, poderá ser possível criar cadeias de confiança que permitam identificar mais facilmente uma fonte de identidade eletrónica fraudulenta do que com identidades análogas. Em segundo lugar, as identificações eletrónicas podem tornar mais seguro para os utilizadores o início de sessão nos sistemas de informação, permitindo a autenticação de multi-fator. Um exemplo de autenticação multi-fator é exigir que o utilizador conheça um PIN e tenha um código de identificação eletrónica para aceder a um website. Tal como um cartão multibanco, se um e-ID for perdido ou roubado, não pode ser utilizado sem o PIN ou a palavra-passe. A maioria dos sistemas de informação não utiliza a autenticação multi-fator para o início de sessão do utilizador. Em vez disso, a maioria dos utilizadores controla e mantém múltiplos nomes de utilizador e palavras-passe. Embora a melhor prática seja utilizar uma palavra-passe única para diferentes contas, os indivíduos normalmente reutilizam a mesma palavra-passe em vários *websites*. Isto significa que se a palavra-passe de um utilizador for comprometida num site, ela é comprometida em todos os outros sites que utilizam a mesma palavra-passe. Além disso, se a palavra-passe de um utilizador for comprometida, o utilizador deve localizar e analisar todas as contas que reutilizarem essa mesma palavra-passe. Em contraste, com uma identificação eletrónica, o utilizador só tem de alterar a palavra-passe uma vez. Além disso,

uma vez que os utilizadores têm de se lembrar de várias palavras-passe atualmente, utilizam frequentemente uma palavra-passe mais fraca, mas mais fácil de lembrar, em vez de uma palavra-passe mais forte, mas mais complexa. Se os utilizadores apenas tiverem uma única identificação eletrónica a gerir, terão mais incentivos para utilizar palavras-passe fortes (Castro, 2011).

3.2.8. Aspetos tecnológicos

Os seguintes aspetos tecnológicos passam pelas tecnologias apresentadas e envolventes relativas ao eID.

- Forma de e-ID

Em geral, os países escolhem entre várias tecnologias para disponibilizar identidades eletrónicas, podendo ser as seguintes apresentadas: *smartcards*, telemóveis, palavras-passe únicas e certificados. Os cartões de contacto são mais predominantes em alguns países europeus, incluindo a Bélgica, Estónia, Itália, Portugal e Espanha. Os cartões sem contacto são normalmente utilizados nos Estados Unidos em cartões de crédito, como por exemplo no MasterCard PayPass, para pagar tarifas de alguns sistemas, tais como a cobrança eletrónica de portagens.

Os dirigentes políticos devem estar conscientes das questões de usabilidade relacionadas com as diferentes tecnologias de identificação eletrónica existentes. Para utilizar um *smartcard* nas transações online, como o início de sessão num *website* ou a assinatura de um documento eletrónico, as pessoas devem inserir o respetivo cartão e-ID num leitor de cartões ligado a um computador e, em seguida, introduzir um PIN ou palavra-passe para autorizar a transação. Para utilizar um *smartcard* em casa, os utilizadores precisam de ter leitores de cartões e o software correto instalado no computador. Para satisfazer as necessidades de todos os utilizadores, o software também deve estar disponível para os múltiplos sistemas operativos.

Alguns países disponibilizam apenas um tipo de identidade eletrónica, enquanto outros oferecem outras opções. O caso da Áustria apresenta talvez um dos sistemas de identidade eletrónica mais neutros do ponto de vista tecnológico. Em vez de limitar os e-ID a uma única forma de identificação emitida pelo governo, os austríacos podem utilizar a funcionalidade e-ID no *smartcard* ou dispositivo da sua escolha por exemplo, telemóvel ou computador.

Também na Estónia, um indivíduo pode utilizar um telemóvel ou um *smartcard* como identidade eletrónica.

- Plataforma Aberta (*Open Platform*)

Alguns países desenvolveram uma identidade eletrónica com um objetivo específico, por exemplo, para ser utilizada como documento de viagem aquando no controlo das fronteiras ou para aceder a serviços *e-Government*. Outros países construíram o sistema de identidade eletrónica com a intenção de criar um serviço de identidade que possa ser utilizado para múltiplos fins, tanto no governo como no sector privado. A possibilidade de extensão permite que a e-ID seja utilizada para mais do que um objetivo e que por sua vez seja possível evoluir ao longo do tempo. A criação de uma identidade eletrónica com uma plataforma aberta (*Open Platform*), ou seja, um conjunto de normas abertas que outros podem desenvolver, permite aos desenvolvedores inovar de forma independente e criar novas aplicações para os utilizadores e por sua vez integrar as identidades eletrónicas em vários sistemas. Isto é particularmente necessário para permitir que outras entidades se tornem fornecedores de atributos e forneçam dados ou credenciais que os utilizadores de e-ID possam partilhar com outros fornecedores de serviços.

Parte da realização de uma plataforma aberta envolve a criação de uma Interface de Programação de Aplicações (API) totalmente documentada, em que os programadores podem utilizar para interagir com a identidade eletrónica. Isto concede aos desenvolvedores as informações técnicas de que estes necessitam para conceber produtos e serviços que utilizam uma identidade eletrónica. Além disso, alguns *tokens* e-ID, como os *smartcards*, têm memória que pode armazenar dados característicos da aplicação. Alguns países que utilizam cartões para a identidade eletrónica, incluindo a Áustria, a Bélgica, a Finlândia, a Itália e Portugal, permitem que os dados específicos da aplicação sejam escritos na identidade eletrónica. Em contrapartida, as especificações dos cartões de identidade eletrónica noutros países, incluindo a Estónia, a Dinamarca e os Países Baixos, não dispõem desta funcionalidade.

- Biometria

Os métodos de identificação biométrica incluem, por exemplo, digitalização de impressões digitais ou íris, reconhecimento de voz ou rosto, imagem das veias das mãos, etc. As características biométricas individuais de um utilizador são geralmente armazenadas de

forma codificada no seu perfil e são utilizadas para verificação. É feita uma distinção entre características estáticas, anatómicas e características dinâmicas (características comportamentais). Estas características são gravadas passivamente, por exemplo, por câmaras, ou ativamente, por exemplo, através da colocação das mãos num scanner. As vantagens da identificação biométrica são a disponibilidade das características e o facto de não ser necessária informação adicional (conhecimento) por parte do utilizador. O esquecimento é, assim, quase impossível (Fiebig, 2020).

Muitos sistemas de identificação, tais como ID nacionais, passaportes e cartas de condução, utilizam informações biométricas, tais como impressões digitais ou fotografias, para evitar que uma identificação seja utilizada por outra pessoa que não o proprietário. Pelo que, alguns sistemas de identificação eletrónica começaram a incorporar dados biométricos. Exigir a utilização de dados biométricos para completar uma transação acrescenta um nível adicional de segurança ao associar a utilização de uma identidade eletrónica a um indivíduo específico. Alguns exemplos de dados biométricos incluem impressões digitais, geometria da mão, reconhecimento facial e reconhecimento da íris. A adição de dados biométricos a uma identidade eletrónica requer uma infraestrutura organizacional e tecnológica para a captação dos dados biométricos aquando da inscrição dos utilizadores no sistema para além de que, a utilização da biometria com e-ID pode exigir tecnologia adicional, como os leitores de impressões digitais.

Uma objeção comum à utilização de informações biométricas é que as informações biométricas de um indivíduo ao contrário de uma palavra-passe não podem ser alteradas se alguma vez forem comprometidas. A segurança da utilização de dados biométricos não advém do seu sigilo, mas sim da sua unicidade, isto significa que a biometria pode ajudar a evitar que alguém utilize a identidade eletrónica de outra pessoa. Por exemplo, uma pessoa pode partilhar um PIN mas não pode partilhar uma impressão digital. A informação biométrica é particularmente útil quando é recolhida utilizando *hardware* seguro num ambiente controlado para evitar que terceiros tentem falsificar os mesmos. Ainda assim, podem existir objeções por parte dos utilizadores relativamente ao uso dos seis dados biométricos e por consequência ser um obstáculo na implementação, embora questões de privacidade relacionadas com a utilização de dados biométricos pudessem ser ultrapassadas através de um sistema de identificação bem estruturado. Por exemplo, a Bélgica optou por

não implementar dados biométricos na identificação eletrónica devido aos custos e às potenciais reações dos utilizadores.

- Interoperabilidade

A interoperabilidade pode ser vista como um inibidor para o futuro crescimento e sucesso dos cartões nacionais de identidade eletrónica. Existem, no entanto, algumas atividades em curso que podem ser vistas como ilustrativas da tentativa de abordar a interoperabilidade sob diversos ângulos. A maior parte dos esforços para estabelecer sistemas de identificação eletrónica interoperáveis ocorreu entre os Estados-Membros da União Europeia. Por exemplo, o Cartão de Cidadão Europeu estabelece uma norma física e técnica para os bilhetes de identidade europeus. Em maio de 2008, a Comissão Europeia estabeleceu igualmente o projeto "*Secure idenTity acrOss boRders linKed*" (STORK), para permitir aos cidadãos de diferentes países utilizar os seus cartões de identidade eletrónica através das fronteiras. Estes esforços exigem que as nações estabeleçam medidas técnicas e jurídicas para assegurar a interoperabilidade transfronteiriça.

- Acessibilidade do cartão e-ID

A acessibilidade é um fator importante para conseguir a adoção generalizada das identidades eletrónicas, sendo a mesma influenciada tanto pelo custo da identidade eletrónica como pela prosperidade relativa da população. Os países maiores devem beneficiar de economias de escala e ver um custo médio por pessoa inferior para as identidades eletrónicas. Os países mais ricos deveriam por sua vez ter mais probabilidades de criar iniciativas de identidade eletrónica, uma vez que os programas seriam mais acessíveis.

Determinados cartões de identidade eletrónica exigem uma taxa adicional para instalar os certificados digitais utilizados para autenticação e assinatura eletrónicas. Esta taxa pode ser paga ao governo ou a uma autoridade certificadora do sector privado. O custo total da identidade eletrónica depende igualmente da frequência com que a identidade eletrónica deve ser renovada e da taxa de renovação associada. Por exemplo, em Espanha, o cartão de identidade eletrónica é válido por cinco anos para as pessoas com menos de trinta anos, dez anos para as que têm entre trinta e setenta anos e não expira para as que têm mais de setenta. O certificado digital, porém, só é válido por trinta meses (Heichlinger & Gallego, 2010). O custo da solução de identidade eletrónica depende igualmente dos eventuais extras necessários, como os leitores de cartões.

3.3.Projeto STORK (Secure idenTity acrOss boRders linKed)

O STORK foi lançado quando catorze Estados-Membros da UE e do EEA reuniram-se para formar uma parceria para concorrer a uma bolsa piloto em larga escala (*Large Scale Pilot* - LSP) no âmbito da Comissão Europeia Competitividade e Inovação (CIP) no fluxo do Programa de Apoio à Política de Tecnologias de Informação e Comunicação (ICT-PSP). O projeto teve início em 2008 com a Áustria, Bélgica, Estónia, França, Alemanha, Islândia, Itália, Luxemburgo, Portugal, Eslovénia, Espanha, Suécia, Países Baixos e Reino Unido. A extensão de 2010 incluiu a Finlândia, Lituânia, Noruega, e República Eslovaca.

O STORK LSP começou como um "LSP tipo A" em junho de 2008 e durou três anos, até maio de 2011. A ideia dos LSP de tipo A passa por fazer avançar os principais domínios da política europeia em matéria de ICT através de projetos em larga escala conduzidos pelos próprios Estados-Membros e cofinanciados pela Comissão Europeia. Quatro dessas áreas chave foram definidas no Programa CIP ICT-PSP, sendo o eID um dos domínios-chave que finalmente deram origem ao STORK. A estrutura do projeto STORK pode ser dividida em três fases sucessivas (Philip Schütz, et al., 2011):

1. Primeiro veio um exercício de levantamento de stocks. O objetivo era obter uma visão aprofundada dos sistemas nacionais de identificação eletrónica que devem ser incorporados no quadro de interoperabilidade da STORK eID. Os aspetos jurídicos, operacionais e técnicos foram investigados.
2. A segunda fase consistiu no desenvolvimento e implementação de especificações técnicas comuns. Esta fase deu origem ao quadro de interoperabilidade do STORK eID.
3. O quadro de interoperabilidade foi implantado em várias aplicações de produção nacional. Foram definidos seis projetos-piloto deste tipo.

O projeto teve início em 2008 com a Áustria, Bélgica, Estónia, França, Alemanha, Islândia, Itália, Luxemburgo, Portugal, Eslovénia, Espanha, Suécia, Países Baixos e Reino Unido. A extensão de 2010 incluiu a Finlândia, Lituânia, Noruega, e República Eslovaca.

3.3.1. Transferência de atributos através da infraestrutura do STORK

A estrutura de interoperabilidade STORK eID ligou os sistemas eID de 18 países europeus através de componentes PEPS e *middleware*. O projeto definiu e implementou um protocolo

comum de pedido/resposta de autenticação e transferência de atributos entre diferentes países da UE para permitir aos cidadãos o acesso a serviços no estrangeiro enquanto ainda estão a ser autenticados no seu país de origem. Este protocolo foi baseado no protocolo Security Assertion Markup Language (SAML) 2.0, que foi estendido para conter atributos sobre pessoas físicas. STORK foi testado em vários serviços piloto, tais como chat mais seguro, mobilidade estudantil, mudança de endereço ou Serviço de Autenticação da Comissão Europeia (ECAS). Além disso, a estrutura STORK também foi estudada para ser explorada para validação de certificados digitais, uma vez que a implementação da validação de certificados ainda hoje é intensamente estudada (Berbecaru D, 2019).

A estrutura STORK definiu dois modelos de interoperabilidade, a saber, o modelo proxy e o modelo *middleware*. Um país que aderisse ao modelo proxy tinha de executar um único *gateway* chamado PEPS. Este componente foi logicamente chamado de C-PEPS no país em que o cidadão foi autenticado e S-PEPS no país Prestador de Serviços (SP – *Service Provider*), conforme ilustrado na figura 14. No modelo *middleware*, os SPs integravam os eIDs estrangeiros usando um *middleware* específico do país, por exemplo, o descrito no trabalho de Zwattendorfer.

O projeto STORK tratou apenas dados sobre pessoas singulares (cidadãos) que foram explorados em alguns serviços públicos testados, por exemplo, o ECAS foi melhorado com o apoio à autenticação através do STORK. Neste contexto, no STORK, o Fornecedor de Identidade ou IdP(*Identity Provider*) foi responsável pela autenticação de uma pessoa e forneceu também um conjunto limitado de atributos pessoais, tais como o nome dado, apelido e data de nascimento, que foram normalmente armazenados juntamente com a informação pessoal do utilizador no IdP onde o utilizador se registou e obteve as suas credenciais de autenticação.

3.3.2. Arquitetura STORK e atributos suportados

Nesta parte, é descrita tanto a arquitetura quanto os atributos trocados entre os principais atores da STORK. Cada PEPS tinha duas partes implementando dois tipos de protocolos, a saber, uma parte específica e uma parte comum. A parte específica foi utilizada para a comunicação com os SPs e IdPs nacionais, enquanto a parte comum foi utilizada para a comunicação com os outros nós do PEPS e implementou o protocolo de comunicação STORK (baseado no SAML 2.0 WebSSO Profile) especificado no projeto.

O pedido de autenticação transfronteiriça foi enviado de um SP para a sua interface PEPS nacional chamada S-PEPS, e, quiçá, foi encaminhado para a interface PEPS do país do cidadão chamada C-PEPS. Após autenticação bem-sucedida, a resposta de autenticação SAML contendo também os atributos valorizados foi devolvida através da infraestrutura PEPS de volta ao SP requerente. Podemos observar o fluxo de trabalho da mensagem na figura 15 que é detalhado de seguida baseado em (Berbecaru D, 2019).

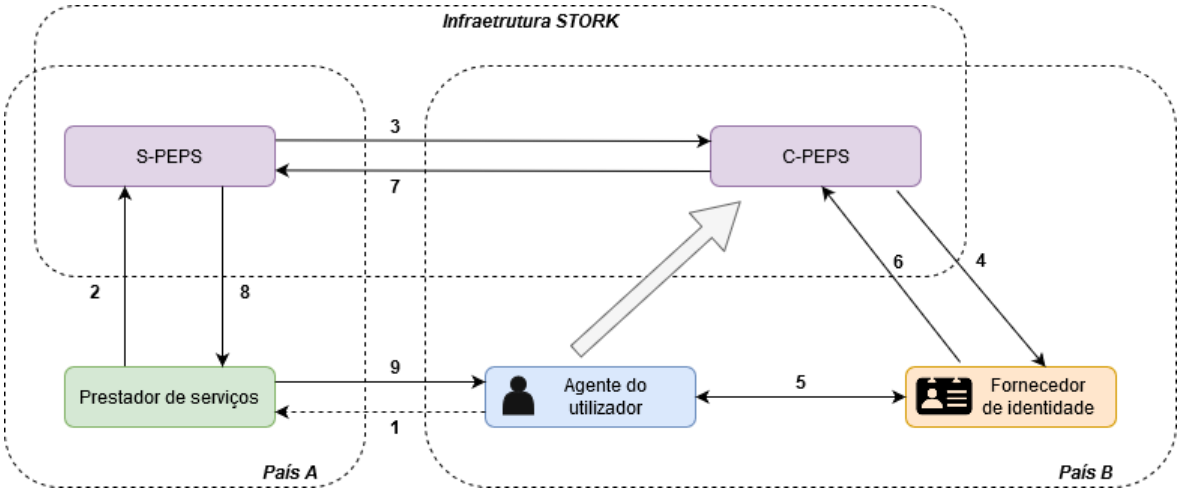


Figura 15 - Autenticação e transferência de atributos através da infraestrutura da STORK (Berbecaru D, 2019)

1-2. Para aceder a um serviço de STORK baseado na web, o SP pediu primeiro ao utilizador que escolhesse o país no qual ele se autenticará (passo 1). Embora o protocolo de comunicação entre SP e S-PEPS fosse específico para MS, a maioria dos países também utilizou o protocolo STORK para essa conexão. Ao selecionar o país, o SP gerou um pedido de autenticação STORK (*AuthnRequest*), que era um tipo especial de SAML2 *AuthnRequest*; em seguida, assinou-o digitalmente com uma chave privada SP (assimétrica), e o enviou para o S-PEPS através do navegador do utilizador (passo 2).

O STORK *AuthnRequest* incluía um conjunto de atributos de identificação e autenticação solicitados pelo SP para conceder acesso ao serviço, por exemplo, *eIdentifier*, *givenName*, *eMail*, e o nível QAA (*Quality Authentication Assurance*), ou seja, o nível mínimo de autenticação necessário para autenticar o utilizador. O país do cidadão também foi enviado para o S-PEPS, por exemplo, como um parâmetro no formulário HTTP.

3. Em seguida, o S-PEPS construiu uma nova STORK *AuthnRequest*, que foi assinada digitalmente com a chave privada S-PEPS (assimétrica) armazenada numa loja dedicada ao PEPS e, posteriormente, foi enviada para o C-PEPS (passo 3) usando o SAML2 POST

Binding. Este pedido foi baseado no recebido do SP e enumerar os atributos de utilizador necessários. O C-PEPS validou o STORK *AuthnRequest* recebido do S-PEPS utilizando a sua chave pública, que tinha de ser incluída certificado-chave em cada PEPS. Este mecanismo seria alterado no eIDAS, explorando os metadados SAML, que detém os certificados digitais necessários para validar as assinaturas nas mensagens SAML. Os atributos também seriam criptografados (esta funcionalidade não estava presente nem no STORK nem no STORK2). A seguir, construiu uma nova STORK *AuthnRequest*, que foi assinada digitalmente com a chave privada (assimétrica) do PEPS. Observamos que, em STORK, o PEPS foi projetado para entrar em contato com um IdP único; assim, o código permitiu configurar uma URL única para o IdP. No entanto, na parte específica do MS, cada país foi permitido alterar a seleção do IdP, por exemplo, permitindo ao cidadão selecionar de uma lista de IdPs aquele a ser usado para autenticação naquela transação.

4-5. Após a seleção do IdP, o pedido foi enviado (através do browser do utilizador) para o IdP, utilizando o SAML2 POST Binding (passo 4). A IdP autenticou o cidadão utilizando a(s) sua(s) credencial(is) de autenticação nacional(is) e um processo/protocolo de autenticação específico para cada país (passo 5).

6. A IdP construiu uma resposta de autenticação STORK, que era também um tipo de elemento de resposta especial SAML2. A resposta de autenticação incluiu a identificação e a informação de autenticação solicitadas num elemento de avaliação SAML2. Cada atributo de identificação e autenticação foi agrupado num elemento específico de atributo SAML2, que foi definido no perfil SAML2 STORK. Finalmente, a resposta de autenticação STORK foi digitalmente assinado pelo IdP com a sua chave privada e enviado para o C-PEPS utilizando o SAML2 POST vinculativo.

7. Após validação da assinatura na resposta SAML2, utilizando a chave pública do IdP incluída na loja de chaves de certificados no PEPS, o C-PEPS processou internamente a mensagem recebida. Todos os atributos foram extraídos do elemento Assertion do SAML2, depois foram filtrados, o que significa que os atributos que não foram solicitados foram descartados, enquanto os que foram solicitados foram verificados se foram valorizados. Caso os atributos obrigatórios não tenham sido devolvidos, foi gerado um erro e a transação foi interrompida. Na parte específica do MS, foram também realizadas outras operações, como a derivação de atributos, por exemplo, o atributo *ageOver* foi derivado da data de nascimento devido a requisitos de proteção da privacidade. Além disso, o C-PEPS exigia o

consentimento do utilizador para a guarda dos seus atributos ao S-PEPS. Se o consentimento foi dado, o C-PEPS criou uma resposta SAML2 assinada que continha os atributos avaliados e enviou-a ao S-PEPS através do navegador do utilizador com o método HTTP POST.

8-9. O S-PEPS validou a assinatura na resposta SAML2 utilizando a chave pública do C-PEPS armazenada na loja de chaves de certificados no C-PEPS. Em seguida, extraiu todos os atributos do elemento de certificação do SAML2 e mapeou-os (se necessário) para um formato reconhecido pelo SP. Uma vez que se assume que o protocolo STORK foi utilizado na comunicação entre SP e S-PEPS, não foi necessário fazer mais nenhum mapeamento/filtragem de atributos em S-PEPS. O S-PEPS criou uma resposta SAML2 assinada que inclui os atributos valorizados e enviou-a ao SP (passo 8), onde os atributos certificados foram extraídos e verificados para permitir o acesso ao serviço solicitado (passo 9).

3.3.3. Atributos STORK

STORK não só alargou o formato SAML 2.0 para conter os atributos de utilizador pessoal mais comuns, por exemplo, *eIdentifier*, *givenName*, *surname*, *dateOfBirth*, *canonicalResidenceAddress* e *fiscalNumber*, como também permitiu que um documento assinado fosse transferido através da infraestrutura (o chamado atributo signedDoc) ou mesmo uma autorização de residência, um pseudónimo, ou o estado civil, mas, tanto quanto se sabe, estes atributos não foram efetivamente utilizados em cenários de caso de utilização. Além disso, definiu também o nível Quality Authentication Assurance (QAA), indicando a qualidade da autenticação que está a ser solicitada. Para estabelecer a confiança, os métodos de autenticação utilizados pelos sistemas nacionais de identificação eletrónica foram classificados em quatro classes de garantia de GQA (mínima, baixa, substancial e elevada). A classificação é comparável às LOA definidas como trust ratings para a administração dos EUA. Para dar acesso a um serviço, um SP pode solicitar um determinado nível mínimo de GQAA no pedido de autenticação, que foi enviado ao IdP responsável pelo processo de autenticação efetivo do cidadão. Se o IdP autenticasse o cidadão com um método cujo nível de garantia cumprisse a GQA solicitada (ou superior), então a resposta de autenticação e os atributos eram enviados para o SP; caso contrário, era gerado um erro e a transação era interrompida.

Note-se que a maioria destes atributos pessoais tinha uma estrutura simples, tipicamente, cada atributo tinha um valor. A seguinte tabela 5 apresenta uma seleção de alguns atributos importantes para pessoas singulares utilizados para identificação e autenticação transfronteiriça, enquanto o conjunto completo de atributos definidos em STORK se encontra no trabalho de (Berbecaru D, 2019).

Tabela 5 - Principais atributos da pessoa singular em STORK, STORK 2.0 e infraestruturas eIDAS (Berbecaru D, 2019)

SAML Atributo Nome STORK & STORK 2.0	eIDAS	Descrição
eIdentifier	PersonIdentifier	Identificador único da pessoa singular
Nome próprio (*givenName*)	CurrentGivenName	Nome próprio da pessoa singular
Apelido (*surname*)	CurrentFamilyName	Apelido da pessoa singular
Date de nascimento (dateOfBirth)	DateOfBirth	Data de nascimento de uma pessoa singular
canonicalResidenceAddress	CurrentAddress	Endereço atual da pessoa singular, tal como registado junto da autoridade do Estado-Membro (base64 codificada)
gender	Gender	Género
eMail	-	E-mail da pessoa singular
age	-	Idade da pessoa singular
isAgeOver		Limite de idade da pessoa singular
fiscalNumber	-	Número de identificação fiscal da pessoa singular

Na STORK 2.0, o foco passou a ser a definição e troca de novos atributos (por exemplo, para pessoas coletivas e para domínios académicos específicos) e de novas entidades, as chamadas APs. Descrevemos o nosso trabalho na adaptação da parte específica do nó

nacional responsável pela transferência das mensagens de autenticação e atribuição, a implementação de uma AP, e as limitações encontradas.

A infraestrutura do eIDAS é intensamente discutida porque implementa o Regulamento eIDAS na Europa. No entanto, por defeito, esta infraestrutura apenas transfere informações mínimas sobre pessoas sejam elas singulares ou coletivas. Para poder construir serviços, são necessários novos atributos, específicos do sector.

3.3.4. Implementação a nível europeu

No âmbito do projeto STORK o Fornecedor de Autenticação permite que um cidadão estrangeiro se autentique num serviço português, ou que um cidadão nacional se autentique num serviço de um outro Estado Membro. A generalização dos serviços transfronteiriços é uma das prioridades da Comissão Europeia e a AMA é a entidade nacional com responsabilidade técnica e política para articular a posição portuguesa. Segundo (Martins, 2013), no preciso momento do relatório de atividades de 2012 estava a ser desenvolvido o projeto STORK 2.0, o qual prevê a adição de certificação de atributos, a par dos mecanismos de autenticação forte já implementados.

STORK 2.0, juntamente com parceiros da equipa CEF Digital e da task force eIDAS, apresentou o estado do projeto e a história de sucesso que reúne 58 organizações de 19 Estados-Membros, num Seminário sobre identificação e autenticação eletrónica (Parlamento Europeu, 25/3/2015). O autor Daniel Quer da STORK 2.0 escreveu a 31 de março de 2015, “Sou espanhol, e gostaria de comprar uma casa na Grécia. Mas terei, no entanto, de passar longas horas em aviões com o único objetivo de assinar uma grande quantidade de papelada. Porque não posso provar a minha identidade e assiná-la online?” sabemos que os europeus fazem negócios noutros países, dessa forma têm de cumprir procedimentos onerosos com agências publicas de outros Estados-Membros. É por isso que, quando se trata de identificação e autenticação em serviços transfronteiriços, a simplicidade deve ser tão fundamental como a exatidão da informação. É neste preciso momento que o projeto STORK entra em ação, disponibilizando uma infraestrutura transfronteiriça destinada a integrar os modelos de identificação eletrónica existentes em muitos Estados-Membros e a permitir serviços transfronteiriços que pretendem criar eficiências tanto no setor público como privado.

Um tópico que foi levantado foi relativamente aos atributos de identidade STORK 2.0. Atributos para além da identidade são a funcionalidade adicional que STORK 2.0 propõe, em comparação com o STORK. Surgindo a questão: "Será um nome completo e um número de identificação, suficiente para identificar alguém?" as pessoas também têm papéis que as identificam como sendo quem são. Através destes atributos, STORK 2.0 permite abordar as muitas funções diferentes que se podem ter, e permite associar detalhes pessoais adicionais ao seu ID eletrónico.

O projeto-piloto europeu STORK e o seu sucessor STORK 2.0 criaram um sistema de ponte, uma arquitetura pan-europeia de gestão da identidade eletrónica para permitir que os meios de autenticação de um país sejam aceites por candidaturas noutro país da União Europeia. Por exemplo, os certificados digitais de um país X podem ser utilizados para autenticar cidadãos no país Y. Estas mesmas plataformas, STORK e STORK 2.0, foram testadas m vários casos de utilização piloto, como para mobilidade de estudantes, para acesso Wi-fi ou para validação de certificados digitais. O que inicialmente faltava no STORK era a definição de responsabilidades claras e segurança jurídica no que diz respeito a casos de serviços sensíveis, como nos domínios bancários, financeiros e aplicações de saúde. No entanto, os resultados e conclusões do projeto STORK foram utilizados como base na definição do regulamento de identificação eletrónica, autenticação e serviços de confiança (eIDAS), o código foi explorado para contruir uma implementação da amostra eIDAS e o protocolo STORK foi utilizado como ponto de partida na definição das especificações técnicas do eIDAS. Em 2019, muitos países já haviam criado nós eIDAS, atuando como pontes nacionais, que fazem parte da infraestrutura eIDAS e realizaram testes de conformidade dos nós eIDAS com a Comissão Europeia.

Para autenticar as pessoas e fornecer-lhes atributos básicos, os nós eIDAS estão ligados aos IdPs nacionais que fazem parte de um esquema de identificação eletrónica notificando esse país. A Alemanha, Itália, Bélgica, Espanha, Estónia e Croácia já notificaram os seus esquemas de eID ao abrigo do eIDAS, enquanto que outros países se encontravam em vias de o fazer. Sendo que, encontram-se a realizar a adaptação da interface do seu nó nacional do eIDAS para se ligarem aos esquemas nacionais do eID, de modo a permitir aos seus cidadãos autenticarem-se noutros países utilizando credenciais de autenticação emitidas por um dos seus IdPs(Identity Provider) notificados (Ribeiro, Leitold, Esposito, & Mitzam, 2017).

Os problemas relacionados com as normas nacionais incompatíveis para eID e eSignature foram o ponto de partida para o Projecto STORK. Iniciado em 2008 e concluído em 2012, STORK (Secure IdenTity acrOss boRders linked) foi a primeira tentativa de permitir a interação do eID local, nacional, com serviços estrangeiros. O projeto mostrou que este cenário é possível quer através da utilização de *middleware* para que o utilizador possa aceder diretamente ao sistema de serviços estrangeiros, quer através da utilização de um Serviço de Proxy. Após a sua conclusão, o projeto STORK foi continuado com STORK 2 com a intenção de alargar a interoperabilidade do eID à representação eletrónica e aos mandatos eletrónicos. O projeto abordou áreas importantes como: eBanking, eHealth, eLearning e Serviços Públicos e envolveu mais de 55 parceiros de 19 países europeus (membros e associados da UE).

4. Cartão de Cidadão Português e assinatura digital

"O Cartão de Cidadão é um documento de cidadania que permite ao cidadão identificar-se de forma segura. Para além de um documento de identificação físico, o Cartão de Cidadão é um documento eletrónico que possibilita a realização de várias operações sem necessidade de interação presencial." É designado como o documento de cidadania português desenvolvido no âmbito do programa XVII Governo Constitucional, criado como política integradora de desenvolvimento científico e tecnológico, integrado no programa científico desenvolvido como projeto de modernização.

A 5 de fevereiro de 2007 foi publicada a Lei nº7/2007, que cria o cartão de cidadão e rege a sua emissão e utilização. A criação do Cartão de cidadão conduziu à substituição de cinco outros cartões, são eles: o bilhete de identidade, cartão de eleitor, cartão de contribuinte, cartão de beneficiário da Segurança Social e cartão de utente do Serviço Nacional de Saúde (SNS), de forma a evitar a dispersão de suportes físicos sem reduzir os números identificadores afetos a cada cidadão. Desta forma, apresenta como funcionalidade imediata a identificação visual tal como o antigo Bilhete de Identidade sendo o presente Cartão de cidadão dotado de uma nova funcionalidade de identificação e autenticação eletrónica. Adicionalmente, o cartão de cidadão apresenta informação acerca do sexo, altura, nacionalidade, filiação, data de nascimento e data de validade, como podemos observar na figura 16 e figura 17. Sendo que a frente do cartão de cidadão contém informação textual específica sobre a identificação do titular do mesmo. O verso do cartão de cidadão contém informação textual específica dos atuais documentos de identificação sectoriais do titular bem como uma zona de leitura ótica.

Figura 16 - Informação inscrita na frente do Cartão de Cidadão

Figura 17 - Informação inscrita no verso do Cartão de Cidadão

O **cartão de cidadão como documento físico:**

- permite ao respetivo titular provar a sua identidade perante terceiros através da leitura de elementos visíveis, coadjuvada pela leitura ótica de uma zona específica;

O **cartão de cidadão como documento digital permite ao respetivo titular:**

- provar a sua identidade perante terceiros através de autenticação eletrónica. Sendo que, nenhuma autoridade ou entidade pública ou privada pode exigir para efeitos de identificação qualquer outro dado pessoal do titular de cartão de cidadão que não seja facultado pelos respetivos meios eletrónicos;
- autenticar de forma unívoca através de uma assinatura eletrónica qualificada a sua qualidade de autor de um documento eletrónico, de onde decorre que nenhuma autoridade ou entidade pública ou privada pode recusar o valor probatório da assinatura eletrónica aposta pelo cidadão num documento eletrónico.

Com o intuito de integrar o cartão de cidadão no plano de desenvolvimento e política a implementar no nosso país, tanto a nível público como a nível privado, foram designados como objetivos estratégicos (Rito, 2018):

- Garantir uma maior segurança na identificação dos cidadãos;
- Harmonização do sistema de identificação civil dos cidadãos nacionais com os requisitos da União Europeia;
- Simplificação da vida dos cidadãos, através da agregação física de vários cartões:
- Promoção do uso dos serviços eletrónicos, com recurso a meios de autenticação e Assinatura Digital Qualificada;
- Melhoria da prestação dos serviços públicos, alinhando a modernização organizacional e tecnológica;

- Racionalização de recurso, meios e custos para o Estado, para os cidadãos e para as empresas;
- Promoção da competitividade nacional por via da reengenharia e da simplificação de processos e de procedimentos.

A sociedade encontra-se em contacto com o desenvolvimento do mundo digital atual, sendo que é cada vez usual a realização de transações eletrónicas, pelo que os objetivos anteriormente apresentados vão de encontro ao desenvolvimento tecnológico existente. No ponto de vista da segurança o cartão de cidadão apresenta as seguintes características de segurança simples apresentadas nas seguintes figuras 18 e 19 apresentadas.

Figura 18 - Características de segurança simples na frente do cartão de cidadão

Figura 19 - Características de segurança simples no verso do cartão de cidadão

4.1.1. Características e funcionalidades eletrónicas

O cartão de cidadão tem um formato *smartcard.* dado que possui um microcomputador embebido também designado de chip. Alguma informação como por exemplo, a data e local

de emissão do documento, estado civil e o número de eleitor apenas pode ser consultada através do seu chip com a introdução de códigos de acesso.

No chip do cartão de cidadão residem os dados inscritos no cartão, com exceção da assinatura digitalizada, sendo que as aplicações referidas permitem a execução das seguintes funcionalidades também observadas na figura 20 (UCMA/UMIC/DGRN, 2007):

- IAS – aplicação responsável pelas operações de autenticação e assinatura eletrónica;
- EMV-CAP – aplicação responsável pela geração de palavras-chave únicas por canais alternativos (por exemplo: telefone);
- Match-on-card – aplicação responsável pela verificação biométrica de impressões digitais.

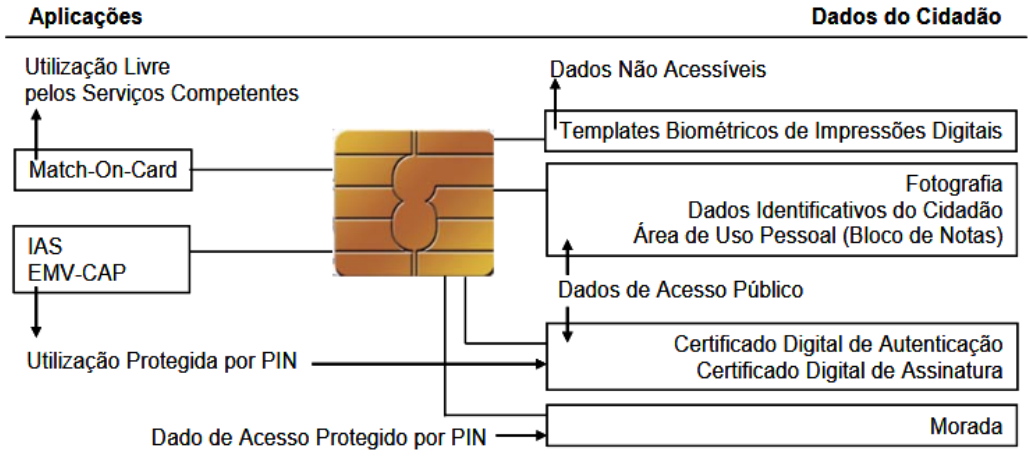


Figura 20 - Informação e aplicações residentes no chip/smartcard

Do ponto de vista eletrónico e com base na leitura (Zuquete, 2013), compreende-se que o *smartcard* do cartão de cidadão permite:

- Guardar informação pessoal para validação informática interna da identidade do titular. Concretamente, esta informação é construída por elementos descritivos (referências biométricas) de impressões digitais do titular. Estas referências biométricas são usadas apenas internamente ao smartcard para validar uma impressão digital comunicada ao mesmo;"
- Guardar informação privada. Informação privada é informação que o titular pode usar, mas não conhecer ou divulgar. Concretamente, esta informação é constituída por três chaves criptográficas:
    1. Uma chave simétrica de autenticação do titular.

2. Uma chave privada de um par de chaves assimétricas RSA, que serve para autenticar o titular.
3. Uma chave privada de um par de chaves assimétricas RSA, que serve para produzir assinaturas digitais do titular;"

- Guardar informação reservada. Informação reservada é informação que o titular conhece, mas que apenas disponibiliza de forma fidedigna, via *smartcard*, a quem desejar ou a quem tiver autorização para a obter, independentemente da vontade do titular. Concretamente, esta informação é constituída pela morada do titular;
- Guardar informação pública de grande dimensão, não memorizável. Esta informação é constituída pela fotografia do titular e por certificados X.509v3 de chaves públicas do titular, chaves essas que podem ser usadas para autenticar o titular ou a assinatura digital;
- Guardar toda a informação do titular observável no cartão de cidadão (fotografia, nome, data de nascimento, os diversos números de identificação, validade do cartão, etc.);"

"As operações realizadas pelo *smartcard* em nome do respetivo titular necessitam que o mesmo indique um código secreto (PIN)." Cada cartão de cidadão possui 3 PIN, cada um com 4 algarismos. Tendo cada um deles uma funcionalidade, sendo elas, para autorizar a indicação da morada, para autenticação do titular e para produzir uma assinatura digital. Os PIN anteriormente referidos são os elementos chave que tornam o *smartcard* do Cartão de Cidadão pessoal, ou seja, a perda do cartão de cidadão não permite a quem o encontrar o usufruto das respetivas funcionalidades porque o número de tentativas erradas de descoberta é limitado. Em caso de perda do mesmo e de forma a evitar que alguém descubra o PIN, o Cartão de Cidadão é fornecido com um código de cancelamento, pelo que pode ser comunicado às autoridades competentes um número de 8 algarismos para invalidar todas as funcionalidades do *smartcard* em caso de extravio.

4.1.2. Certificados digitais utilizados pelo Cartão de Cidadão

Os certificados presentes no Cartão de Cidadão são certificados X.509v3 de chaves públicas do titular tendo estes certificados sido referidos num capítulo anterior, as chaves podem ser utilizadas para autenticar o titular e a sua assinatura digital.

Um certificado digital é um documento com uma estrutura específica que possui uma chave pública de uma dada entidade e uma assinatura digital do certificado feito pela entidade emissora do mesmo. A entidade emissora pode ser uma pessoa, uma organização, uma

aplicação informática ou qualquer outra entidade confiável pela Autoridade de Certificação (*Certification Authority*, CA) (Gomes, 2015). Os certificados digitais são documentos com um tempo de validade limitado, podendo este tempo ser controlado de duas formas: através de um prazo de validade não alterável sendo este indicado no próprio certificado e através de certificados de revogação. Um certificado de revogação é um certificado especial emitido por uma Autoridade de Certificação, onde se declara que uma dada chave pública pertencente a uma dada entidade deixa de ser válida a partir de uma determinada data. Normalmente, estes certificados de revogação são emitidos pela mesma entidade que emite os certificados.

Desta forma, os certificados digitais são elementos que têm como base a criptografia com chave pública sendo que referenciando a assinatura digital estes são essenciais num modelo de segurança, com o objetivo de tentar impossibilitar ou dificultar ao máximo a sua falsificação (Almeida, 2009).

Tendo em conta as leituras (Barbosa M. , 2005) aquando da validação de informação assinada digitalmente, geralmente o processo consiste nos seguintes passos realizados pelo destinatário:

1. Verificar se a identidade indicada pelo emissor está de acordo com a identidade indicada no certificado;
2. Verificar se o certificado é válido;
3. Verificar que a informação que recebe está de acordo com as permissões e/ou privilégios do emissor;
4. Utilizar a chave pública contida no certificado para verificar a assinatura da informação recebida.

Pelo que, quando a informação assinada pelo emissor é aceite pelo destinatário e esta permanece inalterada, o certificado passa a ser utilizado pelo emissor. Por sua vez, o emissor valida o certificado e a identidade do destinatário, utiliza a chave pública contida no certificado para cifrar a informação e envia a informação ao destinatário que a decifra com a sua chave privada. Na seguinte figura 21 é possível observar e por sua vez identificar a hierarquia das entidades de certificação dos certificados presentes no Cartão de Cidadão.

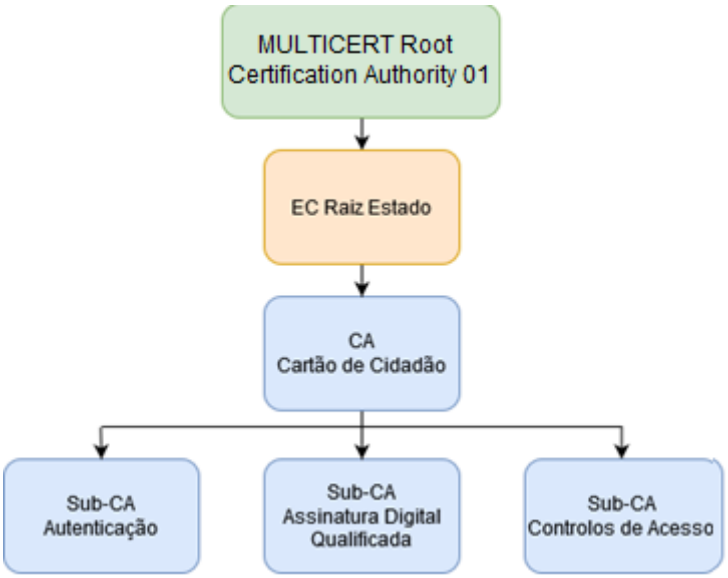


Figura 21 - Hierarquia de entidades de certificação dos certificados presentes no Cartão de Cidadão

Conforme a consulta (Zuquete, 2013) e (Almeida, 2009) a infraestrutura PKIX é a PKI adotada na Internet, adaptando os certificados X.509v3 à Internet e especificando as extensões, ou seja, quando presentes no cartão de cidadão o mecanismo de extensão permite diferenciar o tipo de utilização da chave pública. Na figura 22 podemos observar uma representação da extensão *Key Usage* que garante o não-repudio da assinatura estando este presente no certificado de assinatura digital qualificado do cartão de cidadão.

[Certificado de Assinatura Digital Qualificada]

```
X509v3 Key Usage: critical
    Non Repudiation
```

[Certificado de Autenticação]

```
X509v3 Key Usage: critical
    Digital Signature, Key Agreement
```

Figura 22 - Extensão Key Usage dos certificados X.509 presentes no Cartão de Cidadão (Almeida, 2009)

Com base na Lei Portuguesa referida anteriormente, a Lei N. º7/2007 de 5 de Fevereiro, cria o cartão de cidadão e rege a sua emissão, substituição, utilização e cancelamento. Acerca da identificação eletrónica e assinatura eletrónica é essencial compreender pontos importantes como eficácia, estrutura e funcionalidades bem como certificados digitais, destacando-se os seguintes artigos:

Artigo 1.º da Lei n.º 7/2007, de 5 de Fevereiro, "*o cartão de cidadão é um documento autêntico que contém os dados de cada cidadão relevantes para a sua identificação e inclui*

o número de identificação civil, o número de identificação fiscal, o número de utente dos serviços de saúde e o número de identificação da segurança social."

Nos termos do Artigo 4.º- Eficácia, *"O cartão de cidadão constitui título bastante para provar a identidade do titular perante quaisquer autoridades e entidades públicas ou privadas, sendo válido em todo o território nacional, sem prejuízo da eficácia extraterritorial reconhecida por normas comunitárias, por convenções internacionais e por normas emanadas dos órgãos competentes das organizações internacionais de que Portugal seja parte, quando tal se encontre estabelecido nos respectivos tratados constitutivos."*

Artigo 6.º - Estrutura e funcionalidades

"1 — O cartão de cidadão é um documento de identificação múltipla que inclui uma zona específica destinada a leitura óptica e incorpora um circuito integrado.

2 — O cartão de cidadão permite ao respectivo titular:

a) Provar a sua identidade perante terceiros através da leitura de elementos visíveis, coadjuvada pela leitura óptica de uma zona específica;

b) Provar a sua identidade perante terceiros através de autenticação electrónica;

c) Autenticar de forma unívoca através de uma assinatura electrónica qualificada a sua qualidade de autor de um documento electrónico.3 — A leitura óptica da zona específica do cartão, mencionada na alínea a) do n. º2, está reservada a entidades ou serviços do Estado e da Administração Pública, bem como à identificação do titular no âmbito das especificações técnicas do cartão para documentos de viagem"

Artigo 18.º - Certificados digitais

"1 — Com o cartão de cidadão é emitido um certificado para autenticação e um certificado qualificado para assinatura electrónica qualificada necessários à sua utilização electrónica.

2 — O certificado de autenticação é sempre activado no momento da entrega do cartão de cidadão.

3 — O certificado qualificado para assinatura electrónica qualificada é de activação facultativa, mas só pode ser activado e utilizado por cidadão com idade igual ou superior a 16 anos.

4 — Também não há lugar à activação do certificado qualificado para assinatura electrónica qualificada se o titular do pedido de cartão de cidadão se encontrar interdito ou inabilitado.

5 — De cada vez que pretenda utilizar alguma das funcionalidades de comunicação electrónica activadas no cartão de cidadão, o respectivo titular tem de inserir previamente o seu código pessoal (PIN) no dispositivo de leitura pertinente

.6 — Os certificados são revogáveis a todo o tempo e, após revogação, a emissão de novos certificados associados ao cartão de cidadão só é possível com a respectiva substituição.

7 — Ao certificado para autenticação e ao certificado qualificado para assinatura electrónica qualificada aplica-se o disposto no Decreto-Lei n.o290-D/99, de 2 de Agosto, republicado pelo Decreto-Lei n.o62/2003, de 3 de Abril, e alterado pelos Decretos-Leis n.os165/2004,de 6 de Julho, e 116-A/2006, de 16 de Junho, estando aqueles certificados sujeitos às regras legais e regulamentares relativas ao Sistema de Certificação Electrónica do Estado."

Como legislação aplicável também se apresenta a seguinte:

A **Portaria n.º 201/2007, de 13 de Fevereiro**, regula, no período que antecede a expansão a todo o território nacional, a localização e as condições de instalação dos serviços de recepção dos pedidos do cartão de cidadão.

A **Portaria n.º 202/2007, de 13 de Fevereiro**, aprova o modelo oficial e exclusivo do cartão de cidadão para os cidadãos nacionais e para os beneficiários do estatuto referido no n.º 2 do artigo 3.º da Lei n.º 7/2007, de 5 de Fevereiro.

A **Portaria n.º 203/2007, de 13 de Fevereiro**, regula o montante das taxas devidas pela emissão ou substituição do cartão de cidadão, as situações em que os atos devem ser gratuitos e a taxa devida pela realização do serviço externo, no âmbito do pedido de emissão ou substituição do cartão.

4.1.3. Estatísticas

Consultando as estatísticas disponibilizadas no website da Autenticacao.gov podemos verificar as autenticações realizadas com o cartão de cidadão e da chave móvel digital. Pelo que se apresentam os dados estatísticos sobre autenticações eletrónicas feitas com os meios Autenticação.gov a evolução do número de autenticações, total de autenticações por ano e total acumulado, total de autenticações por meio e top 10 de entidades com autenticações.

Consultado o *website* https://www.autenticacao.gov.pt/estatisticas-de-autenticacao, a setembro de 2020, as estatísticas apresentadas são as seguintes:

- **Evolução do número de autenticações**, neste ponto através da visualização e análise do gráfico 1 podemos observar que de 2015 a 2020 as autenticações eletrónicas realizadas têm vindo a aumentar, existem pontos em que observamos uma redução dessas mesmas autenticações sendo que existe um pico de autenticações em 2020 e de momento indica uma descida nesse mesmo número.

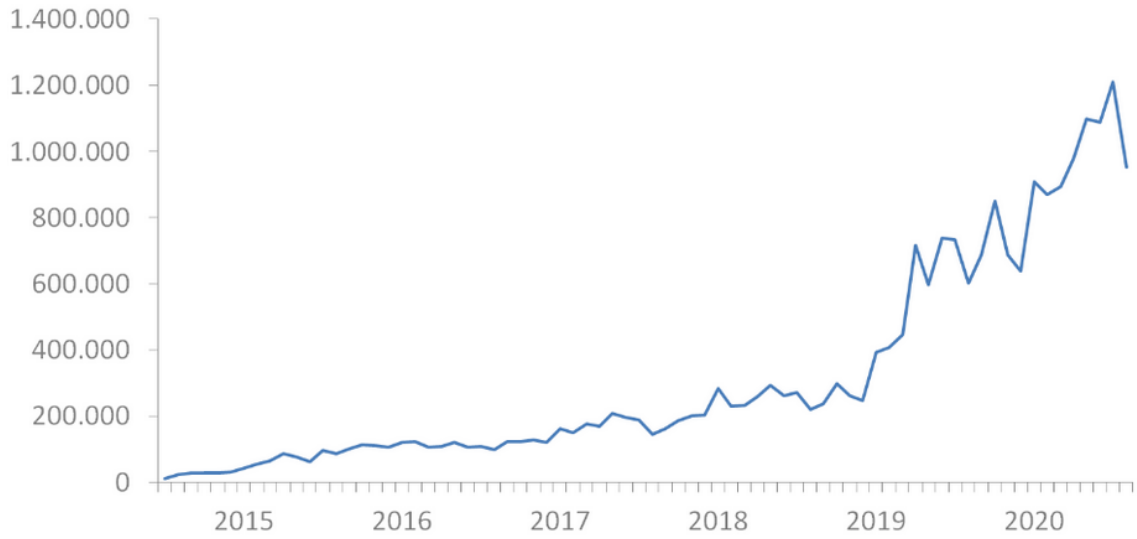


Gráfico 1 - Evolução do número de autenticações

- **Autenticações por ano,** de acordo com os registos consultados no gráfico 2, de 2014 até ao presente ano (2020) existe um aumento de 7.854.151 autenticações realizadas. De ano para ano, o maior aumento apresentado é o de 2018 para 2019 com um aumento de 4.398.209 autenticações. O ano com maior número, como podemos

observar no gráfico, é o ano 2020. O valor 23.265.041 representa o número total de autenticações acumuladas.

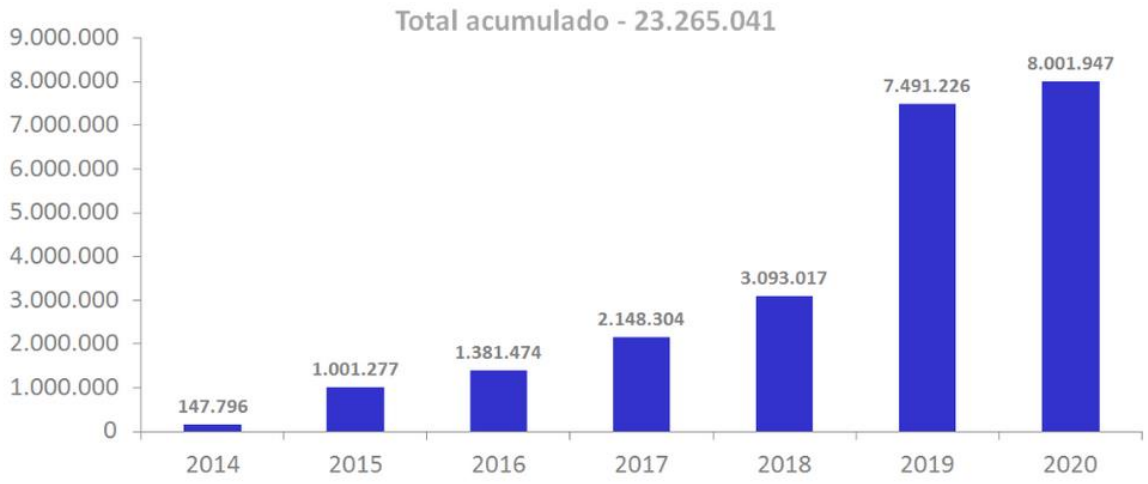


Gráfico 2 - Total de autenticações por ano e total acumulado

- **Autenticações por meio**, de acordo com o seguinte gráfico 3 apresentado, o meio com maior percentagem de autenticações é o Cartão de Cidadão com 38,04% seguido da Chave Móvel Digital com 38,03%. Sendo que o que apresenta menor percentagem é o Notário com 1,87%.

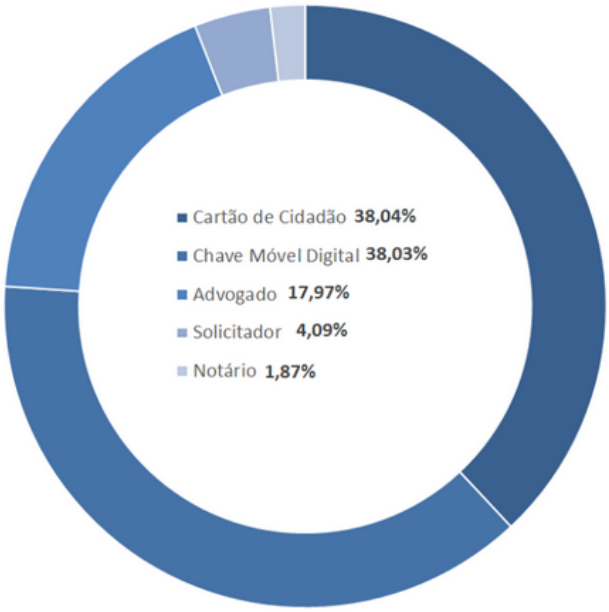


Gráfico 3 - Total de autenticações por meio

- **TOP 10 de entidades**, neste ponto podemos observar as 1º entidades com mais autenticações eletrónicas sendo o Portal SNS – Área do Cidadão o que apresenta o maior número como podemos observar no seguinte gráfico 4.

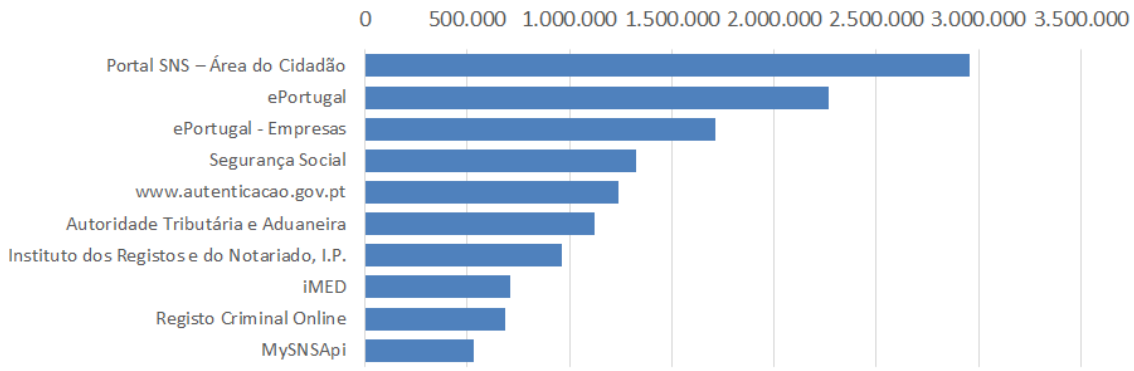


Gráfico 4 - TOP 10 de entidades com autenticações

4.2. Chave Móvel Digital

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e websites da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS. Tendo por base a importância da experiência de utilização, conjugado com as novas possibilidades de assinatura eletrónica qualificada "*server-side*" previstas no Regulamento Europeu 910/2014 que é relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

A chave móvel digital é um meio de autenticação que permite a associação de um número de telemóvel ao número de identificação civil (NIC) isto para um cidadão português e o número de passaporte para um cidadão estrangeiro, permitindo ainda assinar eletronicamente documentos de vários formatos. A assinatura eletrónica qualificada através da Chave Móvel Digital permite ao cidadão português ou estrangeiro, assinar um determinado documento com uma palavra-chave por si escolhida e respetivo código de segurança.

No caso de se realizar a autenticação com Chave Móvel Digital é utilizado o número de telemóvel, o código PIN da chave móvel digital ou o código numérico único e temporário de 6 dígitos enviado por SMS para o número de telemóvel anteriormente referido ou via e-mail. A Chave Móvel Digital permite ao utilizador utilizar a sua chave no Portal SNS, da Segurança Social, IMT, entre outros. Tratando-se desta forma de um método mais simples,

ou seja, o utilizador utiliza uma palavra-passe para os diferentes portais e websites, o código é enviado por SMS ou e-mail, sendo que não requer deslocações ou tempos de espera.

Com a Chave Móvel Digital podemos assinar documentos digitais com a mesma validade de uma assinatura à mão. Sendo que para tal é necessário ter a Chave Móvel Digital ativada, ter a assinatura digital da CMD ativada e código PIN de assinatura da CMD (que pode ser diferente do código PIN da CMD).

Para além do software Autenticação.gov que nos permite assinar um documento digitalmente com a CMD, como será apresentado numa secção posterior, segundo a Agência para a Modernização Administrativa (AMA) existem outras aplicações qualificadas para assinatura com a CMD. São essas aplicações: Prescrições Eletrónicas Médicas - PEM Móvel, WinGCS - Gestão de Cuidados de Saúde e C2020-AssinaturaCMD.

4.2.1. Legislação aplicável

A legislação apresentada e referente à atividade da Chave Móvel Digital é a seguinte apresentada (AMA, 2019):

- 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;
- Despacho 155/2017 (Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário), de 5 de Dezembro de 2017, do Gabinete Nacional de Segurança;
- Decreto-Lei nº 290-D/99, de 2 de Agosto, em todos os pontos que não forem contrariados pelo Regulamento (UE) n.º 910/2014;
- Lei n.º 37/2014,de 26 de Junho com as alterações introduzidas pela Lei n.º 32/2017, de 1 de Junho, e respetiva regulamentação;
- Lei nº 67/98, de 26 de Outubro (Lei da proteção de dados pessoais);•Decreto-Lei nº 36/2003 (Código da propriedade industrial);
- Lei nº 41/2004 (Lei da proteção de dados pessoais no sector das comunicações eletrónicas);
- Regulamento(UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento

de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados);

- Regulamento (UE) nº 611/2013 do Parlamento Europeu e do Conselho, de 24 de Junho de 2013, relativo às medidas aplicáveis à notificação e violação de dados pessoais;
- Lei das Comunicações Eletrónicas, aprovada pela Lei nº 5/2004 de 10 de Fevereiro;
- Decisão da Autoridade Nacional de Comunicações (ANACOM), aprovada por deliberação do respetivo Conselho de Administração, de 12 de Dezembro de 2013, relativa às exigências de comunicação e divulgação ao público de violações de segurança ou perdas de integridade ocorridas em redes e serviços de comunicações;
- Lei nº 109/2009, de 15 de Setembro (Lei do Cibercrime);
- Regulamento (CE) nº 593/2008 do Parlamento Europeu e do Conselho, de 17 de Junho de 2008, sobre a lei aplicável às obrigações contratuais (Roma I);
- Regulamento (CE) nº 864/2007 do Parlamento Europeu e do Conselho, de 11 de Julho de 2007, relativo à lei aplicável às obrigações extracontratuais (Roma II).

4.2.2. Estatísticas

Tendo sido consultado o *website* https://www.autenticacao.gov.pt/estatisticas-de-chave-movel-digital, a setembro de 2020, as estatísticas apresentadas são as seguintes:

- **Evolução do número de ativações**, neste ponto através da visualização e análise do gráfico 5 podemos observar que de 2015 a 2020 as ativações da CMD realizadas têm vindo a aumentar, existem pontos em que observamos uma redução dessas mesmas ativações sendo que existe o maior pico de ativações em 2020 e de momento indica uma descida nesse mesmo número.

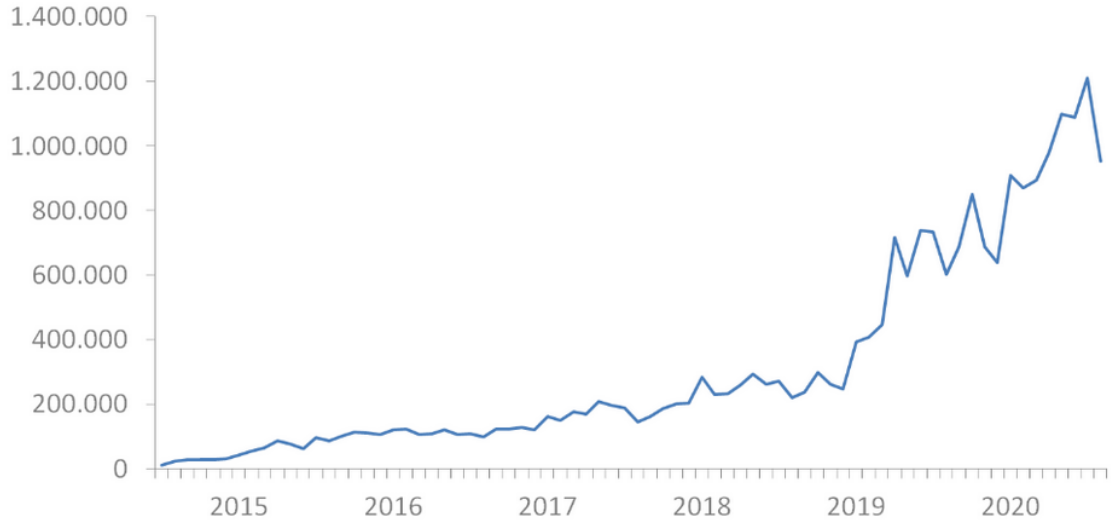


Gráfico 5 - Evolução do número de ativações da Chave Móvel Digital

- **Ativações por ano,** de acordo com os registos consultados no seguinte gráfico 6, de 2014 até ao presente ano (2020) existe um aumento de 724.087 ativações realizadas. De ano para ano, o maior aumento apresentado é o de 2018 para 2019 com um aumento de 704.406 ativações. De 2019 para 2018 visualizamos uma descida na ativação de CMD. O ano com maior número, como podemos observar no gráfico, é o ano 2019. O valor 1.924.904 representa o número total de ativações, sendo o valor 1.322.677 correspondente às CMD ativas.

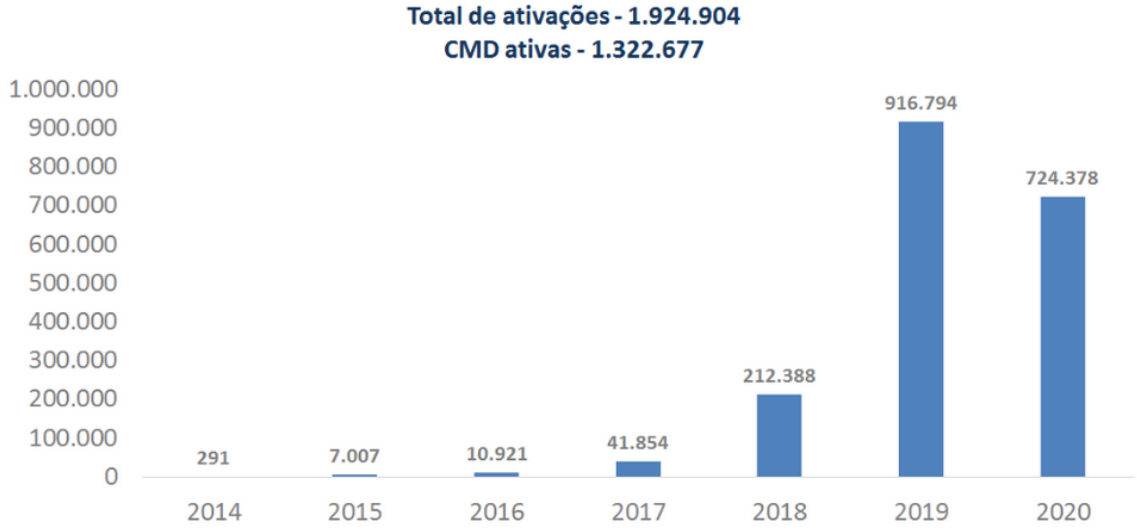


Gráfico 6 - Ativações de CMD por ano, total acumulado e ativas

- **Ativações por documento**, neste ponto no gráfico 7 podemos analisar a percentagem de ativações de Chave Móvel Digital por documento. A maior percentagem

apresentada é de 96,85% correspondendo ao Cartão de cidadão sendo a menor percentagem relativa ao cartão/certificado de residência com 0,06%.

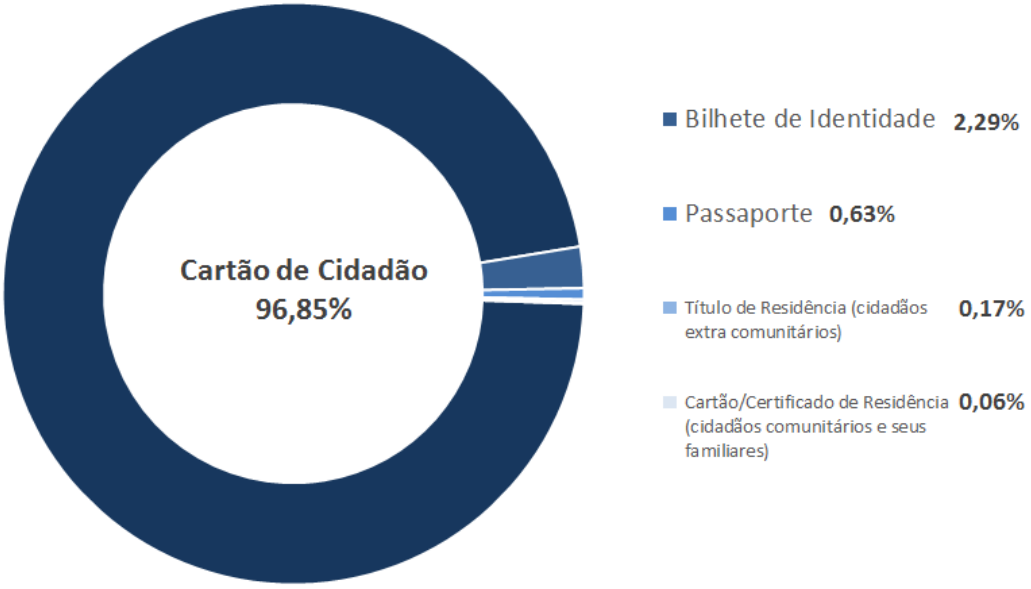


Gráfico 7 - Ativações de CMD por documento

- **Ativações por canal**, relativo a ativações realizadas em canais como Online Portal das Finanças, Online Autenticação.gov entre outros canais representados no gráfico 8. Como se pode observar, o canal que apresenta maior ativações é o Portal das Finanças com 43,42%, seguido posteriormente pelo Presencial IRN com 27,82%. Podemos visualizar que Presencialmente em Balcões de atendimento são realizadas 15,95% de ativações, sendo esta percentagem superior a Online Autenticação.gov.

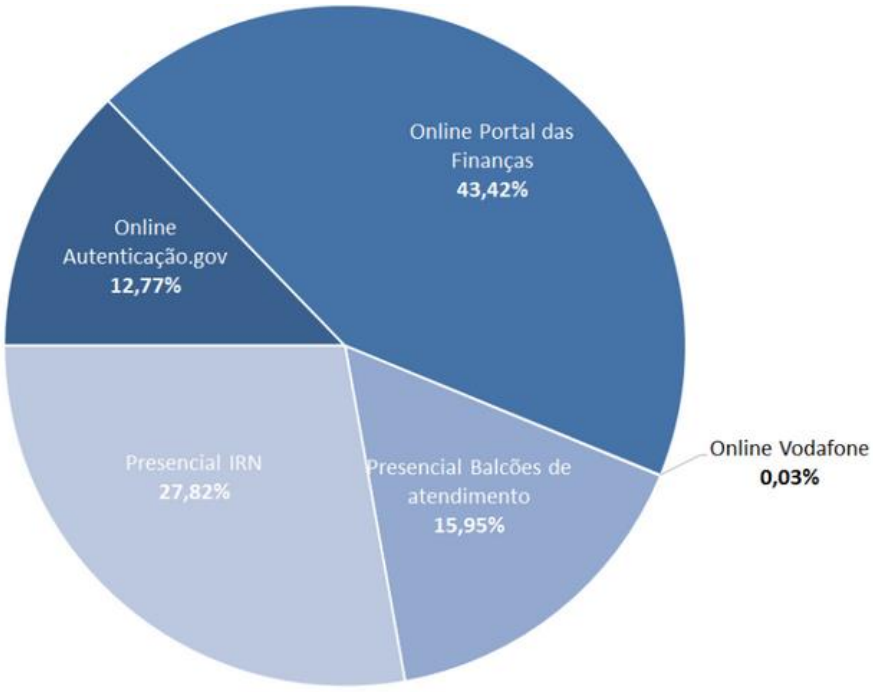


Gráfico 8 - Ativações de CMD por canal

5. Ferramentas de assinatura digital

Neste capítulo serão explorados três softwares que nos permitem assinar digitalmente um documento, abordando as respetivas características e funcionalidades, sendo eles o Software Oficial do CC (Autenticação.Gov), o aCCinaPDF e o Adobe Reader.

5.1. Software Oficial do CC - Autenticação.GOV versão 3.2.0

A aplicação Autenticação.gov para computador permite a gestão do nosso Cartão de Cidadão. Poderemos visualizar as nossas informações, editar as notas, modificar os PINs pessoais e assinar digitalmente ficheiros, ou seja, pode ser utilizada para visualizar e gerir os dados no Cartão de Cidadão e assinar documentos digitais.

Baseado no manual da apresentação da aplicação e para além desta ter sito testada, a presente aplicação permite-nos realizar as seguintes operações:

- Visualizar a informação e foto do cidadão;
- Visualizar da morada do cidadão e confirmação da alteração de morada;
- Editar as notas;
- Imprimir os dados do Cartão de Cidadão;
- Fazer a Assinatura digital em documentos PDF e outros ficheiros;
- Visualizar os certificados do Estado e do cidadão;
- Registar os certificados do Estado e do cidadão (específico de Microsoft Windows);
- Gerir de PINs (Testar PIN, Alterar PIN).

As funcionalidades da aplicação encontram-se divididas em três menus principais, sendo eles: Menu Cartão, Menu Assinatura e Menu Segurança como podemos ver na figura 23.

Figura 23 - Menu inicial da aplicação Autenticação.Gov

Tendo em conta o manual da aplicação podemos ver a explicação e detalhes de todo o menu, subsecções, sendo que neste contexto interessa-nos a parte da assinatura digital, sendo ela simples ou avançada.

- Assinatura digital

A aplicação permite assinar digitalmente ficheiros PDF e outros tipos de ficheiros. A assinatura digital em documentos PDF foi desenvolvida de acordo com a especificação da Adobe, podendo assim ser validada posteriormente no software Adobe Reader. A assinatura digital permite ao titular de um Cartão de Cidadão ou da Chave Móvel Digital, assinar com a chave pessoal existente no seu Cartão de Cidadão ou com a Chave Móvel Digital, sendo este passo realizado porque o cidadão pretende assinar documentos. É possível assinar usando dois modos diferentes:

1. **Assinatura Simples**: Assinatura digital de um documento PDF.
2. **Assinatura Avançada**: Assinatura digital de um documento PDF ou outro qualquer documento com possibilidade de assinar vários documentos ao mesmo tempo, adicionar atributos profissionais, bem como configurar outras opções.

Assinatura digital simples permite assinar um único documento PDF. Para isso uma das opções passa por apenas precisarmos de arrastar o ficheiro para a área de pré-visualização. Neste modo, apenas é possível selecionar a página e mover a assinatura digital para o local pretendido, conforme a figura seguinte. Por fim, carregar no botão Assinar com Cartão de Cidadão ou Assinar com Chave Móvel Digital. Podemos nas seguintes figuras 24 e 25 ver o menu da assinatura e da assinatura simples de um documento PDF.

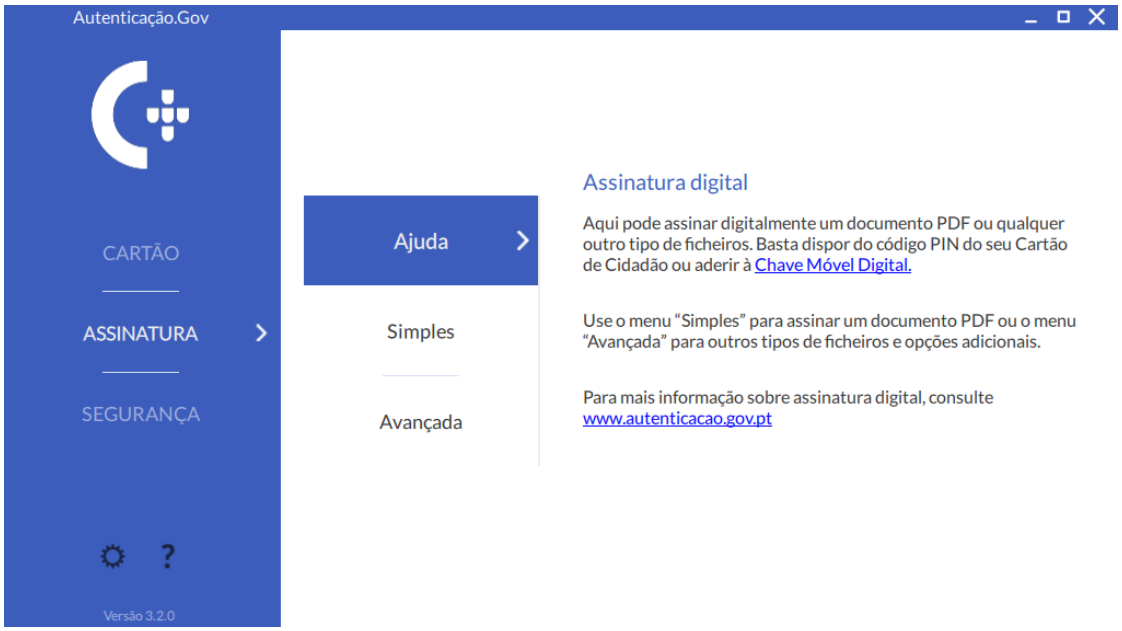


Figura 24 - Menu da Assinatura

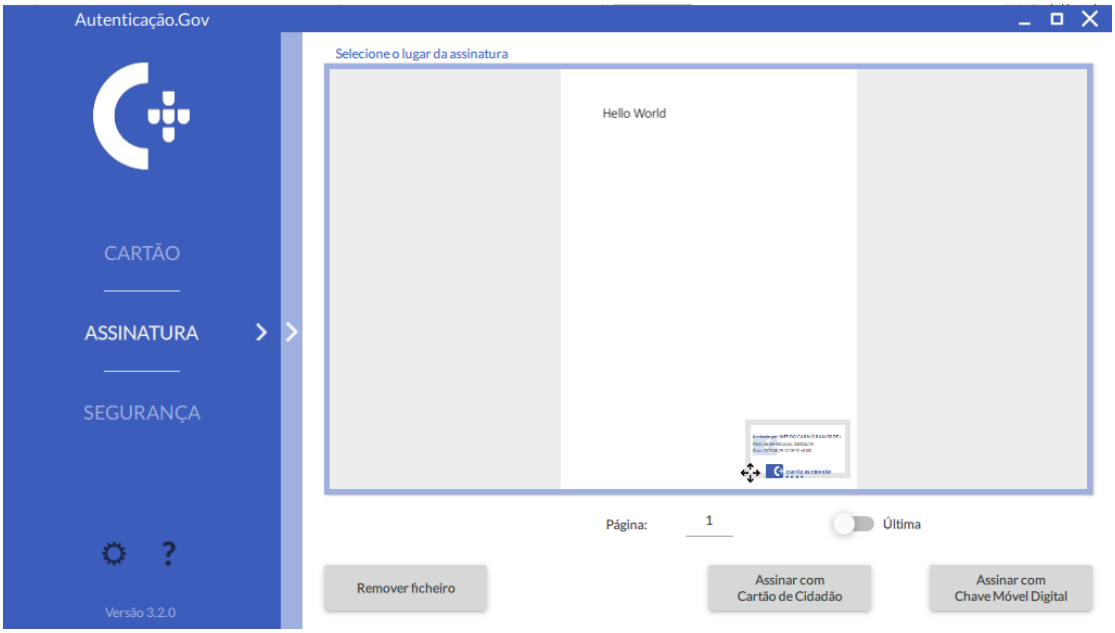


Figura 25 - Menu Assinatura Simples de documento PDF

Podemos ver nas seguintes imagens 26 e 27 como aparece o menu assim que escolhemos a opção que queremos assinar, com o cartão de cidadão ou chave móvel digital.

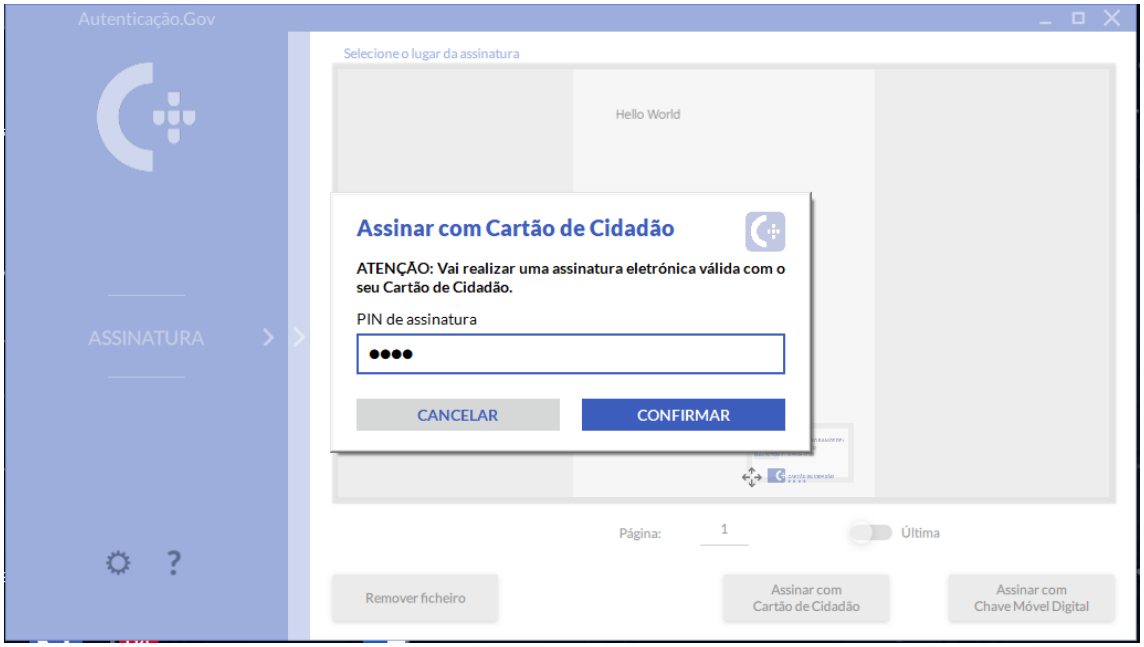


Figura 26 - Assinatura Simples com o Cartão de Cidadão

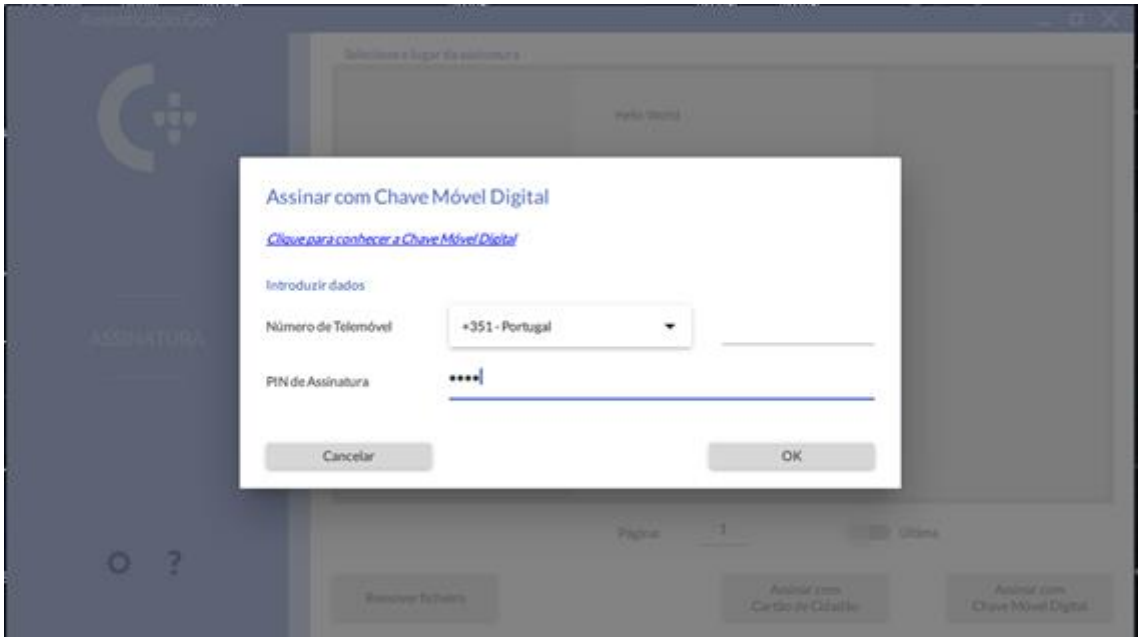


Figura 27 - Assinatura Simples com a Chave Móvel Digital

Assinatura digital avançada de um documento PDF ou outro qualquer documento com possibilidade de assinar vários documentos ao mesmo tempo, adicionar atributos profissionais, bem como configurar outras opções. Assim sendo neste menu permite-nos visualizar o documento a ser assinado, bem como a pré-visualização da própria assinatura. A pré-visualização existe apenas para assinatura do tipo PDF e selecionar um conjunto de configurações e mover a assinatura digital para o local pretendido.

As configurações da assinatura são as seguintes e podem ser visualizadas na figura 28:

- Tipo de assinatura – campo obrigatório, permite selecionar assinatura de ficheiros:
    - PDF: PAdES (PDF Advanced Electronic Signatures). Disponível para assinaturas com Cartão de Cidadão e Chave Móvel Digital.
    - Outros ficheiros: Pacote ASiC com XML Advanced Electronic Signatures (XadES). Disponível para assinaturas com Cartão de Cidadão.
- Motivo da assinatura – campo opcional, permite ao signatário indicar o motivo da sua assinatura. Disponível para assinaturas do tipo PDF.
- Localização onde a assinatura foi efetuada – campo opcional, permite ao signatário indicar o local onde esta assinatura foi efetuada
- Adicionar selo temporal - provando a data à qual a assinatura foi efetuada. Esta é a única forma de provar que o documento existia a determinada hora, pois é aplicada ao documento a data e hora que este está a ser assinado, de forma segura. A hora apresentada no selo visível é a hora local do computador onde foi efetuada a assinatura e pode não coincidir com a hora do selo temporal (obtida a partir de um servidor remoto). Disponível para assinaturas do tipo PDF e Outros Ficheiros.
- Adicionar atributos profissionais - permite ao cidadão autenticar-se na qualidade das funções que desempenha na sociedade enquanto profissional qualificado. Disponível para assinaturas do tipo PDF.

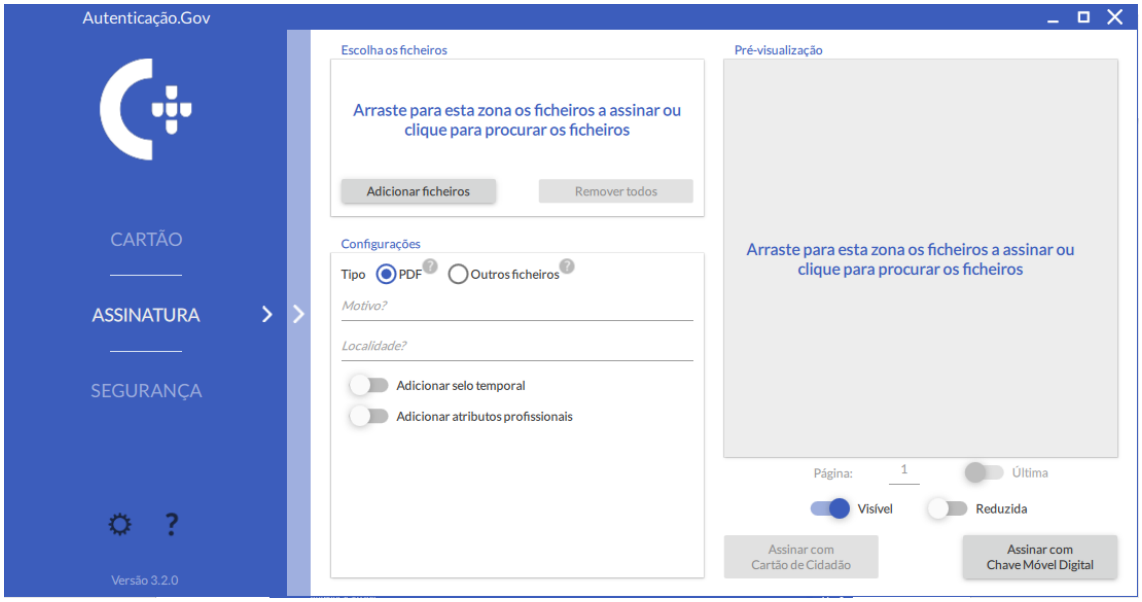


Figura 28 - Menu Assinatura Avançada

Na figura 29 podemos ver os documentos que pretendemos validar em lote, tendo neste caso escolhido PDF, txt e docx. Podemos também adicionar a opção de inserir selo temporal e ver as configurações referidas anteriormente.

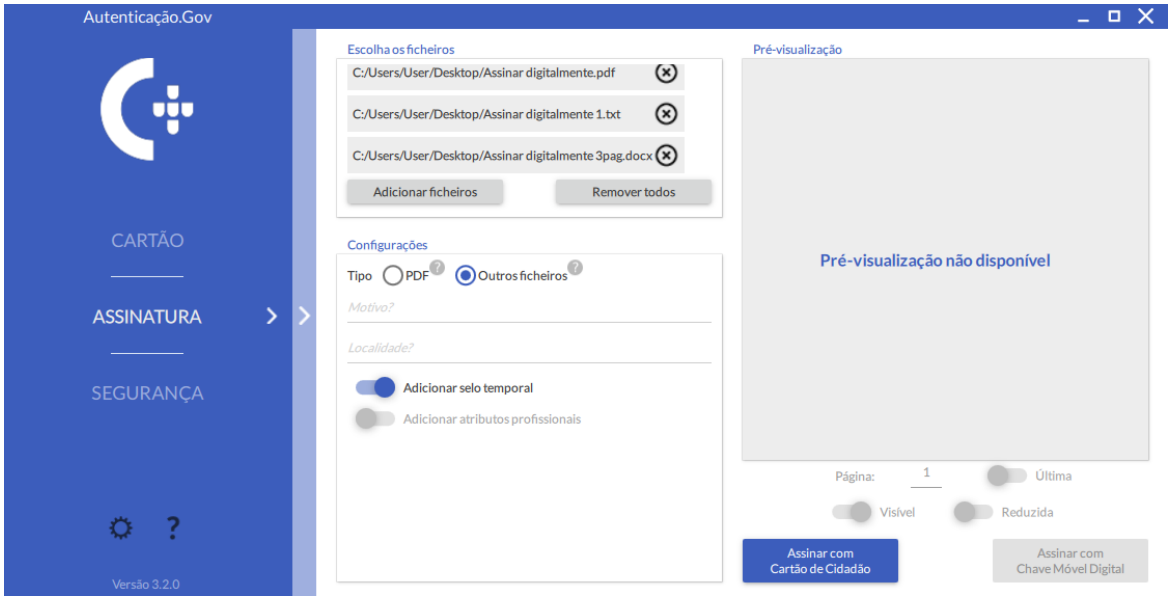


Figura 29 - Assinar lote de documentos

Após realizamos a assinatura digital num documento, podemos fazer a verificação da assinatura digital num documento PDF, em que esta é identificada automaticamente ao abrir o documento no Adobe Reader. Mesmo quando a assinatura não esteja visível (se a opção "Visível" não for selecionada no momento da assinatura), a assinatura deverá ser sempre validada no painel de assinaturas.

O menu segurança da aplicação que podemos ver na figura 30, permite efetuar operações relativas à segurança do Cartão de Cidadão.

Neste menu é possível:

- verificar os certificados do Cidadão e a cadeia de confiança formada pelas várias Entidades de Certificação do Cartão de Cidadão e do Estado Português. O preenchimento do campo "Estado do certificado" corresponde a uma validação junto da Infraestrutura do Cartão de Cidadão e como tal exige ligação à Internet.
- verificar e alterar os códigos PIN do Cartão de Cidadão.
    - PIN de Autenticação: Este PIN é usado para se autenticar em sites e aplicações que suportem o Cartão de Cidadão.
    - PIN de Assinatura: Este PIN é usado para assinar documentos ou transações em aplicações que suportem o Cartão de Cidadão.
    - PIN de Morada: Este PIN é usado para alteração e leitura de morada.

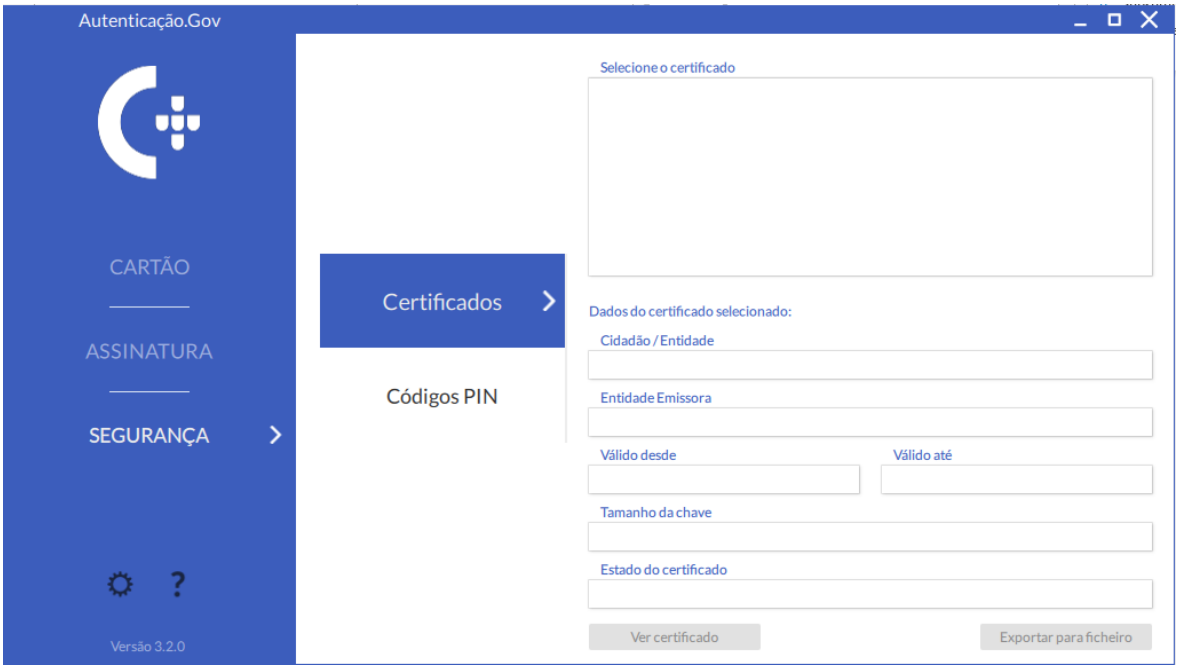


Figura 30 - Menu segurança

- **Integração com aplicações**

O *middleware* do Cartão de Cidadão, instalado com a aplicação Autenticação.Gov permite a interação com outras aplicações do sistema operativo, disponibilizando duas funcionalidades: Autenticação e Assinatura Digital. Realizando a instalação no sistema operativo Windows permite que, ao introduzir um Cartão de Cidadão no leitor, os certificados deste fiquem automaticamente registados no sistema operativo, ficando assim

as funcionalidades de autenticação e assinatura disponíveis às aplicações que utilizam a camada criptográfica do sistema operativo. Alguns exemplos dessas aplicações são: Microsoft Word, Microsoft Excel, Microsoft Outlook e Adobe Acrobat Reader. Nessas aplicações é também possível assinar com a Chave Móvel Digital. Software open source.

5.2.Ferramenta Open Source – aCCinaPDF versão 1.2.3

Como ferramenta Open Source será analisada e realizada a assinatura digital de um documento com o software aCCinaPDF. O aCCinaPDF foi desenvolvido em Java e é um software de criação e validação de assinaturas digitais em ficheiros PDF com o Cartão de Cidadão. Tendo sido desenvolvido pelos alunos Luís Diogo Zambujo e Micael Sousa Farinha do Instituto Politécnico de Leiria.

Apresentando as seguintes características e funcionalidades:

- suporte para ficheiros PDF versão 1.7, para cumprir o RNID (Regulamento Nacional de Interoperabilidade Digital) sendo obrigatório para toda a administração pública;
- não destrói a acessibilidade dos documentos, por isso permite cumprir as diretrizes WCAG 2.0 sendo obrigatório para toda a administração pública;
- produz assinaturas digitais com validação de longo termo, sem esta opção as assinaturas digitais deixam de ser válidas quando o CC do assinante expirar, no máximo ao fim de 5 anos;
- permite fazer assinaturas digitais em lote;
- permite validação de assinaturas digitais em lote;
- multi sistema operativo (Windows e Linux, também deve funcionar no Mac OS, mas não foram realizados testes neste SO, tendo sido realizado um update a 10 de maio de 2017, com a nota de “macOS fix”);
- facilidade de validação das assinaturas digitais por outros leitores de PDF graças à inclusão da hierarquia de certificados digitais do Cartão de Cidadão no próprio documento;
- fácil de instalar (não requer configurações da hierarquia de certificados digitais);
- é gratuito e open source (é disponibilizado sob a licença AGPL.);

Os requisitos do aCCinaPDF relativamente à validação de PDFs assinados com o Cartão de Cidadão são os seguintes:

- instalar o Oracle Java, versão 1.7 ou superior;
- ligação à Internet, dado que sem a qual não é possível **assinar** ou **validar assinaturas** com validação de longo termo;

Requisitos para assinar PDFs com o Cartão de Cidadão para além dos que foram enumerados acima são instalar o software oficial do CC, dado que este software é necessário para o aCCinaPDF interagir com o CC. Para além disso é necessário um leitor de *smartcards* e respetivos *drivers* configurados, sendo também essencial o Cartão de Cidadão com

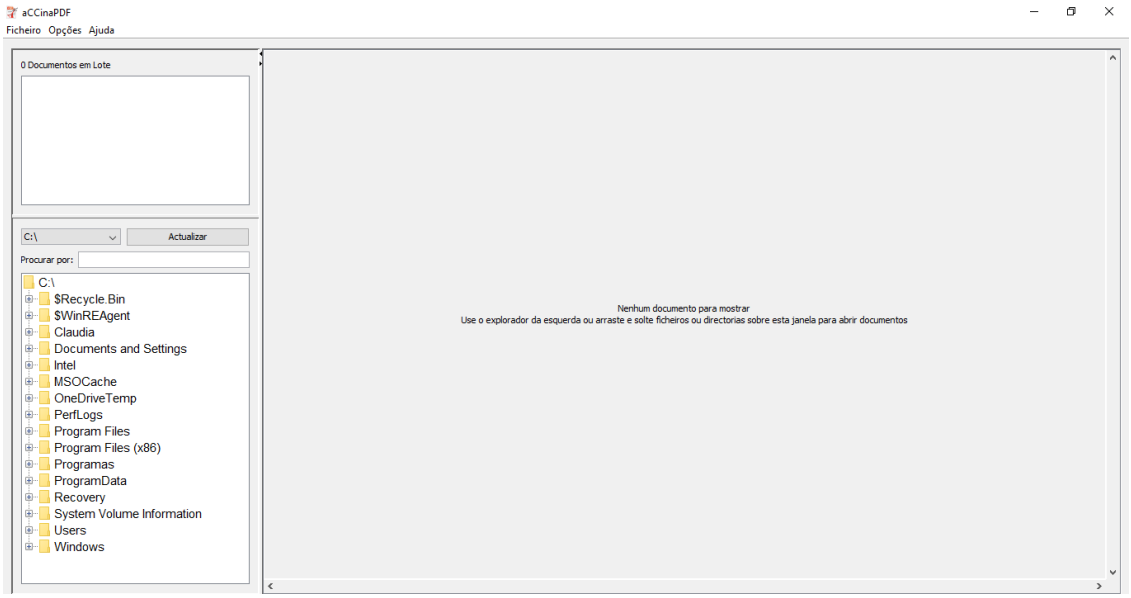


Figura 31 - Página inicial quando iniciamos o aCCinaPDF

assinatura digital ativa. Podemos observar na figura 31 a página inicial do aCCinaPDF. Para o caso de a assinatura não se encontrar ativa temos de nos dirigir ao registo civil para pedir a ativação, tendo de levar a carta que nos foi enviada com os PINs. De seguida adicionamos o/s documento/s para que estes sejam adicionados digitalmente, sendo que desta forma permite-nos assinar lotes de documentos como podemos ver nas figuras 32 e 33.

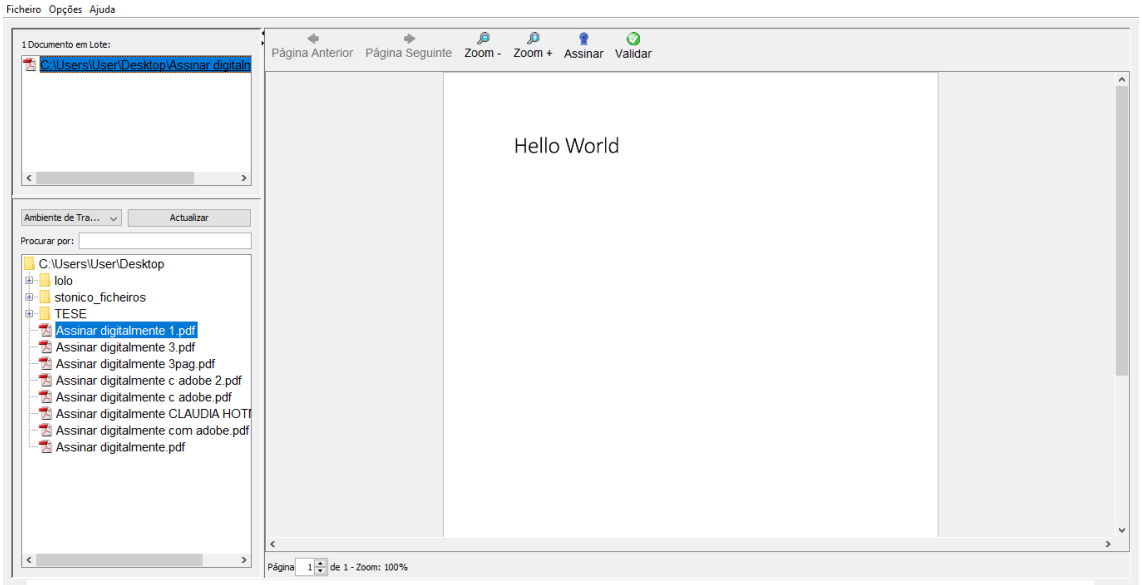


Figura 32 - Adicionar um documento PDF para ser assinado

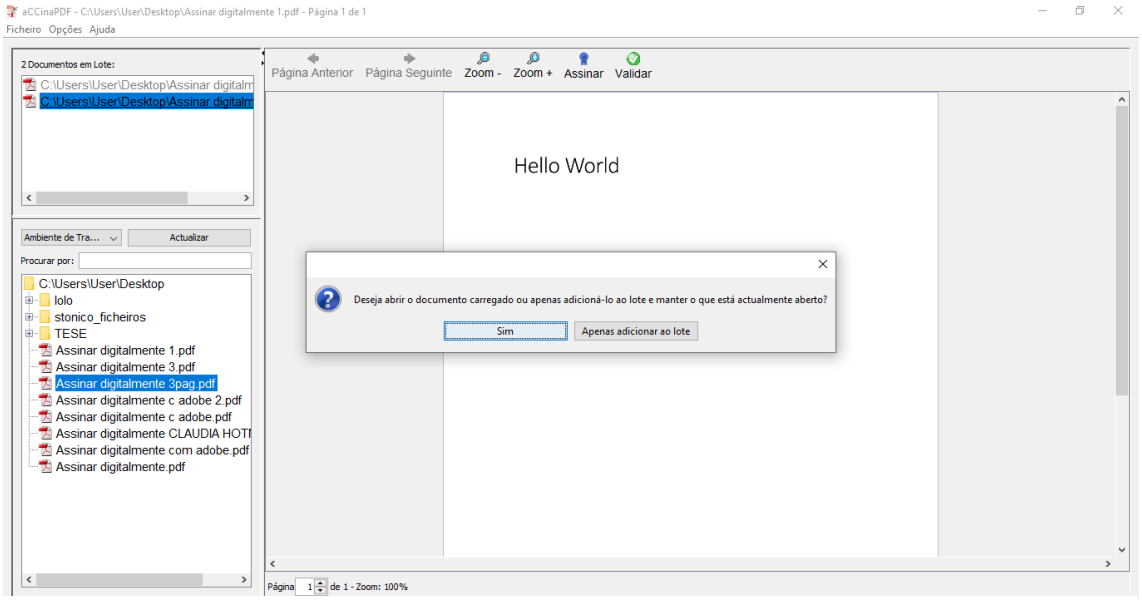


Figura 33 - Adicionar um segundo documento PDF

Depois de selecionar os documentos assinamo-los com o nosso cartão de cidadão, como podemos ver na figura 34 podemos definir se queremos sem certificação ou não permitir alterações por exemplo, incluindo o *timestamp*.

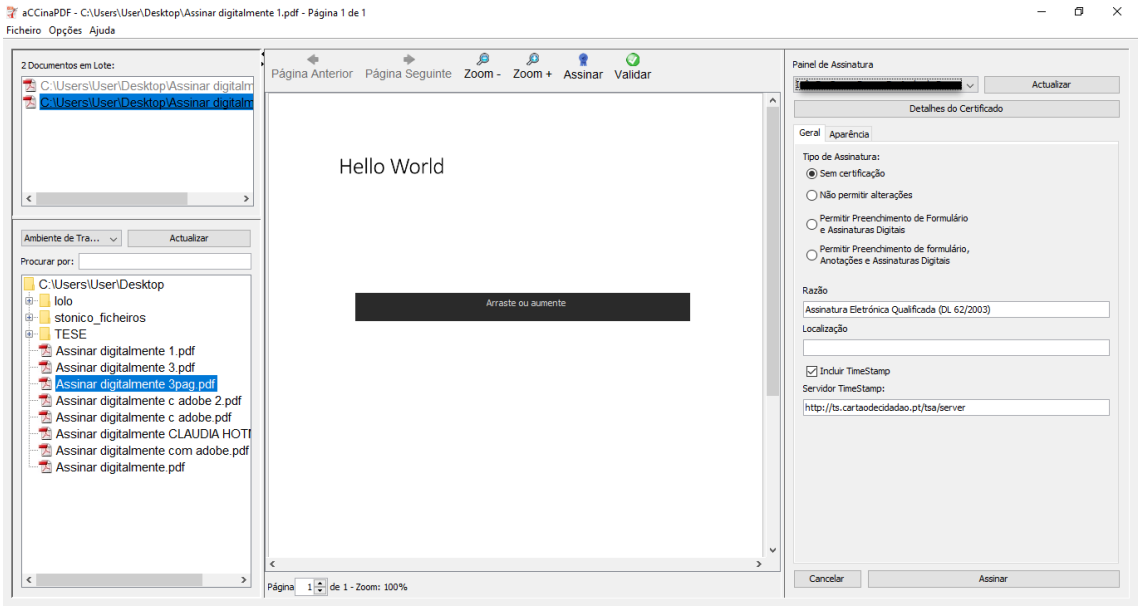


Figura 34 - Assinar o lote de documentos

Também é possível vermos os detalhes dos certificados, ver figura 35, bem como qual a identidade e até quando a validade.

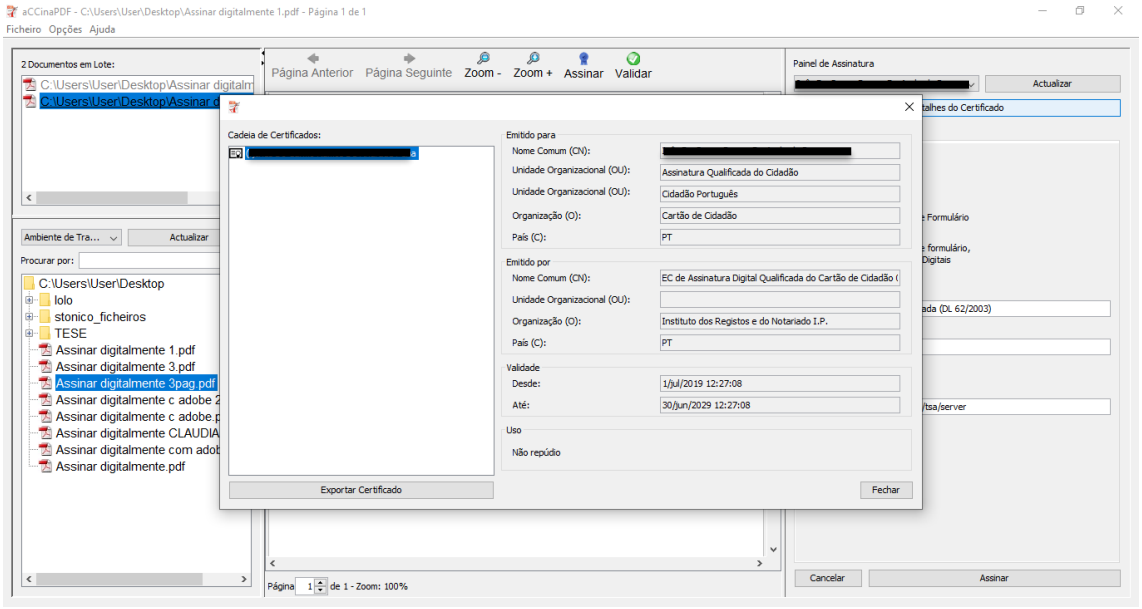


Figura 35 - Detalhes do certificado

Nesta fase e observando a figura 36, podemos escolher se pretendemos assinar todos os documentos que estão no lote ou apenas o documento que está aberto.

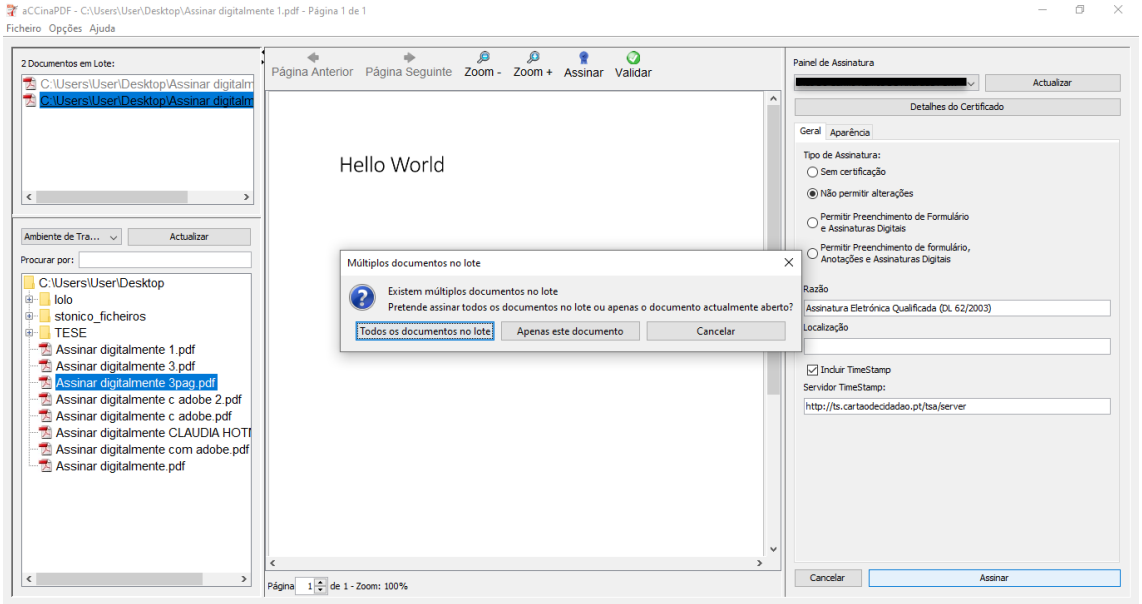


Figura 36 - Assinar todos os documentos ou apenas um documento

De seguida assinamos o documento com o cartão de cidadão, tendo em conta que necessitamos ter a aplicação "Autenticação.Gov" instalada como vemos na figura 37 e depois na figura 38 verificamos que os dois documentos foram assinados com sucesso.

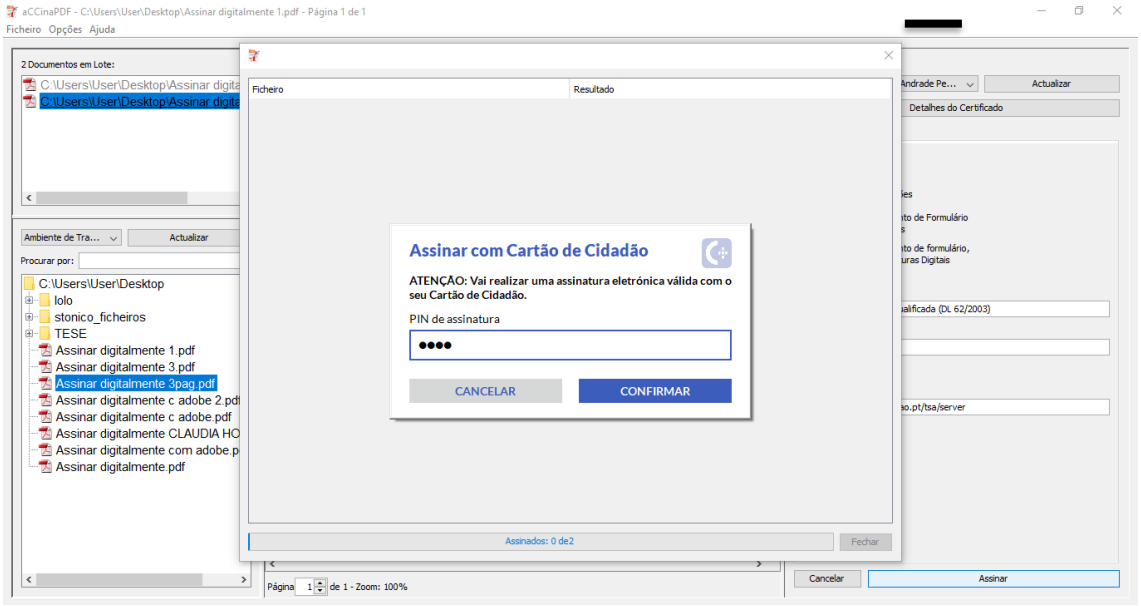


Figura 37 - Assinar um documento com o Cartão de Cidadão

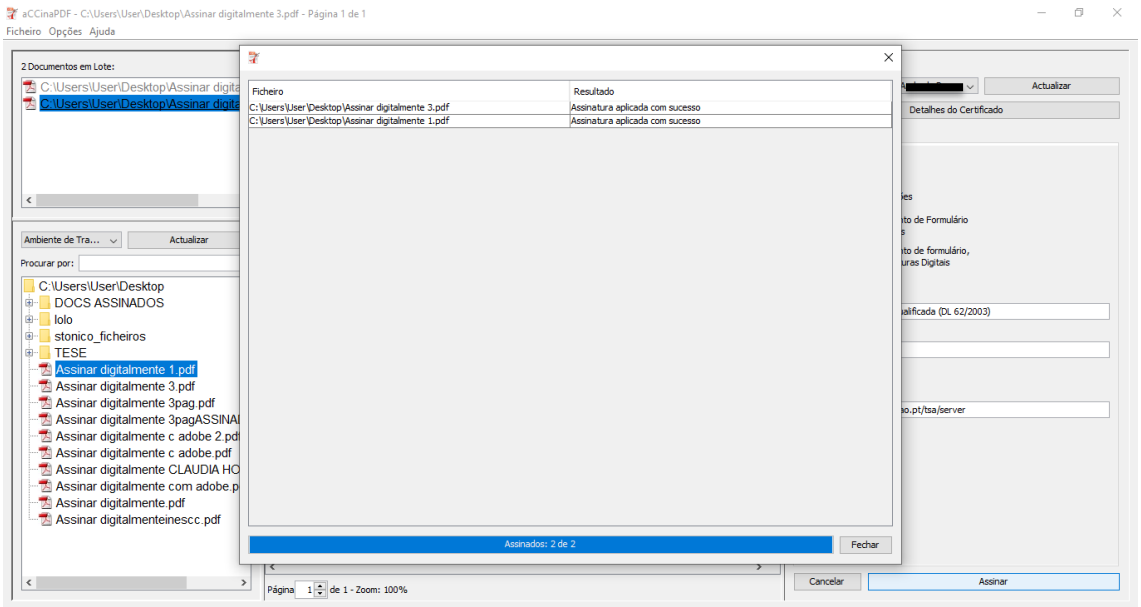


Figura 38 - Dois documentos assinados com sucesso

Por fim realizamos a validação da nossa assinatura, mostrando que o documento está certificado e não foi modificado, o certificado foi verificado e validado e para além disso que a assinatura inclui carimbo de Data e Hora válido. A assinatura está habilitada a validação de longo termo e não permite alterações, verificamos isso na figura 39.

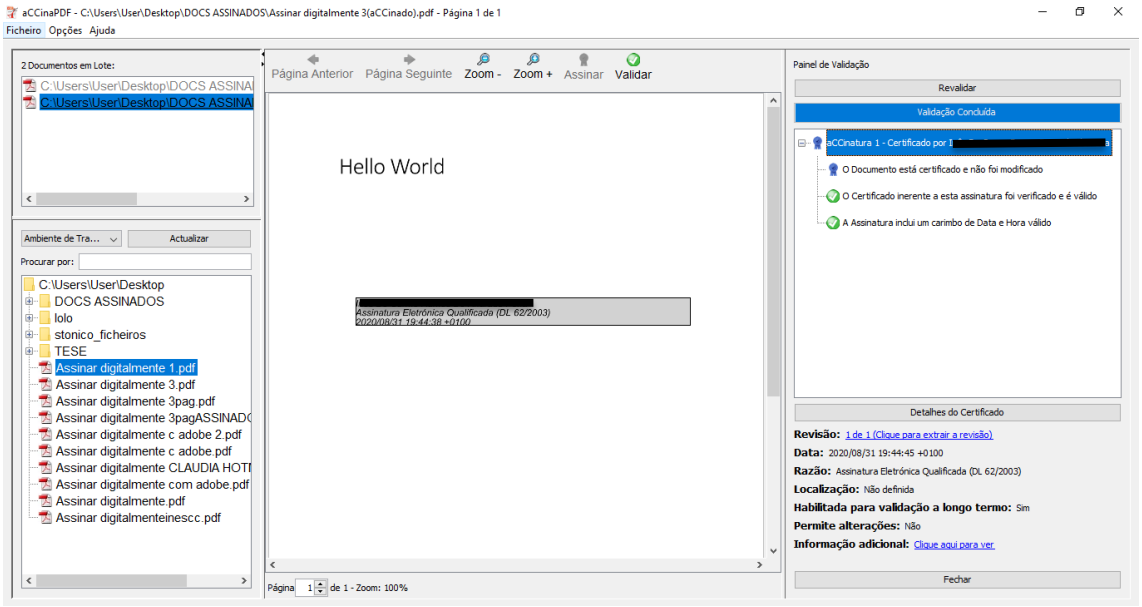


Figura 39 - Validação da assinatura

5.3. Adobe Acrobat Reader DC versão 2019.008.20071

O Adobe Acrobat disponibiliza um conjunto de soluções para as assinaturas eletrónicas e digitais que podem usar o software Acrobat Reader para assinar ficheiros PDF e validar os arquivos que recebem de terceiros. É caracterizado por ser um software gratuito que permite ao utilizador exibir, imprimir, assinar e fazer comentários em documentos PDF com confiança. Para além das características anteriores também facilita a colaboração, o compartilhamento, a revisão e até mesmo a assinatura de PDFs em qualquer lugar e dispositivo que tenhamos connosco.

Desta forma o processo de assinatura passa pela escolha do documento PDF que pretendemos assinar digitalmente, seguidamente no menu ferramentas selecionamos o certificado digital que pretendemos usar para assinar o documento como podemos ver nas seguintes figuras 40 e 41.

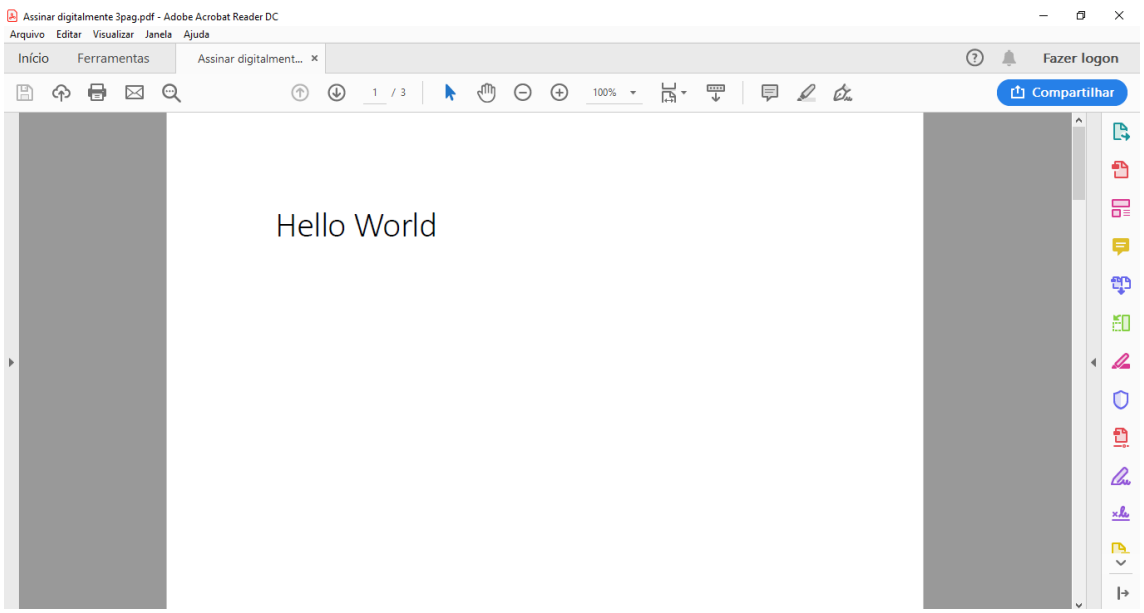


Figura 40 - Documento PDF que pretendemos assinar

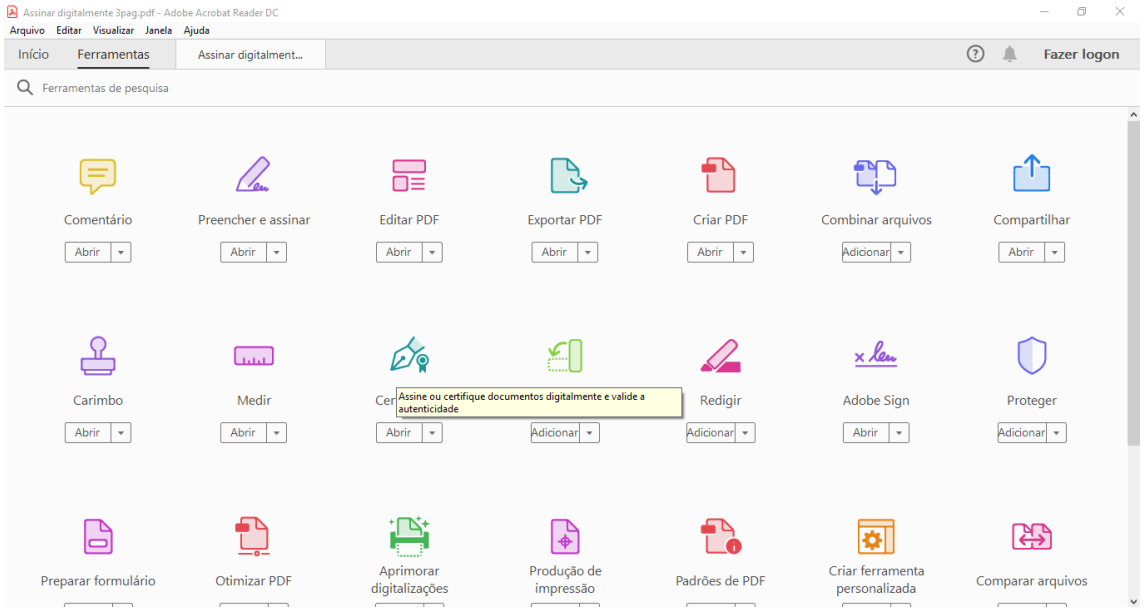


Figura 41 - Menu ferramentas

De seguida selecionamos a área onde pretendemos que fique a nossa assinatura digital como podemos observar na seguinte figura 42. Assinamos e após gravarmos o documento este é guardado. Estando a usar um cartão ou um *token* USB temos de adicionar o pin do nosso dispositivo.

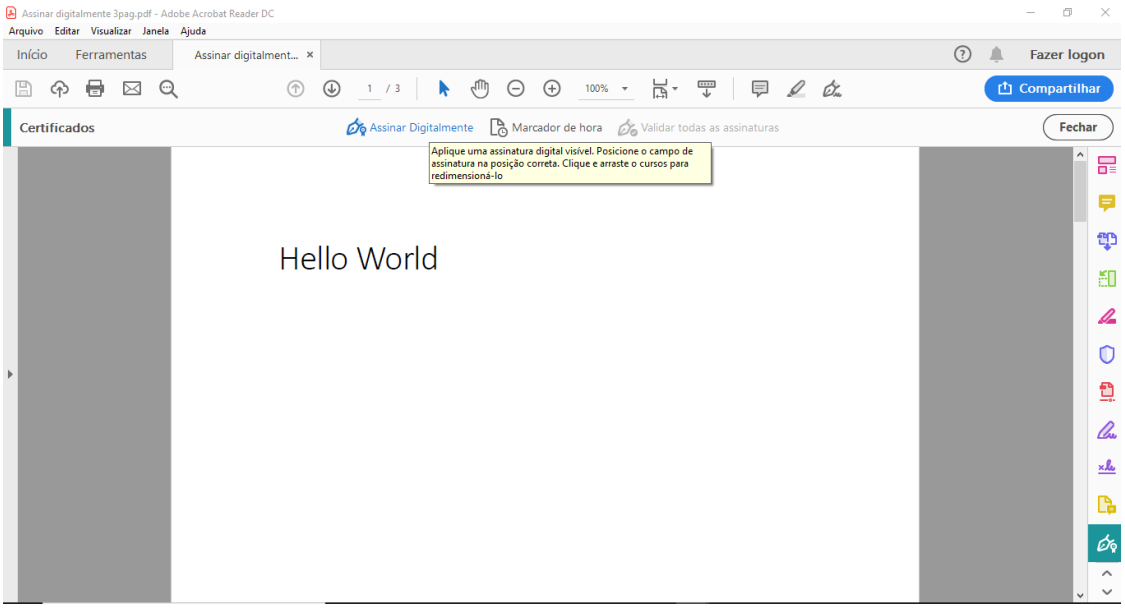


Figura 42 - Assinar digitalmente

Podemos da mesma forma visualizar os certificados e ver se estão válidos e o que estes nos permitem fazer, figuras 43 e 44.

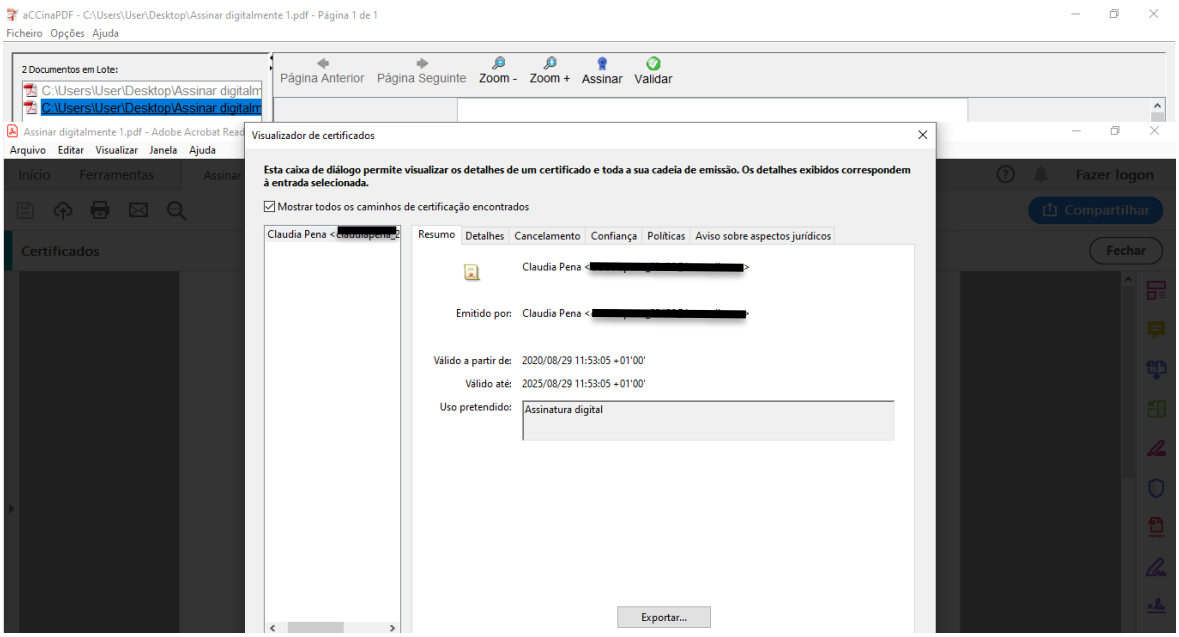


Figura 43 – Detalhes do certificado, validade e qual o uso pretendido

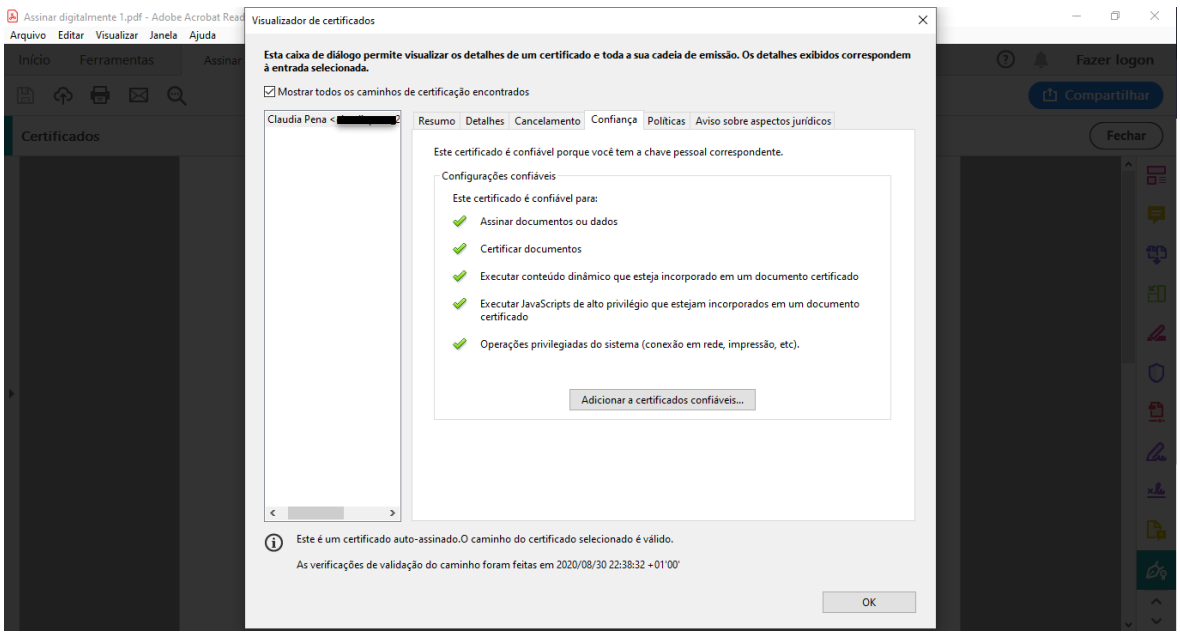


Figura 44 - Detalhes do certificado, configurações confiáveis

Neste momento o nosso documento já se encontra assinado digitalmente e a nossa assinatura é válida, como podemos verificar na figura 45. Ao selecionar a nossa assinatura e para vermos mais detalhes sobre a mesma clicamos no painel assinaturas. O carimbo de hora garante a validade de longo prazo (LTV) do contrato assinado, bloqueando a assinatura, bem como o documento. Basicamente, prover um bloqueio para o bloqueio. Isso é essencial para a conformidade de assinatura digital porque os certificados de assinatura pessoais podem

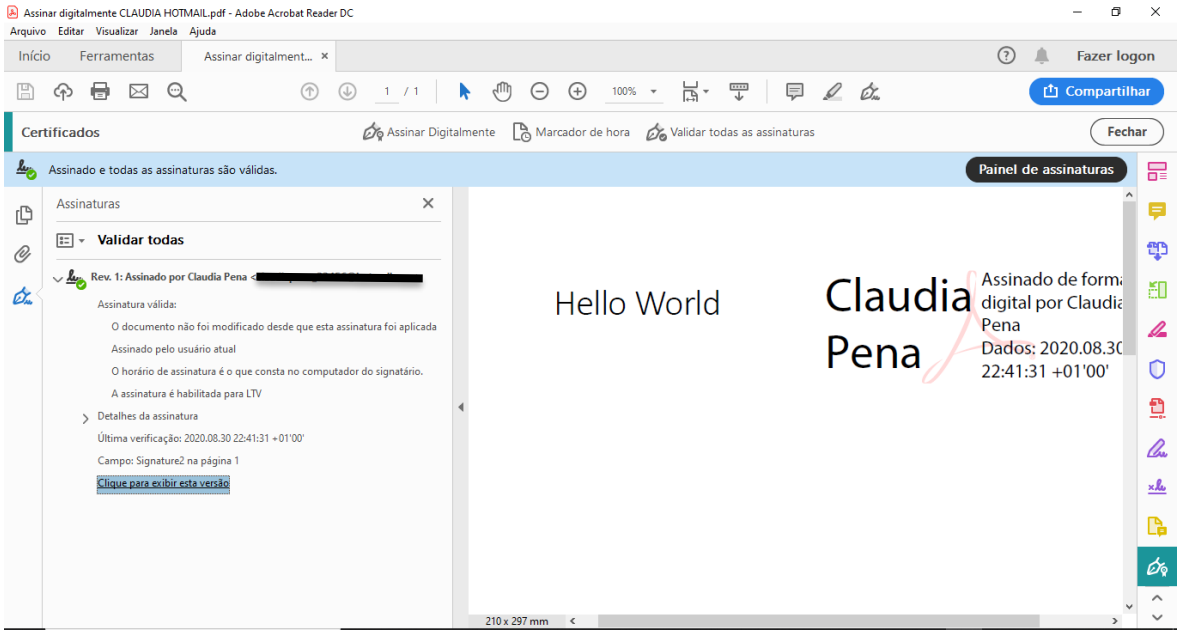


Figura 45 - Detalhes da assinatura

expirar, enquanto que o carimbo de hora do LTV pode ser renovado ao longo do tempo sem alterar a validade da assinatura. O carimbo de hora do LTV garante que o certificado era

válido quando foi aplicado e estende a validade do contrato assinado para além do escopo de tempo real do certificado do signatário. Sendo que a Adobe fornece carimbos de hora em conformidade com o eIDAS. Na figura anterior podemos observar que a assinatura está habilitada para LTV, ou seja, a longo prazo e qual a última verificação.

A seguinte tabela 6 apresentada corresponde à comparação dos softwares anteriormente mencionados. Tendo em conta e sendo relativos aos pontos: assinatura de longo termo, assinar um documento ou lote de documentos, validar a assinatura, timestamp e tipo de documento (PDF ou outro). O que se apresenta mais completo é o aCCinaPDF, tendo em conta apenas o tipo de documento PDF, apresenta a vantagem de assinar em lote e de validar a assinatura para além da assinatura de longo termo e de termos a possibilidade de realizar o timestamp. O software "Autenticação.Gov" é uma sugestão favorável e recomendável tendo em conta que também podemos assinar outro tipo de documento sem ser PDF ainda que tenhamos de recorrer ao Adobe para validar a nossa assinatura.

Tabela 6 - Comparação de funcionalidades existentes nos softwares

	Autenticação.Gov	aCCinaPDF	Abode Reader DC
Assinar com o CC	X	X	X
Assinar com a CMD	X		
Assinatura LTV		X	X
Assinar lote de documentos	X	X	
Validar a assinatura digital		X	X
Timestamp	X	X	X
Assinar PDF	X	X	X
Assinar outros tipos de documentos	X		

6. Discussão sobre o ponto atual e futuro das assinaturas digitais em Portugal

Baseada numa publicação da Abreus Advogados e face aos desafios apresentados dada a presente situação de propagação do COVID-19, que levou à redução de deslocações e em que várias pessoas passaram a trabalhar remotamente, precisámos de nos adaptar e realizar a assinatura de documentos de uma forma que não a manuscrita. Mesmo que existente e utilizada, neste ponto a assinatura eletrónica revela-se um instrumento bastante útil para que seja efetuada a assinatura de documentos à distância. "Na lei portuguesa são apresentadas diferentes formas de assinar digitalmente documentos, servindo estas para objetivos diferentes. Mais precisamente, no Regime Jurídico Aplicável aos Documentos Eletrónicos e Assinatura Digital, para se realizar a assinatura de documentos à distância, foram referidas anteriormente ao longo do presente projeto: a assinatura eletrónica simples, a assinatura eletrónica avançada sendo que esta inclui a assinatura digital e assinatura eletrónica qualificada".

"A assinatura eletrónica qualificada é certificada por uma entidade devidamente credenciada e é a única modalidade de assinatura eletrónica cuja utilização confere a força probatória de um documento particular assinado, (tal como previsto no 376.º do Código Civil). Desta forma, todos contratos para os quais a lei exija a forma de documento escrito e assinado podem ser assinados com recurso à assinatura eletrónica qualificada. Como por exemplo: empréstimos bancários e empréstimos civis entre 2.500€ e 25.000€, contratos de Arrendamento, promessa de cumprimento e reconhecimento de dívida, acordo de cessação de contrato de trabalho, licença de direitos sobre marcas e patentes e a maioria dos acordos com intermediários financeiros".

Sendo que esta mesma entidade certificadora também poderá "certificar os poderes e atributos empresariais do assinante nomeadamente, para vincular uma Pessoa Coletiva num contrato e para participar em plataformas eletrónicas de contratação pública, ou os seus atributos profissionais (como é o exemplo dos advogados). Para esse efeito, atualmente e através do site www.autenticacao.gov.pt, é possível associar a qualidade de administrador, gerente ou diretor ao cartão do cidadão para poder assinar documentos e contratos nessa qualidade. Após a realização dessa associação o administrador, gerente ou diretor que o faça,

está formalmente capacitado para assinar eletronicamente os contratos e os documentos que a lei permite assinar desta forma, incluindo a movimentação de contas bancárias e as atas contendo as deliberações dos órgãos da sociedade".

Por sua vez, o Estado Português também "oferece um Sistema Público de Certificação de Atributos Profissionais (SCAP), (previsto, por exemplo no Artigo 546º do Código das Sociedades Comerciais). Este serviço permite, através do Cartão de Cidadão ou chave móvel digital, a utilização de assinatura eletrónica qualificada na qualidade de titular de um órgão social ou de um atributo profissional".

"A confiança mútua pode permitir que a assinatura simples seja suficiente para vincular as partes e dar segurança às declarações que subscrevem, no entanto, a capacidade de demonstrar a validade do documento ou a identificação do titular será sempre mais facilmente questionável. Assim, assinatura eletrónica avançada traz uma maior segurança às partes uma vez que, através de meios criptográficos, identifica o titular como autor do documento, dependendo apenas da vontade do titular, está sob seu controlo exclusivo e permite detetar qualquer alteração ao documento. Uma modalidade específica de assinatura eletrónica avançada, a assinatura digital, associa-se a um certificado digital de identidade que autentica o assinante, para permitir ao destinatário confirmar de modo mais fidedigno a identidade do signatário e se o documento eletrónico foi alterado depois de aposta a assinatura".

Por sua vez, "não podem ser assinados com recurso a assinatura eletrónica os documentos para os quais a lei exige a forma de escritura pública ou documento particular autenticado ou especificamente uma assinatura manuscrita. Como é o caso, dos contratos relacionados com Imóveis (com a exceção do contrato de arrendamento) e garantias sobre imóveis, contratos de constituição de Sociedades e assinatura dos estatutos, empréstimos civis acima de 25.000€, determinados documentos regidos pelo direito sucessório, tais como o testamento público ou testamento cerrado".

Como podemos analisar e por sua vez compreender, "a assinatura eletrónica constitui um meio legal e eficaz para providenciar a continuidade da atividade económica nas circunstâncias atuais pelo que no futuro esta será continuamente utilizada com a possibilidade de substituir na totalidade o uso da assinatura manuscrita". Sendo que por exemplo, nas câmaras municipais praticamente apenas se utiliza a assinatura digital com o

CC, com a nossa adaptação à presente situação, as escolas também se adaptam e aceitam as pautas escolares assinadas digitalmente, empresas para renovarem contratos dos colaboradores e entre outros, passaram a utilizar cada vez mais este método.

7. Conclusões

De um modo geral, o presente projeto abordou o seu objetivo principal, que consiste no estudo comparativo entre aplicações de Assinatura Digital e respetivas assinaturas, bem como o projeto STORK que foi dado como concluído com sucesso. Sendo ainda esclarecido pela AMA, como podemos ver no Anexo A, que Portugal utilizou o projeto STORK até há cerca de 2 anos e que, entretanto, no contexto do Regulamento (UE) n.º 910/2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, os nós STORK evoluíram para nós eIDAS (com funcionalidades similares). Podendo experimentar, por exemplo, no ePortugal.gov.pt a autenticação europeia e experienciar tal mecanismo. E que se assinarmos digitalmente um documento em Portugal este é válido/reconhecido noutro país da europa desde que a Entidade que emitiu o certificado esteja na Trusted List Europeia, fora da União Europeia depende de acordos bilaterais. Baseada na pesquisa sobre a identificação eletrónica concluímos que na Europa o país com maiores desenvolvimentos relacionados com o mundo das assinaturas digitais é a Estónia.

No contexto das ferramentas e da comparação das mesmas, tendo em conta que de entre outros softwares apenas se decidiu comparar e realizar a assinatura de documentos com a autenticação.gov, o aCCinaPDF e Adobe Reader, podemos dizer que de entre os três softwares instalados e analisando as suas características concluímos que o software aCCinaPDF é o mais integral. O aCCinaPDF apresenta-se como o mais completo por permitir a assinatura de longo termo em que sem esta opção a assinatura deixa de ser válida quando o nosso CC caduca, para além de nos admitir a assinar documentos em lote, o timestamp, funciona em todos os sistemas operativos e ainda permite validar a nossa assinatura depois de assinarmos um documento. A autenticação.gov apresenta como vantagem o facto de podermos assinar documentos sendo estes em formato PDF ou noutro formato quando apresentados em lote bem como utilizar o timestamp, ainda assim é necessário que posteriormente tenhamos de utilizar o Adobe Reader para validar a assinatura e também não permite a assinatura de longo termo. Desta forma o aCCinaPDF é essencialmente o melhor software porque se hoje eu assinar um documento ou um lote de documentos e precisar que este seja válido durante 15 anos, com a característica da assinatura habilitada ao LTV permite-nos que seja válido durante esse período. Enquanto que se

decidisse utilizar a autenticação.gov a assinatura desse mesmo documento iria tornar-se inválida assim que o meu cartão de cidadão caduca, como sabemos a validade do nosso CC é de 5 anos e dessa forma não faria com que a nossa assinatura permanecesse válida nesses 15 anos referidos anteriormente.

De forma a poder melhorar e através da aplicação autenticação.gov nos fosse possível manter o documento válido durante um período maior do que a validade do nosso documento de identificação, a AMA teria de alterar a sua estrutura de forma a conseguir suportar as assinaturas LTV. Neste caso teria de alterar os formatos, ou seja, alterar o formato PDF que utiliza o PAdES para PAdES Long term e o XAdES simples para o XAdES-X. Em que, o XAdES é a forma básica definindo elementos para autenticação e proteção da integridade dos registos, passando para o XAdES-X significaria que acrescentaria carimbos temporais e por sua vez alargando as capacidades de validação a longo termo da assinatura. No caso do PAdES passaria a utilizar a parte 4 PAdES Long Term que utiliza uma extensão à ISO 32000-1 chamada Document Security Store (DSS) para transportar os dados de validação necessários para validar uma assinatura, opcionalmente com a Validation Related Information (VRI) que relaciona os dados de validação com uma assinatura específica (Brzica, Herceg, & Stančić, 2013).

Relativamente à Chave Móvel Digital que também é um dos pontos mencionados no presente projeto, é um sistema simples e a autenticação em portais requer dois passos, em cada autenticação que queremos realizar recebemos um novo código de segurança por sua vez podemos questionar até que ponto é que este é seguro, sendo que entre o processo de recebermos esse código para efetuarmos a autenticação esta pode ser intercetada e sofrermos um ataque de *phishing* ou *man-in-the-middle* por exemplo. Tendo em conta que o número de vezes que queiramos realizar a autenticação será igual ao número de mensagens que iremos receber independentemente do meio, poderemos receber um código de um outro endereço eletrónico como de outro número e inserir sem que nos demos conta de que não era o correto ou o suposto. A CMD foi criada para ser um sistema mais simples e a verdade é que com a correria do dia-a-dia muitas vezes preferimos o processo mais rápido ou o que nos facilita no momento de assinar um documento que precisamos mas até que ponto é que esse é o mais

> seguro ou viável, tendo em conta a proteção dos nossos dados e que por um clique podem passar a pertencer a um terceiro.

O mundo digital está em continuo desenvolvimento e as assinaturas digitais apresentam-se como um método eficaz no contexto de realização da assinatura de documentos, podendo este ser realizado à distância. Desta forma, o impacto de utilização de assinaturas digitais é de que estas proporcionam privacidade dos dados, no sentido de promover a integridade, autenticidade e o não-repudio da informação.

Referências Bibliográficas

A.J. Menezes, S. A. (1996). *Handbook Of Applied Cryptography.* TAYLOR & FRANCIS INC.

Almeida, D. (2009). *Dissertação - Assinatura Electrónica Qualificada.* Lisboa: Instituto Superior Técnico - Universidade Técnica de Lisboa.

AMA. (2019). Declaração de Práticas de Operação do SCMD.

Arora, S. (2008). National e-ID card schemes: A European overview.

Assar, S., Boughzala, I., & Boydens, I. (2011). *Practical Studies in E-Government.*

Barbosa, A. (2010). *Cenários de Utilização do Cartão de Cidadão em Sistemas de Informação Académicos.* FEUP.

Barbosa, M. (2005). *Criptografia Aplicada - ModII.*

Berbecaru D, L. A. (2019). Providing digital identity and academic attributes through European eID infrastructures: Results achieved, limitations, and future steps.

Bishop, M. (2004). *Introduction to Computer Security.*

Björklund, F. (2016). E-government and moral citizenship: the case of Estonia.

Blythe, S. E. (2005). *Digital Signature Law of the United Nations,European Union, United Kingdom and UnitedStates: Promotion of Growth in E-Commerce WithEnhanced Security.*

Brzica, H., Herceg, B., & Stančić, H. (2013). Long-term Preservation of Validity of Electronically Signed Records.

Carvalho, C. (2003). *Infra-estrutura de chave pública do Ministério da Justiça.* DI-FCUL.

Castro, D. (2011). Explaining International Leadership: Electronic Identification Systems.

Clarke, R. (1994). Human identification in information systems: management challenges and public policy issues. Inform Tech People.

Comission, E. (2017). Study on the use of Electronic Identification (eID) for the European Citizens' Initiative.

Connectis. (2016). eID is widely-used in the European digital world.

Datoo, A. (2019). *Legal Data for Banking: Business Optimisation and Regulatory Compliance.* John Wiley & Sons, Ltd.

Estonia, R. o. (2018). *Estonian eID scheme: ID card.*

ETSI, E. T. (2009). ETSI TS 102 778-1 V1.1.1 (2009-07): Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

Fiebig, D. (2020). IDENTITY IN THE AGE OF SOCIAL NETWORKS.

Gomes, C. (2015). *O Impacto dos diferentes tipos de Assinatura Digital nas empresas do Séc. XXI - Casos de estudo: ActivoBank e ISCTE-IUL* . ISCTE-IUL.

Guedes, N. (2008). *Implementação de Solução de Assinaturas Digitais.* IST.

Heichlinger, A., & Gallego, P. (2010). A new e-ID card and online authentication in Spain.

Jean-François, B. (2006). The digital signature dilemma.

Lekkas, D., & Gritzalis, D. (2004). Cumulative notarization for long-term preservation of digital signatures.

Lentner, P. P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services - a comparative legal study.

Lowagie, B. (2012). *Digital Signatures for PDF documents.*

Martins, C. (2013). Relatório de Atividades'2012.

Mason, S. (2017). *Electronic Signatures in Law.* Cambridge University Press .

Mehran Alidoost Nia, A. S. (2014). An Introduction to Digital Signature Schemes.

Pfitzmann, A., & Hansen, M. (2006). Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology.

Philip Schütz, M. F.-H., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G., & (eds.). (2011). *Privacy and Identity Management for Life.*

Ponka, I. (s.d.). Legal Aspects of Digital Signatures and Non-Repudiation.

Ribeiro, C., Leitold, H., Esposito, S., & Mitzam, D. (2017). STORK: a real, heterogeneous, large-scale eID management.

Rito, C. (2018). *Governo Eletrónico - Assinatura Digital Qualificada.* IPLeiria.

Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government.

Stallings, W. (2017). *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE.*

Stančić, H. (2016). LONG-TERM PRESERVATION OF DIGITAL SIGNATURES .

SUBRAMANYA S.R., B. K. (March/April de 2016). Digital signatures.

Tsakalakis, N., Stalla-Bourdillon, S., & O'Hara, K. (2017). Identity Assurance in the UK:technical implementation and legal implications under eIDAS.

UCMA/UMIC/DGRN. (2007). Cartão de Cidadão - O novo documento de identificação dos cidadãos.

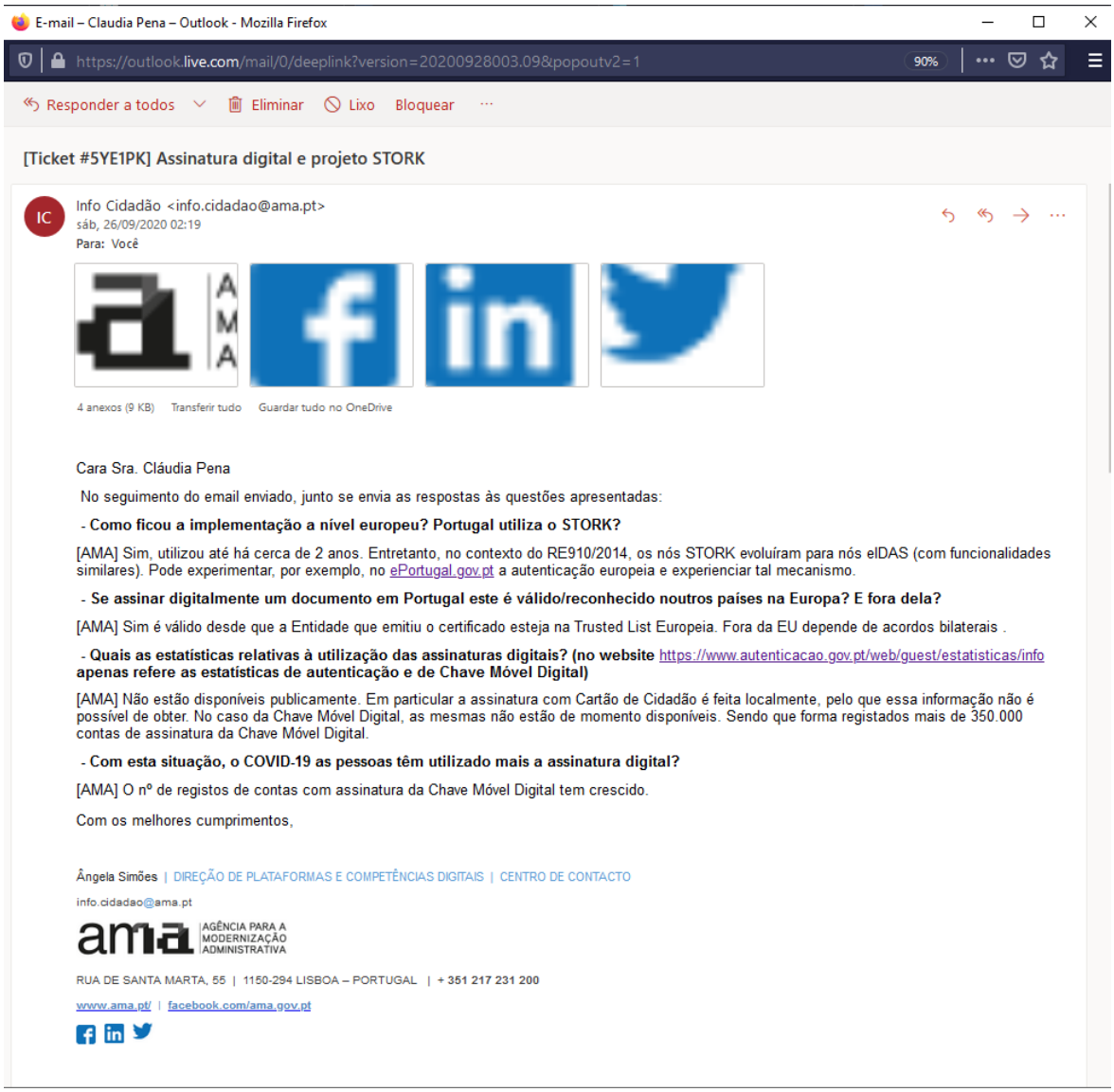
Zhou, J., Bao, F., & Deng, R. (2003). Validating Digital Signatures without TTP's Time-Stamping and Certificate Revocation.

Zuquete, A. (2013). *Segurança em Redes Informáticas - 4ªEdição Aumentada.* FCA.

Anexos

Anexo A – E-mail da AMA

O presente anexo apresenta as respostas da AMA ao e-mail que lhes enviei a solicitar esclarecimento e ajuda relativamente a alguma informação acerca das assinaturas digitais bem como do projeto STORK.



E-mail – Claudia Pena – Outlook - Mozilla Firefox

https://outlook.live.com/mail/0/deeplink?version=20200928003.09&popoutv2=1

Responder a todos | Eliminar | Lixo | Bloquear

[Ticket #5YE1PK] Assinatura digital e projeto STORK

IC

Info Cidadão <info.cidadao@ama.pt>
sáb, 26/09/2020 02:19
Para: Você

4 anexos (9 KB) Transferir tudo Guardar tudo no OneDrive

Cara Sra. Cláudia Pena

No seguimento do email enviado, junto se envia as respostas às questões apresentadas:

- **Como ficou a implementação a nível europeu? Portugal utiliza o STORK?**

[AMA] Sim, utilizou até há cerca de 2 anos. Entretanto, no contexto do RE910/2014, os nós STORK evoluíram para nós eIDAS (com funcionalidades similares). Pode experimentar, por exemplo, no ePortugal.gov.pt a autenticação europeia e experienciar tal mecanismo.

- **Se assinar digitalmente um documento em Portugal este é válido/reconhecido noutros países na Europa? E fora dela?**

[AMA] Sim é válido desde que a Entidade que emitiu o certificado esteja na Trusted List Europeia. Fora da EU depende de acordos bilaterais .

- **Quais as estatísticas relativas à utilização das assinaturas digitais? (no website** https://www.autenticacao.gov.pt/web/guest/estatisticas/info **apenas refere as estatísticas de autenticação e de Chave Móvel Digital)**

[AMA] Não estão disponíveis publicamente. Em particular a assinatura com Cartão de Cidadão é feita localmente, pelo que essa informação não é possível de obter. No caso da Chave Móvel Digital, as mesmas não estão de momento disponíveis. Sendo que forma registados mais de 350.000 contas de assinatura da Chave Móvel Digital.

- **Com esta situação, o COVID-19 as pessoas têm utilizado mais a assinatura digital?**

[AMA] O nº de registos de contas com assinatura da Chave Móvel Digital tem crescido.

Com os melhores cumprimentos,

Ângela Simões | DIREÇÃO DE PLATAFORMAS E COMPETÊNCIAS DIGITAIS | CENTRO DE CONTACTO
info.cidadao@ama.pt
ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
RUA DE SANTA MARTA, 55 | 1150-294 LISBOA – PORTUGAL | + 351 217 231 200
www.ama.pt/ | facebook.com/ama.gov.pt