SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

DECLARAÇÃO DE PRATICAS DA ENTIDADE CERTIFICADORA DE VALIDAÇÃO CRONOLÓGICA DA SISP

Código:	PLRC005
Versão:	1.0
Data da versão:	30/06/2019
Criado por:	SISP
Aprovado por:	Director Geral
Nível de confidencialidade:	Público

Histórico das alterações

Data	Versão	Criado por	Descrição da alteração
30/06/2019	1.0	SISP	Criação

Índice

1. INTRODUÇÃO

1.1. Objectivos

O objectivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Certificação de Validação Cronlogica da SISP, adiante designada de SISP TSA, no suporte à sua actividade de emissão de selos de temporais.

1.2. Publico Alvo

Este documento é público e destina-se a todos quantos se relacionam com a Entidade de Certificação SISP TSA, em particular os Auditores e Colaboradores da SISP.

1.3. Estrutura do documento

Este documento segue a estrutura definida e proposta pelo grupo de trabalho *PKIX* do *IETF*, no documento *RFC 3161 – Internet X.509 Public Key Infrastructure - Time- Stamp Protocol (TSP),* e pela norma *ETSI EN 319 421 v1.1.1 – Electronic Signatures and Infrastructure; Policy and Security Requirements for TSP issuing Time-Stamps*.

2. DOCUMENTOS DE REFERÊNCIA

- Politica de certificados de validação cronológica
- Declaração de práticas da SISP ROOT CA

3. DEFINIÇÕES E ABREVIATURAS

Termo	Definição
UTC – Coordinated Universal Time	Escala de tempo baseada no segundo, como definido na ITU-R Recommendation TF.460-5 [10].
Parte confiante	Receptor de um selo temporal que confia na mesma.
Subscritor	Entidade que requer os serviços de uma ECVC e explícita ou implicitamente concorda com os termos e condições dos mesmos.
Selo Temporal (*Time-Stamp*)	Estrutura de dados que liga a representação electrónica de um datum com uma data/hora particular, estabelecendo evidência de que o datum existia nessa data/hora.
Datum	Conjunto de informações em formato electrónico.
Time Stamp Authority (TSA)	Prestador de serviços de confiança de time-stamp que opera um ou mais TSU
Serviço *Time-stamping*	Serviço de confiança de emissão de selos temporais
Time-Stamping Unit (TSU)	Conjunto de hardware e software que é gerido como uma unidade e tem uma única chave de assinatura de selo temporal activa num determinado momento.
Prestador de Serviços de Confiança(TSP)	Pessoa singular ou colectiva que preste um ou mais serviços de confiança, qualificado ou não.
Hash	Algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo.
Validação Cronologica	Declaração de uma ECVC que atesta a data e hora da criação, expedição ou recepção de um documento electrónico.

Acrónimo	
ANSI	***American National Standards Institute***
CA	***Certification Authority*** **(o mesmo que EC)**
CRL	**Ver LRC**
DL	**Decreto Lei**
DN	***Distinguished Name***
DPVC	**Declaração de Práticas de Validação Cronológica**
EAL	***Evaluation Assurance Level***
EC	**Entidade de Certificação**
EVC	**Entidade de Validação Cronológica**
GMT	**Tempo Médio de *Greenwich (Greenwich Mean Time)***
LRC	**Lista de Revogação de Certificados**
MAC	***Message Authentication Codes***
OCSP	***Online Certificate Status Protocol***
OID	**Identificador de Objecto**
PC	**Política de Validação Cronológica**
PKCS	***Public-Key Cryptography Standards***
PKI	***Public Key Infrastructure*** **(Infra-estrutura de Chave Pública)**
SHA	***Secure Hash Algorithm***
SSCD	***Secure Signature-Creation Device***
TSA	***Time-Stamping Authority*** **(o mesmo que ECVC)**

4. CONTEXTO

4.1. Objectivos

O presente documento é uma Declaração de Praticas de Validação Cronologica (DPVC), e tem por objectivo a definição de um conjunto de práticas para a emissão e validação de selos temporais e para a garantia de fiabilidade desses mesmos selos. Não se pretende nomear regras legais ou obrigações mas antes informar, pelo que se pretende que este documento seja simples, directo e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão de selos temporais qualificados, seguidas pelas SISP TSA, explica o que um selo temporal fornece e significa, assim como os procedimentos que deverão ser seguidos pelas Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos selos temporais emitidos pela EC.

Este documento pode sofrer actualizações regulares.

Os selos emitidos pela SISP TSA contêm uma referência à presente DPVC, Codigo de documento nºMSI012, de modo a permitir que Partes confiantes e outras pessoas interessadas, possam encontrar informação sobre os selos temporais e sobre a entidade que os emitiu.

4.2. Enquadramento

Esta DPVC aplica-se especificamente à EC SISP TSA, e está de acordo com a estrutura em uso no âmbito da ICP-CV e dos seguintes standards:

- *RFC 3161 – Internet X.509 Public Key Infrastructure - Time- Stamp Protocol (TSP)*
- *ETSI EN 319 421 v1.1.1 – Electronic Signatures and Infrastructure; Policy and Security Requirements for TSP issuing Time-Stamps*
- *ETSI EN 319 422 v1.1.1 "Time-stamping protocol and time-stamp profiles"*
- *ETSI EN 319 401 v2.1.1: General policy requirements for Trusted Service Providers*

4.3. Identificação do documento

Este documento é a DPVC da SISP TSA cujo o OID associado é, o 2.16.132.1.3.2.3.1.

É identificado pelos dados constantes na tabela seguinte e, é actualizado sempre que se mostrar necessario:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	2.16.132.1.3.2.3.1
Data de Emissão	30/06/2019
Validade	1 Ano
Localização	https://pki.sisp.cv/

4.4. Participantes na Infra-estrtutura de cahave publica

A SISP, enquanto Entidade Gestora da PKI da SISP, cumpre as disposições previstas nas normas e legislação aplicável, assumindo as competências aí descritas sendo responsável por fornecer serviços e assegurar os procedimentos que possam garantir as funcionalidades a seguir indicadas:

1. Geração dos pares de chaves criptográficas associadas a cada uma das Entidades Certificadoras;

2. Receção e validação dos pedidos de emissão de certificados realizados pelas Entidades de Certificação (EC`s) Subordinadas bem como os demais subscritores;

3. Emissão de certificados, relativos a pedidos de certificados que estejam de acordo com o formato requerido pelas Entidades de Certificação da SISP;

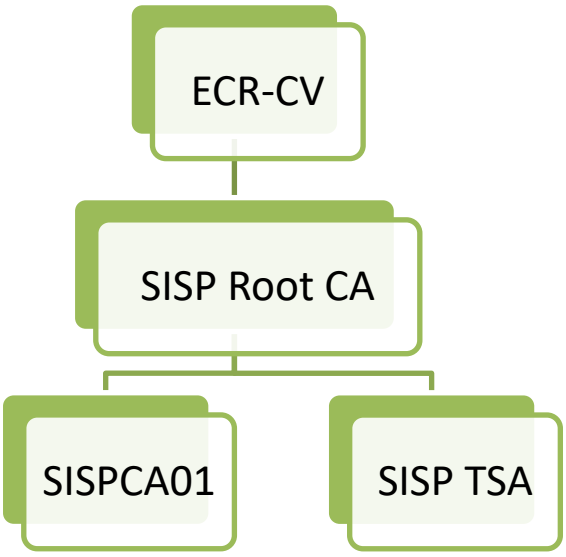
4. Receção e validação dos pedidos de suspensão e revogação de certificados;

5. Publicação dos certificados (quando, onde e se apropriado) e de informação acerca do seu estado;

6. Assegurar a contínua disponibilidade da informação pública, para todos os seus utilizadores;

A PKI da SISP é composta pelas seguintes EC's:

- Entidade Certificadora de Raiz de Cabo Verde (ECR-CV)
- SISP *Root Certification Authority (SISP Root CA)*
- SISP *Certification Authority (SISPCA01)*
- SISP *TimeStamp Certification Authority (SISP TSA)*



4.4.1. SISP ROOT Certification Authority (SISP ROOT CA)

A SISP Root CA insere-se na hierarquia de confiança da ICP-CV, constituindo-se numa entidade de certificação de segundo nível assinada pela Entidade Certificadora de Raiz de Cabo Verde (ECR-CV), estando habilitada apenas a emitir certificados para assinar os certificados das ECs de nível hierárquico imediatamente inferior, conforme lista publicada em http://pki.sisp.cv.

4.4.2. SISP Certification Authority (SISPCA01)

A Entidade Certificadora Subordinada SISPCA01 constitui uma Entidade Certificadora credenciada pela ARME – Agencia de Regulação , conforme a legislação caboverdiana, estando habilitadas, legalmente a emitir todo o tipo de certificado, incluindo certificados qualificados, os de mais elevado grau de segurança previsto na lei.

Encontra-se inserida na hierarquia de confiança da Infraestrtautura de Chaves Publicas de Cabo Verde.

A SISPCA01 pode emitir certificados de,

- Assinatura Qualificada para pessoa singular
- Assinatura Qualificada para representação da pessoa colectiva
- Assinatura Qualificada de Qualidade (Ordens Profissionais)
- Autenticação para pessoa singular e colectiva
- Autenticação *WEB*
- Selo electronico

bem como Validação Online OSCP.

4.4.3. Entidade Certificadora de Validação Cronologica(SISP TSA)

A SISP TSA - Entidade Certificadora de Validação Cronologica é uma entidade certificadora, credenciada pela ARME – Agencia Multisectorial de Regulação Economica e integrante da heirarquia de confiança da SISP, habilitada a emitir todo tipo de selos temporais.

Tem a responsabilidade de fornecer os serviços de selo temporal, que podem ser decompostos em duas componentes:

- Emissão de selos – componente do serviço que gera os selos temporais
- Gestão dos serviços de validação cronológica –componente que monitoriza e controla a operação dos serviços de validação cronológica, de modo a garantir que os mesmos são fornecidos conforme especificado neste documento de práticas e políticas. Esta componente tem a responsabilidade da activação e desactivação do serviço de emissão de selo temporal – por exemplo, para garantir que o relógio, utilizado na emissão do selo temporal, está corretamente sincronizado com o tempo UTC.

Tem ainda a responsabilidade de operar uma ou mais TSU (time-stamping unit) que cria e assina selos temporais em nome da ECVC, cada uma com a sua chave distinta.

INFORMAÇÃO DO CERTIFICADO	
Nome Distinto	C = CV, O = ICP-CV, OU = SISP-Sociedade Interbancaria e Sistemas de Pagamentos, CN = Entidade Certificadora de Validação Cronologica da SISP
Validade	26 de junho de 2025 16:29:25
Thumbprint	e4 6a 80 6b 20 31 83 c6 8a 45 d3 19 e1 b6 60 6b d9 33 91 de
Emissor	CN = Entidade de Certificacao Raiz da SISP 01, OU = SISP-Sociedade Interbancaria e Sistemas de Pagamentos, O = ICP-CV, C = CV

4.4.4. Entidades ou Unidades de Registo

Entidades ou Unidades de Registo são entidades às quais as ECs delegam a prestação de serviços de identificação, registo de utilizadores de certificados, bem como a gestão de pedidos de renovação e revogação de certificados. A SISP poderá actuar como Unidade de Registo e/ou estabelecer acordos com entidades terceiras para que estas desempenham este papel. A lista da Entidades Registo integrantes da PKI da SISP encontra-se publicada em em https://pki.sisp.cv.

4.4.5. Titulares e Subscritores

Pessoa fisica ou colectiva a quem é emitido um certificado/selo temporal enquanto utilizador final.

4.4.6. Responsavel Tecnico

Pessoa a quem é atribuido a responsabilidade pela correcta utilização, protecção e salvaguarda da chave privada de um certificado emitido para um equipamento.

4.4.7. Partes confiantes

As partes confiantes são pessoas singulares ou entidades que confiam no teor, validade e aplicabilidade dos procedimentos utilizados no processo de criação de um selo temporal.

4.4.8. Outros Participantes

4.4.8.1. Autoridade Credenciadora

A Autoridade Credenciadora assume o papel de entidade que disponibiliza serviços de auditoria/inspecção de conformidade, no sentido de aferir se os processos utilizados pela EC nas suas actividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação e nomas vigentes.

Assim, consideram-se como principais atribuições as seguintes:

a) Acreditar as entidades de certificação;

b) Controlar as entidades de certificação;

c) Cobrar taxas pelos serviços de acreditação;

d) Zelar para que as entidades de certificação respondam pelo prejuízo causado a toda entidade, pessoa física ou jurídica que se fie razoavelmente nos certificados;

e) Auditar as entidades de certificação;

f) Zelar para que os dispositivos de segurança de criação de assinaturas electrónicas sejam conformes as condições previstas no artigo 28º do Decreto-lei 33/2007, de 24 de Setembro;

g) Celebrar acordos de reconhecimento mútuo com autoridades de credenciação de países estrangeiros, desde que previamente autorizado pelo departamento governamental responsável pelas comunicações;

h) Manter informações na internet sobre a lista de entidades de certificação, e a suspensão e revogação de certificados digitais, bem como sobre os demais aspectos relevantes da certificação;

i) Definir os requisitos técnicos que qualifiquem a idoneidade de actividades desenvolvidas pelas entidades de certificação;

j) Avaliar as actividades desenvolvidas pelas entidades de certificação autorizadas conforme os requisitos técnicos definidos nos termos da alínea anterior;

k) Zelar pelo adequado funcionamento e eficiente prestação de serviço por parte de entidades de certificação em conformidade com as disposições legais e regulamentares da actividade;

l) O mais que lhe for cometido por lei.

4.4.8.2. Prestadores de Serviços

As entidades que prestam serviços de suporte à PKI da SISP, têm as suas responsabilidades devidamente definidas através de contratos estabelecidos com as mesmas.

4.4.8.3. Auditor de Segurança

Figura independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Credenciadora. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, à Autoridade Credenciadora. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Entidade Credenciadora pode ser encontrada em http://www.pki.ecrcv.cv/.

As Auditorias de conformidade deverão ocorrer, pelo menos, a cada 12 meses, com intuito de confirmar que a SISP, como prestadora qualificada de serviços de confiança e os serviços de confiança que disponibiliza, cumprem os requisitos estabelecidos pelo DR nº18/2007.

4.4.8.4. Fonte de Hora Legal

A hora legal utilizada na validação cronologica é obtida utilizando um equipamento com relógio atomico, dedicado, com cobertura de 12 satelites e nivel de imprecisão de rede entre 1-10 millisegundos e GPS inferior a 1 microsegundo, com referencia a UTC. Utiliza como fonte UTC constante da lista da BIPM, a *USNO – U.S Naval Observatory*.

4.5. Utilização do Selo Temporal

O objetivo dos selos temporais é garantir que um documento (ou ficheiro) existia num determinado momento no tempo. Esta garantia é obtida através da geração de um selo temporal qualificado emitido por uma entidade certificadora credenciada associado ao hash do documento ao qual será feita a aposição do selo temporal.

A associação de um selo temporal ao documento certifica não só a veracidade da hora e data do pedido, mas também a integridade e não repúdio do conteúdo.

4.5.1. Utilização Adequada

Os requisitos e regras definidos neste documento, aplicam-se a todos os selos temporais emitidos pela SISP TSA.

Os selos temporais são emitidos a pedido dos subscritores e de acordo com o RFC 3161 e são também utilizadas pelas Partes Confiantes para validação da associação da data/hora ao datum.

Os selos temporais emitidos pela PKI da SISP devem ser utilizados de acordo com a função e finalidade estabelecida neste documento, nas correspondentes Políticas de Certificados e de acordo com a legislação em vigor.

4.5.2. Utilização Não Autorizada

Os selos temporais emitidos pela PKI da SISP não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela PKI da SISP, não foram desenhados nem está autorizada a sua utilização em actividades de alto risco ou que requeiram uma actividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra actividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

4.6. Gestão das Politicas

A gestão desta DPVC é da responsabilidade do Grupo de Trabalho Segurança, que pode ser contactada pelos telefones e no seguinte endereço:

Nome:	Grupo de Trabalho de Segurança
Morada:	SISP, SA Conj. Habitacional Novo Horizonte, Rua Cidade de Funchal, Achada Santo Antonio – Praia, Cabo Verde
Correio electrónico:	pki@sisp.cv
Site:	https://pki.sisp.cv/
Telefone:	2606310/2626317

A validação desta DPVC (e/ou respetivas PCs) e correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Segurança. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PCs), substituindo qualquer DPC (e/ou respetivas PCs) anteriormente definida.

O Grupo de Trabalho de Segurança deverá ainda determinar quando é que as alterações na DPC (e/ou respetivas PCs) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetivas PCs).

É responsabilidade do Grupo de Trabalho de Auditoria, auditar e determinar a conformidade e aplicação interna desta DPVC (e/ou respetivas PCs), submetendo-a de seguida ao Grupo de Gestão para aprovação.

Todas as politicas, regras e praticas de certificação implementadas no ambito desta DPVC podem ser consultadas no repositorio disponivel em https://pki.sisp.cv.

5. DISPOSIÇÕES LEGAIS

5.1. Obrigações e garantias

De acordo com o previsto no ponto 11.6.

5.2. Responsabilidades de publicação e armazenamento

A SISP mantém um repositório de documentos online onde divulga informação sobre as suas práticas, procedimentos e conteúdo de determinadas políticas, incluindo a DPC. Todas as partes associadas à emissão, utilização ou gestão de certificados da SISP são aqui notificadas de que a mesma pode publicar informação submetida, no seu repositório acessível publicamente, no sentido de disponibilizar informação sobre o estado do certificado digital.

A SISP abstém-se de disponibilizar publicamente informação confidencial, designadamente a relacionada com controlos de segurança, procedimentos, políticas de segurança internas, entre outros.

5.2.1. Repositorios

A SISP S.A. é responsável pelas funções de repositório da SISP TSA, publicando entre outras, informação relativa às práticas adotadas.

O acesso à informação disponibilizada pelo repositório é efetuado através do protocolo HTTPS e HTTP, estando implementado os seguintes mecanismos de segurança:

- A DPVC só pode ser alterada através de processos e procedimentos bem definidos,
- A Plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais atuais de segurança física e lógica,
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

5.2.2. Publicação de Informação

A SISP disponibiliza sempre a seguinte informação pública on-line no URL https://pki.sisp.cv:

- Uma cópia electrónica actualizada desta DPVC;
- Uma copia electronica actualizada da respectiva politica e

outra informação relevante que inclui,

Descrição de comprometimento ou suspeita de comprometimento da chave privada de assinaturados selos temporais, assim como perda de calibração UTC do(s) relógio(s) utilizado(s),

Informação que permita identificar os selos temporais que podem ter sido afetadas, em caso de comprometimento das operações da SISP TSA ou perda de calibração UTC do(s) relógio(s) utilizado(s).

Adicionalmente serão conservadas todas as versões anteriores das DPVC's da SISP TSA, disponibilizando-as a quem as solicite (desde que justificado), ficando, no entanto fora do repositório público de acesso livre.

A SISP garante que as actualizações a esta DPVC e respectivas políticas serão publicadas sempre que houver necessidade de se proceder a uma alteração.

A informação publicada pela SISP estará disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura). A SISP implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

5.3. Auditoria de conformidade

Uma inspeção regular de conformidade a esta DPVC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria da PKI da SISP.

Para além de auditorias de conformidade, a SISP irá efetuar outras fiscalizações e investigações para assegurar a conformidade da Entidades de Certificação constituintes da PKI da SISP com a legislação

nacional bem como com os normativos internacionais aplicáveis. A execução destas auditorias internas, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

As práticas de certificação da SISP são alvo de auditorias periódicas, que terão como mínimo a periodicidade estipulada na lei, ou seja, uma periodicidade anual com a emissão de um relatório à data de 31 de Março do ano civil em causa. Esta auditoria será realizada por um Auditor credencido pela ANAC.-Esta auditoria é realizada tomando como base as normas existentes para o efeito sendo os seus resultados comunicados à entidade credenciadora que poderá tornar público o resultado de todo o processo.

6. VALIDAÇÃO CRONOLÓGICA

6.1. Emissão Selo Temporal

A SISP TSA garante que os selos temporais são emitidos de forma segura, com a hora/data correta e que contem os seguintes parametros:

- O identificador da politica de validação cronologica
- O identificador único do selo temporal
- Os valores de hora/data (*timestamp)*
- O *hash* criptografico dos dados com o timestamp
- O certificado gerado com a chave privada usada pela ECVC
- Um nivel de precisão minimo de 1 segundo relativamente à UTC, cuja sincronização do relogio encontra-se descrito no ponto 4.4.8.4.

Se for detetado que o relógio fornecedor do tempo a incluir no selo temporal não está dentro da precisão indicada, o selo não será emitido, sendo que a ECVC devolverá um erro indicando que a fonte de tempo não está disponível.

6.2. Sincronização do Relogio

A SISP garante que o(s) relógio(s) que fornece a hora/data a incluir no selo temporal está sincronizada com o tempo UTC, com a precisão indicada. Em particular:

- A calibração do relógio é mantida dentro da precisão definida;
- O relógio está protegido contra ameaças que possam resultar numa alteração, não detetada, ao relógio que tenha como resultado uma alteração à precisão definida;
- São detetadas as situações em que o tempo indicado no selo temporal contêm desvios para a precisão definida;
- A sincronização do relógio é mantida quando é introduzido um segundo intercalar, de acordo com o notificado pelo laboratório identificado na secção 4.4.8.4.

6.3. Processamento do pedido de Selo Temporal

O processamento do pedido de selo temporal, efectuada pelo subscritor, é satisfeito de imediato pela ECVC, de acordo com os limites indicados neste documento.

Em caso de comprometimento ou suspeita de comprometimento da chave privada ou perca de calibração da TSU, a emissão de selos temporais será suspensa até que a normalidade das

operações seja reposta.

7. MEDIDAS DE SEGURANÇA FISICA, DE GESTÃO E OPERACIONAIS

A SISP implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nesta DPVC.

Estas regras e policticas seguem as boas praticas recomendadas pelos principais *standards* interncaionais relativos á segurança de informação, designadamente ISO 27001.

7.1. Medidas de segurança física

7.1.1. Localização física e tipo de construção

As instalações da PKI da SISP foram desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas do acesso não autorizado, dano, ou interferência. A arquitetura utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior.

7.1.2. Acesso físico ao local

Os sistemas da *PKI* da SISP estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

Atividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. Acessos físicos são automaticamente registados e gravados para efeitos de auditorias.

7.1.3. Energia e ar condicionado

O ambiente seguro do *PKI* da SISP possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

- Alimentação de energia garantindo alimentação contínua ininterrupta com a potência suficiente para manter autonomamente a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de eletricidade a diesel);

- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente.

7.1.4. Exposição à água

Nada a assinalar.

7.1.5. Prevenção e proteção contra incêndio

O ambiente seguro do *PKI* da SISP tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança;
- Equipamento fixo e móvel de extinção de incêndios estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
- Procedimentos de emergência bem definidos, em caso de incêndio.

7.1.6. Salvaguarda de suportes de armazenamento

Todos os suportes de informação sensível são guardados em cofres e armários de segurança dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho.

7.1.7. Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível são triturados antes da sua eliminação.

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível, antes dos mesmos serem eliminados. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação.

Outros equipamentos de armazenamento (discos rígidos, tapes, ...) são devidamente limpos de modo a não ser possível recuperar nenhuma..

7.1.8. Instalações externas (alternativa) para recuperação de segurança

As instalações alternativas têm os mesmos níveis de segurança do principal.

7.2. Medida de segurança dos processos

A atividade de uma Entidade Certificadora (doravante denominada por EC) depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC é vital garantir uma

adequada segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes;

- É necessário garantir que a EC apenas poderá ser sujeita a ataques do tipo denial-of-service mediante o conluio de um número significativo de intervenientes;
- Quando uma mesma entidade é detentora de várias EC de diferentes níveis de segurança ou hierarquia, por vezes é desejável que os recursos humanos associados a uma EC não acumulem funções (ou pelo menos as mesmas) numa EC distinta.

Pelo exposto, nesta secção, descrevem-se os requisitos necessários para reconhecer os papéis de confiança e responsabilidades associadas a cada um desses papéis. Esta secção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

7.2.1. Grupos de Trabalho

Definem-se como pessoas autenticadas todos os colaboradoras, fornecedores e consultores que tenham acesso ou que controlem operações criptográficas ou de autenticação.

A *PKI* da SISP estabeleceu que os papéis de confiança fossem agrupados em seis categorias diferentes (que correspondem a cinco Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticados, eventualmente pertencentes a diferentes Grupos de Trabalho, assegurando que existem dois membros em cada grupo

7.2.1.1 Grupo de Trabalho de Auditoria

É responsável por efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade da EC..

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
- Registar todas as operações sensíveis;
- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;
- Verificar periódicamente, a integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respectivos e que estão devidamente identificados;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Assumir o papel de “Auditor de Sistema”;
- Validar que todos os recursos utilizados são seguros.

7.2.1.2 Grupo de Segurança

O Grupo de Trabalho de Administração de Segurança é responsável por propor, gerir e implementar todas as políticas da EC, assegurando que se encontram actualizadas, e garantir que toda a informação indispensável ao funcionamento e auditoria da EC se encontra disponível ao

longo do tempo. O Grupo de Trabalho de Administração de Segurança assume também a função de Operação de HSM.

Contsituem responsabilidades deste grupo:

- Gerir o Ambiente de Administração de Segurança;
- Definir e gerir todas as políticas da EC e garantir que se encontram actualizadas e adaptadas à sua realidade;
- Garantir implementação das políticas definidas;
- Assegurar que as PCs da EC são suportadas pela DPC da EC;
- Assegurar que todos os documentos relevantes e relacionados, directa ou indirectamente, com o funcionamento da EC e existentes em formato papel se encontram armazenados no Ambiente de Informação;
- Gerir e controlar os sistemas de segurança física, incluindo acessos, do ambiente de produção;
- Explicar todos os mecanismos de segurança aos funcionários que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de seguranças estabelecidas;
- Calendarizar cerimónias para testes, formações e auditoria dos sistemas de informação;
- Configurar os acessos à aplicação da EC (grupos, regras, logs);
- Configurar perfis de certificados na aplicação da EC;
- Activar a interface de operação da EC;
- Activar as chaves para sua utilização;
- Autorizar a geração de chaves da aplicação. Esta operação é requerida durante a cerimónia de geração de chaves para a EC;
- Arranque do interface de configuração da SISP ROOT CA.

Adicionalmente na função de administração/operação de HSM

- Recuperação da funcionalidade do hardware criptográfico em caso de falha de um HSM;
- Recuperação de chaves em caso de terem sido apagadas acidentalmente;
- Substituição de um conjunto de cartões de administrador. Esta operação só é necessária ser realizada se se deseja ampliar ou reduzir o número de cartões de administrador;
- Substituição de um conjunto de cartões de operador. Esta operação só é necessaria se deseja ampliar ou reduzir o número de cartões de operador ou substituir algum cartão deteriorado;
- Ampliação do número de HSM integrados na infraestrutura;
- Dado que se opera em modo FIPS140-2 Nível 3, autorização para a geração de conjuntos de cartões de operador e chaves. Esta operação só se requere durante a cerimónia de geração de chaves da EC.
- Ativação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção dos cartões de operadores associados às chaves;
- Autorização para a geração de chaves da aplicação. Esta operação só é requerida durante a cerimónia de geração de chaves para a EC;
- Arranque do interface de configuração da EC e do resto das entidades que formam a PKI.

7.2.1.3 Grupo de Administração de Sistemas

O Grupo de Trabalho de Administração de Sistemas é responsável por instalar, configurar e fazer a manutenção (*hardware e software*) da EC, sem afectar a segurança da aplicação.

As responsabilidades deste grupo são:

- Manter um inventário actualizado de todos os produtos relacionados com a EC;
- Instalar, interligar e configurar o *hardware* da EC;
- Instalar e configurar o *software* de base da EC;
- Gerir e actualizar os produtos instalados;
- Preparar comunicados sobre as palavras-chave iniciais;
- Preparar comunicados sobre as Hash do(s) CD(s) de instalação utilizados.

Adicionalmente, compete ao Grupo

- Operar diariamente os sistemas, realizando cópias de segurança e reposição de informação, caso necessário;
- Realizar as tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas;
- Gerir o Ambiente de Operação.

7.2.1.4 Grupo de Registos

O Grupo de Trabalho de Administração de Registo é responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC assim como todos os incidentes sucedidos. Também é missão deste grupo operar a EC no que diz respeito à emissão, suspensão e revogação de certificados.

As responsabilidades deste grupo são emitir, suspender e revogar certificados.

7.2.1.4 Grupo de Gestão

É responsável pela nomeação dos membros dos restantes grupos e pela tomada de decisões de nível crítico para a EC. Este grupo deve ser constituído por um mínimo de 4 (quatro) membros.

As responsabilidades deste grupo são:

- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Administração de Segurança;
- Pedir a aprovação de Políticas ao CG da ICP-CV;
- Designar os membros dos restantes grupos de trabalho;
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados.

7.2.2. Número de pessoas exigidas por tarefa

Existem rigorosos procedimentos de controlo que obrigam à divisão de responsabilidades baseada nas especificidades de cada Grupo de Trabalho, e de modo a garantir que tarefas sensíveis apenas podem ser executadas por um conjunto múltiplo de pessoas autenticadas.

Os procedimentos de controlo interno foram elaborados de modo a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança. O acesso ao hardware criptográfico da EC segue procedimentos estritos envolvendo múltiplos indivíduos autorizados a aceder-lhe durante o seu ciclo de vida, desde a receção e inspeção até à destruição física e/ou lógica do hardware. Após a ativação de um módulo com chaves operacionais, controlos adicionais de acesso são utilizados de modo a garantir que os acessos físicos e lógicos ao hardware só são possíveis com 2 ou mais indivíduos autenticados. Indivíduos com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

7.2.3. Funções que requerem separação de responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por X) entre a pertença ao grupo/subgrupo identificado na coluna esquerda e a pertença ao grupo/subgrupo identificado na primeira linha, no contexto desta EC:

Grupo de Trabalho	Incompativel com				
	(a)	(b)	(c)	(d)	(e)
Administração de Segurança (a)		X	X	X	
Administração de Sistemas (b)	X		X	X	
Administração de Registo (c)	X	X		X	
Auditoria (d)	X	X	X		X
Gestão (e)				X	

7.3. Medidas de Segurança de Pessoal

7.3.1. Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Todo o pessoal que desempenhe funções de confiança na PKI da SISP deve cumprir os seguintes requisitos:

- Ter sido nomeado formalmente para a função a desempenhar;
- Apresentar provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas inerentes à sua função;
- Ter recebido formação e treino adequado para o desempenho da respetiva função;
- Garantir confidencialidade, relativamente a informação sensível sobre a EC ou dados de identificação dos titulares;
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função e,
- Garantir que não desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

7.3.2. Procedimento de verificação de antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

- Confirmação de identificação, usando documentação emitida por fontes fiáveis e,
- Investigação de registos criminais.

7.3.3. Requisitos de formação e treino

É ministrado aos membros dos Grupos de Trabalho formação e treino adequado de modo a realizarem as suas tarefas, satisfatória e competentemente.
Os elementos dos Grupos de Trabalho, estão adicionalmente sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

- Certificação digital e Infraestruturas de Chave Pública;
- Conceitos gerais sobre segurança da informação;
- Formação específica para o seu papel dentro do Grupo de Trabalho;
- Funcionamento do software e/ou hardware usado na PKI da SISP;
- Política de Certificados e Declaração de Práticas de Certificação;
- Recuperação face a desastres;
- Procedimentos para a continuidade da atividade e,
- Aspetos legais básicos relativos à prestação de serviços de certificação.

7.3.4. Frequência e requisitos para ações de reciclagem

Sempre que necessário será ministrado treino e formação complementar aos membros dos Grupos de Trabalho, de modo a garantir o nível pretendido de profissionalismo para a execução competente e satisfatória das suas responsabilidades. Em particular,

- Sempre que exista qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto à PKI da SISP;
- Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos da PKI da SISP.

7.3.5. Frequência e sequência da rotação de funções

Nada a assinalar.

7.3.6. Sanções para ações não autorizadas

Consideram-se ações não autorizadas todas as ações que desrespeitem a Declaração de Práticas de Certificação e as Políticas de Certificação, quer sejam realizadas de forma deliberada ou sejam ocasionadas por negligência.

São aplicadas sanções de acordo com as regras da PKI da SISP e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

7.3.7. Requisitos para prestadores de serviços

Consultores ou prestadores de serviços independentes, tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho e ficando o seu acesso registado no Livro de Presenças próprio.

7.3.8. Documentação fornecida ao pessoal

É disponibilizado aos membros dos Grupos de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas de modo competente e satisfatório.

7.4. Procedimentos de auditoria de segurança

7.4.1. Tipo de eventos registados

Eventos significativos geram registos auditáveis. Estes incluem, pelo menos os seguintes:

- Geração de par de chaves de assinatura para as TSU;
- Pedido de emissão, suspensão e revogação de certificados para as TSU;
- Sincronização UTC do(s) relógio(s);
- Tentativas de acesso (com e sem sucesso) a recursos criticos
- Arranque e paragem de aplicações;
- Cópias de segurança, recuperação ou arquivo dos dados;
- Alterações ou atualizações de software e hardware;
- Manutenção dos sistemas;
- Operações realizadas por membros dos Grupos de Trabalho;
- Alteração de Recursos Humanos;
- Tentativas de acesso (com e sem sucesso) às instalações por parte de pessoal autorizado ou não;

7.4.2. Frequência da auditoria de registos

Os registos são analisados e revistos na base diária e de forma automatizada, produzindo o envio de alertas para o grupo de trabalho de Auditoria, sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas, baseadas na informação dos registos são também documentadas.

7.4.3. Período de retenção dos registos de auditoria

Os registos estão disponíveis online durante o período de validade da certificação, findo o qual são arquivados nos termos descritos na secção7.5.

7.4.4. Proteção dos registos de auditoria

Os registos são analisados exclusivamente por membros do Grupo de Trabalho de Auditoria e reportados ao Grupo de Gestão.

Os registos são protegidos por mecanismos eletrónicos auditáveis de modo a detetar e impedir a ocorrência de tentativas de modificação, remoção ou outros esquemas de manipulação não autorizada dos dados.

As cópias de segurança dos registos da PKI da SISP são armazenadas em local seguro e em cofres que cumprem a norma EN 1143.

A destruição de um arquivo de auditoria em offline só poderá ser efetuada após autorização expressa do Grupo de Gestão e executada na presença de, no mínimo dois elementos, um elemento de segurança e um de auditoria, sendo que este ato deverá ficar registado em log de Auditoria.

7.4.5. Procedimentos para a cópia de segurança dos registos

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade, nomeadamente em tape e em storage.

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

O processo de tratamento e recolha de registos de auditoria é constituído por uma combinação de processos automáticos e manuais, executados pelos sistemas operativos, pelas aplicações da PKI da SISP e pelo pessoal que as opera. Todos os registos de auditoria são armazenados nos sistemas internos da *PKI* da SISP.

7.4.7. Notificação de agentes causadores de eventos

Eventos auditáveis, são registados no sistema de auditoria e guardados de modo seguro, sem haver notificação ao sujeito causador da ocorrência do evento.

7.4.8. Avaliação de vulnerabilidades

Os registos auditáveis, são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebrar a segurança do sistema. São realizados quatro testes de intrusão por ano, de forma a verificar e avaliar vulnerabilidades. O resultado da análise é reportado ao Grupo de Gestão da *PKI* da SISP para rever e aprovar um plano de implementação e correção das vulnerabilidades detetadas.

7.5. Arquivo de registos

7.5.1. Tipo de dados arquivados

Todos os dados auditáveis, são arquivados (conforme indicado na secção 7.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

7.5.2. Período de retenção em arquivo

Os dados sujeitos a arquivo são retidos pelo período de tempo definido pela legislação nacional.

7.5.3. Proteção dos arquivos

O arquivo é protegido de modo a que:

- Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo;
- arquivo é protegido contra qualquer modificação ou tentativa de o remover;
- arquivo é protegido contra a deterioração dos media onde é guardado, através de migração periódica para media novo;
- arquivo é protegido contra a obsolescência do hardware, sistemas operativos e outros software, pela conservação do hardware, sistemas operativos e outros software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal;
- Os arquivos são guardados de modo seguro em ambientes externos seguros, de acordo com a Politica de Retenção de Dados. As cópias de segurança da PKI da SISP são armazenadas em locais seguros e em cofres que cumprem a norma EN 1143.

7.5.4. Procedimentos para as cópias de segurança do arquivo

Cópias de segurança dos arquivos são efetuadas de modo incremental ou total e guardados em dispositivos *WORM (Write Once Read Many*).

7.5.5. Requisitos para validação cronológica dos registos

Algumas das entradas dos arquivos contêm informação de data e hora, que é prestado por um serviço preciso de referência temporal.

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

Os sistemas de recolha de dados de arquivo são internos.

7.5.7. Procedimentos de recuperação e verificação de informação arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade.

São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, deve-se realizar novo arquivo.

7.6. Recuperação em caso de desastre ou comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

7.6.1. Procedimentos em caso de incidente ou comprometimento

Em caso de comprometimento ou suspeita de comprometimento de uma chave de assinatura da TSU, são efetuados os seguintes passos:

- A TSU afetada é desligada;
- O certificado associado é imediatamente revogado; A chave privada é destruída;
- É gerado um novo par de chaves;
- É pedido a emissão de um novo certificado à SISP ROOT CA
- A TSU é inicializada com a utilização do novo par de chaves.

Em caso de perda de sincronismo UTC do relógio da TSU, a TSU será activada, sendo reactivada a partirdo momento em que a situação normal seja reposta.

Para outro tipo de incidente, o mesmo será analisado pelo Grupo de Trabalho adequado, sendo implementadas as medidas que garantam a segurança do serviço de Validação Cronológica, a continuidade da disponibilidade do serviço e a integridade dos selos temporais.

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

No caso dos recursos informáticos, software e/ou dados estarem corrompidos ou existir suspeita de corrupção, as cópias de segurança da chave privada da EC e os registos arquivados podem ser obtidos para verificação da integridade dos dados originais.

Se for confirmado que os recursos informáticos, software e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a SISP TSA suspenderá os seus serviços e notificará todas as Entidades envolvidas.

7.6.3. Capacidade de continuidade da atividade em caso de desastre

A PKI da SISP dispõe dos recursos de computação, software, cópias de segurança e registos arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar operações essenciais (emissão de selos temporais e disponibilização de informação ncessaria para a sua validação).

7.7. Procedimentos em caso de extinção da ECVC

Em caso de cessação de atividade como prestador de serviços de Certificação, a SISP executa os procedimentos previstos no Plano de Cessação de Actividades, conforme artigo 36º do DL nº33/2007.

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da ECVC, esta deve informar de tal facto à Autoridade Credenciadora Nacional e ao Conselho Gestor da IPC-CV.

8. MEDIDAS DE SEGURANÇA TECNICAS

Esta secção define as medidas de segurança implementadas pela *PKI* da SISP para a SISP TSA, de forma a proteger chaves criptográficas geradas por esta e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras assim como dados de ativação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

8.1. Gestão do ciclo de vida do par de chaves

A geração dos pares de chaves da SISP TSA é processada de acordo com os requisitos e algoritmos definidos nesta política.

A geração de chaves criptográficas da SISP TSA é feito por um Grupo de Trabalho, composto por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com procedimentos escritos das operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos no Grupo de Trabalho.

O hardware criptográfico, usado para a geração de chaves da SISP TSA, cumpre os requisitos FIPS 140-2 nível 3 e/ou Common Criteria EAL 4+ e, efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o hardware. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando hardware, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perca de dados, possa haver uma recuperação total e segura das chaves.

A geração do par de chaves da SISP TSA é efetuada por elementos autorizados dos Grupos de trabalho num hardware criptográfico que cumpre os requisitos FIPS 140-2 nível 3 e/ou Common Criteria EAL 4+.

8.1.1. Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão das chaves da SISP TSA utilizada para assinatura dos selos temporais é de 4096 bits RSA.

8.1.2. Geração dos parâmetros da chave pública e verificação da qualidade

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo.

As chaves são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#1.

8.1.3. Algoritmo de assinatura do selo temporal

A assinatura do selo temporal utiliza a função de hash SHA-256 e o algoritmo de assinatura RSA, denominado por sha256withRSA.

8.2. Proteção da chave privada e caraterísticas do módulo criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada e para os módulos criptográficos da SISP TSA. A PKI da SISP implementou uma combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas de assinatuura do selos temporais da SISP TSA.

8.2.1. Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da SISP TSA assim como para o armazenamento das chaves privadas de assinatura do selos temporais, a PKI da SISP utiliza módulo criptográfico em hardware que cumpre as seguintes normas:

- Segurança Física
  - Common Criteria EAL 4+ e/ou
  - FIPS 140-2, nível 3
- Autenticação
  - Autenticação dois factores.

8.2.2. Gestão do ciclo de vida do modulo criptografico

A *PKI* da SISP implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efetuar operações criptográficas sensíveis na EC.

Todas as operações são efetuadas com um mínimo de dois elementos em funções qualificadas dentro da entidade e em tarefa distinta.

Na prática, são empregues nas diversas funções, pelo menos dois elementos (N=2), entre o conjunto total de pessoas com funções atribuídas dentro da entidade (M=staff).

As chaves privadas da *PKI* da SISP encontram-se na posse de mais que um elemento. Esta é ativada mediante a inicialização do software da EC por meio de uma combinação de operadores da SISP TSA e administradores do HSM. Este é o único método de activação da chave privada.

8.2.3. Cópia de segurança da chave privada

A SISP não efectua cópia de segurança das chaves privadas da SISP TSA utilizadas para assinatura de selos temporais.

8.2.4. Processo para ativação da chave privada

A SISP TSA encontra-se online, e a chave privada da TSU é activada quando so sitema é ligado. Esta activação é efectivada através da autenticação no modulo criptografico dos administradores de HSM, sendo obrigatorio a autenticação utilizando dois factores. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

8.2.5. Processo para desativação da chave privada

A chave privada de assinatura da TSU é desativada quando o sistema é desligado. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

8.2.6. Processo para destruição da chave privada

As chaves privadas da SISP TSA são apagadas/destruídas num procedimento devidamente identificado e auditado no mínimo 30 dias após terminada a sua data de validade (ou se revogadas antes deste período).

A PKI da SISP procede à destruição das chaves privadas garantindo que não restarão resíduos destas que possam permitir a sua reconstrução. Para tal, utiliza a função de formatação (inicialização a zeros) disponibilizada pelo hardware criptográfico ou outros meios apropriados, de forma a garantir a total destruição das chaves privadas da EC.

8.3. Outros aspetos da gestão do par de chaves

8.3.1. Arquivo da chave pública

É efectuada uma cópia de segurança de todas as chaves públicas da SISP TSA, permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas dos selos temporais gerados durante seu prazo de validade.

8.3.2. Períodos de validade do certificado e das chaves

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.

Neste sentido a validade dos certificados de validação cronologica e o período em que os mesmos devem ser renovados, é o seguinte:

− Validade maxima de 5 anos e 4 meses.

8.3.3. Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que é gerado um novo par de chaves e submetido o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito da SISP TSA, é designado por renovação de certificado com geração de novo par de chaves

8.4. Medidas de segurança informáticas

8.4.1. Requisitos técnicos específicos

O acesso aos servidores da SISP TSA é restrito aos membros dos Grupos de Trabalho devidamente autorizados. A SISP TSA tem funcionamento online, sendo o pedido de emissão de selos temporais efectudo pelos subscritores.

A ECVC dispõe de mecanismos de protecção e segurança(firewalls) que cumprem os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

8.4.2. Avaliação/nível de segurança

Os vários sistemas e produtos empregues pela SISP TSA são fiáveis e protegidos contra modificações. O módulo criptográfico em Hardware da SISP TSA satisfaz a norma EAL 4+ Common Criteria for Information Technology Security Evaluation e/ou FIPS 140-2 nível 3.

8.5. Ciclo de vida das medidas técnicas de segurança

8.5.1. Medidas de desenvolvimento do sistema

As aplicações são desenvolvidas e implementadas por terceiros de acordo com as suas regras de desenvolvimento de sistemas e de gestão de mudanças.

É fornecida metodologia auditável que permite verificar que o software da SISP TSA não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do software são executadas e auditadas por membros dos Grupos de Trabalho da PKI da SISP.

8.5.2. Medidas para a gestão da segurança

A PKI da SISP tem mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas da ECVC. O sistema da SISP TSA, quando utilizado pela primeira vez, será verificado para garantir que o software utilizado é fidedigno e legal e que não foi alterado depois da sua instalação.

8.5.3. Ciclo de vida das medidas de segurança

As operações de atualização e manutenção dos produtos e sistemas da ECVC da SISP, seguem o mesmo controlo que o equipamento original e é instalado pelos membros do Grupo de Trabalho com adequada formação para o efeito, seguindo os procedimentos definidos para o efeito.

8.6. Medidas de segurança da rede

A ECVC dispõe de mecanismos de protecção e segurança(firewalls) que cumprem os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

9. VERIFICAÇÃO DE SELOS TEMPORAIS

O selo temporal é assinado digitalmente pela TSU da SISP TSA, por um certificado digital com um mínimo de cinco anos de validade. Durante o período de validade do certificado da TSU, a validade da chave privada de assinatura pode ser verificada através do estado de revogação do certificado da TSU, via CRL e/ou OCSP disponibilizada pela SISP TSA.

10. AUDITORIA E AVALIAÇÕES DE CONFORMIDADE

Uma inspeção regular de conformidade a esta DPVC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria da PKI da SISP.

Para além de auditorias de conformidade, a SISP irá efetuar outras fiscalizações e investigações para assegurar a conformidade da Entidades de Certificação constituintes da PKI da SISP com a legislação nacional bem como com os normativos internacionais aplicáveis. A execução destas auditorias internas, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

10.1. Frequência ou motivo da auditoria

As auditorias de conformidade são realizadas regularmente de acordo com a legislação, por um Auditor Externo credencido pela ARME e tem como base as normas existentes para o efeito sendo os seus resultados comunicados à entidade credenciadora que poderá tornar público o resultado de todo o processo.

10.2. Identidade e qualificações do auditor

O auditor é uma figura independente do círculo de influência da Entidade Certificadora de Validação Cronologica, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infra-estruturas de chaves públicas, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança. A sua missão é auditar a infra-estrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, em Março, à Autoridade Credenciadora.

A ARME enquanto Autoridade Credenciadora é responsável pela credenciação do Auditor de Segurança, de acordo com os requisitos e qualificações identificados na legislação aplicavel em vigor. A lista dos auditores de segurança credenciados pode ser consultada no site da ICP-CV.

10.3. Relação entre o Auditor e a Entidade Certificadora

Na sua actuação, o auditor e membros da sua equipa são independentes, em relação à entidade auditada não devendo existir qualquer vinculo de natureza contratual ou de qualquer outro género que possa originar um conflito de interesses.
O Auditor está obrigado ao cumprimento do estabelecido na legislação em vigor no que se reefre à protecção de dados pessoais, a que tiver acesso durante o exercicio das suas funções, designadamente dados pessoais dos subscritores.

10.4. Âmbito da auditoria

As auditorias de segurança são efectuadas com base nas politicas de certificação definidas na presente DPVC em conformidade com a legislação nacional em vigor e demais normas tecnicas, processos e procedimentos.

10.5. Procedimentos após uma auditoria não conforme

Se durante uma auditoria forem detectadas irregularidades, o auditor procede da seguinte forma:

a) Documenta todas as deficiências encontradas durante a auditoria;
b) No final da auditoria, reúne com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões (RPI);
c) Elabora o relatório de auditoria. Este relatório deverá estar organizado de modo a que todas as deficiências sejam escalonadas por ordem decrescente de gravidade/severidade;
d) Submete o relatório de auditoria à Autoridade Credenciadora para apreciação;
e) Depois de apreciado e consolidado, é remetida uma cópia do relatório de auditoria final (RAF), para a entidade;
f) Tendo em conta a irregularidades constantes no relatório, a entidade submetida à auditoria enviará uma relatório de correção de irregularidades (RCI), para a Autoridade Credenciadora, no qual deve estar descrito quais as ações, metodologia e tempo necessário para corrigir as irregularidades encontradas;
g) A Autoridade Credenciadora depois de analisar este relatório toma uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:
    a. Aceita os termos, permitindo que a actividade seja desenvolvida até à próxima inspecção;
    b. Permite que a entidade continue em actividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;
    c. Revoga imediatamente a actividade.

11.OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção aborda aspectos de negócio e assuntos legais.

11.1. Taxas

Poderão ser cobradas taxas de emissão e/ou reemissão de selos temporais. O acesso á informação sobre o estado(OCSP) ou lista de revogação de certificados(CRL) é gratuita. Em caso de revogação de certificados não se prevê o reembolso de valores e taxas.

11.2. Responsabilidade financeira

A ECVC SISP TSA dispõe de um seguro obrigratorio de responsabilidade civil , conforme artigo 45.º do Decreto-Lei n.º 33/2007, de 24 de Setembro.

11.3. Confidencialidade da informação processada

Declara-se expressamente como informação confidencial aquela que não poderá ser divulgada a terceiros sem autorização explícita. Esta informação está sob custódia e só os Grupos de Trabalho devidadamente autorizados têm acesso.

Considera-se informação de acesso público:

- Política de Certificados;
- Declaração de Práticas de Certificação;
- LCR

e toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

A SISP permite o acesso a informação não confidencial sem prejuízo de controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito da SISP.

A coordenação desta responsabilidade é feita pelo CISO. Em caso de quebra de confiança, deverá ser contactado o CISO pelo email ciso@sisp.cv.

11.4. Privacidade dos dados pessoais

A SISP é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação caboverdiana.

É considerada informação privada toda a informação fornecida pelo subscritor, que não seja disponibilizada no selo temporal.

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo subscritor e sobre o qual este indica uma opção de processamento.

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 caboverdeana.

11.5. Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem aos selos temporais, CRL, OID, DPVC e PC, bem como qualquer outro documento, propriedade da PKI da SISP pertence à SISP S.A.

11.6. Representações e garantias

A ECVC da SISP está obrigada a:

a) Realizar as suas operações de acordo com esta Declaração de Práticas,
b) Declarar de forma clara todas as suas Práticas de Validação Cronológica no documento apropriado,
c) Proteger as suas chaves privadas de assinatura de selos temporais,
d) Emitir selos temporais de acordo com o RFC 3161,

e) Emitir selos temporais que estejam conformes com os dados de pedido de selo temporal fornecidos pelo subscritor,
f) Garantir a fiabilidade do processo de geração do selo temporal e da sua entrega ao subscritor,
g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de emissão de selos temporais,
h) Empregar pessoal com qualificações, conhecimento e experiência necessárias para a prestação de serviços de certificação,
i) Publicar a sua DPVC e as Políticas aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores,
j) Colaborar com as auditorias dirigidas pela Autoridade Credenciadora,
k) Operar de acordo com a legislação aplicável,
l) Notificar Autoridade Credenciadora com pelo menos três meses da antecendencia, em caso de cessação de actividade
m) Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais.

É obrigação dos subscritores dos selos temporais:

a) Limitar e adequar a utilização dos selos temporais de acordo com a legislação vigente e com o presente documento,
b) Efetuar o pedido de emissão de selos temporais de acordo com o RFC 3161,
c) Aquando da receção do selo temporal pedido, verificar que o selo temporal foi corretamente assinada pela ECVC SISP TSA,
d) Aquando da receção do selo temporal pedido, verificar que a chave privada utilizada para o assinar é válida (i.e., não foi comprometida),
e) 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 SISP TSA.

É obrigação das partes confiantes dos selos temporais emitidas pela ECVC da SISP:

a) Limitar a fiabilidade dos selos temporais às utilizações permitidas para os mesmos em conformidade com a legislação vigente e com o presente documento,
b) Verificar que o selo temporal foi corretamente assinado,
c) Verificar que a chave privada utilizada para assinar o selo temporal não foi comprometida
d) Assumir a responsabilidade na correta verificação dos selos temporais,
e) Notificar qualquer acontecimento ou situação anómala relativa ao selo temporal, utilizando os meios que a SISP TSA disponibilize para o efeito.

Cabe às fontes legais de tempo utilizadas pela ECVC da SISP:

a) Garantir o acesso ininterrupto à hora fornecida,
b) Garantir a disponibilização de mecanismos que possibilitem o sincronismo entre o seu relógio e o relógio utilizado na emissão de selos temporais,
c) Notificar qualquer acontecimento ou situação anómala.

11.7. Renúnica a garantias

A ECVC SISP TSA recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPVC.

11.8. Limitações às obrigações

A SISP TSA:

- Responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 62 do DL 33/2007, de 24 de Setembro;
- Assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação;
- A responsabilidade da administração / gestão da SISP TSA assenta sobre base objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;
- Só responde pelos danos e prejuízos causados pelo uso indevido do selo temporal reconhecido, quando não tenha consignado no selo temporal, de forma clara reconhecida por terceiros o limite quanto ao possível uso;
- Não responde quando o subscritor superar os limites que figuram neste documento quanto às possíveis utilizações do selo temporal;
- Não assume qualquer responsabilidade no caso de perca ou prejuízo:
    - Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    - Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Politica de Certificados e correspondente DPVC;
    - Ocasionado pelo uso indevido ou fraudulento dos selos temporais emitidos pela SISP TSA.

11.9. Indemnizações

De acordo com a ligislação em vigor.

11.10. Termo e cessação de actividade

Os documentos relacionados com a PKI da SISP (incluindo esta DPVC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão e apenas são eliminados ou alterados por sua ordem.

Esta DPVC entra em vigor desde o momento de sua publicação no repositório da PKI da SISP.

Esta DPVC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão.

O Grupo de Trabalho de Gestão pode decidir em favor da eliminação ou emenda de um documento relacionado com a PKI da SISP (incluindo esta DPVC) quando:

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

- Os seus conteúdos foram comprometidos.

Nesse caso, o documento eliminado será substituído por uma nova versão.

Esta DPVC 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 DPVC ficar revogada será retirada do repositório público, garantindo-se contudo que será conservada durante o periodo previsto na legislação em vigor.

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

11.11. Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar métodos razoáveis para comunicar uns com os outros. Esses métodos podem incluir correio eletrónico assinado digitalmente, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

11.12. Alterações

No sentido de alterar este documento ou alguma das políticas de certificado, é necessário submeter um pedido formal ao Grupo de Trabalho de Segurança, indicando (pelo menos):

- A identificação da pessoa que submeteu o pedido de alteração;
- A razão do pedido;
- As alterações pedidas.

O Grupo de Trabalho de Segurança vai rever o pedido feito e, se verificar a sua pertinência, procede às atualizações necessárias ao documento, resultando numa nova versão de rascunho do documento. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho e às partes afetadas (se alguma) para permitir o seu escrutínio. Contando a partir da data de disponibilização, as várias partes têm 15 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho de Segurança tem mais 15 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento, após o que o documento é aprovado e fornecido Grupo de Trabalho de Gestão para validação, aprovação e publicação, tornando-se as alterações finais e efetivas.

No caso que o Grupo de Trabalho de Gestão julgue que as alterações à especificação podem afetar a aceitabilidade dos selos temporais para propósitos específicos, comunicar-se-á aos utilizadores que se efetuou uma mudança e que devem consultar a nova DPVC no repositório estabelecido.

O Grupo de Trabalho de Segurança deve determinar se as alterações à DPVC obrigam a uma mudança no OID da política ou no URL que aponta para a DPVC.

Nos casos em que, a julgamento do Grupo de Trabalho de Segurança, as alterações da DPVC não afetem a aceitação dos selos temporais proceder-se-á ao aumento do número menor de versão do

documento e o último número de Identificador de Objeto (OID) que o representa, mantendo o número maior da versão do documento, assim como o resto de seu OID associado. Não se considera necessário comunicar este tipo de modificações aos subscritores.

No caso em que o Grupo de Trabalho de Segurança julgue que as alterações à especificação podem afetar a aceitabilidade dos selos temporais para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 11.11.

Todas reclamações entre utilizadores e a PKI da SISP deverão ser comunicadas pela parte em disputa à Autoridade Credenciadora, com o fim de tentar resolvê-lo entre as mesmas partes.

Para a resolução de qualquer conflito que possa surgir com relação a esta DPVC, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo.

11.13. Legislação aplicavel

É aplicável à atividade das entidades certificadoras e de validação cronológica a seguinte legislação específica:

a) Decreto-Lei nº 33 /2007, de 24 de Setembro;

b) Decreto-Lei nº44/2009 de 9 de Novembro;

c) Portaria nº 2/2008, de 28 de Janeiro;

d) Portaria Conjunta nº 4/2008, de Fevereiro de 2008;

e) Decreto Regulamentar nº. 18/2007, de 24 de Dezembro.

11.14. Conformidade com a legislação em vigor

Esta DPVC é objecto de aplicação de leis nacionais, regras, regulamentos, ordenações, decretos e ordens incluindo, mas não limitadas a, restrições na exportação ou importação de software, hardware ou informação técnica.

É responsabilidade da Autoridade Credenciadora zelar pelo cumprimento da legislação aplicável listada na secção 11.13.

11.15. Providências várias

Todas as partes confiantes assumem na sua totalidade o conteúdo da última versão desta DPVC.

No caso em que uma ou mais estipulações deste documento sejam ou tendam a ser inválidas, nulas ou irreclamáveis, em termos jurídicos, deverão ser consideradas como não efetivas.

A situação anterior é valida, apenas e só nos casos em que tais estipulações não sejam consideradas

12.REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANAC, Declaração de Práticas de Certificação da EC Raiz de Cabo Verde.

[2] ANAC, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.

[3] Portaria nº 2/2008, de 28 de Janeiro;

[4] Decreto-Lei nº44/2009 de 9 de Novembro;

[5] Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;

[6] Decreto-Lei nº 33 /2007, de 24 de Setembro;

[7] Portaria nº 4/2008

[8] FIPS 140-2. 1994, Security Requirements for Cryptographic Modules.

[9] ETSI EN 319 401 v2.1.1, General policy requirements for Trusted Service Providers

10] ETSI EN 419 421 v1.1.1, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[11] ETSI EN 419 422 v1.1.1, Time-Stamping Protocol and Time-Stamp Profiles

[12] RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

[13] RFC 3628. 2003, Policy Requirements for Time-Stamping Authorities (TSAs).