MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-43

IMPLANTAÇÃO DO PROJETO DE AUTORIDADE CERTIFICADORA DE DEFESA (AC DEFESA) NO COMAER

2016

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO MAIOR DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-43

IMPLANTAÇÃO DO PROJETO DE AUTORIDADE CERTIFICADORA DE DEFESA (AC DEFESA) NO COMAER

2016

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

PORTARIA EMAER Nº 60/3SC, DE 7 DE NOVEMBRO DE 2016.

Aprova a edição da Instrução que dispõe sobre "Implantação do Projeto de Autoridade Certificadora de Defesa (AC Defesa) no COMAER".

O CHEFE DO ESTADO-MAIOR DA AERONÁUTICA, no uso das atribuições que lhe confere o Inciso IV do Art. 14 do Regulamento do Estado-Maior da Aeronáutica, aprovado pela Portaria nº 129/GC3, de 11 de fevereiro de 2016, tendo em vista o disposto no item 1.3.3 da NSCA 5-1/2011, aprovada pela Portaria COMGEP nº 864/5EM, de 23 de novembro de 2011, resolve:

Art. 1º Aprovar a edição da ICA 7-43 "Implantação do Projeto de Autoridade Certificadora de Defesa (AC Defesa) no COMAER".

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Ten Brig Ar RAUL BOTELHO
Chefe do Estado-Maior da Aeronáutica

(Publicado no BCA nº 192, de 09 de novembro de 2016)

SUMÁRIO

PREFÁCIO

A certificação digital é um sistema que identifica univocamente seu usuário da mesma forma que a identidade tradicional, sendo suportado por uma infra-estrutura nacional de identificação virtual. Pelo arcabouço jurídico que o embasa, possui a mesma validade de uma carteira de identidade no âmbito nacional. É importante para fins de celeridade nos processos e economia de recursos, permitindo utilizar a tecnologia da informação para geração, controle do documento e transmissão do formato inteiramente digital da burocracia.

A utilização da certificação digital permitirá ao COMAER realizar o trâmite documental em conformidade com a Portaria Interministerial MJ/MPOG n° 1.677, de 7 de outubro de 2015, e com o Decreto nº 8.539, de 8 de outubro de 2015, o qual dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

O Ministério da Defesa (MD), por intermédio da Portaria nº 2.806/MD, de 4 de outubro de 2013, determinou a execução do Projeto de Implantação da Autoridade Certificadora de Defesa (AC Defesa), a cargo do Exército Brasileiro (EB). Quando em operação, o sistema deverá ser subordinado diretamente ao MD.

O Projeto é estruturado com duas Autoridades Certificadoras (AC), funcionando em regime de espelhamento a fim de prover continuidade no serviço de autenticação na eventualidade de uma falha catastrófica em uma delas, e uma Autoridade de Registro (AR), responsável pela emissão dos certificados digitais. A AR conta com uma rede de postos de validação, designados Agentes de Registro Remoto (ARR), distribuídos em guarnições militares em todo o Território Nacional.

Em razão da comunalidade e inter-relações deste Projeto com sistemas do COMAER e implantação da nova identidade militar, portadora de um *chip* capaz de receber o certificado digital, é oportuna esta Instrução para garantir a máxima eficiência no aproveitamento deste serviço.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade estabelecer normas e procedimentos, disciplinando atribuições e definindo responsabilidades, relacionados à certificação digital provida pelo Projeto AC Defesa.

1.2 CONCEITUAÇÃO

Para efeito desta Instrução, as expressões abaixo devem ser entendidas de acordo com as conceituações que se seguem.

1.2.1 ASSINATURA DIGITAL

Registro realizado eletronicamente com vistas a assinar ou autenticar determinado documento.

A assinatura digital pode ser realizada por uma entidade (pessoa física, pessoa jurídica, equipamento servidor ou sistema digital) detentora de um certificado digital.

As assinaturas digitais permanecem válidas mesmo após o certificado expirar sua validade. A autoria e a integridade dos documentos assinados podem ser verificadas uma vez que a Autoridade Certificadora (AC) mantém o registro de certificados invalidados emitidos por sua Autoridade de Registro (AR).

1.2.2 AUTORIDADE CERTIFICADORA (AC)

"Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (AR) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada." (Fonte: ITI)

1.2.3 AUTORIDADE CERTIFICADORA DA DEFESA (AC DEFESA)

É uma AC vinculada à ICP-Brasil, desenvolvida e mantida pelo Ministério da Defesa. A AC Defesa tem como finalidade emitir e fornecer certificados digitais para o MD, bem como para as três forças singulares.

A estrutura da AC Defesa possui:

- uma AC Principal (**ACP**) - localizada em Brasília-DF, hospedada no EB, no Centro Integrado de Telemática do Exército (CITEx);

- uma AC Reserva (**ACR**) - localizada no Rio de Janeiro-RJ, hospedada na MB, no Centro de Tecnologia da Informação da Marinha (CTIM); e
- uma Autoridade de Registro (**AR**) - localizada em Brasília-DF, hospedada no COMAER, no Sexto Comando Aéreo Regional (COMAR VI)

Em todas as entidades acima o efetivo é conjunto e vinculado ao MD, porém subordinado administrativamente à OM hospedeira e a uma OM de sua Força para fins de controle de pessoal.

A AC Defesa disponibiliza informações e documentação no sítio www.acdefesa.mil.br.

1.2.4 AUTORIDADE DE REGISTRO (AR)

"Uma Autoridade de Registro (AR) é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota." (Fonte: ITI)

1.2.5 AGENTE DE REGISTRO REMOTO (ARR)

A AR funciona com uma rede de Agentes de Registro Remoto (ARR) nas três Forças Armadas para a coleta dos dados dos solicitantes de certificados. Em cada ARR há, no mínimo, dois militares habilitados pela AR para realizar a entrevista com os usuários e coletar os dados a constar no dossiê para emissão do certificado digital. O dossiê é analisado pela AR e cabe ao ARR apenas a coleta dos dados e a entrega do certificado.

No COMAER, os ARR são localizados nas Seções de Identificação de OM (SIDOM).

1.2.6 CERTIFICAÇÃO DIGITAL

"A certificação digital é uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demandam identificação clara da pessoa que a está realizando pela internet." (Fonte: ITI)

1.2.7 CERTIFICADO DIGITAL

É um documento eletrônico gerado e assinado por uma terceira parte confiável - uma autoridade certificadora - o qual associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos.

Os certificados contêm os dados de seu titular, como nome, número do registro (civil ou militar), assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme

detalhado e especificado na Política de Segurança de cada Autoridade Certificadora. (Fonte: ITI)

Os certificados comuns na ICP-Brasil podem ser do tipo A1 ou A3[1]. A principal diferença entre estes tipos é a geração e o armazenamento das chaves criptográficas.

No certificado tipo A1 o par de chaves pública/privada é gerado no computador do usuário, no momento da solicitação de emissão do certificado. A chave pública será enviada para a Autoridade Certificadora (AC) com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada em seu computador, devendo, obrigatoriamente, ser protegida por senha de acesso. Este certificado é instalado no mesmo computador onde foi efetuada a solicitação do certificado e tem validade de 1 (um) ano.

O certificado tipo A3 é gerado em *hardware* específico, podendo ser em *smart card* ou em *token*. Este tipo de certificado oferece mais segurança que o tipo A1, pois não permite a exportação ou qualquer outro tipo de reprodução ou cópia da chave privada. Também no certificado tipo A3 a chave pública será enviada para a AC junto com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada no cartão ou *token*, impedindo tentativas de acesso de terceiros. Com este método, a chave privada poderá ser transportada, de maneira segura. O certificado tipo A3 tem validade de até 5 (cinco) anos.

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. Ou seja, garantir, com presunção de validade jurídica, que as informações neles contidas foram realmente produzidas, expedidas ou modificas por seus assinantes.

A utilização do certificado digital para qualquer operação implica não-repúdio, não podendo negar a autoria da operação, nem alegar que tenha sido praticada por terceiro. O não-repúdio aplica-se também às operações efetuadas entre o período de solicitação da revogação ou suspensão do certificado e respectiva inclusão na Lista de Certificados Revogados (LCR) publicada pela autoridade certificadora.

O certificado pode ser inutilizado por solicitação ou de forma automática. Neste último caso, isto ocorre após tentativas sucessivas de utilização de senha incorreta; esquecimento da senha; dano à mídia de armazenamento do certificado; e extravio.

---

[1] Os tipos podem ser de **assinatura digital** (Série **A**: de A1 até A4) e de **sigilo** (Série **S**: de S1 a S4). Os da série A são utilizados na confirmação de identidade na *web*, em *e-mail*, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações. A série S (S1, S2, S3 e S4) reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.
A1 e S1 são gerados por *software* e armazenados no computador, com validade de até um ano. A2 e S2 são similares ao anterior, mas armazenados em *smart card* ou *token* sem capacidade de geração de chaves, além de terem validade de até 2 anos. A3 e S3 são gerados por *hardware* presentes no *smart card* ou *token*, podendo ter validade de até 5 anos. 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. [Fonte: DOC-ICP-04]

1.2.8 CHAVES PÚBLICAS E PRIVADAS

É um método de criptografia que utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada usuário ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, a qual deve ser mantida em segredo pelo seu detentor.

Também conhecida como criptografia assimétrica, sendo as duas partes desse par de chaves matematicamente ligadas. A chave pública é usada para encriptar um arquivo ou para verificar uma assinatura digital, enquanto a chave privada é usada para a operação oposta, para decriptar um arquivo ou para criar uma assinatura digital. O termo assimétrico vem do uso de diferentes chaves para realizar essas funções opostas, cada uma a inversa da outra, como contrapartida da criptografia convencional, a qual depende da mesma chave para realizar ambos e, por isso, é conhecida como simétrica. Portanto, as mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente e vice-versa.

1.2.9 COMITÊ GESTOR DO PROJETO AC DEFESA (CG AC DEFESA)

O Projeto AC Defesa possui sua estrutura de Governança encabeçada por um comitê gestor, vinculado ao MD. No CG AC Defesa, têm lugar as três Forças Singulares, com um assento cada, e o EMCFA. O CG AC Defesa é um órgão de assessoramento ao MD sobre o Projeto.

1.2.10 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)

"A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso.

A AC-Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as AC estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil." (Fonte: ITI)

1.2.11 INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI)

"O Instituto Nacional de Tecnologia da Informação (ITI) é autarquia federal que tem por missão manter e executar as políticas da ICP-Brasil. Ao ITI compete ainda ser a primeira autoridade da cadeia de certificação digital – AC Raiz. O ITI, além de desempenhar o papel de AC Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos." (Fonte: ITI)

1.2.12 LEITORA DE *SMART CARD*

É um dispositivo projetado para conectar um *smart card* a um computador. A leitora fará a interface com o cartão, enquanto o computador suporta e gerencia as aplicações.

1.2.13 SISTEMA DE GESTÃO ELETRÔNICA DE DOCUMENTOS (SGED)

É conjunto de tecnologias que permitem gerar, controlar, armazenar, compartilhar e recuperar informações existentes em documentos. Os sistemas GED permitem aos usuários acessarem os documentos de forma ágil e segura, normalmente via navegador web por meio de uma intranet corporativa acessada interna ou externamente.

É a forma de administrar através da tecnologia, promovendo um governo mais eficiente a fim de facilitar ao cidadão o acesso aos serviços públicos.

O SGED do COMAER é o SIGADAER. No MD é utilizado o Sistema Eletrônico de Informações (SEI) em desenvolvimento conjunto entre ministérios, coordenado pelo Ministério de Planejamento, Desenvolvimento e Gestão (MPDG)[2]. O trâmite entre os diversos SGED da Administração Pública Federal (APF) será possível pela padronização de que trata o projeto de Processo Eletrônico Nacional (PEN).

1.2.14 *SMART CARD* OU CARTÃO INTELIGENTE

É um cartão criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas essas chaves, as mesmas não poderão ser exportadas para outra mídia nem serem retiradas do cartão. A solução possui múltiplos níveis de proteção, incluindo recursos físicos e lógicos, evitando a exposição do certificado digital a risco de roubo ou violação.

A utilização do cartão no computador necessita de uma leitora específica e o acesso ao certificado é realizado por meio de senha.

1.2.15 *TOKEN*

É um *hardware* capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Possui a mesma funcionalidade do *smart card* de geração de chaves e inviolabilidade das mesmas. Utiliza porta USB para conexão ao computador, dispensando leitora especifica, mas necessita de *driver* e um gerenciador criptográfico (*software*). Assim como o certificado armazenado em *smart card*, o certificado em *token* é acessado por meio de senha.

[2] Antigo Ministério do Planejamento, Orçamento e Gestão (MPOG).

1.3 ABREVIATURAS

AC Defesa	Projeto Autoridade Certificadora da Defesa
AC	Autoridade Certificadora
ACP	AC Principal
ACR	AC Reserva
APF	Administração Pública Federal
AR	Autoridade de Registro
ARR	Agente de Registro Remoto
BCA	Boletim do Comando da Aeronáutica
CENDOC	Centro de Documentação da Aeronáutica
CG AC DEFESA	Comitê Gestor do Projeto AC Defesa
COMGAP	Comando-Geral de Apoio
COMGEP	Comando-Geral de Pessoal
DIRAP	Diretoria de Administração de Pessoal
DTI	Diretoria de Tecnologia da Informação da Aeronáutica
EMAER	Estado-Maior da Aeronáutica
ICA	Instrução do Comando da Aeronáutica
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Listas de Certificados Revogados
MD	Ministério da Defesa
ODSA	Órgãos de Direção Setorial e de Assessoramento da Aeronáutica
OM	Organização Militar
PEN	Processo Eletrônico Nacional
SEI	Sistema Eletrônico de Informações
SERPRO	Serviço Federal de Processamento de Dados
SGED	Sistema de Gestão Eletrônica de Documentos
SIDENT	Sistema de Identificação da Aeronáutica
SIDOM	Seções de Identificação de OM
SIGADAER	Sistema Informatizado de Gestão Arquivística e. Documental da Aeronáutica
SIGPES	Sistema de Informações Gerenciais de Pessoal
TI	Tecnologia da Informação
USB	*Universal Serial Bus*

1.4 ÂMBITO

A presente Instrução aplica-se às Organizações Militares (OM) do COMAER.

2 CONCEPÇÃO GERAL DE IMPLANTAÇÃO

2.1 ANÁLISE DA SITUAÇÃO

2.1.1 O certificado digital provido pelo Projeto AC Defesa poderá ser utilizado em ampla gama de serviços e sistemas informatizados, mas seu uso deverá iniciar-se, no COMAER, pelo SIGADAER, uma vez que o mesmo já utiliza certificados digitais emitidos pelo SERPRO.

2.1.2 O uso de certificado digital é requisitado nos projetos SEI e PEN, os quais possibilitarão o trâmite de 100% da documentação da APF somente em formato digital. O SIGADAER será adaptado para adequar-se ao PEN, sendo esta tarefa gerenciada pelo CENDOC.

2.1.3 O certificado digital possui custo de emissão e é pessoal, servindo como identidade virtual. O mesmo terá validade fora do âmbito do COMAER, podendo, inclusive, ser utilizado para fins particulares, o que poderá provocar a procura indiscriminada por todos os militares e servidores do COMAER. Por haver custos envolvidos na sua emissão, o certificado deverá ser emitido, sem ônus para o usuário, somente por necessidade funcional.

2.1.4 O Projeto AC Defesa iniciará com um "piloto", na área Brasília, sendo expandido futuramente para a guarnição do Rio de Janeiro e, em uma terceira fase, para todas as demais OM.

2.1.4.1 Até que o Projeto seja considerado operacional, os pedidos de certificado deverão ocorrer somente em suas áreas. Portanto, durante o "piloto" em Brasília, somente militares desta guarnição poderão solicitar os certificados do Projeto AC Defesa.

2.1.5 A capacitação dos ARR é de responsabilidade do Projeto AC Defesa, por intermédio da AR, incluindo o planejamento e os custos envolvidos.

2.1.6 O Projeto AC Defesa tem sua rotina e responsabilidades estabelecidas em Regime de Funcionamento, o qual estabelece, entre outras particularidades:

a) a relação sistêmica entre as AC, a AR e os ARR com o Comitê Gestor da AC Defesa;

b) a subordinação administrativa das AC, da AR e dos ARR às OM hospedeiras;

c) a subordinação administrativa dos efetivos das AC, da AR e dos ARR às OM às quais são adidos; e

d) expediente de funcionamento.

2.1.7 O ITI emitiu novas regras de funcionamento das AC, incluindo a biometria digital, com validade a partir de novembro de 2016. Caso o Projeto AC Defesa inicie o processo de credenciamento a partir desta data, deverá respeitar integralmente as novas regras, porém, se o credenciamento ocorrer antes, poderá funcionar sem a biometria e planejar a adaptação às novas regras de acordo com acertos a serem realizados com o Instituto.

2.2 LINHA DE AÇÃO

2.2.1 CERTIFICADOS DIGITAIS EM *TOKENS* X EMBUTIDOS NA NOVA CARTEIRA DE IDENTIDADE MILITAR

2.2.2 Será utilizada inicialmente a emissão de certificados em *tokens*.

2.2.3 O EMAER emitirá aviso aos ODSA quando a nova carteira de identidade militar puder ser utilizada como mídia para geração e armazenagem dos certificados da AC Defesa. Para isso aguardará parecer da DIRAP quanto à disponibilidade da nova carteira e do CG AC Defesa quanto à adaptação dos ARR para utilizar gravadoras de cartão.

2.2.4 A DIRAP, gerente do projeto de implantação desta, deverá informar à 3ª Subchefia (3SC) do EMAER quando considerar adequada a utilização da nova carteira para armazenar o certificado.

2.2.5 O EMAER, por intermédio da 3SC, acompanhará o Projeto AC Defesa a fim de verificar quando os ARR estarão prontos para operar com gravadoras de *smart card* para geração das chaves.

2.2.6 A responsabilidade pela aquisição e distribuição da leitora de cartão é do Elo de Serviço de TI da OM à qual pertence o usuário, portanto a solicitação do usuário por emissão do certificado na nova carteira de identidade militar deve ser precedida de disponibilidade da leitora em sua OM.

2.2.7 TIPOS DE CERTIFICADOS

2.2.8 Inicialmente serão utilizados somente certificados de assinatura (série A), sendo que os certificados de sigilo (série S) serão disponibilizados pelo Projeto AC Defesa futuramente, acompanhados de instruções a respeito de seu uso.

2.2.9 No COMAER serão utilizados apenas certificados tipo A3, não sendo aceitos tipo A1 por sua menor segurança.

2.2.9.1 Os certificados tipo A3 serão emitidos no seu prazo máximo de validade (5 anos), até que o CG AC Defesa decida de forma contrária.

2.2.10 BIOMETRIA DIGITAL NO COMAER E AC DEFESA

2.2.11 Não será permitido o acesso automatizado, ou direto, ao banco de dados de identidade do COMAER pela AC Defesa. Quaisquer orientações a respeito do fornecimento de dados para a AC Defesa deverão ser homologadas pela 3SC do EMAER, que possui assento no CG AC Defesa.

3 ATRIBUIÇÕES

3.1 EMAER, POR INTERMÉDIO DA 3SC

3.1.1 Na participação no CG AC Defesa, deverá acompanhar o progresso do Projeto AC Defesa de forma a emitir orientações aos ODSA a respeito de alterações de funcionamento no serviço de emissão de certificados e na autenticação digital feita pelas AC.

3.1.2 Deverá coordenar com o COMGEP e com a DTI análise da implantação da certificação digital nos diversos sistemas informatizados do COMAER.

3.2 COMGEP, POR INTERMÉDIO DA DIRAP

3.2.1 Deverá verificar a possibilidade de sinergia entre o projeto de implantação da nova identidade militar e o Projeto AC Defesa para uso de certificados digitais na nova carteira, orientando a 3SC do EMAER.

3.2.2 Deverá analisar a convergência de procedimentos para coleta de dados digitais e/ou analógicos para emissão de carteiras de identidade militar e de certificados digitais pelo Projeto AC Defesa nas SIDOM, considerando que os ARR estão localizados nestas Seções de Identificação, emitindo orientações às SIDOM.

3.2.3 Deverá estudar as adaptações necessárias na base de dados de identidade militar, tanto no atual SIDENT quanto em eventual migração desta base para o SIGPES, com o objetivo de atender às necessidades de adoção de certificação digital pelo Projeto AC Defesa.

3.3 COMGAP, POR INTERMÉDIO DA DTI

3.3.1 Deverá auxiliar a DIRAP nos estudos e análises para adaptação das bases de dados existentes de identidade militar para adoção de biometria digital e certificado digital do Projeto AC Defesa.

3.3.2 Deverá estimar a quantidade de autenticações diárias do SIGADAER junto à AC, informando à 3SC do EMAER.

3.3.3 Deverá analisar a possibilidade de outros sistemas do COMAER virem a utilizar a certificação digital e informar à 3SC no EMAER para análise. Deverá informar a quantidade de certificados de máquina e de usuários, além da quantidade estimada de autenticações diárias à AC[3].

3.3.4 Deverá apoiar tecnicamente a AR com especialistas de TI do CCA-BR.

3.4 COMGAR, POR INTERMÉDIO DO VI COMAR

3.4.1 Deverá apoiar administrativamente a AR.

[3] O Projeto AC Defesa dispõe de grupo permanente de assessoria às equipes de desenvolvimento de sistemas das Forças Singulares que passarão a utilizar a AC Defesa. Para quaisquer adaptações em sistemas do COMAER, pode ser feita solicitação de apoio ao Projeto AC Defesa para planejar as adequações aos padrões de certificação da AC Defesa.

4 DISPOSIÇÕES GERAIS

4.1 CRITÉRIOS PARA DEFINIÇÃO DOS DETENTORES DE CERTIFICADOS DIGITAIS DA AC DEFESA

4.1.1 A emissão de certificado pelo Projeto AC Defesa tem caráter funcional. Somente os cargos e funções que necessitam utilizar a certificação digital devem ser computados para solicitar a emissão.

4.1.2 No COMAER, deverão possuir certificados digitais:

a) Oficiais Generais da ativa;

b) Comandantes, Chefes, Diretores e Prefeitos de Aeronáutica - designados em BCA;

c) Agentes Diretores delegados e Ordenadores de Despesa delegados;

d) Operadores de sistemas governamentais que requeiram o uso de certificado digital[4];

e) Eventuais substitutos dos acima mencionados.

NOTA
O certificado digital é válido como assinatura, portanto é crime o substituto assinar com o certificado digital do substituído.

4.1.3 As autoridades dos itens "a" e "b" do item 4.1.2 poderão solicitar a emissão de certificados para outros militares e servidores que o necessitem, publicando em Boletim Interno da OM a justificativa da necessidade de certificado e informando: função e dados do militar/servidor (posto/graduação/nível, nome completo, nº da identidade militar).

4.2 PROCESSO DE SOLICITAÇÃO DO CERTIFICADO DIGITAL EMITIDO PELO PROJETO AC DEFESA

4.2.1 O militar deverá agendar entrevista no sistema da AR pela internet, seguindo as orientações lá existentes.

4.2.2 Na entrevista, a fim de evitar a emissão indevida de certificado, o solicitante deve:

a) no caso de Comandantes, Chefes, Diretores e Prefeitos de Aeronáutica - apresentar cópia do BCA com a designação (exceto para Oficiais Generais);

b) no caso de Agentes Diretores e Ordenadores de Despesa delegados - apresentar cópia do Boletim Interno da OM com a publicação do ato de delegação; e

c) para os demais militares - apresentar cópia do Boletim Interno de acordo com o mencionado em 4.1.3.

4.2.3 Quando perto de sua expiração e mantida a necessidade do serviço, o certificado poderá ser reemitido uma única vez, prorrogando sua validade pelo mesmo período anterior. O

[4] Alguns exemplos: SIASG, SISCOMEX, SISCOSERV e e-CAC.

detentor deverá enviar solicitação formal à AR, assinada digitalmente com o certificado digital a ser renovado.

4.3 OUTROS SISTEMAS DO COMAER QUE UTILIZAM CERTIFICAÇÃO DIGITAL

4.3.1 Os responsáveis por sistemas do COMAER que já utilizam certificação digital, vinculada ou não à ICP-Brasil, devem analisar a conveniência de passar a utilizar a AC Defesa. Caso julguem adequado e oportuno, devem enviar solicitação à 3SC do EMAER para propor estudo.

4.4 RESPONSABILIDADES DOS DETENTORES DE CERTIFICADOS DIGITAIS DO PROJETO AC DEFESA

4.4.1 Observar regras para criação de senhas de acesso ao certificado.

4.4.2 Ser o único usuário do certificado, não cedendo o mesmo e a senha de acesso a terceiros como assessores, secretárias e substitutos eventuais.

4.4.3 Garantir a proteção e o sigilo de suas chaves privadas, senhas e mídias criptográficas.

4.4.4 Garantir proteção física do *token* contra riscos à integridade física da mídia, como acesso indevido, descargas eletromagnéticas, calor excessivo e outras condições ambientais.

4.4.5 Em caso de comprometimento de sua chave privada, como perda do *token* ou suspeita de conhecimento da senha por terceiros, solicitar imediata revogação do certificado à AR.

5 DISPOSIÇÕES TRANSITÓRIAS

5.1 O Projeto AC Defesa está em fase de auditoria para credenciamento pelo ITI, assim como a nova identidade militar em cartão inteligente (*smart card*) está ainda em implantação. Em vista disso, os militares e servidores do COMAER detentores de certificados do SERPRO adquiridos pelo COMAER e que estejam com prazo de vencimento no ano de 2016, devem buscar a revalidação de seus certificados junto ao SERPRO, de forma a não haver interrupção da capacidade de assinar digitalmente os documentos. Esta situação deverá permanecer até que o Projeto AC Defesa esteja emitindo regularmente certificados, o que será informado pelo EMAER aos ODSA.

5.2 A partir do momento que a AC Defesa estiver emitindo certificados regularmente, as futuras solicitações de renovação de certificados do SERPRO devem ser avaliadas pelo EMGEP quanto à possibilidade de ser substituídas por novo certificado da AC Defesa.

5.3 Para fins de planejamento de trabalho da AR, os ODSA deverão encaminhar para a 3SC do EMAER a quantidade estimada de emissão de certificados digitais necessários, por SIDOM, em até 30 dias da data de publicação desta ICA.

5.4 Interações com o sistema da AC Defesa deverão ser realizadas por intermédio da 3SC do EMAER, a qual possui assento no CG AC Defesa.

5.5 Certificados de outras Autoridades Certificadoras e de Registro são válidos e podem ser utilizados no COMAER, de acordo com orientação específica da DTI.[5]

[5] Para lista de AC válidas, ver no sítio do ITI na internet. Para tipos de *tokens* válidos nos sistemas do COMAER, ver sítio da DTI na INTRAER.

6 DISPOSIÇÕES FINAIS

Os casos não previstos nesta Instrução deverão ser submetidos à apreciação do EMAER.

REFERÊNCIAS

BRASIL. *Decreto nº 8.539, de 8 de outubro de 2015*. Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. [Brasília, DF], out. 2015.

BRASIL. *Portaria Interministerial MJ/MPOG n° 1.677 de 7 de outubro de 2015*. Define os procedimentos gerais para o desenvolvimento das atividades de protocolo no âmbito dos órgãos e entidades da Administração Pública Federal. [Brasília, DF], out. 2015.

BRASIL. *Portaria N º 3.004/MD, de 14 de novembro de 2012*. Determina a elaboração do Projeto de Implantação da Autoridade Certificadora de Defesa. [Brasília, DF], nov. 2012.

BRASIL. *Portaria nº 2.806/MD, de 4 de outubro de 2013*. Projeto de Implantação de Autoridade Certificadora do Ministério da Defesa (AC Defesa). [Brasília, DF], out. 2013.

_____. Comando da Aeronáutica. Comando-Geral do Pessoal. *Confecção, numeração e controle de publicações*: **ICA 5-1**. [Brasília, DF], 2004.

_____. Comando da Aeronáutica. Comando-Geral do Pessoal. Correspondência e atos oficiais: ICAER: **ICA 10-1**. [Brasília, DF], 2005.

_____. Instituto Nacional de Tecnologia da Informação (ITI). *Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil*: **DOC-ICP-01 ver 4.5**. [Brasília, DF], 2015.

_____. Instituto Nacional de Tecnologia da Informação (ITI). *Política de Segurança da ICP-Brasil*: **DOC-ICP-02 ver 3.0**. [Brasília, DF], 2008.

_____. Instituto Nacional de Tecnologia da Informação (ITI). *Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil*: **DOC-ICP-04 ver 6.1**. [Brasília, DF], 2015.

Sítio da Associação dos Registradores Imobiliários de São Paulo (ARISP). *http://www.ar.arisp.com.br/conteudo/faq_cnpj.htm* - Acessado em 07/07/2016.

Sítio da UOL. *http://tecnologia.hsw.uol.com.br/certificado-digital4.htm* - Acessado em 07/07/2016.

Sítio da Wikipedia. *https://pt.wikipedia.org/wiki/Gerenciamento_eletrônico_de_documentos* - Acessado em 07/07/2016.

Sítio do Instituto Nacional de Tecnologia da Informação (ITI). *http://www.iti.gov.br/certificacao-digital/certificado-digital* - Acessado em 07/07/2016.