NORMA TÉCNICA – D 03

REQUISITOS PARA ENTIDADES CERTIFICADORAS QUE EMITEM CERTIFICADOS QUALIFICADOS

Lisboa, 03 de Novembro de 2009

A Autoridade Nacional de Segurança

Assinado de forma digital por José Deolindo Torres Sobral
DN: cn=José Deolindo Torres Sobral, c=PT, o=Presidência do Conselho de Ministros, ou=Gabinete Nacional de Segurança - Autoridade Nacional de Segurança
Dados: 2009.11.03 16:26:06 Z

(José Torres Sobral)

1. REFERÊNCIAS

a. CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, de Junho de 2003.

b. CWA 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations with Backup - Protection Profile - CMCSOB-PP, de Maio de 2004.

c. CWA 14169: Secure Signature-Creation Devices "EAL 4+", de Março de 2004.

d. Decreto Regulamentar n.º 25/2004, de 15 de Julho, do Ministério da Justiça.

e. Decreto-Lei n.º 290-D/99, de 02Ago, republicado pelo DL 88/09 de 09 de Abril.

f. Portaria 597/2009, de 04 de Junho.

g. Directiva 1999/93/CE, de 13 de Dezembro de 1999.

h. ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates, versão 1.4.3, de Maio de 2007.

i. ETSI TS 101 861: Time stamping profile, versão 1.3.1, de Janeiro de 2006.

j. ETSI TS 101 862: Qualified certificate profile, versão 1.3.3, de Janeiro de 2006.

k. ETSI TS 102 023: Electronic signatures and Infrastructures (ESI); policy requirements for time stamping authorities, versão 1.2.1, de Janeiro de 2003.

l. ETSI TS 102 176-1: Electronic Signatures and Infrastructures (ESI), Algorithms and Parameters for Secure Electronic Signatures - Part 1: Hash functions and asymmetric algorithms, versão 2.0.0, de Novembro de 2007.

m. ETSI TS 102 280: X.509 V.3 certificate profile for certificates issued to natural persons, versão 1.1.1, de Março de 2004.

n. GNS-NT D 02: "Requisitos mínimos de segurança física de instalações de Entidades Certificadoras".

o. ISO/IEC 15408-1:2005: Information technology - Security techniques - Evaluation criteria for IT security" - Part 1: Introduction and general model"

p. ISO/IEC 27001: Information technology-Security techniques-Information security management systems-Requirements, de Outubro de 2005.

q. RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, de Novembro de 2003.

r. SCEE – Politica de Certificados do SCEE e Requisitos mínimos de Segurança, de 14Julho de 2006.

s. Decreto-lei nº 170/2007 de 03 de Maio.

2. SITUAÇÃO

Uma Entidade Certificadora (EC), enquanto fornecedora de serviços de certificação electrónica, gere e disponibiliza certificados electrónicos, de modo a suportar a utilização de assinaturas electrónicas.

De acordo com a legislação europeia e nacional, assume-se que as EC utilizarão uma Infra-estrutura de chave pública (ICP) para a gestão do ciclo de vida dos certificados, nomeadamente, para o registo, emissão e revogação dos diversos certificados e chaves.

Neste contexto, as EC, obrigatoriamente, disponibilizam um conjunto de funções/serviços nucleares. Opcionalmente disponibilizam serviços suplementares.

Consideram-se serviços nucleares:

- Serviço de **Registo**: tem como objectivo verificar e garantir a identidade do titular. O "output" deste serviço será passado para o Serviço de Geração de Certificados.
- Serviço de **Geração (emissão) de Certificados**: tem como objectivo gerar e emitir certificados, previamente validados pelo Serviço de Registo.
- Serviço de **Disseminação:** tem como objectivo disponibilizar os certificados aos titulares.
- Serviço de **Gestão de Revogações**: tem como objectivo processar os pedidos de revogação e implementar as acções necessárias. O resultado deste serviço será difundido através do Serviço sobre o Estado das Revogações.

- Serviço sobre o **Estado das Revogações:** tem como objectivo, disponibilizar informação sobre o estado das revogações dos certificados às partes confiantes. Este serviço pode ser disponibilizado em tempo real (Online Certificate Status Protocol (OCSP)) ou através de actualizações periódicas regulares (Certificate Revocation List (CRL)).

Os serviços suplementares são os seguintes:

- O Serviço de **Fornecimento do Dispositivo Seguro de Criação de Assinaturas** (Secure Signature Creation Device (SSCD)): tem como objectivo preparar e fornecer o respectivo dispositivo ao titular do certificado.
- O Serviço de **Validação Cronológica**: tem como objectivo, a geração e distribuição de "*tokens*" de validação cronológica, de forma a ligar criptograficamente os dados com valores de tempo seguros.

3. OBJECTO/FINALIDADE

A presente norma tem como objectivo agrupar os diversos critérios e requisitos estabelecidos em legislação e normativos nacionais e internacionais de modo a proporcionar de forma integrada uma visão global sobre as condições de elegibilidade das EC que emitem Certificados Qualificados.

4. ÂMBITO

A presente norma aplica-se às EC que emitem Certificados Qualificados.

5. EXECUÇÃO

As EC que emitem Certificados Qualificados devem proceder ao seu **Registo** junto da Autoridade Credenciadora (AC) (Artigo 9º do Decreto-Lei n.º 290-D/99, referência 1. e. e Artigo 2º da Portaria 597/2009, referência 1. f.). Para tanto preenchem o formulário "Pedido de Registo/Credenciação e Filiação/Integração no SCEE" disponível no *website* do GNS.

Tendo como referência a legislação, regulamentos e especificações técnicas em vigor, as EC que emitem Certificados Qualificados devem assegurar que as suas instalações, procedimentos, atributos do pessoal, equipamentos e sistemas obedecem a todas as normas de segurança aplicáveis ao exercício da sua actividade.

Neste contexto, as EC que emitem Certificados Qualificados, estabelecidas em Portugal, obedecem aos seguintes requisitos:

a. Elaborar uma **Politica de Certificados Qualificados**:

1) A política de certificados a utilizar pode ser, consoante o caso:

a) Definida pelo ETSI: "QCP public" ou "QCP public +SSCD";

b) Definida pela EC: desde que equivalentes às definidas na alínea anterior;

c) Para Entidades públicas integradas no Sistema de Certificação Electrónica do Estado (SCEE): "id-scee-assinatura".

2) Os certificados são emitidos em conformidade com o descrito nos:

a) ETSI TS 101862 (referência 1.j);

b) ETSI TS 102280 (referência 1.m);

c) ETSI TS 102176-1 (referência 1.l).

Os algoritmos e parâmetros a utilizar devem reflectir com especial atenção a durabilidade dos esquemas de assinatura relativamente à sua resistência a ataques ("Table 14: Recommended Signature Suites for a resistence during X years"), uma vez que afecta directamente o período de validade que se pretende atribuir a cada certificado.

b. Efectuar uma **Avaliação de Riscos,** em conformidade com o descrito na norma ISO/IEC 27001 (referência 1.p).

c. Elaborar uma **Declaração de Práticas de Certificação,** utilizando a estrutura definida no RFC 3647 (referência 1.q).

d. Elaborar um **Plano de Segurança**, de acordo com o descrito no artigo 27º do Decreto-Regulamentar 25/2004 (referência 1.d.).

e. Elaborar um **Plano de Contingência**, de acordo com o descrito no artigo 28º do Decreto-Regulamentar 25/2004 (referência 1.d.).

f. Estabelecer/adaptar a sua **actividade operacional** de acordo com os requisitos definidos nos documentos:

1) ETSI TS 101456 (referência 1.h.);

2) CWA 14167:1 (referência 1.a.);

3) Quando se trate de uma EC pública, adequar-se às regras do SCEE (referência 1.r.).

g. Constituir uma **Estrutura de Pessoal**, responsável pelas funções de gestão da ICP, na qual contemple os cargos/funções definidos no artigo 29º do Decreto-Regulamentar 25/2004 (referência 1.d.).

h. Contratar os serviços de um **Auditor de Segurança Credenciado** pelo GNS, fora da sua estrutura organizativa, no âmbito do definido no artigo 30º do Decreto-Regulamentar 25/2004 (referência 1.d.)

i. Utilizar sistemas fiáveis:

1) O **Dispositivo Seguro de Hardware (HSM)** a utilizar na EC para as operações que dizem respeito à geração, armazenamento e assinatura de certificados e listas de revogação, requer a conformidade e respectiva certificação numa das seguintes normas (ou critérios reconhecidos como equivalentes):

a) FIPS 140-2 Level 3; ou

b) CWA 14167-2 (referência 1.b.); ou

c) ISO 15408 (referência 1.o.) no nível EAL 4 ou superior;

2) **Software** para gestão do ciclo de vida dos certificados e chaves:

a) Conformidade e respectiva certificação segundo os requisitos definidos no documento CWA 14167-1 (referência 1.a.).

b) Em alternativa a utilização de produtos/sistemas avaliados segundo a norma ISO 15408 (referência 1.o.), em EAL 4 ou superior, ou perfil equivalente.

j. Desenvolver a actividade em **instalações físicas** adequadas, em conformidade com os requisitos definidos na Norma Técnica do GNS - NT D-02 (referência 1.n.).

k. Se for EC privada, cumprir os **requisitos patrimoniais** legais em vigor (artigo 14º do Decreto-Lei n.º 290-D/99, referência 1.e. e Critérios de adequação dos capítulos III e IV do Decreto-Lei n.º 290-D/99).

l. Se for EC privada, dispor de **seguro de responsabilidade civil** (artigo 16º do Decreto-Lei n.º 290-D/99, referência 1.e. e Critérios de adequação dos capítulos III e IV do Decreto-Lei n.º 290-D/99).

m. Quando aplicável e caso a EC disponibilize:

1) O serviço de **Fornecimento de SSCD** (artigo 10º do Decreto-Regulamentar 25/2004, referência 1.d.):

a) Assegurar a sua conformidade e respectiva certificação segundo os requisitos definidos nos documentos:

(1) CWA 14169 (referência 1.c.);

(2) ISO 15408 (referência 1.o.) em EAL 4+.

2) O serviço de **Validação Cronológica** (artigo 12º do Decreto-Regulamentar 25/2004 (referência 1.d.):

a) Elaborar Politica de Certificados e Declaração de Práticas de Certificação em conformidade com o documento ETSI TS 102023 (referência 1.j.);

b) Cumprir os requisitos definidos nos documentos:

(1) CWA 14167-1 (referência 1.a.);

(2) ETSI TS 101861 (referência 1.i.).

As EC Credenciadas, além das disposições aplicáveis às EC que emitem Certificados Qualificados, atrás referidas, devem cumprir os requisitos listados no artigo 34º do Decreto Regulamentar n.º 25/2004, referência 1.d.).

6. DIVERSOS

As EC registadas no GNS, podem, caso o pretendam, solicitar a sua Credenciação, Filiação ou Integração no SCEE, junto da AC.

Em qualquer caso preenchem, na parte respectiva, o impresso relativo ao "Pedido de Registo/Credenciação ou Filiação/Integração no SCEE de Entidade Certificadoras", disponível no *website* do GNS.

As EC que apresentem garantias de cumprimento de todos os requisitos técnicos e de segurança referidos no DL 290-D/99, de 02Ago e no Decreto Regulamentar Nº 25/2004 de 15Jul, do Ministério da Justiça, poderão solicitar a Credenciação ou a sua Renovação, junto da AC.

De acordo com a legislação nacional, as Assinaturas Electrónicas Qualificadas emitidas por uma EC credenciada têm a força probatória de documento particular assinado, nos termos do artigo 376 do Código Civil.

A Credenciação de EC poderá surgir:

- Por imposição legal (p.ex., para adesão/filiação no SCEE);
- Para obtenção de valor probatório pleno nas assinaturas electrónicas;
- Para obtenção de fiabilidade junto dos parceiros comunitários ou com países com quem Portugal tem protocolos firmados.

7. ACRÓNIMOS

AC	Autoridade Credenciadora
CEN	European Committee for Standardization
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
EC	Entidade Certificadora
ETSI	European Telecommunications Standards Institute
GNS	Gabinete Nacional de Segurança
ICP	Infra-estrutura de Chave Pública
OCSP	Online Certificate Status Protocol
SCEE	Sistema de Certificação Electrónica do Estado
SSCD	Secure Signature Creation Device

8. ANEXOS

Nada a referir.

9. DISTRIBUIÇÃO

Permitida a distribuição pela Internet