MARINHA DO BRASIL

DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO DA MARINHA

31/010

Rio de Janeiro, RJ, 31 de outubro de 2023.

DCTIMARINST Nº 31-05A

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

Referências:
A) Portaria nº 2.806/MD, de 3 de outubro de 2013, do Ministério da Defesa;
B) Portaria nº 1.672/MD, de 17 de março de 2023, do Ministério da Defesa;
C) Declaração de Práticas de Certificação da AC Defesa;
D) Política de Segurança da AC Defesa;
E) Políticas de Certificados de Assinatura Digital da AC Defesa; e
F) Políticas de Certificado de Sigilo da AC Defesa.

1. PROPÓSITO

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

2. INTRODUÇÃO

A referência A 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 Agentes de Registro Remotos (ARR) em todo o Território Nacional, conforme referência B.

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 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 pela AC Principal, AC Reserva, Autoridade de Registro e as ARR;

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. Postos de Atendimento (PA): instalações físicas situadas em todo Território Nacional, onde é realizada a identificação, coleta e/ou verificação biométrica e validação da solicitação de certificados;

3.8. Agentes de Registro Remotos (ARR): função dos militares que realizam as tarefas relativas a solicitações de Certificados Digitais nos PA;

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 armazenados no computador e deverão ser protegidos por senha de acesso, tendo validade de até 1 ano. Certificados A3 e S3 são armazenados em *hardware* criptográfico do tipo *token* tendo validade de até 5 anos. Certificados A4 e S4 são armazenados em *hardware* criptográfico do tipo *token*, tendo validade

de até 6 anos. 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: militar ou servidor civil 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 C;

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 C;

d) Gerenciar o cumprimento da referência D;

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 Defesa 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 procedimentos 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 E e F, 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) não utilizar senha fraca ou óbvia;
III) buscar memorizar a senha, evitando-se escrevê-la ou mantê-la em local inseguro; e
IV) guardar a mídia principal em lugar seguro.

5. ADOÇÃO NA MB

Os certificados digitais emitidos pela AC Defesa são os de Assinatura e Autenticação, dos tipos A1 e A3 para pessoas físicas e pessoas jurídicas.

A emissão dos certificados A1 é feita em 2 etapas: Validação e Emissão. Na etapa de validação é necessário apresentar a documentação exigida, na data agendada e no PA escolhido, para análise e validação. Após a conclusão da etapa de validação, segue-se a etapa de emissão que deverá ser feita no computador do titular de certificado digital, seguindo as

instruções emanadas pela AC Defesa.

A emissão dos certificados A3 está vinculada com a quantidade de *tokens* disponibilizados pelo MD e, devido aos custos envolvidos na sua emissão, serão emitidos pelo critério da estrita necessidade funcional.

Os certificados digitais do tipo A1 e A3, para pessoas físicas, serão emitidos para Almirantes, Titulares de OM, agentes administrativos que necessitem de certificados para autenticação nos sistemas da Administração Pública Federal (APF), como Ordenadores de Despesa, Agentes Financeiros, operadores de sistemas e-consig e os Servidores Civis e Militares que exercem funções administrativas com necessidade do uso da assinatura digital do tipo ICP-Brasil. 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.

Para obter a certificação digital o solicitante deverá realizar o cadastro e agendamento no site https://www.acdefesa.mil.br (no link “Para você”), conferir a relação de documentos necessários, comparecer pessoalmente no PA agendado munido dos documentos originais para conferência. Durante o atendimento será realizado a captura biométrica, cadastro de senha e o recebimento de *token* (para os certificados do tipo A3).

Nos serviços e sistemas digitais de Internet, hospedados na Centro de Dados da MB (CD-MB), a emissão de certificado digital para servidores (SSL) faz parte do processo de Conformidade, Homologação e Hospedagem de Sistemas Digitais (SD). Estes certificados, atualmente, são emitidos sem custos e o procedimento de emissão é realizado pelo CTIM após a homologação do SD.

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. 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 C.

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 que constam nas referências de B a F e informações complementares podem ser acessados no sítio http://www.acdefesa.mil.br/.

8. VIGÊNCIA

Esta DCTIMARINST entra em vigor na presente data.

9. CANCELAMENTO

Esta DCTIMARINST cancela a de nº 31-05.

MARCELO GURGEL DE SOUZA
Contra-Almirante
Diretor
ASSINADO DIGITALMENTE

Distribuição:
Lista 1
DCTIM-31
Arquivo