Política de Certificado de Assinatura Digital Tipo A3

da Autoridade Certificadora SAT SEFAZ SP

PC A3 DA AC SAT SEFAZ SP

Versão 1.2 - 30 de março de 2015

ÍNDICE

Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora SAT SEFAZ SP

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo A3 da Autoridade Certificadora SAT SEFAZ.

1.1.2. A estrutura desta PC está baseada no DOC-ICP-04 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC 5280 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

1.2. Identificação

1.2.1. Esta PC é chamada "Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora SAT SEFAZ SP" e referida como "PC A3 da AC SAT SEFAZ SP". Esta PC descreve os usos relacionados ao certificado de Assinatura Digital correspondente ao certificado tipo A3. O OID (object identifier) desta PC é 1.3.6.1.4.1.30253.3.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se exclusivamente à AC SAT SEFAZ SP.

1.3.1.2. As práticas e procedimentos de certificação da AC SAT SEFAZ SP estão descritos na Declaração de Práticas de Certificação da AC SAT SEFAZ SP.

1.3.2. Prestador de Serviço de Suporte

1.3.2.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC SAT SEFAZ SP é publicada em serviço de diretório e/ou em página web da AC SAT SEFAZ SP:

http://acsat.imprensaoficial.com.br/repositorio.

1.3.2.2. PSS são entidades utilizadas pela AC para desempenhar atividade descrita nesta PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) Disponibilização de infra-estrutura física e lógica;

b) Disponibilização de recursos humanos especializados; ou

c) Disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.2.3. A AC SAT SEFAZ SP mantém as informações acima sempre atualizadas.

1.3.3.Titulares de Certificado

1.3.3.1. Apenas pessoas jurídicas podem ser titulares de certificados.

1.3.4.Aplicabilidade

1.3.4.1. Neste item são relacionadas as aplicações para as quais os certificados definidos por esta PC são adequados;

1.3.4.2. As aplicações e demais programas que admitem o uso de certificado digital de um determinado tipo, aceitam qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.3.4.3. A AC SAT SEFAZ SP leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

1.3.4.4. Os certificados emitidos pela AC SAT SEFAZ SP no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.Dados de Contato

Nome: Secretaria da Fazenda do Estado de São Paulo

Endereço: Av. Rangel Pestana, 300 - São Paulo / SP - 01017-911

Nome: Alexandre Palmeira Mendonça

Telefone: (11) 3243-3452

E-mail: diretordti@fazenda.sp.gov.br

2. DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SAT SEFAZ SP, disponível em pagina web http://acsat.imprensaoficial.com.br/repositorio.

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SAT SEFAZ SP, disponível em pagina web http://acsat.imprensaoficial.com.br/repositorio.

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SAT SEFAZ SP, disponível em pagina web http://acsat.imprensaoficial.com.br/repositorio.

4.3. Controles de Pessoal

4.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

4.3.2. Procedimentos de verificação de antecedentes

4.3.3. Requisitos de treinamento

4.3.4. Freqüência e requisitos para reciclagem técnica

4.3.5. Sanções para ações não autorizadas

4.3.6. Requisitos para contratação de pessoal

4.3.7. Documentação fornecida ao pessoal

5. CONTROLES TÉCNICOS DE SEGURANÇA

5.1.Geração e Instalação do Par de Chaves

5.1.1.Geração do par de chaves

5.1.1.1. O par de chaves criptográficas é gerado pela pessoa responsável, indicada por seu(s) representante(s) legal(s);

5.1.1.2. A geração do par de chaves criptográficas ocorre utilizando o chip criptográfico armazenado dentro do equipamento SAT CSF-e com capacidade de geração de chave protegidos por senha;

5.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA;

5.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico;

5.1.1.5. O usuário deve assegurar que a chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

5.1.1.6. O meio de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

5.1.1.7. O meio de armazenamento não deve modificar os dados a serem assinados, nem impedir que estes dados sejam apresentados ao signatário antes do processo de assinatura. O tipo de certificado emitido pela AC SAT SEFAZ SP e descrito nesta PC é o A3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Cartão Inteligente ou chip criptográfico ambos com capacidade de geração de chave, ou hardware criptográfico homologado junto ao Órgão Técnico determinado pela SEFAZ SP.

5.1.1.8. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é da pessoa responsável, indicada por seus(s) representante(s) legal(s), conforme especificado no Termo de Aceite.

5.1.2. Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado AC SAT SEFAZ SP, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer.

5.1.3. Disponibilização de chave pública da AC para usuários

A AC SAT SEFAZ SP disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários, através de endereço Web: http://acsat.imprensaoficial.com.br/repositorio.

5.1.4.Tamanhos de chave

5.1.4.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC SAT SEFAZ SP é de 2048 bits.

5.1.4.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3, foi definido baseado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

5.1.4.3. Na composição da CSR (Certificate Sign Request) para a solicitação do certificado digital, o expoente da chave pública deve ser de 3 bytes (0x010001).

5.1.5.Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão FIPS (Federal Information Processing Standards) 140-2.

5.1.6.Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (Cryptographic Module Validation Program) do NIST (National Institute of Standards and Technology).

5.1.7.Geração de chave por hardware ou software

A geração das chaves criptográficas do Certificado Tipo A3 desta PC é realizada por hardware criptográfico.

5.1.8.Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

5.2. Proteção da Chave Privada

5.2.1.Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (Federal Information Processing Standards) 140-2.

5.2.2.Recuperação (escrow) de chave privada

Não é permitida, a recuperação (escrow) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

5.2.3.Cópia de segurança (backup) de chave privada

5.2.3.2. A AC SAT SEFAZ SP não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido;

5.2.5.Arquivamento de chave privada

6.2.5.1. A AC SAT SEFAZ SP não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

6.2.5.2. Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

5.2.6.Método de ativação de chave privada

A chave privada é ativada automaticamente no processo de habilitação do equipamento SAT CF-e.

5.2.7.Método de desativação de chave privada

A chave privada pode ser desativada através do processo de desativação do equipamento SAT CF-e.

5.3.Outros Aspectos do Gerenciamento do Par de Chaves

5.3.1.Arquivamento de chave pública

As chaves públicas dos titulares de certificados de assinatura digital emitidos pela AC SAT SEFAZ SP permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

5.3.2.Períodos de uso para as chaves pública e privada

5.3.2.1. As chaves privadas de assinatura dos respectivos titulares de certificados emitidos pela AC SAT SEFAZ SP são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes

chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

5.3.2.2. O período máximo de validade admitido para certificados de Assinatura Digital Tipo A3 da AC SAT SEFAZ SP é de 5 (cinco) anos.

5.4.Dados de Ativação

5.4.1.Geração e instalação dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

5.4.2.Proteção dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

5.5.Controles de Segurança Computacional

5.5.1.Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade.

O equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

5.6.Controles Técnicos do Ciclo de Vida

A AC SAT SEFAZ SP desenvolve sistemas apenas com finalidade relacionada à operação dos sistemas internos da SEFAZ.

5.6.1.Controles de desenvolvimento de sistema

5.6.1.1. A AC SAT SEFAZ SP utiliza um modelo clássico espiral no desenvolvimento dos sistemas. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias

de orientação a objetos. Como suporte a esse modelo, a AC SAT SEFAZ SP utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos informais.

5.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC SAT SEFAZ SP apresentam documentação suficiente para suportar avaliações externas de segurança dos componentes da AC SAT SEFAZ SP.

5.6.2.Controles de gerenciamento de segurança

5.6.2.1. A AC SAT SEFAZ SP verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

5.6.2.2. A AC SAT SEFAZ SP utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

5.7.Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado está em conformidade com o padrão de segurança FIPS 140-2, utilizando o algoritmo RSA.

6. PERFIS DE CERTIFICADO E LCR

6.1.Perfil do Certificado

Todos os certificados emitidos pela AC SAT SEFAZ SP estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

6.1.1.Número de versão

Os certificados emitidos pela AC SAT SEFAZ SP implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

6.1.2.Extensões de certificado

6.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticidade.

6.1.2.2. Extensões Obrigatórias
Os certificados emitidos pela AC SAT SEFAZ SP definem como obrigatórias as seguintes extensões:

a) **Authority Key Identifier**, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC SAT SEFAZ SP;
b) **Key Usage**, crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;
c) **Certificate Policies**, não crítica contém:

• O OID desta PC: 1.3.6.1.4.1.30253.3;

• E o endereço *Web* da DPC AC SAT SEFAZ SP que emite o certificado: (http://acsat.imprensaoficial.com.br/repositorio/dpc/acsefazsp/dpc_acsefazsp.pdf).

d) **CRL Distribution Points**, não crítica: contém os endereços Web onde se obtém a LCR da AC SAT SEFAZ SP:

Para certificados emitidos a partir de 21/12/2012
http://acsat.imprensaoficial.com.br/repositorio/lcr/acsatsefazsp/acsatsefazspcrl.crl

e) **Authority Information Access**, não crítica: A primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. A segunda entrada pode conter o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP. Esta extensão somente é aplicável para certificado de usuário final.
f) **basicConstraints**, não crítica: contém o campo cA=False.

6.1.2.3. Os certificados emitidos pela AC SAT SEFAZ SP possuem a extensão "Subject Alternative Name", não crítica e com os seguintes formatos:

a) Para certificado de aplicação:

a.1) 1 (um) campo otherName, obrigatório, contendo:

i. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ),

6.1.2.4. Os campos otherName, definidos como obrigatórios, estão de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING;

d) Todas as informações de tamanho variável, referentes a números, são preenchidos com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível;

f) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 6.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;

6.1.2.5. A AC SAT SEFAZ SP implementa a extensão "Extended Key Usage", não crítica, contendo o valor "client authentication" (OID 1.3.6.1.5.5.7.3.2).

6.1.2.7 A AC SAT SEFAZ SP implementa a extensão Authority Information Access**,** não crítica, contendo obrigatoriamente o endereço de acesso aos certificados da cadeia de certificação através do link: https://acsat.imprensaoficial.com.br/repositorio/certificados/acsat.p7c e opcionalmente o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (On-line Certificate Status Protocol- OCSP): http://ocsp.imprensaoficial.com.br.

6.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC SAT SEFAZ SP são assinados com o uso do algoritmo RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) conforme o padrão PKCS#1.

6.1.4. Formatos de nome

O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

ST = <Nome do estado por extenso>

O = SEFAZ-SP

OU = AC SAT SEFAZ SP

OU = Autoridade de Registro SEFAZ SP

OU = <Número de identificação da solicitação>

SN = <número serial do equipamento>

CN = <Razão Social><:><número do CNPJ>

O identificador CN contém a denominação da razão social correspondente.

Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

6.1.5.Restrições de nome

6.1.5.1. Neste item são descritas as restrições aplicáveis para os nomes dos titulares de certificados.

6.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
"	22
#	23
'	27
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

6.1.6.OID (Object Identifier) de Política de Certificado

O OID desta PC é: 1.3.6.1.4.1.30253.3.

Todo certificado emitido segundo essa PC, PC A3 da AC SAT SEFAZ SP, contém o valor desse OID presente na extensão Certificate Policies.

6.1.7.Sintaxe e semântica dos qualificadores de política

Os campos **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC SAT SEFAZ SP

(http://acsat.imprensaoficial.com.br/repositorio/dpc/acsefazsp/dpc_acsefazsp.pdf).

6.1.8. Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

6.2. Perfil de LCR

6.2.1. Número(s) de versão

As LCR geradas pela AC SAT SEFAZ SP implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

6.2.2. Extensões de LCR e de suas entradas

6.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC SAT SEFAZ SP e sua criticidade;

6.2.2.2. As LCR da AC SAT SEFAZ SP obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

a) “Authority Key Identifier”: não crítica: contém o hash SHA-1 da chave pública da AC SAT SEFAZ SP.

b) “CRL Number”, não crítica: contém um número seqüencial para cada LCR emitida pela AC SAT SEFAZ SP.

7. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

7.1. Procedimentos de mudança de especificação

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC SAT SEFAZ SP. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

7.2. Políticas de publicação e notificação

A AC SAT SEFAZ SP mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço *Web*:

(http://acsat.imprensaoficial.com.br/repositorio)

7.3.Procedimentos de aprovação

Esta PC A3 da AC SAT SEFAZ SP foi submetida à aprovação, durante o processo de credenciamento da AC SAT SEFAZ SP, conforme o determinado na legislação vigente.

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

8. DOCUMENTOS REFERENCIADOS

8.1. Os documentos que regulamentam a criação e a operação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO para atendimento ao SAT - Sistema Autenticador e Transmissor de Cupons Fiscais Eletrônicos (CF-e-SAT) da SEFAZ estão referenciados no site: http://www.fazenda.sp.gov.br/sat.