Infraestrutura de Chaves Públicas suportando Assinaturas na Cloud baseadas no eIDAS

João Lopes[1,2], Ibéria Medeiros[1], and Sérgio Sá[2]

[1] LASIGE, Faculdade de Ciências da Universidade de Lisboa, Portugal
[2] Ernst & Young, S.A., Portugal
joao.pedro.lopes@pt.ey.com, imedeiros@di.fc.ul.pt, sergio.sa@pt.ey.com

Resumo As transações críticas online requerem prova de identidade dos seus participantes, a qual é garantida por certificados digitais emitidos por infraestruturas de chaves públicas (ICPs) e recorre ao uso de dispositivos físicos (ex., *smartcards*) para armazenamento das chaves privadas destes certificados. A inexistência de uma solução uniforme para transações online que requeiram prova de identidade dentro do mercado único europeu deu lugar à regulamentação dos serviços de confiança e identificação eletrónica (eIDAS) que visa padronizar as ICPs com respeito aos serviços que as utilizam. No entanto, com o emergir de novas tecnologias, em particular a *cloud*, surge a necessidade dos serviços tradicionais de certificados de selos eletrónicos e assinaturas qualificadas transitarem para o eIDAS, de modo a permitirem assinaturas remotas na *cloud*. A solução proposta neste artigo visa a implementação de uma das primeiras ICPs no mercado português com suporte a *assinaturas na cloud baseadas no eIDAS*, sendo a chave privada armazenada remotamente de forma segura. A solução foi implementada numa infraestrutura e avaliada, tendo em vista o cumprimento dos requisitos e normas europeias em vigor, o que permitiu atestar a sua conformidade.

Palavras-chave: Autenticação · assinaturas na *cloud* · infraestrutura de chaves públicas · eIDAS · segurança

1 Introdução

Ao longo das últimas décadas, o mundo tem assistido a uma constante evolução nas comunicações. Vivemos numa era onde o crescimento tecnológico é uma realidade e existe uma demanda constante por novas formas de inovar, capazes de proporcionar mais e melhores serviços para os cidadãos, com recurso, por exemplo à Internet, computadores e *smartphones*.

As transações online dependem deste tipo de tecnologias e dos avanços no setor das comunicações. No entanto, existem certos tipos de transações, como é o caso de *transações críticas online*, que devido à sua natureza, poderão requerer prova de identidade dos seus participantes. Esta é considerada uma propriedade de segurança – a *autenticação* – com o intuito de garantir a identificação do autor de determinada ação, bem como legitimar a mesma face a eventuais fraudes. Esta autenticação poderá ser garantida por meio do uso de assinaturas digitais.

As assinaturas digitais são mecanismos de segurança baseados, em regra, em criptografia de chave pública (i.e., criptografia assimétrica), onde cada interveniente na comunicação possui um par de chaves – pública e privada –, onde a primeira é partilhada e divulgada, enquanto a segunda permanece confidencial e apenas do conhecimento do seu proprietário. Ao enviar uma mensagem, o autor assina-a com a sua chave privada, enquanto o recetor usa a chave pública do autor para verificar a assinatura comprovando, ou não, a autenticidade da mensagem e a identidade do autor. As chaves públicas são disponibilizadas através de certificados digitais, sendo estes mecanismos eletrónicos os que permitem identificar, de forma unívoca, uma entidade numa plataforma digital. Estes são emitidos por Entidades Certificadoras (EC) que integram as Infraestruturas de Chaves Públicas (ICPs), que são as responsáveis pela gestão de chaves públicas.

Presentemente, as ICPs formam a base da segurança na Internet, melhorando os processos de autenticação existentes através de certificados digitais que permitem estabelecer uma associação de confiança entre um certificado emitido e a entidade à qual o certificado pertence. Estes certificados visam aumentar a confiança em entidades terceiras, no que concerne à autenticação e legitimidade das mesmas, quer seja através dos documentos por si assinados digitalmente, dos seus *websites* ou dos serviços por si prestados. No entanto, a Comissão Europeia reconheceu a inexistência de uma solução uniforme para as transações online que requeiram prova de identidade dentro do mercado único europeu, dando lugar à regulamentação para os serviços de confiança e identificação eletrónica (eIDAS) [1] que visa padronizar as ICPs com respeito aos serviços que as utilizam.

Com o emergir de novas tecnologias, em particular a *cloud*, o eIDAS prevê a possibilidade dos serviços tradicionais de certificados de selos eletrónicos e assinaturas qualificadas transitarem para o conceito de assinaturas remotas na *cloud*, contrariamente aos serviços tradicionais existentes onde as assinaturas são locais. Os serviços tradicionais requerem o armazenamento das chaves privadas em dispositivos físicos, tais como *smart-cards* ou *tokens*, os quais têm de estar na posse dos seus proprietários sempre que seja necessário realizar uma autenticação ou assinatura. Estes dispositivos poderão ser difíceis de gerir e a sua segurança é colocada em causa quando estes são danificados, perdidos ou roubados.

O artigo propõe uma solução para a implementação de uma das primeiras ICPs no mercado português com suporte a *assinaturas (remotas) na cloud baseadas no eIDAS*, onde as chaves privadas sejam armazenadas remotamente e de forma segura, abdicando assim da necessidade do uso de dispositivos físicos. A solução baseia-se no uso de Módulos de Hardware Seguros (MHSs), dispositivos responsáveis pelo armazenamento das chaves privadas e geração de assinaturas qualificadas. Na interação com o serviço, o utilizador deverá fazer uso de um ou mais fatores de autenticação, que lhe permitam gerar e atestar a sua própria identidade *cloud*, correspondente a um certificado de selo eletrónico ou de assinatura qualificada, bem como para a assinatura de documentos remotamente, cumprindo assim o requisito do regulamento de que apenas o próprio utilizador possa autorizar a criação de assinaturas em seu nome. A solução foi imple-

mentada numa infraestrutura e avaliada de acordo com os requisitos e normas europeias em vigor, o que permitiu atestar a sua conformidade.

As contribuições do artigo são: (1) uma solução baseada no eIDAS para autenticação em *cloud* com o uso de assinaturas qualificadas; (2) um processo para criação de identidades *cloud*; (3) um processo para realização de assinaturas remotas em *cloud*; (4) a implementação da solução numa infraestrutura e sua avaliação em conformidade com o eIDAS.

2 Trabalho Relacionado

Esta secção discute um conjunto de trabalhos e propostas de solução relativas ao foco do artigo, portanto, não pretende ser exaustiva quanto à discussão de outros trabalhos em áreas próximas.

Guedes [2] deu os primeiros passos de Portugal na implementação de uma ICP com suporte a certificados digitais qualificados, aquando da criação do cartão de cidadão. A arquitetura propunha que a criação de assinaturas digitais se efetivasse na máquina do utilizador, significando que a chave privada estaria na máquina do utilizador, algo que contrasta com a solução aqui apresentada, a qual propõe transitar as assinaturas para a *cloud*, ou seja, serem remotas. O autor já evidenciava algumas tecnologias que poderiam permitir este tipo de soluções remotas, sendo que estas à data não cumpriam alguns dos requisitos ou ainda não se encontravam disponíveis no mercado.

Windekilde et al. [3] realizaram um estudo acerca do impacto no mercado do uso da tecnologia da *cloud*, no que concerne a vantagens e desvantagens. Alguns dos pontos do estudo vão ao encontro da nossa proposta, relativamente às assinaturas remotas na *cloud*. O facto de não ser necessário o uso de dispositivos físicos contendo as chaves privadas (ex., *smart-cards*, *tokens*), poderá trazer vantagens a nível de custo-benefício para os utilizadores, uma vez que elimina-se a necessidade de adquirir estes dispositivos, bem como a dependência do serviço em função da disponibilidade destes.

Hühnlein [4] aborda as vantagens do uso da *cloud* e do eIDAS, discutindo o modo como ambos se poderiam combinar, por forma a permitir serviços de identificação e autenticação eletrónica de entidades, bem como a criação, verificação, validação e preservação de assinaturas digitais com recurso à técnica remota da *cloud*. Elenca as oportunidades existentes para a implementação de soluções que os combinam, tal como a nossa solução proposta.

Zwilling et al. [5] investigaram e analisaram o modo como alguns sistemas de identificação eletrónica se encontravam implementados em alguns dos estados membros europeus, como a Alemanha, Bélgica e Estónia. Alguns destes estados usam do Cartão de Identificação de Cidadão (*eID Card*) para a assinatura de documentos, o que implica a posse de um leitor, contrariamente ao que propomos neste artigo, em que essa necessidade apenas se verifica no momento da geração da identidade *cloud*. A Estónia apresentava uma alternativa ao uso desse cartão, o *Mobile ID*, porém este dependia da intervenção de operadores de telecomunicações e emissão de um novo cartão SIM (*Subscriber Identity Mo-*

dule) apropriado para o serviço de ICPs, onde seria armazenado o PIN (*Personal Identification Number*) necessário para o processo de assinatura de documentos. Esta proposta é semelhante à apresentada pela Autoridade da Tecnologia da Informação de Oman. Os autores concluíram que o uso de múltiplos fatores de autenticação reduz o risco de fraude, pois o esforço em roubar vários fatores é maior do que o necessário para roubar um único. A arquitetura por nós proposta contempla métodos de autenticação envolvendo sempre dois ou mais fatores de autenticação, diminuindo assim o risco do serviço ser comprometido. Apesar do uso dos cartões de identificação ser um elemento comum, os serviços nestes países não oferecem uma solução uniforme, tal como Cuijpers et al. [7] reconheceram no seu trabalho, não sendo assim capazes de disponibilizar serviços de identificação eletrónica a cidadãos de diferentes países da União Europeia.

Zefferer et al. [8] destacam a usabilidade e a segurança como requisitos cruciais em certificados de assinatura qualificada. Reconhecem, no entanto, que o recurso a *tokens* físicos pode introduzir complexidade no uso de certas soluções. A solução por nós proposta abdica destes recursos, sem prescindir da segurança.

A Thales [9], reconhecida companhia na área da segurança de TI, realizou um estudo sobre o impacto que o regulamento eIDAS traria ao mercado. O estudo permite dar uma visão sobre os requisitos do regulamento em termos técnicos, bem como da mudança de paradigma de assinaturas locais com recurso a *tokens* para assinaturas remotas. É ainda de especial relevo para este artigo, uma vez que a tecnologia dos Módulos de Hardware Seguros (MHSs) escolhida é fornecida por este fabricante, o que permite perceber a importância destes equipamentos, bem como do seu alinhamento com as normas e o próprio regulamento eIDAS.

Vale et al. [10] propõem uma abordagem semelhante à por nós apresentada, porém existem diferenças a destacar: a solução dos autores não segue as recomendações do Gabinete Nacional de Segurança (GNS), a entidade responsável pela supervisão das ICPs em Portugal, quanto aos requisitos dos certificados de assinaturas remotas na *cloud*; o código PIN para a geração de uma assinatura é sempre igual; e o cálculo da síntese (*hash*) dos documentos a assinar é feita no lado do utilizador, assumindo-se os dispositivos móveis usados como sendo seguros. Nós propomos a geração de um código único e de validade limitada (*One-Time Password* (OTP)), sempre que um utilizador pretenda assinar um documento, ou seja, um por cada documento a assinar. A síntese do documento é calculada do lado do serviço, num componente certificado e considerado seguro.

3 Arquitetura da Solução de Assinaturas na *Cloud*

Esta secção apresenta a arquitetura da solução proposta, bem como as componentes que a revestem, e os serviços *criação de identidades cloud* e *assinatura remota na cloud* oferecidos por ela, onde o uso do segundo requer o primeiro.

A solução tem por objetivo a implementação de uma ICP que suporte assinaturas qualificadas remotas na *cloud* baseadas no eIDAS, permitindo a autenticação por assinatura qualificada em serviços online, onde a chave privada do utilizador não está na sua posse, mas na *cloud*. A solução impõe diversos meca-

nismos de autenticação diferentes, baseadas em fatores distintos, para garantir a segurança dos serviços e das transações efetuadas.

O regulamento eIDAS introduziu um novo conceito de assinatura de documentos – assinaturas remotas na *cloud* –, a qual é realizada em nome do utilizador e poderá apenas ser invocada segundo a autorização do próprio. Quer isto dizer que, apesar da chave privada deixar de estar na posse do utilizador, este mantém o controlo sobre o seu uso. Também, é introduzido o conceito *identidade cloud* que associa a chave privada armazenada na *cloud* ao certificado gerado.

3.1 Visão Geral da Arquitetura

A arquitetura da solução proposta é apresentada na Figura 1, a qual é constituída por duas camadas interligadas, nomeadamente: *zona de acesso externo* e *zona de alta segurança*, onde diversos mecanismos de autenticação são utilizados nas interações entre estas. A interação entre os clientes (utilizadores) e os serviços oferecidos pela arquitetura é realizada na camada de acesso externo, a qual comunica com a camada de alta segurança, através de um canal seguro, para solicitação dos pedidos dos clientes, após uma correta autenticação dos mesmos, e a receção das respostas a estes. A camada de alta segurança tem como objetivo executar as operações de autenticação de utilizadores, bem como autorizar os acessos às identidades *cloud* e aceder a estas para a realização das assinaturas remotas, inerentes aos pedidos.

Os principais componentes da arquitetura e inseridos nas duas camadas são:

- *Portal web*: redireciona os pedidos/respostas de/para os utilizadores, estabelecendo a ponte entre os utilizadores e a camada de alta segurança;
- *Plataforma de Autenticação, Autorização e Assinatura*: autentica os utilizadores e autoriza o seu acesso às identidades *cloud*, bem como a realização de assinaturas remotas, segundo o eIDAS. Estabelece a ponte entre os pedidos recebidos da camada de acesso externo e os restantes componentes da camada de alta segurança;
- *Infraestrutura de Chaves Pública (ICP)*: entidade responsável pela gestão dos certificados de selos eletrónicos e assinaturas qualificadas;

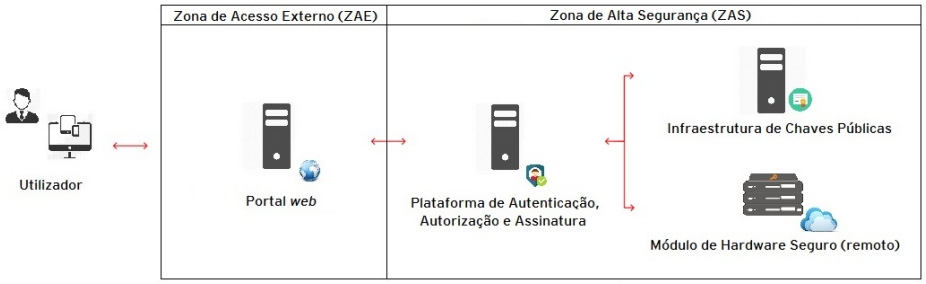

Figura 1. Arquitetura da solução para assinaturas na *Cloud*

– *Módulos de Hardware Seguros (MHSs)*: dispositivos responsáveis pela geração e armazenamento das chaves privadas dos utilizadores, correspondentes às identidades *cloud*.

Os utilizadores, através de um *browser*, acedem ao portal *web* para utilização dos serviços pretendidos. Neste sentido, o utilizador autentica-se no portal com as suas credenciais de acesso, que as redireciona para a plataforma de autenticação para verificação destas. Após uma correta autenticação, os utilizadores podem dar início à realização de pedidos, os quais são redirecionados pela plataforma para a zona de alta segurança. A plataforma comunica com a ICP para realização de ambos serviços: (1) para a geração de certificados, que por sua vez comunica com o MHS para a geração das chaves privadas a associar aos certificados emitidos pela ICP, constituindo assim as identidades *cloud* (ver Secção 3.5); e (2) para a realização de assinaturas remotas na *cloud* de documentos, que comunica com o MHS para verificação da identidade *cloud* a usar (ver Secção 3.6). As chaves geradas dentro do MHS permanecem dentro deste dispositivo e todos os pedidos efetuados à plataforma na camada de alta segurança dependem de autenticações bem sucedidas, que fazem uso de mecanismos de segurança bem definidos, garantindo assim a conformidade com o eIDAS.

3.2 Infraestrutura de Chaves Públicas (ICP)

A ICP deverá ser capaz de emitir e gerir certificados de selos eletrónicos e assinaturas qualificadas, em cumprimento com os requisitos do eIDAS [1], bem como as recomendações do despacho 155/2017 emitido pelo Gabinete Nacional de Segurança (GNS), a entidade responsável pela supervisão das ICPs em Portugal [11]. De acordo com o GNS, os certificados de selos eletrónicos e de assinatura qualificada cuja gestão seja feita pelo prestador qualificado de serviços de confiança em nome do utilizador, uma vez que a chave privada se encontra armazenada remotamente, devem obedecer às seguintes indicações: (1) no campo `subject`, o atributo `organizationUnit` (OU) deve conter o valor `RemoteQSCDManagement`; (2) o `OU` deve ser inscrito no atributo imediatamente anterior ao `commonName`.

A ICP deverá ainda ser constituída pelos seguintes elementos:

– *Entidade Certificadora (EC):* sistema responsável pela geração e revogação de certificados;
– *Autoridade de Registo (RA):* executa funções administrativas da EC, tais como o registo das entidades finais e a emissão de certificados;
– *Autoridade de Validação (VA):* valida os certificados emitidos pela EC usando o protocolo *Online Certificate Status Protocol* (OCSP), responsável pela monitorização do estado dos certificados [12].
– *Autoridade de Validação Cronológica (TSA):* garante a determinação exata do momento temporal em que uma dada ação ocorreu, como por exemplo uma transação online ou a assinatura de um documento.

3.3 Módulos de Hardware Seguros (MHSs)

Os MHSs são a única forma comprovada e auditável de proteger dados criptográficos. São dispositivos dedicados para processar e gerir este tipo de dados, tais como sementes de *One-Time-Passwords* (OTPs), *passwords* de autenticação e chaves privadas. Compreendem todo um conjunto de mecanismos de proteção robustos, quer a nível lógico como físico, de modo a garantir as normas e políticas de segurança aplicáveis a este tipo de tecnologia, o que permite construir uma forte raiz de confiança, num dispositivo que será responsável pela criação de assinaturas qualificadas (de acordo com [11]).

3.4 Plataforma de Autenticação, Autorização e Assinatura

Esta plataforma tem por funcionalidades a execução das operações de autenticação de utilizadores, bem como a solicitação de criação de identidades *cloud* e autorização de acesso a estas identidades para a realização de assinaturas remotas, segundo a regulamentação eIDAS. Também, a plataforma atua como fornecedora de identidades – *Identity Provider (IdP)* – e fornecedora de assinaturas – *Signature Provider (SigP)* – para os utilizadores finais.

Como IdP, deverá ter a capacidade de validar a identidade do utilizador e gerir os níveis de autenticação necessários para cada tipo de ação pretendida (criar identidades *cloud* ou assinar na *cloud*), de acordo com os níveis de garantia exigidos pelo regulamento eIDAS. Como SigP deverá ser responsável, em parte, pela gestão dos dados dos utilizadores, tais como atributos de identidade que se encontrem no repositório interno (seguro e auditável) da plataforma, de modo a poder autorizar o uso das chaves de uma determinada entidade para processar uma assinatura.

3.5 Criação de Identidades *Cloud*

A Figura 2 ilustra o processo de criação de identidades *cloud* que engloba oito passos. Este processo requer o uso de três fatores de autenticação: (1) credenciais

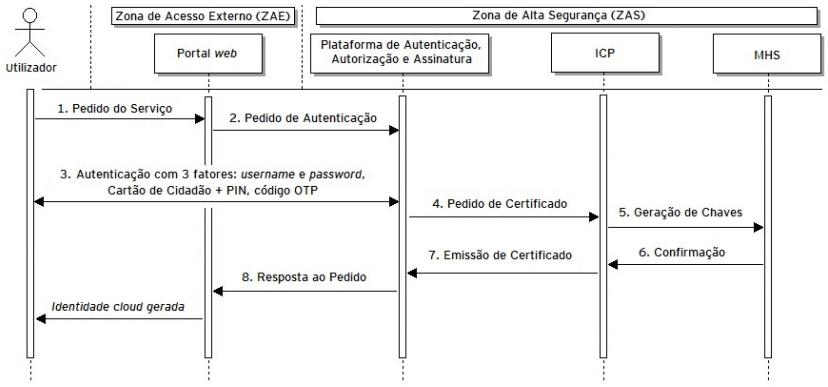

Figura 2. Processo de criação de uma identidade *Cloud*

do utilizador no serviço (*username* e *password*), (2) Cartão de Cidadão com o respetivo PIN e (3) código OTP. O uso do cartão de cidadão e seu PIN de acesso comprovam a identidade do utilizador, uma vez que estes são intransmissíveis.

Para iniciar o processo e após registo no serviço, o utilizador autentica-se no portal *web* com as suas credenciais. É requerida a apresentação do Cartão de Cidadão com o PIN. É enviado um código OTP para o email de registo, de modo a completar o processo de autenticação. Uma vez bem sucedida, o utilizador é autorizado a criar a sua identidade *cloud* (passos 1 a 3). A plataforma gera um pedido à EC da ICP, para a emissão de um certificado (passo 4), que poderá ser de selo eletrónico ou de assinatura qualificada, dependendo do serviço para o qual o utilizador se tenha registado. A EC por sua vez solicita ao MHS a geração de um par de chaves (passo 5). O MHS protege as chaves privadas dos utilizadores com recurso a uma chave mestra, que será usada para cifrar a chave privada de cada utilizador, sendo que o resultado desta operação é uma chave cifrada, e não a chave privada do utilizador. Após confirmação do MHS, o certificado é emitido e enviado à plataforma de autenticação, e a resposta ao pedido de criação de identidade *cloud* enviado ao portal (passos 6 a 8). As chaves do utilizador, a pública e a cifrada (chave privada cifrada com a chave mestra do MHS) são enviadas à plataforma de autenticação, para que sejam armazenadas na sua base de dados interna. Para tal, é gerado um ID único que permite estabelecer a correspondência entre a identidade *cloud* do utilizador e a chave cifrada.

3.6 Assinatura remota na *Cloud*

Um utilizador possuidor de identidade *cloud* pode assinar documentos remotamente, o qual requer dois fatores de autenticação: (1) credenciais do utilizador no serviço (*username* e *password*) e (2) código OTP, um para cada documento a assinar.

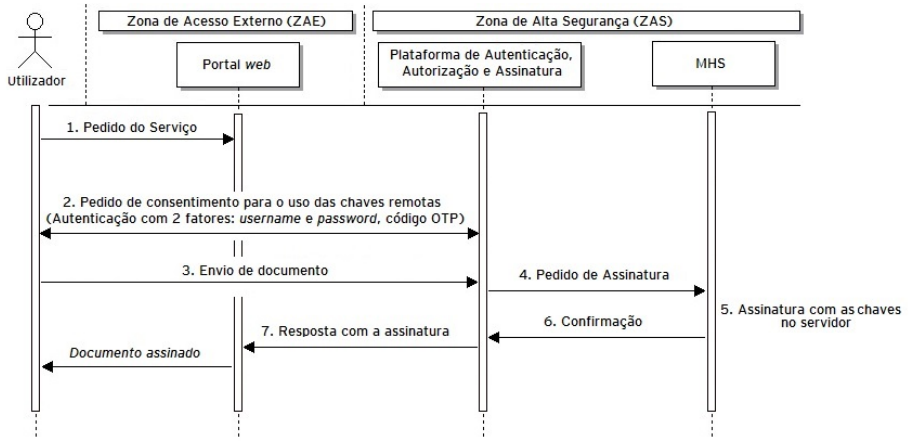

Figura 3. Processo de assinatura remota na *Cloud*

O processo de assinatura remota na *cloud* desenrola-se de acordo com o apresentado na Figura 3 e engloba sete passos. Após o utilizador autenticar-se no portal, é necessário carregar o documento a assinar para o portal, que o redireciona para a plataforma. É então criado um pedido do serviço de assinatura de documento e um pedido para o uso das chaves (passos de 1 a 3). A plataforma calcula a síntese do documento (*hash)* e envia-a para o MHS, juntamente com a chave cifrada do utilizador, para que se proceda à assinatura (passo 4). A chave cifrada, tal como referido na Secção 3.5, está armazenada internamente na plataforma e identificada por um ID único, gerado pela plataforma aquando da criação da identidade *cloud*. Posteriormente, o MHS decifra a chave do utilizador com recurso à chave mestra, para obter a chave privada deste, assina a síntese do documento, originando assim a assinatura, e devolve-a à plataforma, sendo o documento assinado retornado ao utilizador (passos 5 a 7).

4 Implementação

Como referido anteriormente, a solução proposta foi implementada com o objetivo de ser uma das primeiras ICPs no mercado português a suportar *assinaturas na cloud baseadas no eIDAS*. A solução implementada oferece serviços de certificados de selos eletrónicos e de assinatura qualificada, que conferem valor probatório aos documentos assinados nestas condições. A implementação foi dirigida em duas partes principais: a zona de acesso externo, parte acessível aos utilizadores onde é disponibilizado o portal de acesso *web*, e a zona de alta segurança, de acesso restrito, onde se encontram os restantes componentes. A plataforma escolhida para a autenticação, autorização e assinaturas tem o funcionamento de uma API. O portal *web* consome as interfaces da API necessárias ao serviço, sendo a plataforma de acesso reservado e apenas permitido por administradores da ICP.

A nível de MHSs, são utilizados dois destes componentes, configurados em modo de alta disponibilidade cujo objetivo é suportar, de forma redundante, as operações criptográficas nomeadamente a geração e armazenamento das chaves privadas dos utilizadores. Os MHSs escolhidos na nossa solução são certificados pelo organismo reconhecido a nível europeu, a agência certificadora italiana OCSI (*Organismo di Certificazione della Sicurezza Informatica*), que no seguimento do processo de acreditação ao produto escolhido e fundamentando-se no artigo 51 do regulamento eIDAS, permite qualificá-los como dispositivos para a criação de assinaturas qualificadas em conformidade com o regulamento eIDAS (QSCDs) [13]. Estes MHSs apenas interagem com servidores com os quais tenham sido previamente configurados através do painel frontal dos próprios MHSs. Na nossa solução, o acesso foi dado apenas à Entidade Certificadora que compõe a ICP e à plataforma de autenticação, autorização e assinatura, descrita na Secção 3.4. Alterações nesta configuração dos MHSs exigem o acesso físico aos mesmos, o que requer a passagem por diversos níveis de segurança definidos na própria infraestrutura.

5 Avaliação

O objetivo da avaliação foi verificar se a solução implementada está em conformidade com as normas emitidas pelo Comité Europeu de Normalização (CEN) e pelo Instituto Europeu de Normas para as Telecomunicações. Estas são duas organizações oficialmente reconhecidas pela União Europeia e pela Associação Europeia de Livre Comércio (EFTA) como sendo responsáveis pela definição de normas a nível europeu. Neste sentido, os testes realizados basearam-se nas orientações e requisitos apresentados pelas seguintes listas de verificação (*checklists*):

1. **CEN EN 419 241:2014**: *Security Requirements for Trustworthy Systems Supporting Server Signing* [14]:
   - Requisitos gerais para os Prestadores de Serviços de Confiança;
   - Requisitos para Certificados de Assinatura Qualificada;
   - Requisitos para Certificados de Selos Eletrónicos;
   - Requisitos gerais de Segurança (Gestão, Sistemas e Operação, Identificação e Autenticação, Sistemas de Controlo de Acessos, Gestão de Chaves, Monitorização e Auditoria, Arquivamento, Resiliência, Segurança de Componentes Chave, Autenticação do Assinante, Criação de Assinaturas).
2. **ETSI EN 319 411-1**: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* [15]
3. **ETSI EN 319 411-2**: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates* [16]:
   - Disposições gerais das Declarações de Práticas de Certificação (DPCs) e Políticas de Certificados (PCs);
   - Práticas dos Prestadores de Serviços de Confiança;
   - Estrutura para a definição de outras Políticas de Certificados.
4. **Regulamento eIDAS n.º 910/2014** [1]:
   - Secção 4.1 (Requisitos gerais para os Prestadores de Serviços de Confiança);
   - Secção 4.2.1 (Certificados Qualificados para Assinatura Eletrónica);
   - Secção 4.2.2 (Certificados Qualificados para Selos Eletrónicos).

Atualmente, a série EN 419 241 apresenta duas variantes, CEN EN 419 241-1 e CEN EN 419 241-2, tendo em vista a especificação dos requisitos para o regulamento eIDAS, no que respeita ao uso de dispositivos remotos para a criação de assinaturas qualificadas, geridos por prestadores de serviços de confiança. A primeira parte detalha as especificações técnicas, naquela que é uma adaptação dos requisitos já apresentados na versão de 2014. Já a segunda parte diz respeito aos perfis de proteção para os módulos de ativação de assinaturas nos dispositivos usados para a criação de assinaturas qualificadas remotas (*remote QSCDs*). Os

requisitos desta lista correspondem a um componente que deverá correr dentro dos MHSs mas que ainda não foi desenvolvido, uma vez que o tema ainda se encontra em discussão. Os fabricantes irão disponibilizar este componente assim que haja um consenso entre os reguladores europeus que discutem a matéria.

Seguindo as indicações emitidas para a Comissão Europeia e para os organismos nacionais de supervisão por parte da DTCE (*Digital Trust and Compliance Europe*) [17], a organização para a conformidade e confiança digital na Europa, na ausência da definição desse componente deverão ser considerados os MHSs atualmente no mercado que estejam em conformidade com a versão CEN EN 419 241:2014 atualmente em vigor, uma vez que estes cumprem os requisitos de segurança previstos na Diretiva 99/93/CE [18] e a certificação requerida pelo artigo 30 (3), alínea b, do eIDAS [1]. Assim, o caminho adotado na implementação desta solução teve em consideração a recomendação emitida por este regulador europeu, pelo que foi considerada a versão de 2014 (CEN EN 419 241:2014) uma vez que é aquela que se encontra atualmente em vigor e para a qual existem MHSs disponíveis no mercado em conformidade com a mesma. Esta decisão justifica-se também pelo facto de ser a única forma de completar o processo de certificação e auditoria da solução proposta, de modo a colocar o serviço já em produção. A recomendação estende-se também ao facto de, na ausência de versões finais aprovadas de normas, poderão considerar-se as suas versões ainda em aprovação (*draft*), o que no nosso caso abrange as normas ETSI EN 319 411-1 e ETSI EN 319 411-2.

Após o preenchimento destas listas de verificação, confirmou-se a conformidade da solução nos pontos considerados, à exceção dos requisitos da CEN EN 419 241:2014 relativos ao uso de *tokens* físicos, algo que era expectável dado que a versão da lista de verificação considerada não contempla ainda a possibilidade de assinaturas remotas na *cloud*.

6 Conclusão

Este artigo apresentou uma solução com vista a implementar uma das primeiras infraestruturas de chaves públicas em Portugal capazes de produzir assinaturas remotas na *cloud* em conformidade com o regulamento eIDAS. A solução propõe um processo para a criação de identidades *cloud* e outro para a realização de assinaturas remotas, onde o segundo necessita do primeiro, e diversos mecanismos de autenticação para garantir a segurança das diversas interações. Foram identificadas lacunas na regulamentação que suporta o eIDAS, motivadas pela existência de normas ainda em aprovação (*draft*), o que força o mercado a regular-se por normas antigas. A solução foi implementada em ambiente real, avaliada/auditada internamente, verificando-se o cumprimento dos requisitos exigidos pelas atuais normas europeias em vigor.

Agradecimentos Este trabalho foi parcialmente suportado pela empresa EY-Portugal e pelos fundos nacionais através da Fundação para a Ciência e a Tecnologia (FCT) com referência à Unidade de Investigação LASIGE (UID/CEC/00408/2013).

Referências

1. Official Journal of the European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014)
2. Guedes, N.: Implementação de Solução de Assinaturas Digitais. Instituto Superior Técnico, Lisboa, Portugal (2008)
3. Windekilde, I., Catalina, I.: Cloud computing - Impact on business. Aalborg University Copenhagen (2014)
4. Hühnlein, D.: Towards eIDAS as a Service. Ecsec GmbH, Michelau, Germany (2014)
5. Alazri, Y.: Mobile ID (Mobile PKI). Information Technology Authority. Sultanate of Oman (2016)
6. Zwilling, A., Smetsers, J., Eekelen, M.: Electronic Identity Management Systems in the European Union. Radboud University (2017)
7. Cuijpers, C., Schroers, J.: eIDAS as guideline for the development of a pan European eID framework in FutureID. Radboud University/KU Leuven, Nijmegen, Netherlands (2015)
8. Zefferer, T., Krnjic, V.: Usability evaluation of Electronic Signature based e-Government solutions. E-Government Innovation Center (EGIZ), Austria (2012)
9. Thales e-security: The Impact of the European eIDAS Regulation
10. Vale, P., Cardoso, C., Portela, R., Chaves, R.: RSIGN: Secure Remote Qualified Signature Solution. INESC-ID, IST, Universidade de Lisboa. Multicert (2017)
11. Gabinete Nacional de Segurança (GNS): Despacho 155/2017. Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário. Portugal (2017)
12. Santesson, S. et al. RFC 6960 - PKIX OCSP. University of Ottawa (2013)
13. OCSI. Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE - Rapporto di Accertamento - Thales nShield HSM Family (2016)
14. European Committee for Standardization (CEN). European Standard (EN) 419 241:2014: Security Requirements for Trustworthy Systems Supporting Server Signing (2014)
15. European Telecommunications Standards Institute (ETSI). European Standard (EN) 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2018)
16. European Telecommunications Standards Institute (ETSI). European Standard (EN) 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2018)
17. Cattaneo, D. Digital Trust and Compliance Europe: DTCE Position Paper on Remote Signing (2015)
18. Parlamento Europeu. 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 (1999)