Relatório Técnico

Autor: AMA	**Data:** 04/Novembro/2020
Assunto: Dados pedidos pelas ECs para emissão de selo eletrónico qualificado para utilizar no SCAP	
Assunto: SCAP	
Observações: -	

1. Contextualização

O fornecedor de atributos (FA) do SCAP, ao validar que o cidadão possui o atributo pedido, assina o hash do documento submetido pelo cidadão, adicionando à assinatura a informação do atributo indicada nos artigos 12° e 13° da portaria n.° 73/2018 de 12 de março. A assinatura efetuada pelo FA (i.e., a aposição do selo eletrónico):

i. É efetuada recorrendo a um selo eletrónico qualificado (ou certificado qualificado para selo eletrónico) emitido por uma Entidade de Certificação credenciada para a emissão desses certificados (*QCert for ESeal*) de acordo com o Regulamento da UE 910/2014, para o que

ii. Utiliza um dispositivo qualificado de criação de selo eletrónico (*QSCD – Qualified Seal Creation Device*) sob controlo exclusivo do FA.

Para tal,

A. A AMA, através de acordo a efetuar com o FA, disponibiliza um QSCD para custódia da chave privada (neste caso, um HSM[1]), sob controlo exclusivo do FA;

B. O FA, com o apoio técnico da AMA, efetuará a operação de geração de par de chaves no QSCD disponibilizado pela AMA. Nesta operação, para além de gerar o par de chaves para assinatura, o FA obterá ainda o CSR (*Certificate Request*);

C. Munido do CSR, o FA poderá efetuar o pedido de selo eletrónico qualificado a uma Entidade de Certificação credenciada para a emissão desses certificados (*QCert for ESeal* com custódia de chave privada em QSCD da AMA);

D. Após obter o selo eletrónico qualificado, o FA fornece-o à AMA, que efetuará a sua configuração na aplicação de aposição do selo eletrónico.

[1] HSM – *Hardware Security Module*.

2. Obtenção de selo eletrónico qualificado para Fornecedor de Atributos do SCAP

Após o FA efetuar a geração do par de chaves e ter obtido o CSR (*Certificate Request*), pode efetuar o pedido de selo eletrónico qualificado a uma Entidade de Certificação credenciada para a emissão de certificado de selo eletrónico qualificado (*QCert for ESeal*) com custódia da chave privada em QSCD da AMA.

Para a emissão do selo eletrónico qualificado (*QCert for ESeal*) com custódia da chave privada em HSM, a Entidade de Certificação pode efetuar as questões identificadas na seguinte tabela, devendo ser fornecidas as respetivas respostas.

Questão colocada pela Entidade de Certificação	**Resposta**
Validade do selo eletrónico qualificado	Recomenda-se 2 ou 3 anos. Note que antes da finalização do prazo de validade será necessário gerar novo par de chaves e pedir novo certificado.
Nome do QTSP [2]que faz custódia operacional da chave privada	AMA - Agência para a Modernização Administrativa, I.P.
Link para a Trusted List do QTSP	https://webgate.ec.europa.eu/tl-browser/#/trustmark/PT/VATPT-508184509
A chave privada encontra-se num QCSD de acordo com o Regulamento (UE) nº 910/2014	A marca e modelo do QSCD usado para custódia operacional da chave privada é "Thales nShield Connect XC". Encontra-se referenciado como "*nShield Solo XC Hardware Security Module v12.50.7*" na *Compilation of :* *Member States' notifications on:* • *Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014* • *Certified Qualified Signature Creation Devices under Article 31(1)-(2) and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014,* *and* *information from the Member States on:* • *Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014*

[2] QTSP – *Qualified Trust Service Provider*

	disponível em https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds. A credenciação Common Criteria do QSCD pode ser acedida através do portal https://www.commoncriteriaportal.org/products/, estando disponíveis os seguintes documentos: • *Security Target*[3], • *Certification Report*[4], • CCRA Certificate[5].
Descrição do processo de geração da chave privada	A geração da chave privada é efetuada, em cerimónia de geração de chave privada no Thales nShield Connect XC, pela entidade que pede o certificado de selo eletrónico qualificado, com apoio técnico da AMA. No final desta cerimónia, para além de gerar o par de chaves no Thales nShield Connect XC, a entidade que pede o certificado de selo eletrónico qualificado define o segredo de acesso à chave privada, assim como obtém o CSR (*Certificate Request*).
Descrição do processo de ativação da chave privada	A ativação da chave privada é efetuada no HSM (QSCD) pela entidade detentora do respetivo certificado de selo eletrónico qualificado, através de API disponibilizada pelo SCAP.
Frequência de ativação da chave privada	A chave privada é ativada sempre que a entidade detentora do respetivo certificado de selo eletrónico qualificado toma a iniciativa de a ativar, para aposição de selo eletrónico.
Responsáveis pela ativação da chave privada	A chave privada é ativada pela entidade detentora do respetivo certificado de selo eletrónico qualificado.
Descrição dos casos de uso de utilização do certificado a emitir	Casos de uso de acordo com portaria n.º 73/2018 de 12 de março.

[3] Acessível em https://www.commoncriteriaportal.org/files/epfiles/nShield%20Solo%20XC%20HSM%20Security%20Target%20v1.0.pdf
[4] Acessível em https://www.commoncriteriaportal.org/files/epfiles/Certification_Report_NSCIB-CC-163968-CR.pdf
[5] Acessível em https://www.commoncriteriaportal.org/files/epfiles/Certificate%20163968%20incl%20eIDAS%20reference%2023-7-2020%20(3).pdf.