multicert
Engineering for digital security

Declaração de Divulgação de Princípios

Política

MULTICERT_PJ.CA3_24.1_0001_pt.doc

Identificação do Projeto: PKI da MULTICERT

Identificação da CA: PKI da MULTICERT

Nível de Acesso: Público

Versão: 3.0

Data: 10/07/2017

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3 –, 2740-266 Porto Salvo, Oeiras- Portugal
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

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

Palavras-chave: MULTICERT CA, EC MULTICERT, Declaração de Divulgação de Princípios

Tipologia documental: Política

Título: Declaração de Divulgação de Princípios

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 10/07/2017

Versão atual: 3.0

Identificação do Projeto: PKI da MULTICERT

Identificação da CA: PKI da MULTICERT

Cliente: ---

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	20/10/2008	Rascunho Inicial	MULTICERT
2.0	29/06/2016	Versão Aprovada	MULTICERT
2.1	29/11/2016	Revisão de acordo com ETSI EN 319 411-1	MULTICERT
2.2	21/01/2017	Revisão de acordo com regulamento 910/2014	MULTICERT
3.0	10/07/2017	Versão Aprovada (versão equivalente na língua Inglesa 1.0)	MULTICERT

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0001_pt	Declaração de Práticas de Certificação	MULTICERT
MULTICERT_PJ.CA3_24.1.2_0002_pt	Política de Certificado de Assinatura Digital Qualificada	MULTICERT
MULTICERT_PJ.CA3_24.1.2_0009_pt	Política de Certificado de Servidor Web	MULTICERT

Resumo Executivo

Este documento foi elaborado tendo em conta as especificações técnicas relatadas no anexo A da norma "ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirement".

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/.

Renato Isaias Rodrigues Portela
Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.07.24 12:15:52 +01'00'

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.07.24 16:15:14 +02'00'

Sumário

Introdução

Objetivos

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

A infraestrutura da Entidade de Certificação MULTICERT fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado digital. A Entidade de Certificação MULTICERT estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A Entidade de Certificação MULTICERT está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014, 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 12 capítulos.

1 Declaração de Divulgação de Princípios

A MULTICERT divulga a todos os seus clientes e potenciais partes confiantes, os termos e condições de utilização dos seus serviços de certificação digital, numa linguagem acessível e de fácil compreensão.

Não deverá, este documento, ser entendido como um resumo de todas as práticas e políticas seguidas pela EC MULTICERT, mas sim de alguns pontos mais importantes, pelo que a leitura deste documento deve ser complementada com a leitura da Declaração de Práticas de Certificação disponível em https://pki.multicert.com/index.html.

2 Contatos da Entidade de Certificação da MULTICERT

MULTICERT, Serviços de Certificação Electrónica S.A.
Lagoas Park, Edifício 3, Piso 3,
2740-266 Porto Salvo
Oeiras - Portugal
Telefone: +351 217 123 010
Facsimile: +351 217 123 011
Email: pki.documentacao@multicert.com

3 Tipos de Certificados, procedimentos de validação e utilização

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

- **Certificados Qualificado**s
  - Assinatura para pessoa singular (Formato X.509) – A assinatura eletrónica é o único meio legalmente aceite para assinar documentos eletrónicos. Com o certificado digital de assinatura qualificada, o titular pode assinar correio eletrónico, documentos eletrónicos e, inclusivamente, fazer transações eletrónicas. Ao utilizar o certificado digital de assinatura qualificada, o titular garante a integridade dos conteúdos, autenticidade da sua assinatura e não repúdio, não podendo negar que assinou determinado conteúdo. Neste formato a MULTICERT oferece os seguintes tipos de certificados:
    - **Particular** - Certificado emitido que inclui o nome do seu titular, que será utilizado para assinar documentos
    - **Qualidade** - Certificado com as mesmas características do Particular, no entanto acrescido de um atributo de qualidade, associado a uma entidade/organização (ex. Médico, Engenheiro, Diretor Comercial, Administrador, etc).

- **Efeitos de Representação** – Certificado com as mesmas características do Particular, no entanto acrescido de um atributo no qual é conferido os efeitos de representação de uma Organização ao seu titular. Estes poderes de representação são delegados ou conferidos pelos representantes legais da organização.

- Assinatura para pessoa coletiva – Selo Eletrónico (Formato X.509) – Certificado emitido para a Organização, ou seja o titular do certificado é uma pessoa coletiva. Este Certificado pode ser utilizado, a título de exemplo, para assinatura de faturas eletrónicas (emissão de grandes volumes com segurança acrescida), extratos de conta eletrónicos, declarações eletrónicas, certidões e outros tipos de documentos emitidos online por entidades públicas.
- Autenticação de sítios web (Formato X.509) - Certificado digital cujo objetivo é garantir a autenticidade de um sítio web, a titularidade de um domínio ou a confidencialidade da informação transacionada.

– **Certificado Avançados**, Certificados emitidos para particulares e profissionais, permitindo a assinatura eletrónica de documentos (sem valor probatório) e a identificação eletrónica segura e unívoca de uma pessoa.

– **Certificados de Aplicação**

– Certificados utilizados para assinatura de documentos, para identificação de VPNs ou para outro tipo de serviços

Todos os certificados emitidos pela MULTICERT CA, 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/index.html.

Os procedimentos de validação utilizados com a finalidade de emissão de certificados digitais qualificados seguem os métodos "cara-a-cara" ou equivalentes, conforme descrito no capítulo 3.2 da Declaração de Práticas de Certificação[1] e nas respetivas Políticas de Certificados.

Os métodos de validação utilizados nos restantes tipos de certificados não implicam a utilização do método "cara-a-cara" ou equivalente e encontram-se descritos no capítulo 4 das respetivas Políticas de Certificados[1].

4 Limitação de confiança nos certificados

A utilização dos certificados emitidos para os titulares deve obedecer ao descrito nas respetivas políticas de certificados[1].

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.

[1] Disponível em: https://pki.multicert.com/CA.html

Os serviços de certificação oferecidos pela EC MULTICERT, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram um atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

5 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 e,

b) Enquanto o certificado se mantiver válido, ou esteja no estado Ativo.

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

Um certificado pode ser revogado por uma das seguintes razões:

– Comprometimento ou suspeita de comprometimento da chave privada ou da senha de acesso à chave privada (exemplo: PIN de assinatura);

– Perda da chave privada;

– Inexatidões graves nos dados fornecidos;

– Comprometimento ou suspeita de comprometimento da chave privada da Entidade de Certificação ou da Entidade de Certificação de topo (EC Raiz da Multicert e/ou *Baltimore CyberTrust Root*);

– 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 (EC Raiz da Multicert e/ou *Baltimore CyberTrust Root*);

– 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 correta 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 correto (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 efetuado 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, o certificado que assinou este e assim consecutivamente até chegar à EC raiz.

6 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 objetivos da sua emissão.

7 Limitação de responsabilidades

A Entidade Certificadora MULTICERT:

a) Responde pelos danos causados a qualquer pessoa que exerça sua atividade de acordo com os regulamentos aplicáveis e aos usos especificados na CPS.

b) Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele.

c) Assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação.

d) A sua responsabilidade da administração / gestão assenta sobre base objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços

e) Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso.

f) Não responde quando o titular superar os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular.

g) Não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações e,

h) Não assume qualquer responsabilidade no caso de perca ou prejuízo:

   ii) Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro de força maior,

   iii) Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC,

   iv) Ocasionado pelo uso indevido ou fraudulento dos certificados ou CRL emitidos por ela.

8 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-se disponíveis em http://pki.multicert.com.

9 Política de privacidade

A MULTICERT tem implementadas medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa, garantindo que a informação do titular, constante nos respetivos certificados digitais, não se encontra publicada sendo processada de acordo com as Políticas de Certificados da EC da MULTICERT, disponíveis em http://pki.multicert.com.

10 Indemnizações

De acordo com a legislação em vigor.

11 Legislação e normas

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

- Regulamento nº 910/2014 de 23 de Julho de 2014 do Parlamento Europeu e do Conselho, relativo à identificação electrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.4.

12 Repositórios, Auditorias e normas de segurança

Toda a informação referente à Entidade de Certificação da MULTICERT encontra-se disponível publicamente no repositório acessível em https://pki.multicert.com/.

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 Organismo de Avaliação da Conformidade (devidamente registado no Organismo Nacional de Acreditação), o qual emite um Relatório de Conformidade (CAR) a ser disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança.

As Auditorias de conformidade deverão ocorrer, pelo menos, a cada 12 meses, com intuito de confirmar que a MULTICERT, como prestadora qualificada de serviços de confiança e os serviços de confiança que disponibiliza, cumprem os requisitos estabelecidos pelo Regulamento 910/2014.

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 EN 319 401 v2.1.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 v2.1.1 (2016-02) 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;
- ETSI EN 319 412-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
- ETSI EN 319 412-2 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- ETSI EN 319 412-3 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-4 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- ETSI EN 319 412-5 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ETSI EN 319 421 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- ETSI EN 319 422 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
- 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 e que revoga a Diretiva 1999/93/CE;
- CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.4.