Declaração de Divulgação de Princípios

Política

MULTICERT_PJ.CA3_24.1_0001_pt.doc

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Nível de Acesso: Público

Versão: 1.3

Data: 25/03/2009

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Estr. Casal do Canas, Lote 6 – Alfragide – 2720-092 Amadora, Portugal
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CA3_24.1_0001_pt.doc

Palavras-chave: EC MULTICERT

Tipologia documental: Política

Título: Declaração de Divulgação de Princípios

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 25/03/2009

Versão actual: 1.3

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Cliente: ---

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	20/10/2008	Rascunho Inicial	Sara Loja
1.1	23/01/2009	Revisão de Conteúdos	Sara Loja
1.2	25/03/2009	Revisão de Conteúdos	Sara Loja
1.3	25/03/2010	Revisão de Conteúdos	Nuno Ponte

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0001_pt.doc	Declaração de Práticas de Certificação	José Miranda
MULTICERT_PJ.CA3_24.1.2_0002_pt.doc	Politica de Certificado de Assinatura Digital Qualificada	José Miranda

Resumo Executivo

Este documento foi elaborado tendo em conta as especificações técnicas relatadas no anexo B da norma "*ETSI TS 101 456 : Policy requirements for certification authorities issuing qualified certificates*".

A Declaração de Divulgação de Princípios da Entidade de Certificação da MULTICERT não constitui uma Política de Certificados sob a qual se regem os certificados emitidos pela Entidade de Certificação MULTICERT. Para este efeito devem ser consultadas as Políticas de Certificados e Declaração de Práticas de Certificação disponíveis em http://pki.multicert.com/pol/.

Sumário

Introdução

Objectivos

Este documento pretende resumir, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infra-estrutura de chave pública da Entidade de Certificação da MULTICERT.

A infra-estrutura da Entidade de Certificação MULTICERT fornece uma hierarquia de confiança, que promove a segurança electrónica do titular do certificado digital. A Entidade de Certificação MULTICERT estabelece uma estrutura de confiança electrónica que proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

A Entidade de Certificação MULTICERT está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/gns/pt/assinatura/), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação).

Público-Alvo

Este documento deve ser lido por:

- Titulares de Certificados emitidos pela Entidade de Certificação MULTICERT

Estrutura do Documento

Este documento encontra-se dividido em 10 capítulos.

1 Contactos da Entidade de Certificação da MULTICERT

MULTICERT, Serviços de Certificação Electrónica S.A.
Estrada Casal de Canas, Lote 6 – Alfragide,
Amadora, 2720-092 Portugal
Telefone: +351 217 123 010
Facsimile: +351 217 123 011
Email: info@multicert.com

2 Tipos de Certificados, procedimentos de validação e utilização

A Entidade de Certificação da MULTICERT emite os seguintes tipos de certificados digitais:

- Certificado Digital de Assinatura Qualificada (Formato X.509) – A assinatura electrónica é único meio legalmente aceite para assinar documentos electrónicos. Com o certificado digital de assinatura qualificada, o titular pode assinar correio electrónico, documentos electrónicos e, inclusivamente, fazer transacções electrónicas. Ao utilizar o certificado digital de assinatura qualificada, o titular garante a integridade dos conteúdos, autenticidade da sua assinatura e não repudio, não podendo negar que assinou determinado conteúdo.

  A assinatura electrónica preenche os seguintes requisitos:

  i) Identifica de forma unívoca o titular como autor do documento;

  ii) A sua aposição ao documento depende apenas da vontade do titular;

  iii) É criada com meios que o titular pode manter sob seu controlo exclusivo;

  iv) A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.

- Certificado Digital de Autenticação (Formato X.509) – A utilização do certificado Digital de autenticação permite ao titular comprovar a sua identidade perante um sistema de informação.

O estado dos certificados de assinatura e autenticação, podem ser verificados através do serviço OCSP (*Online Certificate Status Protocol*) e/ou da consulta das LRC (Listas

de Revogação de Certificados) emitidas para cada um dos casos e disponíveis em https://pki.multicert.com/.

3 Limitação de confiança nos certificados

A utilização dos certificados emitidos para os titulares deve obedecer ao descrito nas respectivas políticas de certificados disponíveis em http://pki.multicert.com/pol.

Os certificados emitidos pela EC MULTICERT são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob a EC MULTICERT, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado emitido sob a EC MULTICERT.

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pela legislação aplicável.
Os certificados emitidos pela EC MULTICERT não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.
Os serviços de certificação oferecidos pela EC MULTICERT, não foram desenhados nem estão autorizados a ser utilizados em actividades de alto risco ou que requeiram um actividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra actividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

4 Responsabilidades dos Titulares

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

a) a quem estiver designado no campo "*Subject*" do certificado;

b) enquanto o certificado se mantiver válido e não estiver na Lista de Revogação de Certificados da Entidade de Certificação.

O titular pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro acto que recomende esta acção. A Entidade de Certificação guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efectua o pedido de revogação.

Um certificado pode ser revogado por uma das seguintes razões:

- Comprometimento ou suspeita de comprometimento da chave privada;
- Perda da chave privada;
- Inexactidões graves nos dados fornecidos;

- Comprometimento ou suspeita de comprometimento da senha e acesso à chave privada (exemplo: PIN de assinatura);
- Comprometimento ou suspeita de comprometimento da chave privada da Entidade de Certificação ou da Entidade de Certificação de topo (raiz auto-assinada ou GTE Cyber Trust);
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
- Revogação do certificado da Entidade de Certificação da MULTICERT ou da Entidade de Certificação de topo (raiz auto-assinada ou GTE Cyber Trust);
- Incumprimento por parte da Entidade de Certificação ou titular das responsabilidades previstas;
- Sempre que haja razões credíveis que induzam que o serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa.

Na utilização do certificado e da chave pública deve ser garantido o cumprimento das seguintes condições:

a) ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados.

b) ser responsável pela sua correcta utilização;

c) ler e entender os termos e condições descritos nas Politicas e práticas de certificação;

d) verificar os certificados (validação de cadeias de confiança) e Listas de Revogação de Certificados tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) confiar nos certificados, utilizando-os sempre que estes estejam válidos.

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correcto (pessoa ou sistema) com o qual irão utilizar mecanismos de assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma Entidade de Certificação (EC) de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efectuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela Entidade de Certificação. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da Entidade de Certificação (EC) que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então

poderá necessitar um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de EC assinados por outras EC.

5 Verificação do estado de certificados emitidos pela EC MULTICERT

Outras partes que confiam nos certificados emitidos pela Entidade de Certificação da MULTICERT devem:

- Verificar o estado do certificado no momento da sua utilização, utilizando os mecanismos OCSP e LRC indicados anteriormente, e assumir a responsabilidade dessa verificação;
- Obedecer ao especificado nas Políticas de Certificado do certificado em causa;
- Utilizar o certificado adequadamente de acordo com os objectivos da sua emissão.

6 Limitação de responsabilidades

A Entidade de Certificação da MULTICERT não se responsabiliza pelo uso indevido dos certificados digitais.

A Entidade de Certificação da MULTICERT não se responsabiliza por qualquer utilização dos certificados digitais que não conste na Declaração de Políticas de Certificação ou na Política de Certificados.

A utilização dos certificados digitais emitidos para os titulares e a protecção das chaves privada/pública é da exclusiva responsabilidade do titular.

7 Acordos aplicáveis, Declaração de Práticas de Certificação e Políticas de Certificação

Todos os acordos aplicáveis, Declarações de Política de Certificação e Políticas de Certificação encontram disponibilizados em http://pki.multicert.com.

8 Política de privacidade

A informação do titular constante nos respectivos certificados digitais não se encontra publicada, e é processada de acordo com a Política de Certificação da Entidade de Certificação da MULTICERT.

9 Legislação e normas

A Entidade de Certificação da MULTICERT baseia-se essencialmente nos seguintes documentos jurídicos:

- Directiva 1999/93/CE de 13 Dezembro 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas
- Decreto-Lei nº 62/2003, de 3 de Abril de 2003, altera o Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital.
- Decreto Regulamentar nº 25/2004 de 15 de Julho de 2004, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital.
- Despacho nº 27008/2004, de 14 de Dezembro, publicado no D.R II, nº 302, de 28 de Dezembro;
- Portaria nº 1350/2004, de 23 de Outubro;
- Despacho nº 16445/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- Aviso nº 8134/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- Portaria nº 1370/2000, publicada no D.R . nº 211, II série de 12 de Setembro.

10 Auditorias e normas de segurança

Todas as intervenções realizadas à Entidade de Certificação da MULTICERT são escrutinadas por auditores internos. A Entidade de Certificação da MULTICERT é auditada por um auditor independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Credenciadora, conforme o disposto no artigo 33.º do Decreto-Lei n.º 62/2003. A sua missão é auditar a infra-estrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, em Março, à Autoridade Credenciadora. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Entidade Credenciadora podem ser encontrados em http://www.gns.gov.pt/gns/pt/assinatura/ .

Os Certificados Digitais Qualificados emitidos pela Entidade de Certificação da MULTICERT cumprem todos os requisitos técnicos definidos nas seguintes normas:

- CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile;
- CWA 14169:2004 - Secure signature-creation devices "EAL 4+" ;
- ETSI TS 101 456 V1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI);
- ETSI TS 101 862 V1.3.3 (2006-01) Qualified Certificate profile;
- ETSI TS 102 042 V1.4.3 (2007-12) Policy requirements for certification authorities issuing public key certificates;
- ETSI TS 102 176-1 v2.0.0 (2007-11) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 280 v1.1.1 (2004-03) X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons;