**Certificados Digitais**

1.1.3. São 11 (onze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 7 (sete) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de **Certificados de Assinatura Digita**l: i. A1 ii. A2 iii. A3 iv. A4 v. T3 vi. T4 vii. A CF-e-SAT

Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

b) Tipos de **Certificados de Sigilo**: i. S1 ii. S2 iii. S3 iv. S4 1.1.4.

Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo

Os tipos de certificados indicados acima, 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. 1.1.5. Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

Tipo de Certificado

Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)

A1 e S1 Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima A2 e S2 Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica

**A3 e S3 Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO**.

A4 e S4 Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

T3 e T4 Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO. A CF-e-SAT Hardware criptográfico

**A1, A2, S1 e S2 = SOFTWARE (**Processo de Geração de Chave Criptográfica)

**A3, A4, S3, S4, T3, T4 e A CF-e-SAT = HARDWARE (**Processo de Geração de Chave Criptográfica)

A assinatura digital acontece em 2 etapas:

* 1° Etapa - Tudo começa com a própria geração da assinatura, ou seja, no momento em que a pessoa assina o documento. Esse remetente cria o documento original e extrai um resumo do documento (o chamado “Hash”), que é gerado automaticamente pelo próprio software que a pessoa está usando para assinar o documento. A partir de então o remetente, com sua chave privada, criptografa esse resumo. Atenção: o que foi criptografado nesse momento foi apenas o resumo da mensagem. O documento original segue intacto.
* 2° Etapa - Nessa etapa da assinatura digital diz respeito à validação. É nesse momento que será feita a verificação da mensagem para se saber se ela foi assinada pelo remetente e, somente então, ela será validada.

**TIPOS DE CERTIFICADO**

* **Série A (A1,A2,A3 e A4)**  
    
  - Reúne os certificados de assinatura digital, utilizados na confirmação de identidade na web, em e-mail, em redes VPNs e em documentos eletrônicos com verificação da integridade de suas informações. Quando pensar na série **A**, pense em **A**UTENTICIDADE, ASSINATURA DIGITAL.

* **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. Quando pensar em série **S**, pense em **S**IGILO, CODIFICAÇÃO DE DOCs e DADOS.

**VALIDADE(ANOS):**A1/S1 vale 1 ano | A2/S2 vale 2 anos | A3/S3 vale 3 anos | A4/S4 vale 3 anos.

**GERAÇÃO DE CHAVE:** A1/S1 e A2/S2: Soft | A3/S3 e A4/S4: Hard

**TAMANHO DAS CHAVES(BITS)**: A1/S1, A2/S2, A3/S3 = 1024 Bits | A4/S4 = 2048 Bits

**RSA:** Algoritmo **assimétrico** que usa duas chaves: uma para encriptação e outra para decriptação. Resolve o problema de distribuição de chaves da criptografia simétrica com o envelopamento digital. É considerado um dos algoritmos mais seguros e o primeiro a possibilitar a assinatura digital. **O tamanho das chaves varia entre 512 e 2048 bits**. Seu funcionamento baseia-se na dificuldade computacional de se fatorar um número inteiro grande. Quanto maior a chave, maior a segurança e menor a velocidade de execução.

**AES:** Também é conhecido como Rijndael e também é um algoritmo **simétrico de cifra de bloco**. Veio para substituir os algoritmos DES, requer pouca memória e é bastante rápido. É um padrão de criptografia utilizado pelo governo dos Estados Unidos desde 2002. **O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.** Cada bloco é tratado como uma matriz de 4x4 bytes. Por meio do ataque XSL a segurança computacional deste algoritmo pode ser reduzida, entretanto, ainda assim, o AES é considerado um algoritmo computacional bastante seguro.

**DES**- Algoritmo de chaves **simétricas**, com **bloco de 64 bits subdividido em 56 bits da chave** e **8 bits de paridade.**

**RC4** é uma cifra de fluxo criada em 1987 por Ron Rivest para a RSA Security de **tamanho de chave variável** com operações **orientadas a byte.**

O algoritmo é baseado no uso de uma permutação aleatória. A análise mostra que o período da cifra muito provavelmente é maior que **10^100 [ROBS95a]**. De oito a dezesseis operações de máquina são necessárias por byte de saída, e a cifra pode executar muito rapidamente em software. **RC4** é usado nos padrões ***Secure Sockets Layer/Transport Layer Security (SSL/TLS)***, que foram definidos para a comunicação entre **navegadores** e **servidores Web.**

**SSL ou TLS**utilizam criptografia **assimétrica** (chave pública + chave privada). Confidencialidade e Integridade.

* **Início da Conexão:** É estabelecida uma**conexão de chaves assimétricas, dentro dessa conexão é compartilhada uma chave simétrica que será utilizada posteriormente;**
* **Troca de Dados:** os**dados são transmitidos criptografados com a chave simétrica compartilhada no início da conexão**. Isso se deve ao fato de a **criptografia simétrica ser muito menos dispendiosa computacionalmente**em relação a criptografia assimétrica.

Os **Certificados Secure Socket Layer (SSL)** são o método padrão usado na Internet para proteger as comunicações entre os usuários da Web e os sites. Essa tecnologia autentica a identidade de um site e criptografa as comunicações entre o usuário e o site.

O **Certificado SSL de Validação Avançada (EV SSL)** é um tipo de Certificado SSL.

Um consórcio de especialistas em segurança da Internet (Autoridade de Certificação/Fórum de Navegadores), incluindo a VeriSign, criou o SSL de Validação Avançada (EV SSL) para combater a epidemia cada vez maior de atividades fraudulentas na web, conhecidas como phishing.

O phishing é uma técnica usada pelos criminosos na web para induzir os usuários a revelar informações pessoais e financeiras confidenciais a um site falsificado.

Esses sites de phishing têm a aparência de um site conhecido, mas eles são apenas a fachada enganosa de uma atividade ilegal. Pode ser muito difícil diferenciar um site de phishing do site legítimo. E, devido a essa ameaça, tornou-se mais importante do que nunca a autenticação dos sites como legítimos por instituições independentes confiáveis, antes que os usuários forneçam informações nesses sites.

**Protocolo de Diffie-Hellman:**

* É usada para intercambio de chaves entre usuários;
* É baseado na operação de logaritmos discretos;
* Logaritmo discreto é baseado na raiz primitiva;
* Requer autoridade de certificação (chave pública confiável).
* não permite assinatura digital.

Algoritmos de criptografia simétrica tem um custo computacional menor para cifrar e decifrar a mensagem do que algoritmos assimétricos.

O Princípio de Kerckhoffs afirma que a segurança dos dados encriptados deve depender do conhecimento da chave usada, podendo o método ou algoritmo usado ser de conhecimento público.

**Sistema assimétrico**: duas chaves, uma privada e uma pública.

Se o remetente usa a privada dele mesmo e o destinatário usa a pública: Autenticidade garantida. Se o remetente usa a pública (agora do destinatário) e o destinatário usa a privada: Confidencialidade garantida. Essas são as únicas duas garantias da criptografia por chaves assimétricas. Ponto final.

Quanto à INTEGRIDADE que ficou confuso para alguns: Quando você vai usar a criptografia em ASSINATURAS DIGITAIS, num documento grande por exemplo, em vez de criptografar todo o documento, você aplica a função HASH que vai gerar um código daquele documento onde aí sim se tem por garantia a INTEGRIDADE. Só depois de usada a função HASH é que se aplica a criptografia, esse documento é enviado para o destinatário "em aberto" pois a assinatura digital SÓ GARANTE INTEGRIDADE E AUTENTICIDADE.

Então é preciso ter em mente que temos duas situações: Criptografia de chaves assimétricas e assinaturas digitais que também envolve criptografia, porém não se confundem.

Em suma:

Criptografia assimétrica = Autenticidade e Confidencialidade

Assinatura digital = Integridade e Autenticidade (não repúdio).

Controles de Acesso:

* **Baseado em perfis:** Também conhecido como Role Based Access Control (RBAC), o acesso é determinado em função de grupos de trabalho (departamentos) ou do próprio cargo exercido pelo usuário. No caso, cada perfil terá seus privilégios aplicados de forma genérica.
* **Mandatório (Obrigatório):** Essa classificação de controle costuma ser representada pelo acrônimo **MAC (Mandatory Access Control)**. Por meio desta funcionalidade, é o sistema quem aplica as políticas de acesso, obedecendo às configurações de privilégio (definidas pelo administrador de sistemas) e a rotulação das informações (feita pelo gestor da informação).Geralmente, o controle de acesso mandatório é utilizado por empresas que trabalham com dados críticos e sensíveis, ou seja, onde o acesso não autorizado pode acarretar em graves consequências.
* **Discricionário:** No controle de acesso discricionário**(Discretionary Access Control – DAC),** quem determina as regras e critérios de acesso às informações é o proprietário do recurso. Em poucas palavras, o proprietário da informação define os usuários que podem acessá-la. Sendo assim, para que esse tipo de controle de acesso nas informações seja implantado corretamente, é necessário que todo e qualquer objeto armazenado no sistema tenha um proprietário e este concederá as permissões de acesso aos devidos usuários. Criar o controle de acesso nas informações é um grande passo para assegurar a segurança e integridade dos dados contidos no sistema. No entanto, o processo requer um bom planejamento para que seja escolhido o mecanismo adequado para o perfil da empresa.