

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ROOT CA DA GTS

Global Trusted Sign

Referência do Documento | DP01_GTS_V9

ÍNDICE

| | |
|--|----|
| 1. Referências | 5 |
| 2. Documentos Associados | 5 |
| 3. Lista de Distribuição | 5 |
| 4. Histórico do Documento | 5 |
| 5. Classificação do Documento | 5 |
| 6. Registo da Revisão | 5 |
| 7. Introdução | 6 |
| 7.1. Âmbito | 6 |
| 7.2. Público-Alvo | 6 |
| 7.3. Estrutura do Documento | 6 |
| 8. Enquadramento | 6 |
| 9. Participantes na Infraestrutura de Chave Pública | 7 |
| 9.1. Entidades Certificadoras | 7 |
| 9.2. Autoridade de Registo | 12 |
| 9.3. Subscritores e Titulares | 12 |
| 9.4. Outros Participantes | 12 |
| 10. Utilização do Certificado | 13 |
| 10.1. Utilização Adequada | 13 |
| 10.2. Utilização não autorizada | 13 |
| 11. Gestão de Políticas | 14 |
| 11.1. Responsabilidades de Publicação e Repositório | 14 |
| 11.2. Alterações às Políticas | 15 |
| 12. Identificação e Autenticação | 16 |
| 12.1. Atribuição de Nomes | 16 |
| 12.2. Validação de Identidade Inicial | 18 |
| 12.3. Identificação e Autenticação para Pedidos de Renovação de Chaves | 18 |
| 12.4. Identificação e Autenticação para Pedidos de Revogação de Chaves | 18 |
| 13. Requisitos Operacionais do Ciclo de Vida do Certificado | 18 |
| 13.1. Pedido de Certificado | 18 |
| 13.2. Emissão de Certificado | 18 |
| 13.3. Aceitação de Certificados | 18 |
| 13.4. Uso do Certificado e Par de Chaves | 19 |
| 13.5. Renovação de Certificados | 19 |
| 13.6. Renovação de Certificados com Geração de Novo Par de Chave | 19 |
| 13.7. Modificação de Certificados | 19 |
| 13.8. Revogação de Certificados Emitidos pela ROOT CA | 19 |
| 13.9. Serviço sobre o estado do Certificado | 20 |
| 14. Controlos de Segurança Física, de Gestão e Operacionais | 21 |

| | |
|--|----|
| 14.1. Controlos de Segurança Física | 21 |
| 14.2. Controlos dos Processos..... | 22 |
| 14.3. Medidas de segurança de Pessoal | 25 |
| 14.4. Procedimentos de Auditoria de Segurança | 26 |
| 14.5. Arquivo de Registos | 28 |
| 14.6. Recuperação em caso de desastre ou comprometimento | 29 |
| 15. Controlos de Segurança Técnicos..... | 31 |
| 15.1. Geração e Instalação de Pares de Chaves..... | 31 |
| 15.2. Proteção da Chave Privada e Características do Modulo Criptográfico | 32 |
| 15.3. Outros Aspectos da Gestão do Par de Chaves | 33 |
| 15.4. Dados de Ativação..... | 33 |
| 15.5. Controlos de Segurança Informática..... | 33 |
| 15.6. Ciclo de Vida dos Controlos de Segurança | 33 |
| 15.7. Controlos de Segurança da Rede | 34 |
| 15.8. Validação Cronológica | 34 |
| 16. Perfil de Certificado e de Listas de Revogação de Certificados..... | 34 |
| 16.1. Perfil de Certificado | 34 |
| 16.2. Perfil de Listas de Revogação de Certificados | 34 |
| 17. Auditoria e Avaliação de Conformidade..... | 35 |
| 17.1. Frequência ou motivo da auditoria..... | 35 |
| 17.2. Identidade e qualificações do Organismo de Avaliação da Conformidade..... | 35 |
| 17.3. Relação entre o Organismo de Avaliação da Conformidade e a ROOT CA GTS | 36 |
| 17.4. Âmbito da auditoria..... | 36 |
| 17.5. Procedimentos após uma auditoria com irregularidades identificadas | 36 |
| 17.6. Comunicação de resultados..... | 37 |
| 18. Outras Situações e Assuntos Legais..... | 37 |
| 18.1. Responsabilidade Financeira | 37 |
| 18.2. Confidencialidade da Informação Processada | 37 |
| 18.3. Privacidade dos Dados Pessoais..... | 38 |
| 18.4. Direitos de Propriedade Intelectual | 39 |
| 18.5. Representações e Garantias..... | 39 |
| 18.6. Renúncia de Garantias | 41 |
| 18.7. Limitações às Obrigações..... | 41 |
| 18.8. Indeminizações | 41 |
| 18.9. Termo e Cessão da Atividade..... | 41 |
| 18.10. Notificação Individual e Comunicação dos Participantes..... | 42 |
| 18.11. Alterações | 42 |
| 18.12. Disposições para Resolução de Conflitos | 42 |
| 18.13. Legislação Aplicável | 42 |
| 18.14. Conformidade com Legislação em Vigor | 42 |

| | |
|--|----|
| 18.15. Providências Várias | 43 |
| Anexo A – Definições e Acrônimos | 44 |

| | |
|--------------------------------------|--|
| 1. Referências | Regulamentação Europeia Nº 910/2014 ETSI 319 411-1 ETSI 319 412 ETSI 319 401 RFC 5280: Internet X.509 PKI - Certificate and CRL Profile, 2008 CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.6.3 |
| 2. Documentos Associados | DP05_GTS - Declaração de Divulgação de Princípios da ROOT CA GTS |
| 3. Lista de Distribuição | Partes interessadas da hierarquia de confiança da GTS |
| 4. Histórico do Documento | 31-07-2017 Versão 1 12-09-2017 Versão 2 15-01-2018 Versão 3 05-03-2018 Versão 4 01-06-2018 Versão 5 01-04-2019 Versão 6 02-05-2020 Versão 7 24-06-2020 Versão 8 23-09-2020 Versão 9 |
| 5. Classificação do Documento | D Público |

6. Registo da Revisão

| N.º da Versão | Elaborado | Aprovado | Motivo |
|---------------|--|---|--|
| 9 | 23-09-2020 SegAdm Sandra Mendes y Fernández | 23-09-2020 Grupo de Gestão Tolentino de Deus Faria Pereira | Atualização de registos e colaboradores do Grupo de Confiança da GTS |

7. Introdução

7.1. Âmbito

O presente documento especifica as políticas e os procedimentos que serão seguidos pela Global Trusted Sign, enquanto prestadora qualificada de serviços de confiança no âmbito do regulamento 910/2014 (adiante designada por GTS), no suporte à sua atividade de emissão de certificados qualificados e avançados da Entidade Certificadora Raiz da GTS (adiante designada por ROOT CA GTS).

7.2. Público-Alvo

O presente documento apresenta-se disponível publicamente e é destinado a todos os participantes que se relacionem, de alguma forma, com a Entidade Certificadora Raiz da GTS.

7.3. Estrutura do Documento

No âmbito da presente declaração de práticas assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique, recomenda-se o estudo prévio acerca dos referidos tópicos, permitindo assim uma melhor compreensão do presente documento.

De forma a facilitar a leitura e consequente análise deste documento com as práticas difundidas e recomendadas internacionalmente, optou-se por incluir todas as secções estabelecidas no índice da norma "ETSI EN 319 411-1 v1.1.1. Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", pelo que se não houver nada designado sobre o assunto, será incluída a expressão "nada a assinalar".

Os acrónimos e definições estão definidos no Anexo A do presente documento.

8. Enquadramento

O presente documento de Declaração de Práticas de Certificação, ou DPC especifica os requisitos de segurança, políticas e práticas aplicáveis pelo prestador qualificado de serviços de confiança que emita certificados. As políticas e requisitos de segurança encontram-se definidos em termos de requisitos para a gestão do ciclo de vida dos certificados qualificados em conformidade com as políticas de certificados existentes.

A presente DPC respeita e implementa os standards seguintes:

- 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
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, v1.2.0
- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, v1.1.1

- ETSI EN 319 401 v2.1.1: General policy requirements for Trusted Service Providers
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003.

A GTS não tem suporte para o serviço de “cross-certificates”.

O presente documento é a Declaração de Práticas de Certificação da ROOT CA GTS cujo OID associado é 1.3.6.1.4.1.50302.1.1.1.1.0, enquanto o OID associado à Política de Certificados da ROOT CA GTS é 1.3.6.1.4.1.50302.1.1.2.1.0:

| Informação do Documento | |
|-------------------------|---|
| Nome do Documento | Declaração de Práticas de Certificação da ROOT CA GTS |
| Versão do Documento | 9 |
| Estado do Documento | Aprovado |
| OID | 1.3.6.1.4.1.50302.1.1.1.1.0 |
| Data de Emissão | 17-09-2020 |
| Validade | 17-09-2021 |
| Localização | https://pki.globaltrustedsign.com/index.html |

Nota: Atualizações regulares neste documento são realizadas sempre que se justificarem.

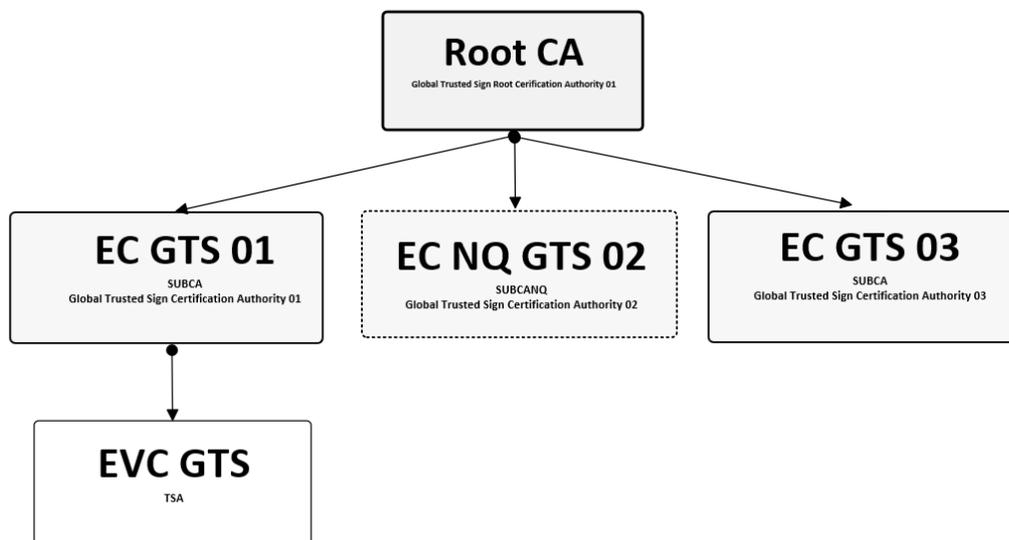
9. Participantes na Infraestrutura de Chave Pública

9.1. Entidades Certificadoras

A GTS, enquanto prestador qualificado de serviços de confiança, disponibiliza uma hierarquia de confiança credenciada pelo Gabinete Nacional de Segurança (<http://www.gns.gov.pt/trusted-lists.aspx>), conforme previsto na legislação portuguesa e europeia.

É composta por um conjunto de equipamentos, aplicações, recursos humanos e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir assim a adequada gestão do ciclo de vida dos certificados descritos no presente documento.

A hierarquia de confiança da GTS é composta pela Entidade Certificadora Raiz da GTS (ROOT CA GTS), as Entidades Certificadoras da GTS (EC GTS01 e EC GTS03), a Entidade Certificadora Não Qualificada da GTS (EC NQ GTS) e a Entidade Certificadora de Selos Temporais da GTS (EVC GTS). Estas entidades certificadoras estão descritas nos pontos 9.1.1, 9.1.2 e 9.1.3 do presente documento e encontram-se ilustradas de seguida:


Legenda:

- 1 – **Root CA GTS** - Entidade Certificadora Raiz da GTS
- 2 – **EC GTS 01** - Entidade Certificadora da GTS
- 3 – **EC NQ GTS 02** - Entidade Certificadora Não Qualificada da GTS
- 4 – **EVC GTS** - Entidade Certificadora de Validação Cronológica da GTS
- 5 – **EC GTS 03** - Entidade Certificadora da GTS

9.1.1. Entidade Certificadora Raiz da GTS (ROOT CA GTS)

A ROOT CA GTS é uma entidade certificadora credenciada pelo Gabinete Nacional de Segurança, de acordo com o Regulamento (UE) N.º 910/2014, estando deste modo habilitada, legalmente, a emitir certificados para Entidades Certificadoras Subordinadas.

O certificado da ROOT CA GTS:

| Informação do Certificado | |
|--------------------------------|--|
| Nome Distinto | CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |
| Algoritmo de Assinatura | Sha256RSA |
| Nº de Série | 7d 9f 44 7c b2 77 97 a8 59 57 bf 11 dd 8f 99 f5 |
| Validade | 01/07/2017 a 01/07/2037 |
| Marca Digital | 70 d1 2e f7 f5 90 18 87 47 88 42 c6 4e 05 ef 2c 0a 63 92 9d |
| Emissor | CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |

9.1.2. Entidade Certificadora da GTS (EC GTS)

A Entidade Certificadora da GTS emite:

1. Certificados qualificados para autenticação de sítios Web (SSL/TLS)

Os serviços de autenticação de sítios web fornecem meios que dão aos visitantes de um sítio web a garantia de que existe uma entidade genuína e legítima responsável pelo sítio. Estes serviços contribuem para a criação de segurança e confiança na realização de negócios *online*, pois os utilizadores têm confiança nos sítios web que tenham sido autenticados, pela garantia de autenticidade, titularidade e confidencialidade da informação transacionada.

A prática de emissão de certificados qualificados para autenticação de sítios web da EC GTS está em conformidade com os requisitos do CA/Browser fórum disponíveis em <http://www.cabforum.org>:

- Organization Validation: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- Extended Validation: Guidelines for the issuance and management of Extended Validation Certificates

Isso inclui a validação do domínio dos certificados requisitados (dono do domínio, domínio wild-card e CAA Records) conforme definido no CA/B Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.6.3 capítulo 3.2.2.

Em caso de inconsistência entre esta DPC e estes Requisitos do CA/B Forum, os Requisitos assumem precedência.

2. Certificados para assinatura eletrónica qualificada

Os certificados para assinatura eletrónica qualificada permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo, bem como a integridade do documento.

3. Certificados para selos eletrónicos

Os certificados para selos eletrónicos permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento.

Os certificados da EC GTS:

| Informação do Certificado | |
|----------------------------------|--|
| Nome Distinto | CN = Global Trusted Sign Certification Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |
| Algoritmo de Assinatura | Sha256RSA |
| Nº de Série | 5d f5 55 01 8c 89 45 56 59 8d cf d9 13 3b 87 ab |
| Validade | 11/08/2017 a 11/08/2023 |
| Marca Digital | 2b 30 32 d4 9d 12 74 af 30 ab a3 ec 29 a6 a0 25 ae f6 dc bc |
| Emissor | CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |

| Informação do Certificado | |
|----------------------------------|--|
| Nome Distinto | CN = Global Trusted Sign Certification Authority 03, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |
| Algoritmo de Assinatura | Sha256RSA |
| Nº de Série | 1e 0a 5a 4e b2 45 99 3c 5e b9 2f 31 48 db 0c f6 |
| Validade | 11/05/2020 a 11/05/2028 |
| Marca Digital | 60 2f 17 18 96 72 78 f5 88 4f 33 16 f2 65 9b c1 f3 cc b2 46 |
| Emissor | CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |

9.1.3. Entidade Certificadora de Selos Temporais da GTS (EVC GTS)

A EVC GTS é uma entidade certificadora de validação cronológica habilitada a emitir selos temporais qualificados.

A monitorização do serviço de emissão de selos temporais tem o objetivo de detetar qualquer desvio maior que os requisitos impostos pela norma ETSI EN 319 421 (conforme explicado no capítulo 9.4.3). Serão monitorizados todos os offsets entre as máquinas que suportam o serviço de emissão de selos temporais com o objetivo de gerar alarmística relevante que será usada para tomar iniciativas corretivas.

Esta EVC GTS tem a responsabilidade de operar uma ou mais TSU (time-stamping unit) para a criação e assinatura de selos temporais em nome da GTS, cada uma com a sua chave distinta de assinatura, cujo relógio utilizado para emitir selos temporais está sincronizado não só com o próprio relógio atómico da GTS, mas também, para efeitos de redundância, com mais duas fontes acreditadas conforme a norma ETSI EN 319 421.

O certificado da EVC GTS:

| Informação do Certificado | |
|--------------------------------|---|
| Nome Distinto | CN = Global Trusted Sign Timestamping Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |
| Algoritmo de Assinatura | Sha256RSA |
| Nº de Série | 04 bd 81 30 e4 ae 61 40 5a 99 43 db 7a 72 4f 47 |
| Validade | 02/03/2018 a 02/03/2023 |
| Marca Digital | 21 16 db 77 7e 72 fd 57 61 2a 24 27 8f d2 05 c8 bc fd a3 98 |
| Emissor | CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT |

9.1.4. Entidade Certificadora Não Qualificada da GTS (ECNQ GTS)

A Entidade Certificadora da GTS emite:

Certificados avançados para assinatura pela Entidade Certificadora Não Qualificada da Global Trusted Sign, enquanto prestadora de serviços de confiança, que cumprem os requisitos definidos no Regulamento (UE) Nº 910/2014 (no que for aplicável), no ETSI EN 319 401, v2.1.1 e ETSI EN 319 411-1, v1.1.1.

O certificado da EC NQ GTS:

| Informação do Certificado | |
|--------------------------------|--|
| Nome Distinto | CN = Global Trusted Sign NQ Certification Authority 02, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT |
| Algoritmo de Assinatura | Sha256RSA |
| Nº de Série | 7e 88 a8 ed 54 02 9f c6 5c 96 00 8e 0a cf bd c1 |
| Validade | 23/03/2019 até 23/03/2025 |
| Marca Digital | 7e 55 0f f3 8f 70 2e eb 5d 8f f0 e2 02 75 78 3f be 83 57 38 |
| Emissor | CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT |

9.2. Autoridade de Registo

A Autoridade de Registo (RA) é a entidade responsável pela análise e avaliação dos pedidos de serviços da GTS, nomeadamente à veracidade dos documentos e validação da identidade dos titulares dos certificados e pedidos. Esta RA tem o direito de aprovar ou rejeitar os pedidos após a devida validação. Adicionalmente a RA tem autoridade para aprovar a revogação de certificados.

As Autoridades de Registo da Global Trusted Sign estão em conformidade com os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas independentes, assim como Auditorias Internas realizadas Global Trusted Sign regularmente.

9.2.1. Autoridade de Registo Interna

No âmbito da Entidade de Certificação Global Trusted Sign, a autoridade de registo é executada pelos serviços internos da mesma, que têm responsabilidade de validação dos dados necessários, conforme explicitado nas Políticas específicas da Global Trusted Sign, para cada um dos serviços disponibilizados.

9.2.2. Autoridade de Registo Externa

A Global Trusted Sign, não dispõe de Autoridades de Registo Externas.

9.3. Subscritores e Titulares

No âmbito da presente declaração de práticas, os titulares são as entidades certificadoras que pertencem à hierarquia de confiança da GTS.

Os membros dos grupos de trabalho, nomeadamente da Administração de Segurança, agem como subscritores, responsabilizando-se pela correta utilização do certificado, bem como pela proteção e salvaguarda da respetiva chave privada.

9.4. Outros Participantes

9.4.1. Entidade Supervisora

A Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras prestadoras de serviços de confiança qualificados.

No panorama nacional, essa função é desempenhada pelo Gabinete Nacional de Segurança (GNS). A Entidade Supervisora contribui para a confiança nos certificados qualificados, pelas competências que exerce sobre as EC que os emite. No âmbito das suas funções, a Entidade Supervisora exerce os seguintes papéis relativamente às Entidades Certificadoras:

- **Notificação de intenção:** procedimento de aprovação dos serviços de confiança prestados pelos prestadores de serviços qualificados, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, o hardware, software e os procedimentos de acesso e de operação;
- **Organismo de avaliação da conformidade:** enquanto organismo competente para realizar a avaliação da conformidade dos serviços de confiança prestados pelos prestadores de serviços qualificados;

- **Fiscalização:** Inspeções efetuadas para confirmar que tanto os prestadores qualificados de serviços de confiança como os serviços de confiança que prestam cumprem os requisitos estabelecidos pelo Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho.

9.4.2. Entidades Externas

A atividade dos prestadores de serviços que suportam a GTS no desempenho das suas funções enquanto prestadora qualificada de serviços de confiança é contratualizada de modo a garantir a atribuição formal das funções e responsabilidades de cada uma das partes, bem como o cumprimento das políticas e práticas instituídas na GTS.

9.4.3. Organismo de avaliação da conformidade

O Organismo de avaliação da conformidade (*Conformity Assessment Body – CAB*) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

10. Utilização do Certificado

Os certificados emitidos na hierarquia de confiança da ROOT CA GTS são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, para com o objetivo de garantir a identificação, autenticação, integridade, não repúdio e, ainda, confidencialidade.

Os certificados qualificados emitidos pela ROOT CA GTS de acordo com esta DPC são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

10.1. Utilização Adequada

Os certificados emitidos pela ROOT CA GTS são regulamentados por esta Declaração de Práticas de Certificação e serão utilizados de acordo com a função e finalidade aqui estabelecidas e nas correspondentes Políticas de Certificados, de acordo com a lei em vigor.

As Partes Confiantes podem verificar a cadeia de confiança de um certificado emitido pela ROOT CA GTS, garantindo assim a autenticidade e identidade do titular.

10.2. Utilização não autorizada

Os certificados emitidos na hierarquia de confiança da ROOT CA GTS não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente, ressalvada a exceção de poderem ser utilizados em outros contextos quando legalmente previstos na legislação aplicável.

Os serviços de certificação prestados pela ROOT CA GTS não garantem o cumprimento de requisitos de alta disponibilidade e resiliência, que os qualifique para a sua utilização em serviços ou infraestruturas críticas, 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.

11. Gestão de Políticas

A gestão da declaração de práticas de certificação da ROOT CA GTS é da responsabilidade do grupo de Administração de Segurança da mesma.

| Nome | Grupo de Administração de Segurança da ROOT CA GTS |
|---------------------------|---|
| Morada | ACIN iCloud Solutions Estrada Regional 104 N°42-A 9350-203 Ribeira Brava Madeira Portugal |
| Correio Eletrónico | info@globaltrustedesign.com |
| Página Internet | https://www.globaltrustedesign.com |
| Telefone | 707 451 451 |

A Declaração de Práticas de Certificação (DPC) deve ser aplicada internamente, bem como auditada pelo grupo de trabalho Auditor de modo a garantir a sua conformidade. Esta auditoria deve resultar num relatório, que deve ser submetido ao Grupo de Gestão da ROOT CA GTS, para aprovação.

11.1. Responsabilidades de Publicação e Repositório

A ROOT CA GTS disponibiliza um repositório, em ambiente web, de informação relativa às práticas adotadas e o estado dos certificados emitidos, nomeadamente:

- **Entidade Certificadora Raiz da GTS (ROOT CA GTS)**
 - Certificado da ROOT CA GTS;
 - Lista de Revogação de Certificados (LRC) da ROOT CA GTS;
 - Declaração de Práticas de Certificação (DPC) da ROOT CA GTS;
 - Políticas de Certificados (PC) da ROOT CA GTS;
 - Outra informação relevante.
- **Entidade Certificadora da GTS (EC GTS)**
 - Certificado da EC GTS;
 - Lista de Revogação de Certificados (LRC) da EC GTS;
 - Declaração de Práticas de Certificação (DPC) da EC GTS;
 - Políticas de Certificados da EC GTS;
 - Outra informação relevante.

- **Entidade Certificadora de Selos Temporais da GTS (EVC GTS)**
 - Certificado da EVC GTS;
 - Declaração de Práticas de Certificação (DPC) da EVC GTS;
 - Políticas de Certificados da EVC GTS;
 - Outra informação relevante.
- **Entidade Certificadora Não Qualificada da GTS (EC GTS)**
 - Certificado da EC NQ GTS;
 - Lista de Revogação de Certificados (LRC) da NQ EC GTS;
 - Declaração de Práticas de Certificação (DPC) da EC GTS;
 - Políticas de Certificados da EC NQ GTS;
 - Outra informação relevante.

O repositório das diversas entidades certificadoras pode ser acessado 24x7 em <https://pki.globaltrustedesign.com/index.html>. O repositório será atualizado sempre que haja uma alteração num dos documentos publicados.

A ROOT CA GTS efetua as seguintes publicações, com a seguinte periodicidade de publicação:

- O certificado da ROOT CA GTS é publicado após a sua emissão;
- A LRC é publicada trimestralmente;
- Novas versões ou alterações nas DPC e/ou respetivas Políticas de Certificados (PC), serão publicadas após a sua aprovação pelo Grupo de Gestão.

Foram implementados os seguintes mecanismos de controlo de acesso de segurança:

- Quaisquer alterações à informação publicada no repositório são efetuadas através de processos formais de gestão documental;
- A infraestrutura tecnológica que suporta o repositório e a sua publicação encontra-se em conformidade com as boas práticas de segurança da informação, incluindo os requisitos físicos bem como a gestão por uma equipa com as competências necessárias para a função;
- É garantido que o acesso à informação contida nos repositórios se efetua, apenas e só, em modo de leitura. Para tal, foram implementados mecanismos de segurança de forma a garantir que apenas pessoas autorizadas possam escrever ou modificar a informação contida nos repositórios.

11.2. Alterações às Políticas

Todos os documentos relacionados com a atividade da ROOT CA GTS, incluindo o presente documento (DPC), e quaisquer alterações subsequentes, tornam-se efetivos após publicação no repositório.

A ROOT CA GTS pode decidir em favor da eliminação ou emenda de um documento quando:

- Os seus conteúdos são considerados incompletos, imprecisos ou erróneos;
- Os seus conteúdos foram comprometidos.

O documento eliminado ou alvo de emenda é substituído por uma nova versão.

A validação da DPC e conseqüentes correções ou atualizações são da responsabilidade do Grupo de Administração de Segurança e devem:

- Ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida.
- Determinar, após alterações na DPC, se identificadores dos objetos (OID) devem ser alvos de alguma alteração.

O Grupo de Gestão é a entidade responsável pela aprovação e autorização de modificações destes documentos.

Os subscritores são notificados por correio eletrónico quando se efetua uma mudança da DPC e que devem consultar a nova no repositório estabelecido.

Se a GTS determinar que a alteração ao identificador (OID) da política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem implicar uma mudança no identificador da política de certificados.

Todos os documentos relacionados com a atividade da ROOT CA GTS, e quaisquer alterações subsequentes, permanecerão ativos até publicação de nova versão ou alteração.

12. Identificação e Autenticação

12.1. Atribuição de Nomes

A ROOT CA GTS garante a emissão de certificados contendo um *Distinguished Name* (DN) X.509 a todos os titulares que submetam documentação contendo um nome verificável de acordo com o preconizado no RFC 5280.

A atribuição de nomes segue as convenções seguintes:

- Certificados de autenticação de sítios web é atribuído o nome qualificado do domínio e/ou do serviço de confiança, de acordo com a ETSI EN 319 412-4 v1.1.1;
- Certificados de assinatura qualificada para pessoa singular é atribuído o nome real do titular, de acordo com a ETSI EN 319 412-2 v2.1.1;
- Certificados de assinatura qualificada para pessoa singular em associação com uma pessoa coletiva é atribuído o nome do titular e a sua relação com a pessoa coletiva, de acordo com a ETSI EN 319 412-2 v2.1.1;
- Certificados de selos eletrónicos é atribuído o nome da pessoa coletiva, de acordo com a ETSI EN 319 412-3 v1.1.1.

Adicionalmente, a atribuição dos nomes cumpre os requisitos especificados nas políticas de certificados, para cada tipo de perfil apresentado.

Os vários tipos de certificados podem conter os seguintes campos no DN:

| Atributo | Código | Regras |
|-------------------|--------------|---|
| Country | C | Código do país do titular do certificado |
| Organization | O | Este campo corresponde à organização (ou equivalente) à qual o titular do certificado pertence. |
| Organization Unit | OU | Este campo corresponde informação relativa à unidade organizativa (ou equivalente) a que o titular do certificado pertence. |
| Common Name | CN | Nome único do titular do certificado. No caso dos servidores de sítios Web, este será designado pelo FQDN (CN = "FQDN."), sendo proibida a sua designação através do endereço IP. No caso dos certificados de assinatura qualificada, contém o nome do titular ou o seu pseudónimo. No caso dos certificados de selos eletrónicos, contém o nome da pessoa coletiva. |
| Serial Number | serialNumber | Segue as recomendações do ETSI EN 319 412. |

A ROOT CA GTS assegura que os nomes utilizados nos certificados por ela emitidos identificam de uma forma significativa e clara os seus titulares, assegurando que o DN usado é apropriado para um dado titular e que a componente *Common Name* do DN o representa de forma a ser facilmente identificável pelos interessados. Adicionalmente, a ROOT CA GTS garante a não existência de certificados emitidos por esta que, tendo o mesmo nome único, identifiquem entidades distintas.

Na ROOT CA GTS, existem controlos que garantem que o DN e o conteúdo da extensão *KeyUsage* são únicos, não ambíguos e referentes apenas a uma entidade não sendo também permitido o anonimato de titulares no processo de emissão de certificados.

É da responsabilidade da ROOT CA GTS atribuir e aprovar o DN, como também resolver quaisquer disputas que possam surgir com o DN atribuído.

O DN emitidos pela ROOT CA GTS têm em atenção as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja entidade não possa provar ter direito à marca, podendo-se recusar a emitir o certificado com nomes de marcas registadas se concluir que outra identificação seja mais conveniente.

Antes da emissão do certificado, no procedimento de autenticação, a entidade/titular terá de apresentar documentos que demonstrem o direito à utilização do DN requisitado.

Nos casos em que a ROOT CA GTS não seja a entidade responsável pela geração do par de chaves criptográficas a atribuir ao utilizador, esta, antes de proceder à sua emissão, assegurará que o utilizador possui a chave privada correspondente à chave pública constante no pedido de certificado.

O método de prova será necessariamente tão mais complexo e preciso consoante a importância do tipo de certificado pedido, encontrando-se documentado na Política de Certificado do certificado em causa.

12.2. Validação de Identidade Inicial

Para que os certificados qualificados das entidades certificadoras possam ser emitidos na hierarquia de confiança da GTS, é obrigatório que a ROOT CA GTS verifique o pedido e os parâmetros associados ao mesmo.

12.3. Identificação e Autenticação para Pedidos de Renovação de Chaves

Muitas infraestruturas de chave pública permitem a atualização automática de certificados para um subscritor antes do fim do período de validade do certificado existente. Esta ação é conhecida como renovação de rotina e é possível no momento em que já existe uma relação de confiança com o subscritor.

A renovação é tratada como um novo pedido de emissão pela ROOT CA GTS.

12.4. Identificação e Autenticação para Pedidos de Revogação de Chaves

O pedido de revogação deve obedecer às condições descritas em pormenor na secção 13.9.

13. Requisitos Operacionais do Ciclo de Vida do Certificado

13.1. Pedido de Certificado

Os pedidos de emissão de certificados para entidades certificadoras podem ser submetidos pelos membros do grupo de Administração de Segurança.

Nota: O pedido de certificado não implica a sua obtenção se o solicitante não cumprir os requisitos estabelecidos nesta DPC.

13.2. Emissão de Certificado

O processo de emissão de certificados é executado pelos Administradores de Registo na ROOT CA GTS através de uma cerimónia própria para o efeito.

Os certificados são emitidos por interação da ROOT CA GTS com um módulo criptográfico em *hardware* (*Hardware Secure Module* - HSM).

O certificado emitido inicia a sua vigência no momento da sua emissão.

13.3. Aceitação de Certificados

A conclusão da cerimónia implica a aceitação formal por parte dos representantes da entidade subordinada sobre as funcionalidades e conteúdo do certificado, bem como os direitos e responsabilidades.

A ROOT CA GTS não efetua a publicação de certificados emitidos, nem notifica outras entidades da emissão dos mesmos.

13.4. Uso do Certificado e Par de Chaves

Os titulares de certificados utilizam 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 utilização do certificado é sempre da responsabilidade do seu titular.

A utilização do certificado apenas é permitida, e caso aplicável para o tipo de certificado em questão:

- A quem estiver designado no campo do certificado *Subject*;
- Depois de aceitar os termos e condições associados ao tipo de certificado;
- Enquanto o certificado se mantiver válido e não estiver na LRC da ROOT CA GTS.

13.5. Renovação de Certificados

Na ROOT CA GTS não existe um processo de renovação de certificado, estando o titular obrigado a fazer um novo pedido de emissão de certificado com os mesmos parâmetros. Este processo obriga a geração de um novo par de chaves, e respetivo certificado.

A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial que resultam na geração de novos pares de chaves.

13.6. Renovação de Certificados com Geração de Novo Par de Chave

A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial que resultam na geração de novos pares de chaves.

13.7. Modificação de Certificados

A modificação de certificados não é suportada pela ROOT CA GTS.

13.8. Revogação de Certificados Emitidos pela ROOT CA

A revogação de certificados são mecanismos a utilizar quando por algum motivo os certificados deixam de ser fiáveis, antes do período de finalização originalmente previsto.

Na prática, a revogação de certificados é uma ação através da qual, o certificado deixa de estar válido antes do fim do seu período de validade, perdendo, deste modo, a sua operacionalidade.

A suspensão de certificados não é suportada pela ROOT CA GTS.

13.8.1. Revogação de Certificados Emitidos pela ROOT CA

Um certificado pode ser revogado por uma das seguintes razões:

- Cessação de funções;
- Roubo, extravio, destruição ou deterioração do dispositivo de suporte dos certificados;
- Inexatidões nos dados fornecidos;
- Comprometimento ou suspeita de comprometimento das chaves privada do titular;

- Comprometimento ou suspeita de comprometimento da senha de acesso ao certificado;
- Comprometimento ou suspeita de comprometimento das chaves privada da ROOT CA GTS;
- Incumprimento por parte da ROOT CA GTS ou titular das responsabilidades prevista na DPC;
- Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa;
- Utilização do certificado para atividades abusivas

Um pedido de revogação pode ser efetuado de forma legítima por um dos seguintes intervenientes:

- O titular do certificado;
- A Entidade Certificadora ou Entidade Requerente do certificado da entidade subordinada;
- A GTS, no conhecimento de que:
 - Os dados constantes no certificado não correspondem à realidade;
 - O certificado não esteja na posse do seu titular;
- A Entidade Supervisora;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

Todos os pedidos de revogação devem ser endereçados para a ROOT CA GTS por escrito ou por mensagem eletrónica assinada digitalmente.

Os certificados revogados podem ser consultados através da LRC da ROOT CA GTS.

13.9. Serviço sobre o estado do Certificado

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LRC ou num servidor de verificação do estado online (via OCSP).

As LRC podem ser acedidas em <https://pki.globaltrustedsign.com/index.html>, garantindo a sua disponibilidade 24 horas por dia, 7 dias por semana, exceto na ocorrência de alguma paragem de manutenção programada e devidamente comunicada às partes envolvidas.

O fim da subscrição de um certificado ocorre quando o prazo de validade é ultrapassado expirado ou o certificado é revogado, conforme RFC 3647.

13.9.1. Frequência de Emissão de LRC`s (se aplicável)

Os estados dos certificados emitidos pela ROOT CA da GTS podem ser verificados através da consulta da sua CRL. Esta é emitida sempre que haja uma revogação dos certificados emitidos ou, na ausência de alterações no estado dos certificados, de forma trimestral. A disponibilização nos repositórios é feita num período não superior a 30 minutos, sendo o seu download feito em menos de 10 segundos. De modo a garantir a sua disponibilidade, a CRL é disseminada nos seguintes repositórios:

https://pki.globaltrustedsign.com/root/gts_root_crl.crl

https://pki02.globaltrustedsign.com/root/gts_root_crl.crl

13.9.2. Outras Formas de Anúncio de Revogação

A Global Trusted Sign Root CA dispõe de serviços de validação OCSP do estado dos certificados de forma online. Esse serviço poderá ser acedido em <https://ocsp.globaltrustedsign.com>

14. Controlos de Segurança Física, de Gestão e Operacionais

14.1. Controlos de Segurança Física

A ROOT CA GTS foi desenhada de forma a proporcionar um ambiente seguro capaz de proteger os sistemas que suportam a atividade da ROOT CA GTS. As operações da GTS são realizadas numa sala numa zona de alta segurança, dentro de um edifício que garante a existência de diversos níveis de segurança acessíveis apenas às pessoas que dele necessitem para desempenho das suas funções de confiança.

A GTS garante ainda que as suas zonas de alta segurança possuem todo o conjunto de características previstas, bem como os mecanismos necessários por forma a garantir as condições de segurança, no que concerne a:

- Localização física e tipo de construção, com paredes em alvenaria, betão ou tijolo;
- Teto e pavimento com construção similar à das paredes;
- Inexistência de janelas;
- Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, características corta – fogo e funcionalidade antipânico;
- Acesso físico ao local;
- Energia e ar condicionado;
- Exposição à água / inundações;
- Prevenção e proteção face a incidentes/desastres tais como incêndios, inundações e semelhantes;
- Eliminação de resíduos;
- Salvaguarda dos suportes de informação.

Os suportes de informação sensível deverão ser armazenados, de forma segura, em cofres e de acordo com o tipo de suporte e classificação da informação. O acesso a estas zonas deve ser restrito a pessoas devidamente autorizadas.

No final do seu ciclo de vida, documentos e materiais em papel que contenham informações críticas deverão ser eliminados através de métodos eficazes que não permitam a reconstrução dos mesmos.

Outros equipamentos de armazenamento (discos rígidos e afins) devem ser devidamente limpos, de modo a não seja possível recuperar alguma informação através de formatações seguras, ou

destruição física dos equipamentos. No caso de periféricos criptográficos, estes devem ser destruídos segundo as instruções e recomendações dos respetivos fabricantes.

14.2. Controlos dos Processos

A atividade de emissão de certificados digitais da GTS, enquanto entidade certificadora de certificados qualificados, exige o cumprimento de um conjunto de normas europeias.

Estas mesmas normas definem um conjunto de grupos de trabalho, com competências, atividades e regras distintas, que deve ser garantido pela GTS.

Nas funções de confiança está incluído todo o pessoal com acesso aos sistemas de certificação das EC e que na prática podem materialmente afetar:

- Manipulação de informações de subscritor e validação de informação de emissão de Certificado;
- Funções do ciclo de vida dos certificados;
- Configuração e manutenção dos sistemas de certificação.

No âmbito da sua estrutura organizativa são consideradas funções de confiança as descritas a seguir, estando divididas e diferenciadas pela natureza da sua atividade, quer se trate do software para certificação digital. A cada uma delas são cometidas as seguintes responsabilidades consoante o âmbito.

14.2.1. Grupo de Trabalho da Administração de Segurança (AdmSeg)

Responsabilidades: Responsáveis globais sobre segurança dos sistemas, nomeadamente, pela gestão e implementação das regras e práticas de segurança no âmbito dos serviços prestados pela GTS.

Descrição de Tarefas:

- Definição da documentação associada às práticas de segurança da informação da GTS
- Definição dos procedimentos relacionados com a gestão das chaves criptográficas
- Garantia de que toda a documentação associada à GTS se encontra atualizada, adaptada à realidade e armazenada de forma segura de acordo com a sua classificação
- Gestão da implementação das práticas e políticas de segurança, incluindo o controlo de acessos lógico e físico
- Gestão dos riscos associados aos serviços prestados pela GTS
- Monitorização dos eventos de segurança e gestão da alarmística associada a estes
- Participação e resposta aos incidentes de segurança
- Guarda dos artefactos sob a sua custódia

14.2.2. Grupo de Trabalho da Administração de Sistemas (AdmSist)

Responsabilidades: Responsáveis pela instalação, configuração e manutenção dos sistemas, no entanto, com acesso controlado às configurações relacionadas com a segurança.

Descrição de Tarefas:

- Gestão do ambiente de produção
- Instalação, configuração e manutenção dos sistemas e rede tendo acesso controlado às configurações relacionadas com os componentes aplicacionais
- Gestão do desempenho dos sistemas que suportam a atividade da GTS, de modo a garantir que a infraestrutura esteja sempre disponível e operacional, previsão das necessidades futuras que decorrem da atividade da GTS e os seus custos
- Gestão dos incidentes e avarias de *hardware* e *software*
- Reposição do sistema através das cópias de segurança, quando necessário
- Execução e manutenção de documentação (procedimentos) pertinentes à execução das suas funções
- Guarda dos artefactos sob a sua custódia

14.2.3. Grupo de Trabalho de Operação de Sistemas (OpSist)

Responsabilidades: Responsáveis pela operação de rotina dos sistemas de confiança, estando autorizados a realizar as cópias de segurança e sua recuperação.

Descrição de Tarefas:

- Operação diária dos sistemas
- Realização de operações de rotina
- Realização de cópias de segurança
- Guarda dos artefactos sob a sua custódia

14.2.4. Grupo de Trabalho de Administração de Registo (AdmReg)

Responsabilidades: Responsáveis pela aprovação da emissão, suspensão e revogação de certificados digitais (certificados de assinatura qualificada, selos eletrónicos, certificados para autenticação de sítios Web, e selos temporais).

Descrição de Tarefas:

- Emissão e revogação dos certificados
- Submissão dos *Certificate Signing Request* (CSR) para a execução dos processos de registo;
- Elaboração da videoconferência para validação da identidade dos titulares;
- Criação ou atualização das entidades requerentes de serviços de certificação;
- Validação da documentação a ser entregue pelo titular para emissão/revogação de certificados
- Validação da identidade dos titulares por videoconferência.
- Notificação dos titulares quando necessário
- Guarda dos artefactos sob a sua custódia

14.2.5. Grupo de Trabalho de Auditoria (Auditor)

Responsabilidades: Responsáveis pela análise interna da conformidade com as normas nacionais e europeias aplicáveis à atividade da GTS enquanto prestadora de serviços qualificados, estando autorizados a ver e monitorizar os arquivos de atividade dos sistemas de confiança.

Descrição de Tarefas:

- Registo e monitorização de todas as operações sensíveis do sistema
- Registo de todos os procedimentos passíveis de auditoria
- Verificação periódica da conformidade com os processos, políticas e procedimentos em vigor no âmbito da atividade de prestadora de serviços qualificados
- Guarda dos artefactos sob a sua custódia
- Apresentação de sugestões de melhoria

14.2.6. Grupo de Trabalho de Gestão (Gestão)

Responsabilidades: Responsáveis por assegurar os meios técnicos, financeiros e humanos para o correto funcionamento da GTS enquanto prestadora de serviços qualificados.

Descrição de Tarefas:

- Nomeação dos membros dos restantes Grupos de Trabalho
- Revisão e aprovação das Políticas e Declaração de Práticas da GTS
- Guarda dos artefactos sob a sua custódia

14.2.7. Número de pessoas exigidas por grupo

Cada grupo tem 2 pessoas de modo a garantir a redundância dos recursos.

14.2.8. Segregação de funções

A composição dos grupos de trabalho deve respeitar os princípios de privilégio mínimo e segregação de funções.

Deste modo, a tabela a seguir apresenta as incompatibilidades entre os diferentes grupos existentes na GTS, de modo a evitar quaisquer conflitos de interesse.

| Grupo de Trabalho | Incompatível com | | | | |
|--------------------------------|------------------|-----|-----|-----|-----|
| | (a) | (b) | (c) | (d) | (e) |
| (a) Administração de Segurança | | X | X | X | X |
| (b) Administração de Sistemas | X | | | | X |
| (c) Administração de Registo | X | | | | X |
| (d) Operação de Sistemas | X | | | | X |
| (e) Auditoria | X | X | X | X | |

14.3. Medidas de segurança de Pessoal

14.3.1. Requisitos relativos às qualificações, experiências, antecedentes e credenciação

Todos os membros que integrem um dos grupos de trabalho da GTS devem cumprir os seguintes requisitos:

- Apresentar provas da suficiente qualificação e experiência para o desempenho da respetiva função
- Garantir confidencialidade relativamente a informação sensível da GTS ou dados de identificação dos titulares
- Garantir que não desempenham funções que possam causar conflito com as suas responsabilidades nas atividades da GTS
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função
- Ter recebido a documentação necessária para o desempenho da respetiva função
- Ter recebido formação e treino adequado para o desempenho da respetiva função
- Ter sido nomeado formalmente para a função a desempenhar.

14.3.2. Procedimento de verificação de antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer um dos Grupos de Trabalho e inclui a verificação da identidade e do registo criminal, bem como das referências indicadas no curriculum vitae.

14.3.3. Requisitos de formação e treino

Os membros dos Grupos de Trabalho devem estar sujeitos a um plano de formação e treino específico, que englobe os seguintes tópicos:

- aspetos legais relativos à prestação de serviços de certificação
- Certificação digital e Infraestruturas de Chave Pública
- Conceitos gerais sobre segurança da informação
- Formação específica para o Grupo de Trabalho em causa
- Funcionamento do software e/ou hardware usado na GTS
- Política de Certificados e Declaração de Práticas de Certificação
- Procedimentos para a continuidade da atividade
- Recuperação face a desastres.

14.3.4. Frequência e requisitos para ações de reciclagem

Sempre que ocorra qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos existentes, deverá desencadear-se um processo de formação adequado para todos os Grupos de Trabalho. Devem ainda ser realizadas sessões formativas aos elementos das Entidades Certificadoras sempre que ocorram alterações às Políticas de Certificação ou na Declaração de Práticas de Certificação da GTS.

Tais factos devem ser tidos em linha de conta de modo a garantir o nível pretendido de conhecimentos para a execução satisfatória das responsabilidades que compete aos diferentes Grupos de Trabalho.

14.3.5. Frequência e sequência da rotação de funções

Nada a assinalar.

14.3.6. Sanções para ações não autorizadas

Todas as ações não autorizadas e que desrespeitem a Declaração de Práticas de Certificação da GTS e as Políticas de Certificados deverão ser alvo de medidas disciplinares adequadas, quer tenham sido realizadas de forma deliberada ou sejam ocasionadas por negligência.

Poderão ainda, de acordo com a gravidade da infração cometida, ser aplicadas sanções previstas na lei.

14.3.7. Requisitos para prestadores de serviços

O acesso à Zona de Alta Segurança por consultores ou prestadores de serviços independentes exige a supervisão contínua pelos membros dos grupos de trabalho, bem como o registo no livro de presenças existente para o efeito.

14.3.8. Documentação fornecida ao pessoal

Deverá ser disponibilizada aos membros dos Grupos de Trabalho a informação e documentação necessária relativamente às Políticas de Certificados, à Declaração de Práticas de Certificação da GTS, à documentação com a descrição das responsabilidades, obrigações e tarefas dependendo da função e ainda documentação técnica acerca do software e hardware utilizado na Entidade Certificadora da GTS.

14.4. Procedimentos de Auditoria de Segurança

14.4.1. Tipo de eventos registados

Deverão ser registados todo o tipo de eventos significativos, capazes de ser auditáveis, em especial os seguintes:

- Cópias de segurança, restauro ou arquivamento de dados;
- Dispositivos físicos de segurança de entrada/saída dos vários níveis de segurança.

- Manutenções ao sistema;
- Modificações ou atualizações relativamente a software e hardware;
- Mudança de pessoal;
- Ligar e desligar aplicações ou sistemas que intervenham na atividade de certificação;
- Operações realizadas por membros dos Grupos de Trabalho;
- Tentativas, com ou sem sucesso, de acesso a recursos sensíveis da Entidade Certificadora da GTS;
- Tentativas, com ou sem sucesso, de alteração dos parâmetros de segurança;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar contas do sistema;
- Tentativas, com ou sem sucesso, de início e fim de sessão;
- Tentativas, com ou sem sucesso, de operações relativas a pedido, emissão, renovação, modificação, suspensão e revogação de chaves e certificados;
- Tentativas, com ou sem sucesso, de gerar, emitir ou atualizar LCR;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas, com ou sem sucesso, de acesso às Zonas de Alta Segurança da ROOT CA GTS.

O registo dos eventos, efetuado quer por meios automáticos ou manuais, deverá conter, no mínimo, informações tais como a data e hora do evento, a categoria e descrição do mesmo, o número de série do evento, bem como a identificação do agente que o terá originado.

14.4.2. Frequência da auditoria de registos

A auditoria dos registos deverá ser realizada de forma regular, em especial na ocorrência de eventos que possam ser considerados suspeitos ou que possam comprometer, de alguma forma, a atividade em questão. Todos esses eventos deverão ficar registados num relatório sumário, passível de ser analisado, bem como as decisões e ações tomadas em resposta a estes.

14.4.3. Período de retenção dos registos de auditoria

Os registos de auditoria deverão ser mantidos nos sistemas por um período de pelo menos 1 mês após o seu processamento. Após esse período, deverão ser arquivados tal como definido na seção 14.5 do presente documento.

14.4.4. Proteção dos registos de auditoria

Os registos de auditoria devem encontrar-se protegidos contra as tentativas de acessos, alteração, manipulação ou destruição não-autorizadas.

Por norma, os registos eletrónicos devem estar protegidos com recurso a técnicas criptográficas de modo a que ninguém, à exceção das próprias aplicações de visualização de registos, com o controlo de acessos adequado, possa aceder aos mesmos.

Os registos manuais devem ser armazenados em locais que cumpram os requisitos definidos para o efeito, dentro de instalações seguras da ROOT CA GTS. Este tipo de registos de auditoria é considerado informação sensível.

14.4.5. Procedimentos para a cópia de segurança dos registos

Devem ser realizadas cópias de segurança dos registos de auditoria de forma regular.

14.4.6. Sistema de recolha de registos (Interno / Externo)

Os registos são recolhidos e tratados centralmente.

14.4.7. Notificação de agentes causadores de eventos

Os eventos passíveis de serem auditáveis são registados nos sistemas internos da GTS, sendo estes armazenados de forma segura. Não está contemplada qualquer notificação ao agente causador do evento.

14.4.8. Avaliação de vulnerabilidades

Ainda que não ocorram alterações significativas no ambiente global da ROOT CA GTS, deverão ainda assim ser efetuadas avaliações de vulnerabilidades, tendo em vista minimizar ou eliminar potenciais tentativas de quebras de segurança no sistema. O resultado das avaliações deve ser reportado aos responsáveis pela matéria, para que estes as possam rever e aprovar, caso se justifique, um plano de implementação e correção das vulnerabilidades detetadas.

14.5. Arquivo de Registos

14.5.1. Tipo de dados arquivados

A ROOT CA GTS irá arquivar, no mínimo, os seguintes tipos de dados:

- Os registos de auditoria especificados no ponto 14.4.1 do presente documento;
- As cópias de segurança dos sistemas que compõem a infraestrutura da EC;
- Documentação relativa ao ciclo de vida dos certificados.
- Chaves para efeitos de confidencialidade (quando aplicável);
- Contratos estabelecidos entre a EC e outras entidades.

14.5.2. Período de retenção em arquivo

O tempo de retenção dos dados sujeitos a arquivo está definido de acordo com o previsto na legislação nacional, por um período nunca inferior a 7 anos.

14.5.3. Proteção dos arquivos

O arquivo encontra-se protegido de acordo com o que está igualmente previsto para a proteção dos registos de auditoria. Mais se acrescenta que o arquivo se encontra protegido de modo a que apenas os membros autorizados dos Grupos de Trabalho possam consultar e aceder ao mesmo.

14.5.4. Procedimentos para as cópias de segurança do arquivo

De acordo com o disposto no ponto 14.4.5, relativamente aos procedimentos para a cópia de segurança dos registos.

14.5.5. Requisitos para validação cronológica dos registos

Os sistemas de informação utilizados pela ROOT CA GTS devem garantir o registo da data e hora do momento, tendo por base uma fonte de tempo segura.

14.5.6. Sistema de recolha de dados de arquivo (Interno / Externo)

De acordo com o disposto no ponto 14.4.6.

14.5.7. Procedimentos de recuperação e verificação de informação arquivada

Só os membros devidamente autorizados dos Grupos de Trabalho têm acesso aos arquivos para a verificação da integridade da informação, de modo a garantir que os mesmos se encontram em bom estado e que podem ser recuperados.

14.6. Recuperação em caso de desastre ou comprometimento

14.6.1. Procedimentos em caso de incidente ou comprometimento

Em caso de incidente de segurança grave ou comprometimento da ROOT CA GTS, devem ser tomados os procedimentos seguintes:

- Notificação, sem demora indevida, mas sempre no prazo de 24 horas após ter tomado conhecimento do ocorrido, a entidade supervisora e, se necessário, outras entidades, como a entidade nacional competente em matéria de segurança da informação ou a autoridade responsável pela proteção de dados, de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados.
- Se a violação da segurança ou perda de integridade constatada for suscetível de prejudicar a pessoa singular ou coletiva a quem o serviço de confiança tiver sido prestado, será notificada também sem demora indevida a referida pessoa singular ou coletiva da violação da segurança ou da perda de integridade.
- Adicionalmente, e dependendo do tipo de incidente, a EC afetada poderá ser desligada.

Se necessário, em particular se a violação da segurança ou a perda de integridade disserem respeito a dois ou mais Estados-Membros, a entidade supervisora notificada informa do facto as entidades supervisoras dos outros Estados-Membros em causa e a ENISA.

A entidade supervisora notificada informa o público ou exige que o prestador do serviço de confiança o faça, se considerar que a divulgação da violação da segurança ou perda de integridade é do interesse público.

14.6.2. Comprometimento do Algoritmo

Se algum dos algoritmos, ou parâmetros associados, utilizados pela ROOT CA GTS ou seus titulares se tornarem insuficientes para o fim a que se destinam, a ROOT CA GTS deve:

- Informar todos os titulares e outras entidades com as quais a ROOT CA GTS tenha acordos ou outra forma de relações estabelecidas. Adicionalmente, esta informação deve ser disponibilizada para outras entidades dependentes;
- Agendar a revogação de qualquer certificado afetado.

14.6.3. Corrupção dos recursos informáticos, do software e/ou dos dados

Caso os recursos de hardware, software e/ou dados tenham sido alterados ou exista a suspeita de que estes tenham sido corrompidos, deverá iniciar-se um processo de gestão de incidentes tendo em vista o restabelecimento das condições seguras com inclusão de novos componentes de eficácia credível.

A GTS suspenderá os seus serviços e notificará todas as Entidades envolvidas caso se verifique que esta situação tenha afetado os certificados emitidos, incluindo a notificação dos titulares dos mesmos.

14.6.4. Capacidade para continuidade da atividade

A GTS dispõe de um plano de continuidade da atividade, onde estão descritos todos os procedimentos a acionar em caso de desastre onde haja perda ou corrupção de dados, software e equipamentos.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo e que os dados da ROOT CA GTS necessários para retomar as operações são copiados e armazenados em locais seguros e adequados para permitir retomar devidamente as operações da ROOT CA GTS em caso de incidentes/desastres.

As cópias de segurança de informações e software essenciais são realizadas regularmente. Devem ser fornecidas instalações de apoio adequadas para garantir que todas as informações e software essenciais possam ser recuperados após um desastre ou falha nos meios de comunicação (media). Os mecanismos de salvaguardas devem ser testados regularmente para garantir que respondem aos requisitos dos planos de continuidade do negócio.

14.6.5. Procedimentos em caso de Extinção da Entidade de Certificação ou Entidade de Registo

A GTS deve em caso de cessação de atividades, atempadamente proceder às ações seguintes:

- a) Informar a Entidade Supervisora (Gabinete Nacional de Segurança);
- b) Informar todos os titulares dos certificados a partir de uma notificação explanatória com antecedência à cessação formal das atividades da ROOT CA GTS;
- c) Revogar todos os certificados;
- d) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos;
- e) Proceder à destruição definitiva de toda a informação classificada ou garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da ROOT CA GTS, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos

Em caso se procedam alterações do organismo/estrutura responsável de gestão da atividade da ROOT CA GTS, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

15. Controlos de Segurança Técnicos

15.1. Geração e Instalação de Pares de Chaves

A geração dos pares de chaves da ROOT CA GTS é processada de acordo com os requisitos e algoritmos definidos nesta declaração, através de um procedimento formal datado, realizado e assinado por elementos autorizados dos Grupos de Trabalho da Administração de Segurança e de Auditoria.

O processo de geração das chaves é, obrigatoriamente, efetuado diretamente num módulo criptográfico em hardware (HSM). O módulo criptográfico cumpre os requisitos FIPS 140-2 nível 3. Estes certificados são auto-assinados pela ROOT CA GTS.

A ROOT CA GTS funciona em modo *offline*.

No que respeita à dimensão das chaves, foram seguidas as recomendações da norma ETSI TS 119 312 – Electronic Signatures and Infrastructures – Cryptographic Suites. A dimensão definida para as chaves é a seguinte:

- 4096 bits RSA para a chave das entidades certificadoras da GTS.
- 2048 bits RSA para chaves associadas aos restantes certificados que sejam emitidos pela GTS com algoritmo de assinatura sha256RSA.

A geração das chaves da ROOT CA GTS deverá ser feita de acordo com o estipulado no PKCS#11.

15.2. Proteção da Chave Privada e Características do Módulo Criptográfico

A ROOT CA GTS utiliza módulos criptográficos (HSM) para as operações que dizem respeito à geração, armazenamento e assinatura.

Os módulos criptográficos estão em conformidade com o Common Criteria v2.3, FIPS 140-2 e FIPS 140-2 nível 3 (para o módulo criptográfico da ROOT CA GTS).

A segurança do módulo criptográfico da ROOT CA GTS é garantida durante o seu ciclo de vida, garantindo os seguintes:

- A instalação e ativação das chaves privadas no módulo criptográfico é efetuada por elementos de Grupos de Trabalho bem identificados (secção 14.2 Controlos dos Processos e 14.3 Medidas de Segurança de Pessoal);
- As chaves privadas de assinatura guardadas no módulo criptográfico são apagadas no final do seu ciclo de vida;
- O módulo criptográfico não foi adulterado durante o seu transporte;
- O módulo criptográfico não é adulterado enquanto permanece nas instalações seguras da GTS;
- O módulo criptográfico tem um funcionamento correto.

A ROOT CA GTS efetua a retenção da sua chave privada e das chaves privadas de todos os seus clientes através de um HSM guardado em ambiente seguro.

As chaves privadas da ROOT CA GTS:

- Têm pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original e são alvo de cópias de segurança
- São arquivadas internamente em ambientes seguros e por longos períodos de tempo.
- São geradas e armazenadas em HSM não sendo possível a transferência das mesmas para outros meios ou dispositivos.
- São armazenadas de forma cifrada em HSM.

A chave privada deverá ser ativada quando o sistema/aplicação da ROOT CA é ligado. Esta ativação só será efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação por quórum k em N onde $k = 2$. Isso é, é necessário k utilizadores em N para efetuar uma operação administrativa nos HSM (incluindo a ativação da chave privada). A chave privada permanecerá ativa até que o processo de desativação seja executado.

As várias chaves privadas da ROOT CA GTS deverão ser destruídas sempre que deixem de ser necessárias. De uma forma geral, a destruição de chaves deve ser precedida sempre pela revogação do certificado, no caso de estar em vigor, ou caso tenha sido atingido o fim da sua data de validade. Nesse sentido, as chaves deverão ser apagadas/destruídas através de um método formal auditável, de modo a que não seja possível a sua posterior reconstrução. De igual forma, as respetivas cópias de segurança deverão também ser alvo de destruição.

15.3. Outros Aspetos da Gestão do Par de Chaves

A ROOT CA GTS efetua o arquivo das suas chaves e das chaves por si emitidas (para efeitos de assinatura digital), permanecendo armazenadas após a expiração dos certificados correspondentes para verificação de assinaturas geradas durante seu período de validade.

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que após expiração do certificado as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada.

A validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados, é a seguinte:

- O certificado da ROOT CA GTS tem uma validade mínima de 20 anos;
- Um certificado para entidade subordinada emitido pela ROOT CA GTS tem uma validade mínima de 1 ano, e máxima de 6 anos.

15.4. Dados de Ativação

A geração e instalação dos dados de ativação para a chave privada da ROOT CA GTS é feita por pessoal autorizado em ambiente seguro através de um setup inicial do HSM, que exige controlo simultâneo por dois membros dos grupos de trabalho.

Os dados de ativação da chave privada são guardados em ambientes seguros (secção Proteção da Chave Privada e Características do Modulo Criptográfico).

A transmissão dos dados de ativação das chaves privadas para outros HSM é feita, apenas e só quando necessário, de modo a garantir a sua proteção e disponibilidade.

Os dados de ativação são destruídos assim que a chave privada associada for igualmente destruída.

15.5. Controlos de Segurança Informática

A ROOT CA GTS tem um funcionamento *offline*. O acesso aos servidores da ROOT CA GTS é restrito apenas a membros autorizados.

15.6. Ciclo de Vida dos Controlos de Segurança

Todo o desenvolvimento, configuração e alteração do Software/Hardware associados à infraestrutura de chave pública são executadas e auditadas por membros autorizados da ROOT CA GTS.

A ROOT CA GTS possui mecanismos para controlar e monitorizar as configurações dos sistemas da ROOT CA GTS desde a sua primeira ativação até à eventual cessação de atividades.

Todas as operações de atualização e manutenção são executadas por membros autorizados de acordo com os procedimentos adequados para o efeito.

15.7. Controlos de Segurança da Rede

Todos os sistemas da ROOT CA GTS estão na Zona e de Alta Segurança (ZAS). Através dos controlos implementados, é possível garantir a identificação, autenticação e administração dos acessos.

15.8. Validação Cronológica

A informação relacionada com a ROOT CA GTS é registada com a data e hora da criação.

Toda a infraestrutura é sincronizada temporalmente por relógio atómico interno, e adicionalmente por duas fontes UTC alternativas:

- Royal Observatory of Belgium (ORB), Belgica, Bruxelas - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

16. Perfil de Certificado e de Listas de Revogação de Certificados

16.1. Perfil de Certificado

A emissão de certificados segue o perfil de certificados recomendado pela ITU-T X.509 versão 3.

O armazenamento das chaves envolvidas em todos os processos de assinatura ou geração de certificados são guardados num Dispositivo Seguro de Hardware (HSM) certificado e que cumpre os requisitos definidos na legislação nacional e europeia.

O perfil do certificado da ROOT CA GTS está de acordo com o conjunto de standards:

- 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
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers, e os standards relacionados com os serviços qualificados de confiança
- Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

Informação detalhada sobre os perfis dos Certificados da ROOT CA GTS pode ser consultada em:

- <https://pki.globaltrustedsign.com/index.html>

16.2. Perfil de Listas de Revogação de Certificados

As LRC emitidas contêm os campos básicos e conteúdos específicos na tabela seguinte:

| Campo | Valor |
|-------------------------|---|
| Versão | V2 |
| Algoritmo de Assinatura | O algoritmo utilizado pela EC para assinar o certificado é sha256WithRSAEncryption |
| Emissor | DN da entidade certificadora emissora da LCR |
| Data Efetiva | A indicação de quando a LCR foi gerada. |
| Próxima atualização | A indicação de quando será gerada nova LCR. |
| Certificados Revogados | Lista dos certificados revogados que fornece informação do estado dos certificados no que diz respeito, respetivamente, ao número de série do certificado revogado, a data em que foi revogado e o motivo da sua revogação. |

Informação mais detalhada sobre os perfis das LRC pode ser consultada em:

- Lista de Revogação de Certificados (LRC) da ROOT CA GTS
<https://pki.globaltrustedsign.com/index.html>
- Lista de Revogação de Certificados (LRC) da ROOT CA GTS
<https://pki02.globaltrustedsign.com/index.html>
- O perfil dos certificados OCSP pode ser consultado em:
<https://ocsp.globaltrustedsign.com>

17. Auditoria e Avaliação de Conformidade

A GTS irá efetuar auditorias e avaliações de conformidade regulares para assegurar a conformidade da Entidades Certificadoras constituintes da sua hierarquia de confiança de acordo com legislação nacional bem como com as normas internacionais aplicáveis.

Nota: A GTS, ou os seus representantes legais, podem delegar a realização destas auditorias, avaliações ou investigações a entidades externas de auditoria devidamente especializadas e acreditadas para o efeito.

17.1. Frequência ou motivo da auditoria

Na ROOT CA GTS, as auditorias de conformidade serão realizadas regularmente de acordo com a legislação aplicável por uma entidade externa registada e reconhecida para o efeito, tomando como base as normas existentes sendo os seus resultados comunicados à entidade supervisora.

17.2. Identidade e qualificações do Organismo de Avaliação da Conformidade

O Organismo de avaliação da conformidade (Conformity Assessment Body – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

17.3. Relação entre o Organismo de Avaliação da Conformidade e a ROOT CA GTS

O organismo de avaliação da conformidade e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

O Auditor e a parte auditada (Entidade Certificadora) não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares da ROOT CA GTS.

17.4. Âmbito da auditoria

Uma auditoria de segurança é efetuada com base nos requisitos definidos na presente DPC e em conformidade com a legislação nacional aplicável. Tem por objetivo determinar a conformidade dos serviços da ROOT CA GTS com esta Declaração de Práticas e com as Políticas de Certificados definidas. Deve também determinar a correta adequação em relação a diversos documentos, nomeadamente a política de segurança, segurança física, avaliação tecnológica, gestão dos serviços da EC, seleção de pessoal, declarações de práticas de certificação e políticas de certificados em vigor, contratos e política de privacidade.

Pode ser efetuada de forma completa ou parcial, e pode incidir sobre qualquer tipo de documentos/processos.

17.5. Procedimentos após uma auditoria com irregularidades identificadas

Quando são detetadas irregularidades numa auditoria, a CAB procede da seguinte forma:

- a) Documentar todas as irregularidades encontradas durante a auditoria;
- b) No final do processo de auditoria, reunir com os responsáveis da entidade submetida a auditoria e apresentar de forma sucinta o relatório de primeiras impressões (RPI);
- c) Elaborar o relatório de auditoria de acordo com as regras e práticas estabelecidas pela Entidade Supervisora;
- d) Submeter o relatório de auditoria à Entidade auditada;
- e) A entidade submetida à auditoria deve enviar um relatório de correção de irregularidades (RCI) para a Entidade Supervisora, descrevendo as ações, metodologia e tempo necessário para a correção das irregularidades identificadas;
- f) A Entidade Supervisora após a análise do relatório submetido, consoante o nível de gravidade/severidade das irregularidades, tomará uma das três opções seguintes:

- a. Aceitar os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;
- b. Permitir que a entidade continue em atividade por um período máximo de 90 dias para a correção das irregularidades;
- c. Revogação imediata das atividades.

17.6. Comunicação de resultados

Os resultados de todo o processo serão comunicados aos auditores responsáveis e à GTS.

18. Outras Situações e Assuntos Legais

Estabelecem-se alguns aspetos legais e de negócio que importa salientar de seguida:

- Poderão ser cobradas taxas pelos processos de emissão, e/ou renovação de certificados;
- Poderão ser cobradas taxas pelos serviços de validação cronológica;
- Não serão cobradas taxas pela disponibilização dos certificados em repositório;
- O acesso a informação sobre o estado ou lista de revogação de certificados (LRC) é livre e gratuita, não se podendo aplicar qualquer taxa;
- Não estão previstos reembolsos aplicáveis à prestação de serviços de revogação de certificados.

18.1. Responsabilidade Financeira

18.1.1. Seguro de cobertura

As Entidades Certificadoras devem respeitar a legislação em vigor no que se concerne aos seguros de cobertura de responsabilidade civil. Nesse sentido, a GTS dispõe de um seguro de responsabilidade civil, de acordo com o artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

18.1.2. Outros recursos

Nada a assinalar.

18.1.3. Seguro ou garantia de cobertura para utilizadores

A GTS dispõe de um seguro de responsabilidade civil, de acordo com o artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

18.2. Confidencialidade da Informação Processada

O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular terá de ser expressamente autorizado pela própria.

Considera-se informação confidencial:

- As chaves privadas das Entidades Certificadoras;
- As chaves privadas dos titulares dos certificados;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal proporcionada à ROOT CA GTS durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Dados dos membros dos grupos de trabalho da ROOT CA GTS.

Considera-se informação de acesso público:

- Declarações de Práticas de Certificação;
- Políticas de Certificados;
- Listas de Revogação de Certificados (LRC);
- Toda a informação classificada como "pública".

A ROOT CA GTS permite o acesso a informação não confidencial, sem prejuízo do que se venha a estabelecer nas DPC, no domínio dos controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

18.3. Privacidade dos Dados Pessoais

Informação privada é toda a informação fornecida pelo titular do certificado que não esteja publicamente disponível. Informação considerada não-privada é toda a informação tornada pública a partir de certificados e, como tal, não é considerada privada.

A responsabilidade de proteção da informação privada, assim como os procedimentos para notificação e consentimento para utilização da informação privada estão de acordo com a legislação portuguesa, nomeadamente com o regulamento geral de proteção de dados (regulamento 2016/679).

As práticas da ROOT CA GTS garantem a proteção da confidencialidade e integridade dos dados de registo, especialmente quando transmitida entre a ROOT CA GTS e os subscritores e titulares, bem como durante a comunicação entre os componentes distribuídos dos sistemas da ROOT CA GTS.

No âmbito dos serviços prestados, é necessário manter evidências digitais por questões de conformidade com a legislação em vigor e aplicável à ROOT CA GTS. Estas evidências são mantidas de modo a garantir a sua recolha, transmissão e armazenamento seguros.

18.4. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC, PC, bem como qualquer outro documento relacionado, são propriedade da ROOT CA GTS.

As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico que se empregue para o seu armazenamento.

O titular conserva sempre o direito sobre as suas marcas, produtos ou nome comercial contido no certificado.

18.5. Representações e Garantias

É obrigação da ROOT CA GTS cumprir as diretivas seguintes:

- Realizar as suas operações de acordo com esta Declaração de Práticas;
- Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;
- Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais;
- Proteger, em caso de existirem, as suas chaves privadas e as que estejam sob sua custódia;
- Emitir certificados de acordo com o standard X.509;
- Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de input de dados;
- Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
- Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
- Utilizar sistemas fiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir pessoas não autorizadas altere os dados;
- Arquivar sem alteração os certificados emitidos;
- Garantir que pode determinar, com precisão da data e hora, em que emitiu, ou revogou, ou suspendeu um certificado;
- Empregar pessoal com qualificações, conhecimento e experiências necessárias para a prestação de serviços de certificação;
- Revogar os certificados nos termos previstos no presente documento, e atualizar a lista de certificados revogados na LCR, com a frequência estipulada na presente DPC.
- Publicar a sua DPC e as Políticas aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;

- Notificar, com a máxima brevidade possível, por meio de correio eletrónico, os titulares dos certificados nos casos em que a ROOT CA GTS proceda à revogação ou suspensão dos mesmos, indicando o motivo que originou a situação;
- Colaborar com as auditorias externas exigidas pela Entidade Supervisora;
- Operar em conformidade com as políticas, normas e legislação que sejam aplicáveis;
- Garantir a disponibilidade da LCR de acordo com as disposições do presente documento, bem como a disponibilidade do serviço de OCSP;
- Em caso de cessação de atividades deverá comunicar esse facto com uma antecedência mínima de três meses à Entidade Supervisora, assim como todos os titulares de certificados emitidos pela ROOT CA GTS;
- Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento durante o prazo estabelecido no presente documento;
- Disponibilizar os certificados da ROOT CA GTS.

É obrigação dos titulares dos certificados emitidos cumprir as diretivas seguintes:

- Limitar e adequar a utilização dos certificados de acordo com a legislação vigente e com as utilizações previstas no presente documento;
- Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;
- Solicitar de imediato a revogação de um certificado, em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com os procedimentos especificados no presente documento;
- Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspenso ou por ter expirado o período de validade;
- Submeter às Entidades Certificadoras (ou de Registo) a informação que considerem exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;
- Não monitorizar, manipular ou efetuar ações de “engenharia inversa” sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da ROOT CA GTS.

É obrigação das partes confiantes dos certificados emitidos pela ROOT CA GTS:

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com a legislação vigente e com o presente documento;
- Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
- Assumir a responsabilidade na correta verificação das assinaturas digitais;

- Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;
- Assumir a responsabilidade na correta verificação dos certificados emitidos;
- Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
- Notificar qualquer acontecimento ou situação anômala relativa aos certificados, utilizando os meios que a ROOT CA GTS publique no seu espaço Web.

18.6. Renúncia de Garantias

A ROOT CA GTS recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

18.7. Limitações às Obrigações

A ROOT CA GTS responde pelos danos ou prejuízos causados aos utilizadores finais e partes confiantes decorrentes da sua atividade, conforme legislação aplicável.

A ROOT CA GTS não se responsabiliza por qualquer dano ou prejuízo decorrente utilizações abusivas ou fora do âmbito do contrato estabelecido com os utilizadores e/ou partes confiantes.

A ROOT CA GTS não assume qualquer responsabilidade em caso falha dos serviços relacionada com causas de força maior, como desastres naturais, guerra ou outros similares.

18.8. Indeminizações

A ROOT CA GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável em vigor.

18.9. Termo e Cessão da Atividade

Esta DPC entra em vigor desde o momento de sua publicação no repositório da ROOT CA GTS e após aprovação, nos termos do presente documento.

Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão, nos termos do presente documento, ou pela renovação das chaves da ROOT CA GTS, momento em que, obrigatoriamente, se redigira uma nova versão.

Esta DPC será substituída por uma nova versão, com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade.

Quando a DPC ficar revogada será retirada do repositório público, garantindo-se, contudo, que será conservada durante o período definido no presente documento.

As obrigações e restrições que estabelece esta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da ROOT CA GTS, nascidas sob a sua vigência, subsistirão após sua substituição ou revogação, por uma nova versão, em tudo o que não se oponha a esta.

18.10. Notificação Individual e Comunicação dos Participantes

Todos os participantes devem utilizar os mecanismos apropriados para a comunicação coletiva, onde se engloba o correio eletrónico assinado digitalmente, correio postal e formulários assinados, entre outros, recorrendo ao meio mais adequado em função da natureza de cada assunto.

18.11. Alterações

As alterações a esta DPC devem ser aprovadas pelo Grupo de Gestão. As alterações devem ser efetuadas através de documentos, contendo as novas alterações à DPC.

No caso em que o Grupo de Gestão julgue que as mudanças à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes, que se efetuou uma mudança e que devem consultar a nova DPC no repositório estabelecido. O mecanismo de comunicação será o sítio da internet <https://www.globaltrustedesign.com>.

Se a ROOT CA GTS determinar que a alteração ao identificador (OID) da DPC ou política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem implicar uma mudança no identificador da política de certificados.

18.12. Disposições para Resolução de Conflitos

As reclamações devem ser endereçadas ao Grupo de Gestão da ROOT CA GTS, através de carta registada.

Qualquer litígio decorrente da interpretação ou aplicação deste documento regem-se pela lei portuguesa. Para regular esses litígios, as partes elegem o foro judicial da Comarca de Funchal, com exclusão de qualquer outro.

Todas as reclamações entre os utilizadores e a ROOT CA GTS poderão ser comunicadas à Entidade Supervisora com a finalidade da resolução de conflitos que possam eventualmente surgir.

18.13. Legislação Aplicável

A seguinte legislação é aplicável às entidades certificadoras prestadoras de serviços de confiança:

- a) 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
- b) Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

18.14. Conformidade com Legislação em Vigor

O presente documento (DPC) é objeto de aplicação das leis que vigoram em território nacional, bem como das normas e legislações europeias.

18.15. Providências Várias

As partes confiantes assumem, na sua totalidade, o conteúdo da última versão desta DPC.

Em caso, de existirem uma ou mais estipulações do presente documento, que sejam ou tendam a ser inválidas, nulas, ou irreclamáveis em termos jurídicos, deverão ser consideradas como não efetivas. Estas determinações são válidas, apenas e só apenas nos casos em que tais estipulações não sejam consideradas essenciais. É da responsabilidade do Grupo de Gestão avaliar a essencialidade das mesmas.

As práticas adotadas pela ROOT CA GTS garantem a independência dos membros dos grupos de confiança e da administração de topo, e a liberdade face a pressões comerciais, financeiras ou outras que possam influenciar a confiança nos serviços por eles prestados.

A ROOT CA GTS garante as condições para que os seus serviços da sua hierarquia sejam utilizados por pessoas com deficiência, em conformidade com o regulamento europeu 910/2016.

Anexo A – Definições e Acrónimos

| Acrónimos | |
|------------------|--|
| C | <i>Country</i> |
| CN | <i>Common Name</i> |
| DN | Nome Distinto (<i>Distinguished Name</i>) |
| DPC | Declaração de Práticas de Certificação |
| DR | Decreto Regulamentar |
| EC | Entidade Certificadora |
| ER | Entidade de Registo |
| GNS | Gabinete Nacional de Segurança |
| GTS | <i>Global Trusted Sign</i> |
| HSM | Modulo Criptográfico em Hardware (<i>Hardware Secure Module</i>) |
| LRC | Lista de Revogação de Certificados |
| O | <i>Organization</i> |
| OU | <i>Organization Unit</i> |
| OID | Identificador de Objeto |
| PC | Política de Certificado |
| PKCS | <i>Public-Key Cryptography Standards</i> |
| PKI | Infraestrutura de Chave Pública (<i>Public Key Infrastructure</i>) |
| SSL/TLS | <i>Secure Sockets Layer / Transport Layer Security</i> |

| Definições | |
|--|---|
| Termo | Definição |
| Assinatura Eletrónica | Dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar |
| Assinatura Eletrónica Avançada | Assinatura eletrónica que obedeça aos requisitos: a) Esteja associada de modo único ao signatário b) Permita identificar o signatário c) Seja criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo, e d) Esteja ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados |
| Autenticação | Processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar |
| Certificado | Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade. |
| Certificado de Assinatura Eletrónica | Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo |
| Certificado de Autenticação de Sítio Web | Atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido |
| Certificado de Selo Eletrónico | Atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome |
| Certificado Qualificado de Assinatura Eletrónica | Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014 |
| Certificado Qualificado de Autenticação de Sítios Web | Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014 |
| Certificado Qualificado de Selo Eletrónico | Certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento europeu 910/2014 |
| Chave Privada | Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se põe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública |
| Chave Pública | Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves |

| Definições | |
|--|--|
| Termo | Definição |
| Credenciação | Ato pelo qual é reconhecido a um prestador de serviços que o solicite e que exerça a atividade de entidade certificadora em conformidade com os requisitos definidos no Regulamento europeu 910/2014 |
| Criador de um Selo | Pessoa coletiva que cria um selo eletrónico |
| Dados de Identificação Pessoal | Conjunto de dados que permita determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa coletiva |
| Dados de Validação | Dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico |
| Dados para a Criação de um Selo Eletrónico | Conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico |
| Dados para a Criação de uma Assinatura Eletrónica | Conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica |
| Dispositivo de Criação de Assinaturas Eletrónicas | <i>Software</i> ou <i>hardware</i> configurados, utilizados para criar assinaturas eletrónicas |
| Dispositivo de Criação de Selos Eletrónicos | <i>Software</i> ou <i>hardware</i> configurados, utilizados para criar selos eletrónicos |
| Dispositivo Qualificado de Criação de Assinaturas Eletrónicas | Dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014 |
| Dispositivo Qualificado de Criação de Selos Eletrónicos | Dispositivo para a criação de selos eletrónicos que satisfaça <i>mutatis mutandis</i> os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014 |
| Documento Eletrónico | Qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual |
| Endereço Eletrónico | Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos. |
| Entidade Certificadora | Entidade ou pessoa singular ou coletiva credenciada como prestador qualificado de serviços de confiança pela entidade supervisora |
| Entidade de Registo | Entidade que aprova os Nomes Distintos (DN) das entidades subordinadas e, mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo |
| Entidade Supervisora | Entidade competente para a credenciação e fiscalização das entidades certificadoras |
| Função Hash | Operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados iniciais e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função. |
| Hash ou Impressão Digital | Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais |
| HSM | Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro |

| Definições | |
|---|--|
| Termo | Definição |
| Identificação Eletrónica | O processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva |
| Infraestrutura de Chave Pública | Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico |
| LCR | Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas |
| Meio de Identificação Eletrónica | Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha |
| OID | Identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica |
| Organismo de Avaliação da Conformidade | Organismo definido que é acreditado nos termos do regulamento 910/2014 como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados |
| Organismo Público | Entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato |
| Parte Confiante | As partes confiantes ou destinatários são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao datum, ou seja, confiam na veracidade do selo temporal. |
| Política de Certificado | Conjunto de regras que indica a aplicabilidade do certificado a uma comunidade específica e/ou classe de aplicação com requisitos de segurança comuns |
| Prestador de Serviços de Confiança | Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança |
| Prestador Qualificado de Serviços de Confiança | Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora |

| Definições | |
|--|--|
| Termo | Definição |
| Produto | <i>Hardware</i> ou <i>software</i> , ou componentes pertinentes de hardware ou software, que se destinem a ser utilizados para a prestação de serviços de confiança |
| Selo Eletrónico | Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos |
| Selo Eletrónico Avançado | Selo eletrónico que obedeça aos requisitos: a) Esteja associado de modo único ao seu criador b) Permita identificar o seu criador c) Seja criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico, e d) Esteja ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados |
| Selo Eletrónico Qualificado | Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico |
| Selo Temporal Qualificado | Selo temporal que satisfaça os requisitos: a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável, b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada, e c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente |
| Selos Temporais | Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento |
| Serviço de Confiança | Serviço eletrónico geralmente prestado mediante remuneração, que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços, ou b) Na criação, verificação e validação de certificados para a autenticação de sítios web, ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços |
| Serviço de Confiança Qualificado | Serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento europeu 910/2014 |
| Serviço de Envio Registado Eletrónico | Serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada |

| Definições | |
|---|---|
| Termo | Definição |
| Serviço Qualificado de Envio Registrado Eletrónico | <p>Serviço de envio registado eletrónico que satisfaça os requisitos:</p> <p>a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança</p> <p>b) Garantirem, com um elevado nível de confiança, a identificação do remetente</p> <p>c) Garantir a identificação do destinatário antes da entrega dos dados</p> <p>d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável</p> <p>e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados</p> <p>f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado</p> |
| Signatário | Pessoa singular que cria uma assinatura eletrónica. |
| Sistema de Identificação Eletrónica | Sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas coletivas |
| Titular | Ver Signatário. |
| Utilizador | Pessoa singular ou coletiva que utiliza a identificação eletrónica ou o serviço de confiança |
| Validação | Processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico |
| Validação Cronológica | Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico |
| Zona de Alta Segurança | Area de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos |