

Infraestrutura de chaves públicas

Segurança da Informação
Curso Técnico em Redes de Computadores
ETER – FAETEC - Rio de Janeiro - RJ

O problema de compartilhar chaves públicas.

- Uma questão pertinente é: Como o destinatário e o remetente obtiveram acesso às chaves públicas, um do outro?
- Anteriormente, era comum as pessoas publicarem suas chaves públicas em sites na Internet, compartilhar via e-mail para quem solicitasse, entre outros meios.
- Mesmo assim, vários tentaram violar os sistemas, trocando a chave pública por outra chave pública, a do atacante.
- Então, surgiu um problema, que é o compartilhamento das chaves públicas. Como resolver?

Autoridade Certificadora (AC)

- Já em 1978, os autores do artigo que deu origem ao RSA já apontaram o problema do compartilhamento das chaves públicas, e sugerem que deveria haver uma “terceira parte em que todos confiam”.
- Esta terceira parte é a **Autoridade Certificadora (AC)**, e a **Infraestrutura de Chaves Públicas (ICP)** contém a AC e outras entidades importantes.

Infraestrutura de Chaves Públicas (ICP).

- Algumas das funções da ICP são:
 - 1) Criar, proteger, distribuir e revogar certificados;
 - 2) Fazer a ligação entre os mundos digital e o real;
 - 3) Criar processos de trabalho para as pessoas envolvidas;
 - 4) Gerenciar questões financeiras e legais, hardware e software;
 - 5) Relacionar as ACs com as outras ACs.
 - 6) Relacionar as ICPs com outras ICPs.
- Para que isto tudo funcione, a ICP é composta de algumas entidades.

Principais componentes da ICP.



Usuário

Certificado digital.

- O maior problema da ICP é garantir que uma chave pública realmente pertença a quem diz ser seu dono.
- Uma maneira de resolver o problema é distribuir chaves públicas “dentro” de certificados digitais.

O que é o certificado digital?

- Um certificado é um arquivo digital que contém informações como: a versão e número de série do certificado; informações sobre a entidade que gerou o certificado e a entidade usuária do certificado; a validade; a combinação de protocolos usados (MD5 com RSA, SHA-1 com RSA etc.); o tipo de chave pública; a assinatura (sequência de bits que representa o hash cifrado pela AC) e a chave pública (sequência de bits que representa a chave em si).
- O formato padrão dos certificados está especificado na RFC 2459, de 1999, e é conhecido como X.509.

Exemplo de um certificado no formato X.509.

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/Email=server-certs@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After : Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/Email=server-certs@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d3:a4:50:6e:c0:ff:56:6b:e6:cf:5d:b6:ea:0c:
66:75:47:a2:aa:c2:da:84:25:fc:a6:f4:47:51:da:
85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:bl:6b:
29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
3a:c2:b5:66:22:12:d6:87:0d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical
CA:TRUE

Signature Algorithm: md5WithRSAEncryption

07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
a0:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
70:47

Nesse certificado, temos:

- Número serial.
- Algoritmo usado para assinatura (MD5 com RSA).
- Validade.
- Quem autenticou esse certificado.
- Chave pública usada (RSA 1024 bits).
- Assinatura digital feita pela Autoridade Certificadora.

Como isto resolve o problema das chaves públicas?

- O remetente gera um par de chaves (pública e privada), se conecta a uma Autoridade de Registro (AR), vinculada à Autoridade Certificadora (AC) e solicita a criação de um certificado, dentro do qual sua chave pública está inserida.
- O destinatário extrairá desse certificado a chave pública do remetente, e assim poderá enviar mensagens cifradas, de forma que somente o remetente poderá ler.
- Mas... Quem garante a idoneidade da AC?

Estrutura da ICP.

- Uma ICP é uma estrutura grande, composta por hardware, software, pessoas e processos. Basicamente ela é composta de cinco entidades, a saber:
 - Autoridade Certificadora (AC).
 - Autoridade de Registro (AR).
 - Serviços de Diretório.
 - Entidade final.
 - Clientes.

Autoridade Certificadora (AC).

- A AC executa funções como:
 - Gerar o par de chaves para os usuários da ICP;
 - Criar certificados digitais para armazenar as chaves públicas;
 - Assinar os certificados com a sua própria chave privada;
 - Assinar certificados de outras ACs dentro da hierarquia da ICP;
 - Realizar a certificação cruzada com ACs de outra infraestrutura.

Autoridade Certificadora (AC).

- Os usuários de uma ICP precisam confiar na AC. Isto ocorre quando as assinaturas realizadas pela AC são validadas pela chave pública da AC.
- Logo, a chave pública da AC deve ser distribuída livremente, e também é distribuída dentro de um certificado.

Autoridade de Registro (AR).

- A AR é um local físico (um prédio, por exemplo) para onde vão os clientes da ICP que querem um certificado digital assinado por ela.
- Na AR, os profissionais da equipe da ICP comparam as informações da entidade para a qual o certificado está sendo gerado com as informações da pessoa que está solicitando naquele momento.
- A intenção é impedir que um atacante vá até a ICP e solicite um certificado para outra pessoa. Ou seja, é nesse momento que a ICP, através da autoridade de registro, estabelece um vínculo entre o mundo real e o certificado digital.

Funções da AR.

- Algumas das funções da AR são:
 - Atestar a veracidade dos documentos apresentados pelos clientes da ICP;
 - Validar assinaturas e reconhecer firma dos clientes;
 - Fornecer dispositivos que armazenam chaves e certificados – pode ser um pendrive, um smartcard, etc;
 - Receber pagamentos referentes aos serviços da ICP;
 - Armazenar a documentação referente à geração do certificado.

Serviços de Diretório.

- Os serviços de diretório fazem o armazenamento das chaves, certificados e outras informações, e tratam de permitir que a informação seja acessada de forma adequada.
- Por exemplo, é comum a estrutura de chaves (diretório) seguir o formato X.500 (criado pela ITU-T) e o acesso ser via protocolo LDAP.

Revogação de certificados.

- Os serviços de diretório podem revogar certificados, e periodicamente emitem listas de revogação de certificados.
- Um certificado pode ser revogado por vários motivos. Os principais são: violação da segurança das chaves do usuário (roubo, perda, etc); expiração do prazo de validade do certificado; falha nos procedimentos feitos pela AR e violação da segurança da AC que gerou o certificado.
- Quando um certificado é revogado, o proprietário fica impedido de usá-lo, e deve se encaminhar à AR para gerar um novo certificado.

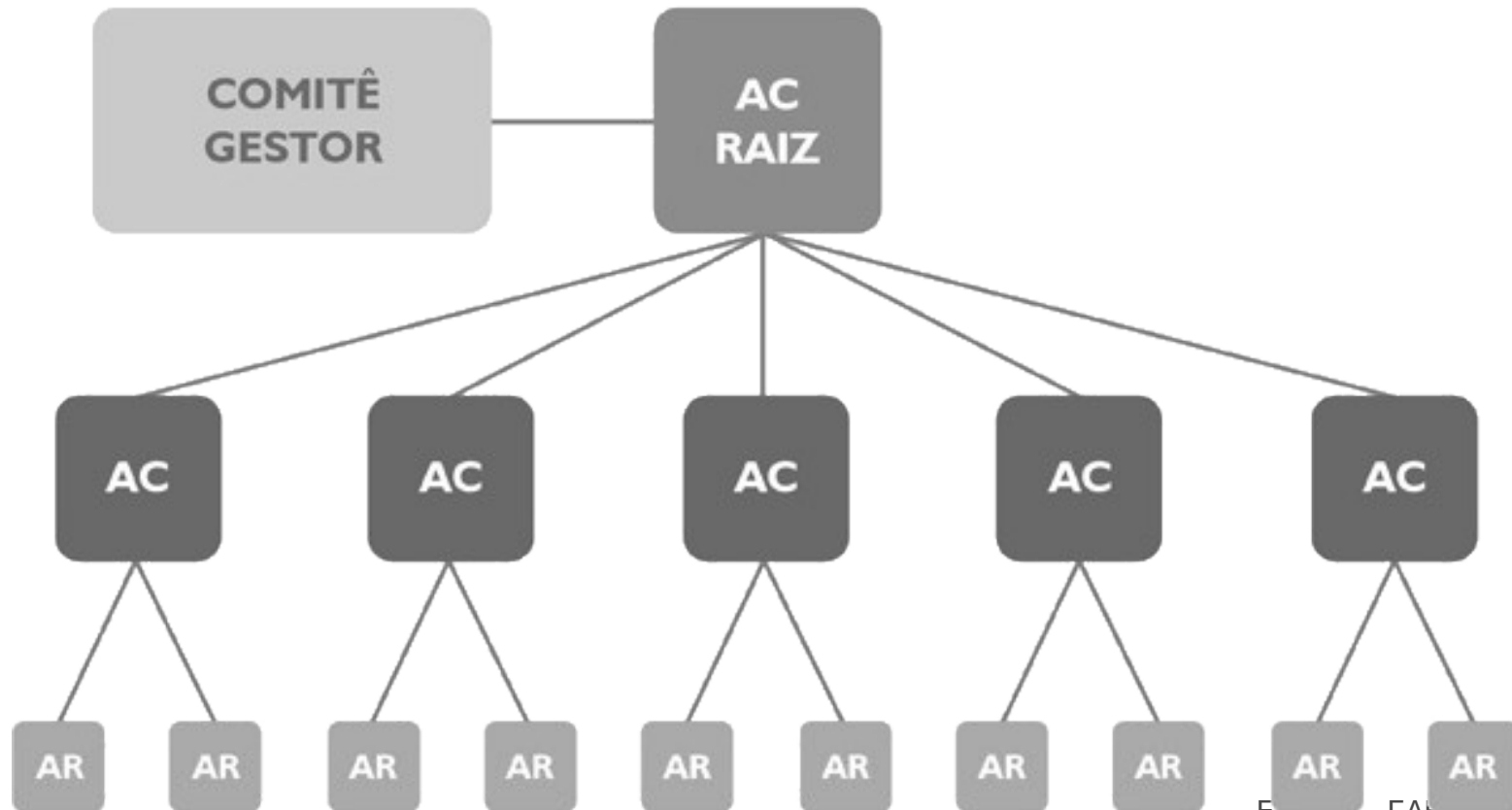
Entidade final e cliente

- As entidades finais são pessoas físicas e jurídicas, sistemas, softwares e hardwares, que podem ser autenticados usando criptografia assimétrica.
- Os clientes (ou usuários) são as pessoas (físicas ou jurídicas) que se responsabilizam pelo certificado em nome de uma entidade final. Logo, eles pagam as taxas, providenciam a documentação necessária, etc.

Hierarquia de ACs.

- Qualquer Autoridade Certificadora pode emitir certificados válidos para entidades finais.
- Elas estão arrançadas na forma de uma árvore, onde uma AC nova é certificada pela sua “AC raiz”. Logo, quando ela emite um certificado, ela fornece o seu próprio certificado, que foi assinado pela AC “de cima”.
- Note que a AC Raiz só emite certificados para as ACs vinculadas a ela.

Hierarquia de ACs.



O ICP-Brasil.

- A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é a ICP certificada pelo governo brasileiro para gerência de certificados digitais, e é uma autarquia federal vinculada ao Instituto Nacional de Tecnologia da Informação (ITI), autarquia vinculada à Casa Civil da Presidência da República.
- O ICP-Brasil foi criada por decreto em 2001 (MP 2200-2/2001), com o objetivo de “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais”.
- <https://www.gov.br/iti/pt-br/assuntos/icp-brasil>

Entes do ICP-Brasil - AC-Raiz.

- Executa as Políticas de Certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Emite a Lista de Certificados Revogados, fiscaliza e audita as ACs, as ARs e demais prestadores de serviço habilitados na ICP-Brasil. Também verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

Entes do ICP-Brasil - AC.

- Entidade, pública ou privada, subordinada à hierarquia da 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).
- Também emite Listas de Certificados Revogados e mantém registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação. Estabelecer e faz cumprir pelas ARs a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

Entes do ICP-Brasil - AR.

- Responsável pela interface entre o usuário e a AC. Vinculada a uma AC, recebe, valida, encaminha solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. A AR é responsável por registrar suas operações. Pode estar fisicamente localizada dentro de uma AC ou ser uma entidade de registro remota.

Entes do ICP-Brasil: PSC.

- O Prestador de Serviço de Confiança (PSC) da ICP-Brasil é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de chaves privadas para usuários finais, além de serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos.

Entes do ICP-Brasil - ACT.

- A ACT é a Autoridade Certificadora do Tempo. Os usuários de serviços de Carimbo do Tempo devem confiar nessa entidade para emissão dos mesmos. Logo, ela tem a responsabilidade geral pelo fornecimento do Carimbo do Tempo.
- O Carimbo do Tempo é um conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere provar a sua existência em determinado período.
- Explicando: Um documento é produzido e seu conteúdo é cifrado. Ele recebe os atributos ano, mês, dia, hora, minuto e segundo, atestado na forma da assinatura realizada com certificado digital servindo assim para comprovar sua autenticidade. A ACT atesta não apenas a questão temporal de uma transação, mas também seu conteúdo.

Entes do ICP-Brasil - PSS.

- O Prestador de Serviço de Suporte (PSS) desempenha atividade descrita nos seguintes documentos:
 - Políticas de Certificado e na Declaração de Práticas de Certificação da AC a que estiver vinculado, diretamente ou por intermédio da AR;
 - Políticas de Carimbo do Tempo;
 - Declaração de Práticas de Carimbo do Tempo da ACT a que estiver vinculado;
 - Atividades da PSBio.
- Desempenha três funções:
 - Disponibilização de infraestrutura física e lógica;
 - Disponibilização de recursos humanos especializados;
 - Disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

Entes do ICP-Brasil - PSBio.

- O PSBio é o Prestador de Serviço Biométrico. Ele é uma entidade com capacidade técnica para realizar a identificação biométrica. Logo, o PSBio torna um registro único feito por um requerente em uma informação a ser compartilhada para um ou mais bancos/sistemas de dados biométricos para toda ICP-Brasil.
- Ela também faz a verificação biométrica do requerente de um certificado digital e a comparação de uma biometria, que possua característica perene e unívoca, de acordo com os padrões internacionais de USO.

ICP-Brasil, em números (2023).

- 1 Autoridade Certificadora Raiz (AC-Raiz);
- 23 Autoridades Certificadoras (AC);
- 9 Autoridades Certificadoras de Tempo (ACT);
- 24 Prestadores de Serviço de Suporte (PSS);
- 7 Prestadores de Serviço Biométrico (PSBio);
- 7 Prestadoras de Serviço de Confiança (PSC);
- Inúmeras Autoridades de Registro (AR).

Tipos de certificados emitidos pela ICP-Brasil.

- Duas famílias de certificados:
 - A: São usados para autenticação e não repúdio.
 - S: São usados para autenticação, não repúdio e confidencialidade.
 - Cada família tem 4 tipos de certificados, que se diferenciam de acordo com quem gerou (software ou hardware), tamanho da chave em bits, onde está armazenado e validade.
 - Por exemplo, o certificado mais comum é o **A3**: gerado por hardware, chave de 1024 ou 2048 bits, armazenamento em smart card ou token USB, validade máxima de 3 anos.
 - Os certificados devem ser adquiridos, por um valor que começa em torno de R\$ 100, dependendo da sua complexidade, validade e uso.

Conclusão e resumo.

- A Infraestrutura de Chaves Públicas (ICP) é uma estrutura criada para resolver o problema do compartilhamento de chaves públicas na criptografia assimétrica.
- A ICP é composta por: autoridade de registro (AR), autoridade certificadora (AC), serviços de diretório, entidades finais e clientes.
- Um certificado digital é um arquivo de texto que contém uma chave pública associada a informações relevantes sobre o seu dono. Uma assinatura digital protege o hash calculado sobre todo o conteúdo do certificado e impede a sua modificação.
- A ICP-Brasil é a infraestrutura de chaves públicas do governo brasileiro.