MARINHA DO BRASIL

DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO DA MARINHA

31/442

Rio de Janeiro, RJ, 26 de junho de 2019.

DCTIMARINST Nº 31-05

Assunto: Utilização de certificados digitais emitidos pela Autoridade Certificadora de Defesa (AC Defesa) no âmbito da Marinha do Brasil (MB).

Referências:
A) Declaração de Práticas de Certificação da AC Defesa (DPC da AC Defesa);
B) Política de Segurança da AC Defesa (PS AC Defesa);
C) Políticas de Certificados de Assinatura Digital da AC Defesa (PC AC Defesa A1, A3 e A4);
D) Políticas de Certificado de Sigilo da AC Defesa (PC AC Defesa S1, S3 e S4);
E) Portaria Normativa nº 71, de 29 de Novembro de 2016, do Ministério da Defesa (MD);
F) Portaria Normativa nº 17/MD, de 13 de abril de 2018, do Ministério da Defesa (MD);
G) Diretriz de Adoção de Certificados Digitais da Autoridade Certificadora de Defesa na Marinha do Brasil; e
F) SGM-105 (5ª Revisão) - Normas Sobre Documentação Administrativa e Arquivamento na Marinha.

1 - PROPÓSITO

Orientar a adoção de certificados digitais emitidos pela Autoridade Certificadora de Defesa (AC Defesa) no âmbito da Marinha do Brasil (MB).

2 - INTRODUÇÃO

A Portaria nº 2.806/MD/2013 instituiu o Projeto de Implantação da Autoridade Certificadora de Defesa (AC Defesa), que atende aos padrões estabelecidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), e tem a missão de prestar serviços de emissão, renovação, revogação e fornecimento de **certificados digitais** no âmbito do Ministério da Defesa (MD), considerando a administração central, os órgãos vinculados e as três Forças Singulares (FS).

A AC Defesa é composta de uma Autoridade Certificadora Principal (ACP) em Brasília, uma Autoridade Certificadora Reserva (ACR) no Rio de Janeiro, uma Autoridade de Registro (AR) em Brasília e diversos postos de validação distribuídos em guarnições militares em todo o Território Nacional, designados como Instalação Técnica Secundária (ITS).

Um certificado digital equivale a um documento formal de identidade no meio eletrônico e pode ser utilizado para realizar diversas operações em ambiente computacional, conferindo integridade, confidencialidade, autenticidade e não-repúdio (ou irretratabilidade) a documentos eletrônicos oficiais e transações eletrônicas. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, a Autoridade Certificadora (AC), que deve cumprir as regras

estabelecidas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), associando uma entidade (pessoa, processo ou servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular, como nome, CPF, assinatura da AC emissora, entre outros. Desta forma, o certificado digital funciona como uma identidade virtual, que comprova e garante o autor de uma mensagem ou transação feita por meio eletrônico, de modo seguro, inequívoco e com presunção de validade jurídica.

3 - DEFINIÇÕES

As seguintes definições e conceitos aplicam-se aos certificados digitais:

3.1 - Assinatura Digital: registro realizado eletronicamente por usuário, identificado de modo inequívoco, com vistas a assinar ou autenticar determinado documento com sua assinatura;

3.2 - Autoridade Certificadora (AC): entidade autorizada a emitir, suspender, renovar ou revogar certificados digitais; bem como a emitir Listas de Certificados Revogados (LCR) e manter registros de suas operações;

3.3 - AC Defesa: AC homologada pelo Instituto Nacional de Tecnologia da Informação (ITI), implantada e mantida pelo MD, que tem por finalidade emitir e fornecer certificados digitais para o MD (incluindo a administração central e órgãos vinculados), bem como para as três Forças Armadas (FA). É constituída por uma AC Principal, uma AC Reserva, uma Autoridade de Registro (AR) e diversas Instalações Técnicas Secundárias (ITS);

3.4 - AC Principal (ACP): instalação responsável pela gestão de certificados digitais emitidos pela AC Defesa e pela interligação com a AC-Raiz da ICP-Brasil;

3.5 - AC Reserva (ACR): instalação redundante capaz de assumir o controle da AC Defesa em caso de inoperância da AC Principal;

3.6 - Autoridade de Registro (AR): instalação de interface da AC Defesa com o público. Recebe, valida, encaminha solicitações de emissão ou revogação de certificados digitais e identifica seus solicitantes presencialmente;

3.7 - Instalação Técnica Secundária (ITS): ambiente físico de uma AR, cujo funcionamento foi homologado pelo ITI, onde é realizada exclusivamente a atividade de coleta e/ou verificação biométrica e validação da solicitação de certificados;

3.8 - Agente de Registro (AGR): função dos militares que realizam as tarefas de validação e verificação de solicitações de Certificados Digitais.;

3.9 - Certificado Digital: arquivo eletrônico que contém dados de uma pessoa ou instituição e um par de chaves criptográficas utilizados para comprovar identidade em ambiente computacional;

3.10 - Certificado Digital de Assinatura e Autenticação: utilizado para a assinatura de documentos, transações eletrônicas etc., com o propósito de provar a autenticidade e a autoria do emissor, garantindo também, a integridade do documento. Pode ser dos tipos A1, A2, A3 ou A4;

3.11 - Certificado Digital de Sigilo: utilizado somente para proporcionar sigilo ou criptografia de dados. São empregados para o envio e/ou armazenamento desses documentos sem expor o seu conteúdo. Pode ser dos tipos S1, S2, S3 ou S4;

3.12 - Tipos de certificados: Certificados A1 e S1 são gerados por software e armazenados no computador, com validade de até um ano. Certificados A2 e S2 são similares ao A1 e S1, mas armazenados em smart card ou token sem capacidade de geração de chaves, com validade de até 2 anos. Certificados A3 e S3 são gerados por hardware presentes no smart card ou token, podendo ter validade de até 5 anos. Certificados A4 e S4 são gerados e armazenados em hardware criptográfico homologado junto à ICP-Brasil, cuja validade depende da tecnologia do gerador utilizado, podendo chegar até 6 ou 11 anos para ambos os certificados. Os tamanhos das chaves variam de acordo com o tipo de certificado e a versão do algoritmo de geração.

Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

3.13 - Documento Eletrônico: documento armazenado sob a forma de arquivo eletrônico, inclusive aquele resultante de digitalização;

3.14 - Lista de Certificados Revogados (LCR): relação com a identificação dos certificados digitais que perderam sua validade por expiração ou suspensão e que, por sua vez, não poderão ser mais utilizados para assinatura digital ou seu reconhecimento;

3.15 - Mídia de Armazenamento do Certificado Digital: dispositivos portáteis, como tokens, que contêm o certificado digital;

3.16 - Titular de Certificado Digital: é uma entidade (pessoa física, pessoa jurídica, equipamento servidor ou sistema digital) autorizada pela AR responsável a receber um certificado digital, emitido pela AC Defesa, para sua própria utilização ou para utilização em equipamentos ou aplicações;

3.17 - Usuário: entidade da MB que tenha acesso, de forma autorizada, às informações produzidas ou custodiadas pela MB; e

3.18 - Senha Fraca ou Óbvia: é aquela na qual se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado em qualquer língua, dentre outras.

4 - RESPONSABILIDADES

4.1 - Compete à Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), dentre outras atribuições:

a) Adequar as normas de Tecnologia da Informação e Comunicações (TIC) da MB para utilização dos certificados digitais;

b) Elaborar e publicar procedimentos para emissão, renovação, revogação e reemissão de certificados digitais;

c) Elaborar e publicar padrões de compatibilidade de certificados digitais e das respectivas mídias de armazenamento utilizados na MB; e

d) Desenvolver, no âmbito de sua área de atuação, outras atividades relativas ao uso dos certificados digitais.

4.2 - Compete ao Centro de Tecnologia da Informação da Marinha (CTIM), dentre outras atribuições, como ACR:

a) Manter a estrutura da ACR guarnecida e operando continuamente de acordo com a referência a;

b) Adotar providências para emissão de certificados digitais em conformidade às instruções da AC Defesa;

c) Atender ao disposto no item "Obrigações da AC Defesa" previsto no documento da referência a;

d) Gerenciar o cumprimento da referência b;

e) Identificar os desvios de segurança praticados e zelar pela adoção das medidas corretivas apropriadas;

f) Gerenciar a execução dos processos relacionados ao ciclo de vida do certificado e à legislação da ICP-Brasil; e

g) Coordenar a segurança, no nível físico e lógico, dos ativos de informação e de processamento da AC Defesas relacionados com a sua área de atuação.

4.3 - Compete aos militares designados como Agentes de Registro Remoto (ARR):

a) Manter a estrutura de ARR em suas OM operando adequadamente, conforme os procedi-

mentos da AC Defesa;

b) Adotar providências para encaminhar as solicitações de emissão e distribuição de certificados digitais em conformidade às instruções da AC Defesa; e

c) Atender rigorosamente o que prescrevem as normas da ICP-Brasil na sua esfera de ação.

4.4 - Compete ao Titular de Certificado Digital:

a) por ocasião da criação de um novo certificado digital, fornecer todas as informações necessárias para sua identificação, de modo completo e preciso, apresentando a documentação necessária para a emissão do certificado digital à AR ou à ARR, tempestivamente;

b) observar as regras definidas para criação e utilização de senhas de acesso ao certificado;

c) estar de posse do certificado digital para o desempenho de atividades profissionais que requeiram seu uso;

d) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto nas referências c e d, de acordo com o tipo de certificado recebido;

e) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

f) solicitar à AC, de acordo com procedimentos definidos para esse fim, a imediata revogação do certificado em caso de comprometimento de sua chave privada ou de inutilização do certificado;

g) alterar imediatamente a senha de acesso ao certificado em caso de suspeita de seu conhecimento por terceiros;

h) informar à AC qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

i) manter a mídia de armazenamento do certificado digital em local seguro e com proteção física contra acesso indevido, descargas eletromagnéticas, calor excessivo e outras condições ambientais que representem risco à integridade dessas mídias; e

j) observar os seguintes procedimentos básicos de segurança:

I) nunca fornecer a senha a terceiros;

II) utilizar senha de, no mínimo, 8 caracteres;

III) não utilizar senha fraca ou óbvia;

IV) utilizar caracteres numéricos e alfanuméricos na criação da senha;

V) buscar memorizar a senha, evitando-se escrevê-la ou mantê-la em local inseguro; e

VI) guardar a mídia principal em lugar seguro.

5 - ADOÇÃO NA MB

Os certificados digitais a serem emitidos pela AC Defesa podem ser de duas categorias:

- de Assinatura e Autenticação, dos tipos A1, A3 e A4; e
- de Sigilo, dos tipos S1, S3 e S4.

Inicialmente, a MB adotará somente certificados de assinatura e autenticação do tipo A3, de acordo com a quantidade de tokens a ser disponibilizado pelo MD e, devido aos custos envolvidos na sua emissão, serão emitidos pelo critério da estrita necessidade funcional. Os certificados digitais do tipo A3 serão emitidos para Almirantes, Titulares de OM e agentes administrativos que necessitem de certificados para autenticação nos sistemas da Administração Pública Federal (APF), como Ordenadores de Despesa, Agentes Financeiros ou operadores de sistemas e-consig. Os casos não previstos para emissão do certificado, devido à necessidade funcional, serão avaliados pelos Titulares das OM. No entanto, a DCTIM poderá ser consultada tecnicamente para orientar às OM na necessidade ou não de emissão de certificados. Este certificado é pessoal e intransferível, com validade máxima de cinco anos podendo ser utilizado mesmo se o titular de

certificado digital for movimentado, ficando o mesmo responsável por sua utilização, guarda e conservação.

Os certificados digitais de sigilo não serão usados no momento da ativação da AC Defesa. Assim, os sistemas digitais ligados à Internet deverão continuar com a utilização de certificados emitidos por outras AC. Futuramente, serão divulgadas novas instruções para migração e instalação de certificados de sigilo, em substituição aos atuais, e os sistemas digitais que terão prioridade na solicitação de emissão.

Nos serviços e sistemas digitais hospedados na Rede de Comunicações Integrada da Marinha (RECIM), os certificados digitais continuarão a ser emitidos pela Autoridade Certificadora da Infraestrutura de Chaves Públicas da Marinha (ICP-MB), controlada pela DCTIM, mantendo-se os procedimentos ora em vigor. Normas específicas para a adoção e migração de certificados da AC Defesa nos sistemas corporativos de informação serão publicadas oportunamente.

6 - PROCEDIMENTOS DE CARÁTER GERAL

O uso de certificado digital da ICP-Brasil é obrigatório para comunicações no âmbito de processos eletrônicos, para autenticação de documento eletrônico resultante de digitalização e para outros procedimentos que necessitem de comprovação de autoria e integridade em ambiente externo à MB. A emissão e distribuição de certificados digitais emitidos pela AC Defesa será realizada por necessidade do serviço, em decorrência da implantação de funcionalidades legais ou tecnológicas que exijam o seu uso. Os documentos eletrônicos utilizados somente no âmbito da MB poderão continuar a utilizar os certificados digitais emitidos pela ICP-MB.

É permitido ao usuário adquirir certificado digital e respectiva mídia de armazenamento por meios próprios para uso na MB, desde que ambos sejam emitidos por uma AC reconhecida pela ICP-Brasil e que possuam características compatíveis com as definições publicadas pela AC Defesa, não sendo cabível, em qualquer hipótese, o ressarcimento pela MB dos custos havidos.

O certificado digital é intransferível e hábil a produzir efeitos legais em todos os atos nos quais vier a ser utilizado, dentro ou fora da MB (referência f). A prática de atos assinados digitalmente importará aceitação das normas regulamentares sobre o assunto e da responsabilidade pela utilização indevida da assinatura digital. Em caso de impossibilidade técnica, os documentos poderão ser produzidos em papel e assinados de próprio punho pela pessoa competente, devendo a versão assinada ser digitalizada e certificada digitalmente. Só é possível garantir a validade de uma assinatura enquanto o certificado é válido. Na hipótese de o certificado digital perder a validade, as assinaturas digitais anteriormente efetuadas permanecem válidas, podendo, também, ser verificadas a autoria e a integridade dos documentos já assinados.

Mantendo-se a necessidade do serviço e mediante solicitação do usuário, a AC Defesa promoverá a renovação de um certificado digital que tiver expirado, limitada a uma única ocorrência. Para certificados de equipamento e aplicações não há processo de renovação. Nos demais casos devem ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado, conforme descrito na referência a.

O certificado digital será inutilizado quando ocorrer:

- digitação sucessiva de senha incorreta na tentativa de utilização do certificado;
- dano ou formatação da mídia que armazena o certificado;
- esquecimento da senha de utilização do certificado; ou
- perda ou extravio.

A inutilização é efetuada automaticamente por solução de TI para o caso descrito na alínea a) anterior, ou mediante solicitação de revogação à AC para os demais casos. A inutilização implica na emissão de um novo certificado digital.

O uso inadequado do certificado digital fica sujeito à apuração de responsabilidade penal, civil e administrativa, na forma da legislação em vigor.

7 - DISPOSIÇÕES FINAIS

Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações aplicam-se ao responsável pelo uso do certificado.

Os documentos em referência e informações complementares podem ser acessados no sítio http://www.acdefesa.mil.br/ .

8 - VIGÊNCIA

Esta DCTIMARINST entra em vigor na presente data.

LUCIANA MASCARENHAS DA COSTA MARRONI
Contra-Almirante (EN)
Diretora
ASSINADO DIGITALMENTE

Distribuição:
Lista 1
DAdM (Bol MB)
DCTIM-31
DCTIM-SECOM