GUIA DE INFORMAÇÕES

Sumário

Guia de Informações AC-Defesa

O projeto AC-Defesa visa instituir uma Autoridade Certificadora para atender as demandas por certificados no Ministério da Defesa e nas três Forças. Trata-se de um projeto relevante por conta da conjuntura mundial relacionada à segurança da informação.

A Autoridade Certificadora da Defesa (AC-Defesa) possui previsão de entrar em funcionamento em janeiro de 2015. Desta forma, o seu conhecimento e divulgação torna-se essencial em diversos níveis e setores das Forças. Este Guia de Informações foi elaborado com o objetivo de esclarecer os questionamentos mais frequentes sobre certificação digital.

As dúvidas relacionadas com o projeto, funcionamento e uso de certificação digital podem ser encaminhadas ao endereço eletrônico **suporte@acdefesa.mil.br**. No corpo da mensagem, solicita-se a identificação com nome, Organização Militar e Força a que pertence. Os esclarecimentos serão incorporados nas próximas versões do Guia de Informações AC-Defesa.

1. O que é assinatura digital ?

A assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento.

Cabe distinguir assinatura digital da assinatura digitalizada. A assinatura digitalizada é a reprodução da assinatura autógrafa como imagem por um equipamento tipo *scanner*. Ela não garante a autoria e integridade do documento eletrônico.

Os atributos da assinatura digital são:

- comprovar a autoria do documento eletrônico;
- possibilitar a verificação da integridade do documento, ou seja, quando houver qualquer alteração a assinatura não será validada;
- partindo do princípio que o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura, pode-se assegurar ao destinatário o "não repúdio" do documento eletrônico, ou seja, o emissor não pode negar a autenticidade da informação.

2. O que é criptografia simétrica e criptografia assimétrica ?

A criptografia simétrica é baseada em algoritmos que podem utilizar uma mesma chave, denominada chave secreta, utilizada tanto no processo de cifrar quanto no de decifrar o texto. Para a garantia da integridade da informação transmitida é imprescindível que apenas o emissor e o receptor conheçam a chave. O problema da criptografia simétrica é a necessidade de compartilhar a chave secreta com todos que precisam ler a mensagem, possibilitando a alteração do documento por qualquer das partes.

A criptografia assimétrica utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par. As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. A chave pública pode ser conhecida pelo público em geral, enquanto que a chave privada somente deve ser de conhecimento de seu titular.

3. O que é certificado digital ?

Na prática, o certificado digital funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a *web*, permitindo a presunção de validade jurídica de documentos eletrônicos.

Para esta finalidade, o certificado digital embarca a chave pública do proprietário a qual pode ser utilizada por uma entidade com o propósito de verificar a autenticidade de uma assinatura digital.

A veracidade de um certificado digital é atestada mediante a assinatura por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC).

Seguindo regras pré-estabelecidas, a AC associa uma entidade (pessoa, processo, servidor) a uma chave pública no momento em que é gerado e assinado (pela AC) um certificado digital.

O certificado contém os dados de seu titular conforme detalhado nas políticas de cada Autoridade Certificadora.

As principais informações que geralmente constam em um certificado digital são:

- chave pública do titular;
- nome e endereço eletrônico (*e-mail*);
- período de validade do certificado;
- nome da Autoridade Certificadora que emitiu o certificado;
- número de série do certificado digital;
- assinatura digital da Autoridade Certificadora.

4. O que é Autoridade Certificadora (AC) ?

Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, 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.

A AC 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 em sua Declaração de Práticas de Certificação (DPC).

Além de tudo, estabelece e faz cumprir, pelas Autoridades Registradoras (AR) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

5. O que é Autoridade de Registro ou Autoridade Registradora (AR) ?

Uma Autoridade de Registro ou Autoridade Registradora (AR) é responsável pela interface entre o usuário e a Autoridade Certificadora.

A AR é vinculada a uma AC e 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 possuir sua própria instalação técnica.

6. O que é uma Lista de Certificados Revogados (LCR) ?

Lista de Certificados Revogados (LCR) é uma lista, assinada pela AC, de certificados que foram revogados, ou seja, não são mais válidos.

Toda vez que um sistema de Tecnologia da Informação (TI), conectado à internet, pretende realizar a assinatura digital em um documento eletrônico, o sistema busca o endereço eletrônico (presente no certificado digital ao qual a assinatura digital está vinculada) que indica o sítio de um repositório de certificados digitais revogados mantido pela autoridade certificadora emitente do certificado digital. Este repositório representa uma Lista de Certificados Revogados (LCR).

Se o certificado daquele que está tentando assinar está presente nesta lista e a política de uso do certificado não permita a assinatura, o usuário não poderá realizar a assinatura digital.

Procedimento similar deve ocorrer com quem recebe assinatura digital e deseja validá-la. Se o certificado daquele que realizou a assinatura está presente na LCR então a assinatura será rejeitada de acordo com a política de uso do certificado.

7. O que são Declaração de Práticas de Certificação (DPC), Política de Segurança (PS) e Política de Certificado (PC) ?

A Declaração de Práticas de Certificação (DPC) descreve os processos relacionados ao ciclo de vida dos certificados digitais emitidos por determinada Autoridade Certificadora que, obrigatoriamente, deve torná-lo público. Para a emissão dos certificados, as Autoridades Certificadoras possuem deveres e obrigações que são escritos na Declaração de Práticas de Certificação.

A Política de Segurança (PS) trata-se de um documento que tem por finalidade estabelecer as diretrizes de segurança que fundamentam as normas e os procedimentos de segurança que devem ser implementados por uma Autoridade Certificadora.

A Política de Certificado (PC) descreve o tipo, conteúdo e possibilidades de cada certificado digital que pode ser emitido por uma autoridade certificadora. A PC deve estar condizente com regras estabelecidas na DPC da autoridade certificadora em questão.

Cada autoridade certificadora possui suas políticas e caso determinada AC seja credenciada no nível ICP-Brasil, deve praticá-las atendendo pelo menos aos requisitos mínimos regulados pelo Instituto Nacional de Tecnologia da Informação (ITI).

8. O que é ICP-Brasil ?

A veracidade de um certificado digital é atestada mediante a assinatura por uma terceira parte confiável, ou seja, a assinatura de uma Autoridade Certificadora. Mas o que garante que a assinatura desta AC é confiável ? Neste caso, para validar a assinatura digital desta AC é necessário verificar a veracidade do certificado digital desta AC. Isto se resolve recorrendo a assinatura de uma outra AC, que chamamos de AC de nível superior à primeira AC em questão.

Este processo se torna recursivo configurando uma cadeia hierárquica de confiança, que é o modelo adotado pela ICP-Brasil. É possível perceber que existe um certificado digital que não é assinado por nenhuma outra AC (topo da cadeia hierárquica). Este certificado é chamado de Certificado Raiz sendo um certificado auto-assinado emitido por uma AC-Raiz.

No contexto da ICP-Brasil, o certificado auto-assinado trata-se do certificado digital da AC-Raiz da ICP-Brasil.

Desta forma, 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 de um indivíduo ou entidade.

Observa-se que o modelo adotado pelo Brasil foi o de certificação com raíz 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.

9. O que é AC-Raiz ?

A Autoridade Certificadora Raiz (AC-Raiz) é a primeira autoridade da cadeia de certificação.

No contexto da ICP-Brasil, a AC-Raiz 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 (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil.

Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

10. O que é AC-Defesa ?

Trata-se da Autoridade Certificadora do Ministério da Defesa (MD) (AC-Defesa). O projeto foi implantado em 2013 e vislumbra a criação de uma autoridade certificadora de Defesa credenciada pela ICP-Brasil.

Ela tem como missão emitir e fornecer certificados digitais para o Ministério da Defesa, bem como para as três Forças: Marinha do Brasil (MB), Exército Brasileiro (EB) e Força Aérea Brasileira (FAB).

A AC-Defesa será composta de uma Autoridade Certificadora Titular em Brasília, uma Autoridade Certificadora Reserva no Rio de Janeiro, uma instalação técnica integrando uma Autoridade de Registro (AR) em Brasília e 106 (cento e seis) agentes de registro remotos distribuídos em guarnições militares no território nacional.

11. Quais usuários terão direito a um certificado digital emitido pela AC-Defesa ?

Inicialmente, terão direito a certificado digital ICP-Brasil emitido pela AC-Defesa os militares e servidores civis do Ministério da Defesa, Marinha do Brasil, Exército Brasileiro e Força Aérea Brasileira.

12. Quais as etapas necessárias previstas pela ICP-Brasil para emitir um certificado digital ?

Para a emissão de um certificado digital é necessário cumprir basicamente duas etapas conhecidas como validação e verificação.

A validação da solicitação de certificado, realizadas mediante a presença física do interessado, compreende a confirmação da identidade de um individuo ou de uma organização, a conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.

A verificação da solicitação de certificado compreende a confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:

- por agente de registro distinto do que executou a etapa de validação;

- em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;
- somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;
- antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

13. O que é um agente de registro previsto pela ICP-Brasil ?

É um profissional que realiza as etapas necessárias no processo de emissão e revogação de certificados nas Autoridades de Registro.

Há duas categorias de agentes de registro: validador e verificador. O primeiro realiza a etapa de validação e o segundo realiza a etapa de verificação no processo de emissão do certificado.

O agente de registro que realiza a etapa de verificação obrigatoriamente deverá se localizar dentro da instalação técnica de uma autoridade de registro.

14. O que é um agente de registro remoto no contexto da AC-Defesa ?

Trata-se de um agente de registro que realiza a etapa de validação por meio de acesso remoto ao sistema.

Estão previstos 106 (cento e seis) agentes de registro remotos para o funcionamento da AC-Defesa distribuídos pelo território nacional.

Os usuários da AC-Defesa poderão se dirigir a qualquer um dos agentes de registro remoto para realizar a etapa de validação no processo de emissão do certificado digital, independente de estar localizado em um órgão do Ministério da Defesa, da Marinha do Brasil, do Exército Brasileiro ou da Força Aérea.

15. Quais são os tipos de certificados digitais previstos pela ICP-Brasil ?

São 10 (dez) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 6 (seis) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir.

Tipos de Certificados de Assinatura Digital (garantir autenticidade de conteúdo):

- A1
- A2
- A3
- A4
- T3
- T4

Tipos de Certificados de Sigilo (garantir sigilo de conteúdo):

- S1
- S2
- S3
- S4.

Os certificados de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

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

Certificados do tipo T3 e T4 somente podem ser emitidos por equipamentos das Autoridades de Carimbo do Tempo (ACT) credenciadas na ICP-Brasil. Os certificados T3 e T4 estão associados com *Timestamp* ou Carimbo de Tempo aplicado a uma assinatura digital ou a um documento eletrônico. O Carimbo de tempo prova que a assinatura ou o documento existia na data incluída no carimbo.

A utilização de carimbos do tempo no âmbito da ICP-Brasil é facultativa, ou seja, documentos eletrônicos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil são válidos com ou sem o carimbo do tempo.

Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança dos níveis 3 e 4 respectivamente, exceto pelo tamanho das chaves criptográficas utilizadas.

O processo de geração de chaves criptográficas definido pela Políticas de Certificação de determinada AC deverá ser realizado, para cada tipo correspondente de certificado previsto pela ICP-Brasil, conforme a Tabela a seguir:

Tipo de Certificado	Chaves Criptográficas	Exemplo de Utilização
A1	Geração em *software* e utilização em *software*	Roteador, Servidor Web, etc. utilizando o certificado para autenticação
S1	Geração em *software* e utilização em *software*	Pessoa Física utilizando sua chave privada em *software* para criptografar dados de conteúdo sigiloso
A2	Geração em *software* e utilização em *hardware*	Pessoa Física utilizando dispositivo criptográfico (*smartcard* ou *token*) para se autenticar
S2	Geração em *software* e utilização em *hardware*	Pessoa Física utilizando sua chave privada em dispositivo criptográfico (*smartcard* ou *token*) para criptografar dados de conteúdo sigiloso
A3	Geração em *hardware* e utilização em *hardware*	Pessoa Física utilizando dispositivo criptográfico (*smartcard* ou *token*) para se autenticar
S3	Geração em *hardware* e utilização em *hardware*	Pessoa Física utilizando sua chave privada em dispositivo criptográfico (*smartcard* ou *token*) para criptografar dados de conteúdo sigiloso
T3	Geração em *hardware* e utilização em *hardware*	Comprovação de que determinado documento emitido estava válido em determinado momento, por exemplo, certidões de cartório, autorizações, .etc
A4	Geração em *hardware* e utilização em *hardware*	Pessoa Física utilizando dispositivo criptográfico (*smartcard* ou *token*) para se autenticar
S4	Geração em *hardware* e utilização em *hardware*	Pessoa Física utilizando sua chave privada em dispositivo criptográfico (*smartcard* ou *token*) para criptografar dados de conteúdo sigiloso
T4	Geração em *hardware* e utilização em *hardware*	Comprovação de que determinado documento emitido estava válido em determinado momento, por exemplo, certidões de cartório, autorizações, etc

16. O que são *smartcards* e *tokens* ?

São dispositivos criptográficos (*hardware*) que podem embarcar chaves privadas e certificados digitais.

Smartcard é o mesmo que Cartão Inteligente e demanda a utilização de uma leitora que deve ser conectada a um sistema de TI.

Token é um termo utilizado para qualquer dispositivo utilizado em segurança que se conecte a um sistema de TI. O mais conhecido é o *token* USB que é semelhante a um *pendrive* e possui a facilidade de conexão com diversos sistemas de TI devido ao USB (tipo de conexão) amplamente difundido.

O *smartcard* e o *token* USB são utilizados com certificados digitais A2, S2, A3, S3, T3, A4, S4 e T4.

17. Quais tipos de certificados a AC-Defesa empregará ?

Inicialmente, serão empregados os certificados digitais A1, S1 e A3.
O dispositivo criptográfico a ser empregado com o certificado digital A3 será o *token* USB nos primeiros anos de operação.

18. Como utilizar o certificado digital ?

Para utilizar o certificado digital, antes de qualquer procedimento, é necessário assegurar-se de que o sistema de Tecnologia da Informação (TI) de interesse permite realizar e verificar assinaturas digitais.

Em caso positivo, é necessário que o usuário tenha algum tipo de certificado digital emitido em seu nome. De posse do certificado, o usuário deve selecionar o documento eletrônico que deseja assinar e submetê-lo ao sistema para que este invoque as funções necessárias para a realização da assinatura digital.

Cabe ressaltar que para utilizar determinados tipos de certificados é necessário instalar o *driver* do dispositivo criptográfico, ao qual o certificado está embarcado, na máquina do usuário final.

Por exemplo, no caso de certificados digitais do tipo A3, é necessário instalar o aplicativo do fabricante do *token* ou *smartcard* que abriga o certificado digital. Somente desta maneira, o sistema operacional da máquina do usuário reconhecerá a mídia e, consequentemente, o certificado digital.

19. Como fazer que meu sistema utilize certificado digital ?

Para que um sistema de TI utilize certificado digital é necessário que o sistema permita realizar e verificar assinaturas digitais.

Para realizar assinaturas digitais, é necessário integrar ao código-fonte de um sistema de TI determinadas *Aplication Programming Interfaces* (API) e bibliotecas criptográficas na linguagem de programação ao qual o sistema está implementado.

As APIs e bibliotecas habilitam funcionalidades que permitem utilizar os certificados digitais para realizar e verificar assinaturas utilizando todas as informações necessárias constantes nos certificados digitais.

Existem diversas APIs e bibliotecas criptográficas disponíveis. Algumas são de código-fonte aberto e outras são proprietárias.

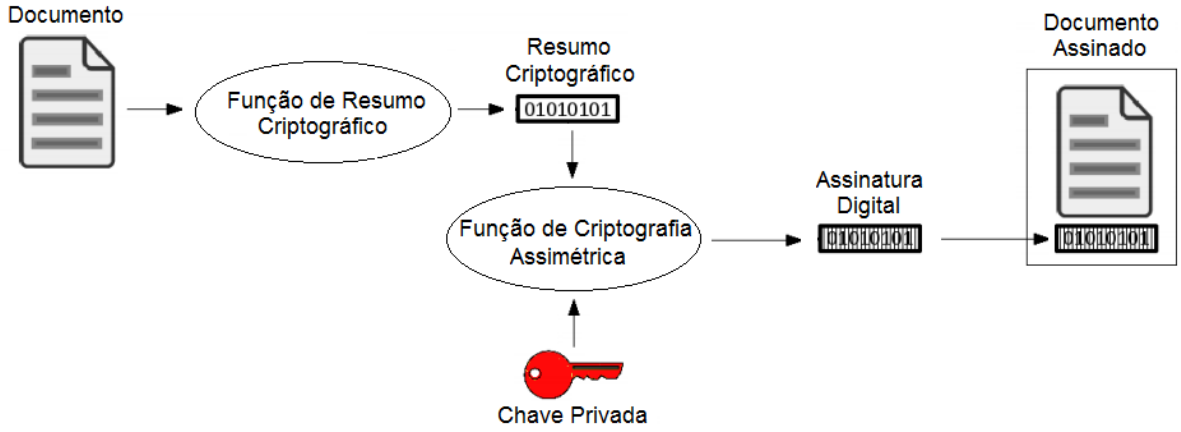
As APIs e bibliotecas podem ser integradas a um sistema de TI específico ou não. Se não forem integrados, funcionam como um assinador digital independente e devem ser instalados a parte. Estas soluções são conhecidas como *softwares* de assinatura digital, sigilo e autenticação.

A ICP-Brasil prevê normas e procedimentos para os *softwares* de assinatura digital, sigilo e autenticação.

20. Supondo que eu assine um documento eletrônico utilizando certificado digital, como garantir que o documento eletrônico não foi alterado e que a assinatura digital é minha e está válida ?

A assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática, que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento.

A técnica permite não só verificar a autoria do documento, como também estabelece uma “imutabilidade lógica” de seu conteúdo, pois qualquer alteração do documento, como por exemplo a inserção de mais um espaço entre duas palavras, altera a assinatura.



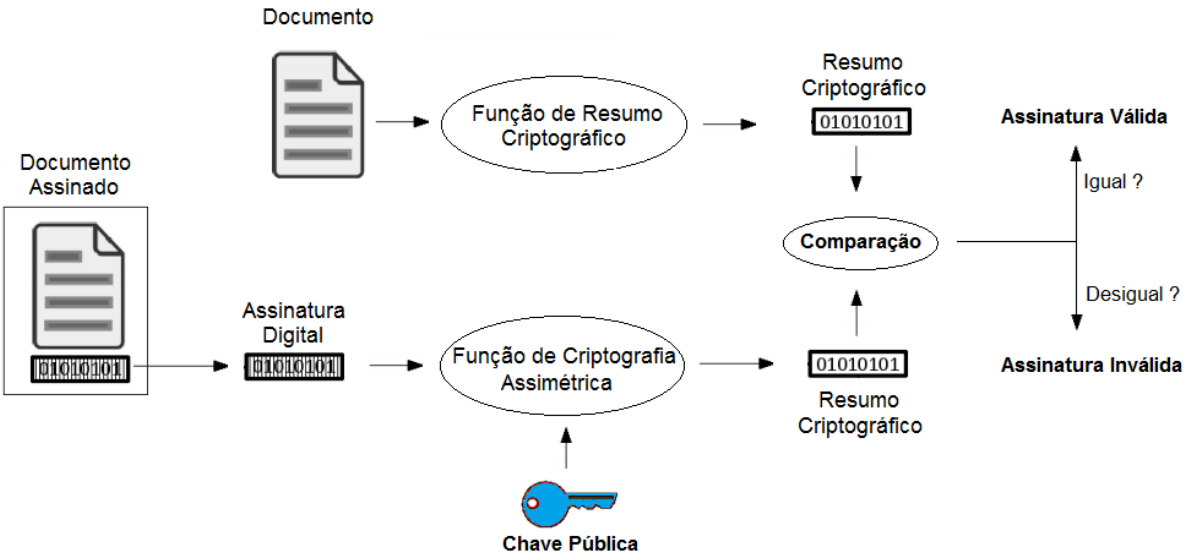
O diagrama apresenta, de forma simplificada, o processo criptográfico de criação de uma assinatura digital:

- o sistema utilizado pelo signatário deve gerar um resumo criptográfico de um documento eletrônico;
- o sistema utilizado pelo signatário deve cifrar o resumo criptográfico com sua chave privada, associada a uma chave pública constante do seu certificado digital, gerando a assinatura digital;
- o documento eletrônico e a assinatura digital ficam associados para futura validação.

No caso de certificados digitais do tipo A3, a chave pública, bem como outras informações constantes do certificado digital, permanecem em uma região de memória do *token* ou *smartcard* acessível, ou seja, é possível extrair estas informações da mídia.

A chave privada, única e exclusiva do proprietário, permanece numa região de memória inacessível da mídia (*tamper proof*), ou seja, não acessível para ser extraída.

Ao receber o documento eletrônico assinado digitalmente, o sistema de TI habilitado para trabalhar com certificação digital realizará a prova da assinatura digital. Para isto o sistema deve receber o documento assinado digitalmente e as informações públicas mínimas necessárias enviadas conjuntamente com o documento eletrônico (certificado digital do autor da assinatura). Além disso, deve ter sido instalado no sistema do receptor da assinatura o certificado raiz da cadeia de certificação do certificado digital do emissor da assinatura.



O diagrama apresenta, de forma simplificada, o processo criptográfico de verificação de assinatura digital:

- o documento eletrônico e a assinatura digital associada são disponibilizados para o verificador, juntamente com o certificado digital do signatário;
- o sistema utilizado pelo receptor calcula novamente o resumo criptográfico do documento eletrônico;
- o sistema utilizado pelo receptor decifra a assinatura digital com a chave pública do signatário, contida no certificado digital, obtendo o resumo criptográfico gerado e cifrado pelo signatário no momento da assinatura;
- o sistema utilizado pelo receptor compara os resumos criptográficos obtidos nos passos anteriores. Se forem iguais, significa que o documento eletrônico esta íntegro e que é possível identificar o signatário por meio do certificado digital. Caso contrário, a assinatura digital é inválida.

21. Como posso usar a AC-Defesa para fornecer documentos eletrônicos assinados digitalmente ?

A AC-Defesa não fornecerá documentos eletrônicos (certidões, licenças, registros, etc.) assinados digitalmente.

O usuário final deve submeter o próprio certificado digital além dos documentos eletrônicos de seu interesse a um sistema de TI habilitado para que uma assinatura digital possa ser realizada.

A utilização da AC-Defesa recai exclusivamente na emissão de certificados digitais ICP-Brasil. Para esta finalidade a AC-Defesa destina-se a manter toda uma estrutura física, lógica e de pessoal para creditar confiabilidade dos certificados digitais aos quais ela emite.

Por exemplo, se um militar do Exército Brasileiro deseja obter uma certidão ou documento comprobatório de quitação ou finalidade semelhante emitido por determinado órgão do Exército, este órgão deve ter implementado em seu sistema as funcionalidades que habilitem o uso de certificação digital (funcionalidades que habilitem a emissão de assinaturas digitais). Além disso, este sistema deve ter um certificado digital o qual poderá ser emitido pela AC-Defesa.

22. A AC-Defesa fornecerá que facilidades para o desenvolvedor ?

Além de emitir certificados digitais para o público específico do Ministério da Defesa e as três Forças, a estrutura da AC-Defesa possuirá equipe técnica destinada a operação, manutenção e evolução da solução de *software* empregada na AC-Defesa.

Esta equipe poderá desenvolver aplicativos e interfaces relacionados com certificação digital para uso pela própria AC-Defesa. A equipe também poderá auxiliar os desenvolvedores que desejem introduzir a assinatura digital em suas aplicações por meio de notas técnicas e orientativas ou, em casos mais específicos, por meio de consultorias. Entretanto, o trabalho de desenvolvimento sempre será do próprio interessado.