# Entendendo a Infra-Estrutura de Chaves Públicas

**Fabiano Albernaz Lemos**
Fundação Getúlio Vargas
Gestão de Negócios em Tecnologia da Informação
Rio de Janeiro - RJ
E-mail: fabiano.lemos@usa.net

## Abstract

This white paper looks at the business advantages associated with conducting business over the Internet using advanced network technologies, including Virtual Private Networks (VPNs) and browser-based applications like intranets and extranets. It examines the role of strong authentication in securing these electronic business environments and building the foundation necessary to establish trusted, secure electronic communications over the Internet.

## Resumo

Este trabalho observa as vantagens competitivas de negócios associadas ao fato de conduzí-los via Internet utilizando avançadas tecnologias de rede, incluindo *Virtual Private Networks* (VPN) e aplicações baseadas em Browser, tais como Intranets e Extranets. Também examinará, o uso de autenticação forte para garantir a segurança necessária nestes ambientes de negócio eletrônico, criando assim, as bases fundamentais para prover comunicação eletrônica segura e confiável através da Internet.

## I. O Problema da Gerência de Chaves

### A necessidade da Criptografia de Chave Pública

O jeito que o mundo faz negócios está mudando, e a segurança corporativa deve mudar concordantemente.

Para ilustrar, o correio eletrônico (email) não mais carrega memos e notas, mas também contratos e informações financeiras sensitivas. A rede (Web) está sendo utilizada não somente para publicar brochuras corporativas, mas para distribuição de software e comércio eletrônico. *Virtual Private Networks* (VPNs) são extensões das redes corporativas dentro da Internet. Extranets tornam a Internet em uma seletiva e compartilhada VPN.

E-mail seguro, acesso a Web, comércio eletrônico, VPNs e Extranets requerem alta segurança, a qual provê confidencialidade, autenticação, controle de acesso e integridade de dados. Certificados Digitais e criptografia de chave pública estão emergindo como sendo os viabilizadores preferenciais da segurança forte. Muitas das grandes organizações desenvolverão criptografia de chave pública e certificados digitais para toda a companhia nos próximos anos.

A criptografia de chave pública requer uma infraestrutura de chave pública (*Public Key Intrastructure* – **PKI**), que são os serviços essenciais para se gerenciar os certificados digitais e as chaves de criptografia para pessoas, programas e sistemas.

**O que é Criptografia de Chave Pública?**

A criptografia utiliza algorítimos matemáticos e processos para converter texto legível em um emaranhado de texto ilegível ou criptografado e vice-versa. Aplicações de criptografia incluem:

- Encriptação de Dados para confidencialidade.
- Assinaturas Digitais para prover o não-repúdio (responsabilidade) e verificação da integridade dos dados.
- Certificados para autenticar as pessoas, aplicações e serviços, e para controle de acesso (autorização)

Existem dois tipos de algorítmos de criptografia: o Simétrico (segredo compartilhado) e o Assimétrico (chave pública).

Na criptografia simétrica, remetente e destinatário utilizam a mesma chave tanto para encriptar quanto para decriptar. Então, diversos clientes precisam ter esta mesma chave. Como a encriptação não é disponível a priori para distribuição de chaves, a distribuição de chaves através da rede não é uma opção segura. Outras opções como a contratação de um serviço seguro de *Courier*, é caro e vagaroso.

A criptografia de chave pública, por outro lado, usa pares de chaves: uma chave pública que está disponível para todos e uma diferente, a chave privada, conhecida somente pela pessoa, aplicação ou serviço que a detém posse. A chave pública pode ser transmitida sem ser previamente criptografada, sob meios inseguros já que ela não é segredo, enquanto que a chave privada deve ser mantida em sigilo. Então, o processo de distribuição de chaves é extremamente simplificado ao utilizar-se criptografia de chave pública.

A chave primária do remetente pode ser utilizada para produzir uma assinatura digital, um bloco encriptado de dados que, quando decriptada pelo destinatário, verifica a identidade do remetente (provê desta forma o não repúdio), assim como, a integridade dos dados. Algumas organizações emitem um par especial de chaves de assinatura. A diferença entre chaves criptográficas e as chaves de assinatura é que elas não precisam ser armazenadas, reduzindo assim a exposição aos acessos não autorizados à chave privada.

Criptografia de chave pública também pode ser utilizada para distribuição segura de chaves simétricas através de redes inseguras. Em cada umas destas aplicações, o acesso a chave pública não permite acesso de autor aos dados protegidos.

**Certificados Digitais validam as Chaves Públicas**

Chaves Públicas fortes, armazenadas como objetos de leitura (*Read-Only*) em serviços de diretórios seguros, provêm a segurança necessária contra golpes de troca ou forje de chaves. Contudo, um invasor pode pretender ele mesmo ser o serviço de diretório seguro e fornecer a chave pública forjada, permitindo desta forma que o invasor e não o destinatário a decriptar mensagens encriptadas com a chave. Por isso, um jeito de se validar as chaves públicas se torna necessário. Os certificados provêm a validação de chaves.

Um certificado digital, como o próprio nome já diz, é um documento digital (ex. um arquivo formatado) que esconde a chave privada de uma pessoa, aplicação ou serviço. Uma autoridade certificadora confiável (AC) cria o certificado e o assina digitalmente utilizando-se a chave privada da AC. Como seu objetivo principal é a criação de certificados, a AC é o componente central do PKI. Utilizando a chave pública da AC, as aplicações verificam a emissão da assinatura digital fornecida pela AC, e depois, a integridade do conteúdo do certificado (mais importantemente a chave pública e a identidade da pessoa, aplicação ou servidor).

**Muitas Aplicações: Muitas Chaves e Certificados**

Inicialmente, muitas organizações gerenciavam chaves e certificados manualmente, e baseado por aplicação em separado. Isto funciona aceitavelmente quando organizações desenvolvem aplicações para um número moderado de usuários dentro de uma pequena quantidade de aplicativos. Contudo, com o crescimento do uso das chaves públicas, as tarefas de gerenciamento de chaves tornaram-se mais desafiadoras. A maioria das organizações evoluem para uma abordagem consolidada, automatizada e baseada em PKI.

## II. Componentes e Funções do PKI

Abaixo seguem os três principais componentes funcionais para o PKI:

- A Autoridade Certificadora (AC), é uma entidade que emite os certificados. Um ou mais servidores corporativos, ou de terceiros confiáveis tais como: *VeriSign* ou *GTE*, podem prover as funções de uma Autoridade Certificadora.

- Repositório de chaves, certificados e CRLs (*Certificate Revocation Lists*) são usualmente baseados em serviços de diretório como o LDAP (*Light-weight Directory Access Protocol*)

- Uma função de gerência, tipicamente implementada via gerência de console

Se o PKI provê um procedimento automático de recuperação de chaves, ele também pode ser um serviço de recuperação de chaves. Recuperação de chaves é uma função avançada requerida para restaurar dados ou mensagens quando uma chave é perdida.

Além disso, pode existir em separado uma Autoridade de Registro (AR), que é uma entidade dedicada ao registro de usuários e aceitação de pedidos de emissão de certificados. Registro de usuários, é o processo de coletar informações do usuário e verificar a identidade do mesmo, as quais são utilizadas para efetivamente registrá-lo em concordância com a política vigente. Isso tudo é distinto do processo de criação, assinatura e emissão de um certificado. O departamento de Recursos Humanos pode exercer as funções de uma AR, por exemplo, enquanto o Departamento de Tecnologia da Informação gerencia a AC. Uma AR em separado também torna mais difícil para qualquer departamento subverter aos sistemas de segurança.
Organizações podem escolher em ter o registro sob responsabilidade de uma AR separada, ou inclusa como função da própria Autoridade Certificadora (AC).

Note que AC, AR e os demais são componentes funcionais que podem ser implementados de várias formas seja em Hardware ou Software. Em particular, uma AC pode ser implementada em um ou mais servidores, assim como a AR o pode. Sistemas executando funções de AC e AR são regularmente referenciados como sendo Servidores de Certificado e Servidores de Registro respectivamente.

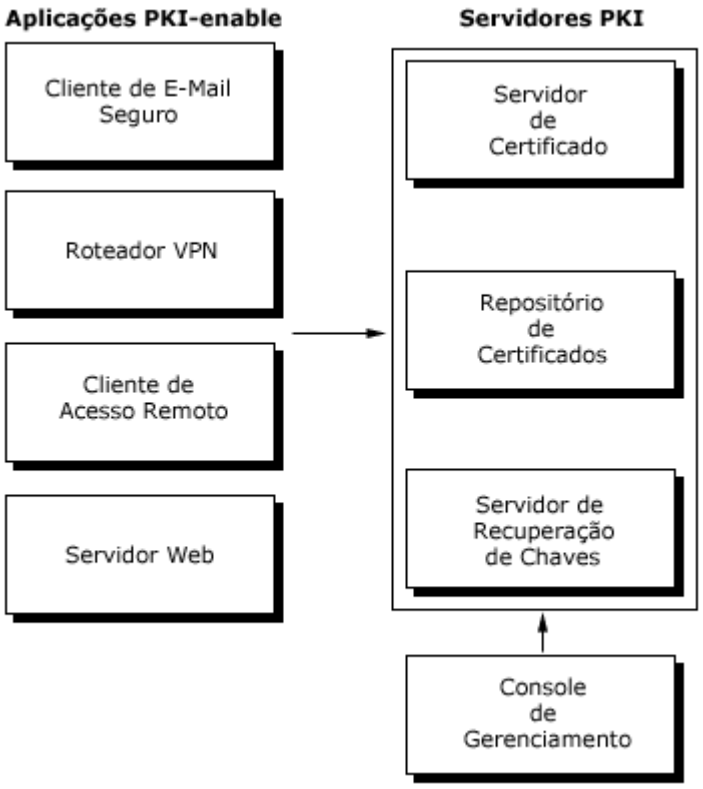


**Figura 1. Os principais componentes do servidor PKI são o de certificado, de repositório, o de recuperação de chaves e normalmente acompanhado de um console de gerenciamento**

### Funções do PKI

As funções mais comuns do PKI são a emissão de certificados, a revoga de certificados, a criação e publicação de CRLs, e ciclo de vida de uma chave. Funções elaboradas e emergentes incluem a selagem (time-stamp) e validação de certificados baseados concomitantemente com a política de segurança vigente.

### Emissão de Certificados

A CA assina os certificados, autenticando assim a identidade do requerente, dando garantia pública e notória para a assinatura e identidade de um indivíduo. Além disso, a AC “sela” o certificado com uma data de expiração. A AC pode retornar o certificado ao sistema requerente e/ou enviá-lo para um repositório.

### Revogando Certificados

O certificado pode ficar inválido antes mesmo do vencimento da data de expiração. Por exemplo, um empregado pode demitir-se, trocar de nome ou a sua chave privada pode estar comprometida. Sob estas circunstâncias, a AC revoga o certificado incluindo o número serial do certificado na próxima lista CRL.

### Armazenando e Buscando Certificados e CRLs

O jeito mais comum de se armazenar e buscar certificados e CRLs é feito utilizando-se serviços de diretório, com acesso via LDAP. Outras opções incluem os diretórios compatíveis X.500, HTTP, FTP e Email.

### Provendo Confiança

Cada usuário deve ter no mínimo uma chave pública de uma AC em que ele deve confiar implicitamente. Organizações podem estabelecer e manter a confiança através de um gerenciamento único e seguro do domínio sob a aprovação regular de auditorias que observam as políticas e procedimentos da AC, repetidamente em intervalos de tempo regulares.

| Função | Descrição | Implementação |
|---|---|---|
| Registro de Usuários | Coleta as informações do Usuário | Função da AC, ou AR em separado |
| Emissão de Certificados | Cria os Certificados em resposta à requisição do Usuário ou Administrador | Função da AC |
| Revoga de Certificados | Cria e publica CRLs | Software administrativo associado a AC |
| Armazenamento e Busca de Certificados e CRLs | Faz com que os Certificados e as Listas de Certificados Revogados (CRLs) fiquem disponíveis para usuários autorizados | O repositório para Certificados e Listas de Certificados Revogados é usualmente um serviço de diretório seguro e replicado acessível via LDAP |
| Caminho de validação de um Certificado | Impõe, baseado em uma Política, regras sobre a cadeia de certificação e valida se todas as regras são cumpridas | Função da AC |
| Selagem de Certificados | Põe um selo de tempo em cada certificado | Função da AC ou Servidor de Tempo dedicado (*Time Server*) |
| Gerenciamento do Ciclo de Vida de uma Chave | Atualiza, arquiva e restaura chaves | Automatizado em software ou executado manualmente |

**Tabela 1. Principais funções do PKI**

Contudo, organizações precisam avaliar (e aceitar ou rejeitar) certificados de ACs de outras unidades de negócios ou de parceiros. Isso pode ser implementado através de processamento hierárquico de certificação ou certificacão cruzada direta.

### Certificação Hierárquica

A melhor arquitetura de certificação hierárquica são aquelas mantidas por organizações de serviços PKI, tal como a *VeriSign*. Tipicamente nesta arquitetura:

1) Existe uma única raiz no topo da árvore.
2) A raiz certifica as Autoridades Primárias de Certificação (APC), que emitem, suspendem e revogam certificados de todas as ACs dentro da hierarquia
3) APCs certificam ACs. APCs também podem fazer certificação cruzada com entidades tipo APC dentro do PKI de outros vendedores.

4) ACs autorizam ACs subordinadas, que pertence à companhia de serviço de PKI ou ao próprio cliente
5) No final da hierarquia podem residir as Autoridades Locais de Registro (ALR) que avaliam as aplicações de certificados em nome da raiz, APC, ou AC que emitem o certificado em si.

Se um usuário ainda não confia num certificado assinado por uma AC, o usuário procura no nível de cima por uma AC confiável que certificou a chave pública da AC em questão.

**Certificação Cruzada** – Uma AC pode emitir a outra AC um certificado que permite a outra AC a emitir certificados que serão reconhecidos pela primeira AC. A certificação cruzada funciona diretamente, sem a participação de terceiros.

**Certificação Hierárquica e Cruzada podem ser combinadas** – Pode fazer sentido implementar ambas as certificações, a hierárquica e a cruzada dentro de um domínio único e seguro, para diferentes propósitos ou em tempos diferentes. Por exemplo, um sistema hierárquico baseado em um parceiro terceiro confiável, pode vir a ser necessário quando se define ou se expande um PKI, porém o volume de interoperabilidade do dia-a-dia pode ser completado via certificação cruzada.

### Selagem de Tempo (*Time Stamping*)

Em adição ao conteúdo e a autenticidade de uma transação, a exata hora da transação pode ser importante. Por exemplo, uma transação que deve ser submetida até um certo intervalo de tempo para se ter validade na transação. A solução para se ter transações confiáveis é combinar assinatura digital com a selagem. E isso pode ser alcançado aumentando o PKI com um serviço de selagem.

### Caminho de validação de um Certificado

Avaliar um certificado pode requerer a pesquisa através de uma longa cadeia de ACs. Idealmente, toda AC no caminho deveria suportar qualquer requerimento associado com a validação. Este tipo de validação ainda não é uma parte padrão das funcionalidades da AC. Contudo, alguns vendedores estão começando a suportá-lo e trabalham afim de definir um padrão nesta área.

Se a política de mapeamento de caminhos concorda com a política da outra AC, é possível a interoperabilidade se eles suportarem políticas similares mas não necessariamente iguais. Pode ser desejável a proibição desta política de mapeamento, sendo assim, o caminho somente será validado se as ACs tiverem políticas idênticas.

### Gerenciamento do Ciclo de Vida de uma Chave

O PKI tem diversas funções tais como, a emissão de um certificado e a listagem de certificados na CRL, em resposta a um pedido corrente. Em contraste, funções de ciclo de vida, tais como atualizações, salva e arquivamento das chaves, são executadas rotineiramente.

Cada usuário provavelmente tem um número de chaves tal, que estas precisam de gerenciamento do ciclo de vida. Por exemplo, usuários geralmente têm no mínimo um par de chaves para cada aplicação segura (Ex: email, encriptamento de arquivos no desktop, VPN). Algumas aplicações usam vários pares de chaves para diferentes propósitos, tais como assinatura digital, encriptação e autenticação.

**Atualizando Chaves** – Novas chaves são usualmente emitidas em intervalos de tempo regulares, tal como um ano ou dois, afim de reduzir a exposição das chaves que estão desconhecidamente comprometidas.

**Salva de Chaves** – Usuários freqüentemente esquecem senhas que protegem suas chaves privadas; ou muitos perdem as chaves, por exemplo, numa pane de disco ou ataque de vírus. A empresa deve ser capaz de recuperar as chaves para o usuário.

**Arquivando Chaves** – Quando empregados deixam a empresa, o gerente de rede impede o uso das chaves de criptografia para o uso futuro, ao mesmo tempo que ele retém a chave afim de acessar arquivos encriptados e mensagens de correio. Chaves utilizadas para assinatura digital podem ser retidas tanto quanto os documentos assinados, assim a assinatura pode ser verificada. Note que, muitas organizações arquivam chaves de criptografia mas não as chaves de assinatura, já que a disponibilidade de arquivos contendo chaves de assinatura podem estimular o abuso via embuste de identidade.

**Gerenciamento de Ciclo de Vida de Chaves Automático: Uma função crítica** – O esforço requerido para gerenciar chaves manualmente pode limitar a escalabilidade do PKI. Este tipo de gerenciamento automático de chaves é uma função crítica para um PKI de grande escopo.

## III. Como as Aplicações funcionam com o PKI

O PKI gerencia as chaves e os certificados digitais utilizados para implementar criptografia dentro das aplicações, tais como email e mensagens, navegadores e servidores Web, EDI (*Eletronic Data Interchange*); em aplicações que estabelecem transações seguras ou sessões de comunicação sobre a Internet (meio inseguro) ou em VPNs utilizando protocolos, tais como: S/MIME, SSL e IPSEC; e em funções como arquivos e códigos assinados digitalmente. Em adição, aplicações desenvolvidas "*in-house*" podem ser compatíveis com o PKI.

### Email e Mensagens

Email seguro e mensagens usam pares de chaves para encriptação das mensagens e arquivos e para a assinatura digital. Por exemplo, programas de email tais como *Microsoft Exchange* e o *Notes* da *IBM* estão constantemente aumentando o uso da criptografia para enviar informações sensíveis. O mesmo se aplica para programas *Groupware* baseados em troca de mensagens, tal como o *GroupWise* da *Novell*. Os sistemas EDI suportam transações financeiras que requerem autenticação, privacidade e integridade de dados.

O protocolo mais comum de encriptação de email é o S/MIME (*Secure Multipurpose Internet Mail Extensions*) o qual é a extensão segura do padrão MIME

### Acesso Internet

Navegadores e servidores Web utilizam criptografia para autenticação e confidencialidade, e para aplicações tais como, banco online e shopping online. Tipicamente, utilizando SSL (*Secure Sockets Layer*), os servidores autenticam eles mesmos para seus clientes. O SSL também encripta o tráfego de dados. A autenticação do cliente também é uma opção. SSL não é limitado ao HTTP (*HyperText Transfer Protocol*) mas também suporta protocolos como o FTP (*File Transfer Protocol*) e TELNET.

### VPN

Encriptação e autenticação são as principais tecnologias usadas para converter canais comuns de Internet em VPNs (*Virtual Private Networks*), usada para privacidade entre sites (de roteador-a-roteador) ou para acesso remoto seguro (cliente-servidor). Estas funções são implementadas no contexto da criação de um túnel que empacota um protocolo dentro de outro protocolo. Por exemplo, o encapsulado pode ser o PPP, enquanto o protocolo encapsulador é o IP. O padrão

emergente para túneis site-a-site é o protocolo IP seguro (IPSEC) desenvolvido pelos engenheiros do IETF.

**Arquivos e Códigos Assinados Digitalmente**

Incrementar a confiança de programas baixados na Internet e seus arquivos tem elevado a preocupação sob o ponto de vista da segurança, particularmente na área de controle de vírus. Tecnologias como *Microsoft AuthentiCode* usam assinaturas digitais da RSA para verificar a integridade do código-fonte. Um PKI pode ser utilizado para aumentar em escala este tipo de solução, afim de atingir um grande número de usuários e diversos programas que requerem este tipo de serviço.

## IV. PKI - Padrões Relacionados

Os padrões na arena do PKI se dividem em dois grupos: os que especificamente definem o PKI, e os padrões de nível de usuário que recaem sobre o PKI, mas não o definem.

A figura dois mostra o relacionamento entre as aplicações e infra-estrutura, e seus padrões associados.

**Padrões PKI**

Padrões de PKI permitem que múltiplos PKIs interoperem e que múltiplas aplicações façam interface com um único e consolidado PKI.

Em particular, padrões são necessários para:

- Procedimentos de Matrícula/Inscrições
- Formatos dos certificados
- Formatos de CRLs
- Formato para mensagens de inscrição/matrícula de certificados (pedidos de clientes, certificação, servidor emite certificado)
- Formatos de Assinatura Digital

O foco primário dos padrões de PKIs interoperavéis é o grupo de trabalho do *Internet Engineering Task Force* (IETF), conhecido como grupo PKIX (PKI para certificados X.509)

**Visão Geral – PKIX**

Os quatro principais componentes no modelo PKIX são: O usuário (ou “entidade fim”), AC, AR, e Repositório

| Componente | Parte de um PKI ? | Descrição |
|---|---|---|
| Usuário (entidade fim) | Não | Usuário do PKI e/ou sistemas de usuário final, que são o assunto de um certificado |
| Autoridade Certificadora (AC) | Sim | Emite, armazena e revoga certificados |
| Autoridade Registradora (AR) | Sim | Um sistema opcional que permite a AC delegar certas funções de gerenciamento, tal como, registro de usuários |
| Repositório | Sim | Um sistema ou coleção de sistemas distribuídos que armazenam e permitem que entidades fim acessem certificados e CRLs |

**Tabela 2. Principais componentes do modelo PKIX**

**Componentes padrões PKIX** – As especificações são baseadas em outros dois padrões: X.509 do ITU (*International Telecommunication Union*) e PKCS (*Public Key Cryptografy Standards*) da *RSA Security*. X.509 prentende especificar serviços de autenticação para serviços de diretório X.500. De fato, a sintaxe de certificado do X.509 foi adotado fora dos ambientes X.500. Contudo, X.509 não intenciona definir por completo um PKI interoperável. Para suplementar o X.509, vendedores, usuários e comitês de padronização têm se voltado primeiramente para os padrões de fato do PKI definidos no PKCS

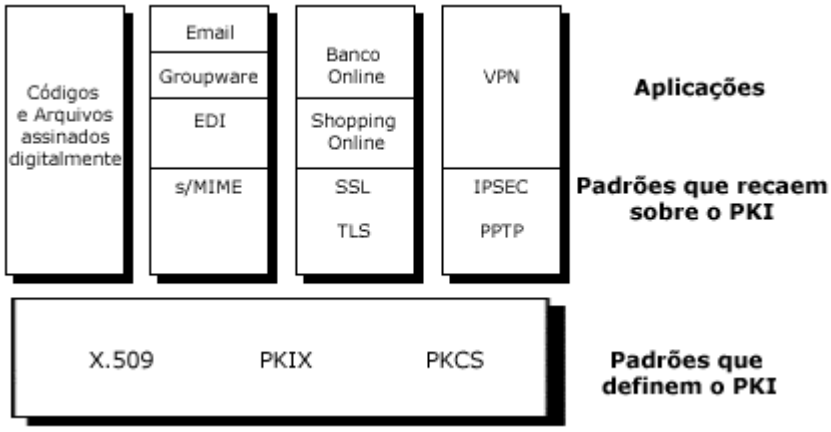


**Figura 2. Os padrões PKI que o definem. Padrões de segurança para aplicações podem requerer, assumir ou permitir o uso do PKI.**

**X.509** – O fundador, universalmente suportado, padrão PKI é o ITU X.509. O papel principal do X.509 é definir um formato padrão para o certificado digital.

**PKCS** – É uma série de padrões que cobrem o PKI nas áreas de inscrição e renovação de certificados e distribuição das listas CRL. Para a interoperabilidade, os três padrões mais importantes são: PKCS #7, "*Crytographic Message Syntax Standard*", PKCS #10, "*Certificate Request Syntax Standard*" e o PKCS #12, "*Personal Information Exchange Syntax Standard*".

**Padrões que recaem sobre o PKI**

A maioria dos padrões de segurança são planejados para funcionar com um PKI. Por exemplo, SSL (*Security Sockets Layer*), TLS (*Transport Layer Security*), S/MIME (*Secure Multipurpose Internet Mail Extensions*), SET (*Secure Eletronic Transactions*) e IPSEC (*IP Security*), todos assumem, requerem ou permitem o uso de um PKI.

**S/MIME**

S/MIME é o padrão da IETF para troca de mensagem segura. S/MIME assume um PKI para assinar digitalmente as mensagens e para suportar encriptação das mensagens e anexos, sem requerer préviamente o segredo compartilhado. Como o email é a mais madura das aplicações Internet, o comitê S/MIME assumiu a direção de implementar e extender os padrões PKI, levando vantagem sempre que possível sobre os padrões PKI, e completando outros padrões adicionais quando necessário. Os mais importantes padrões definidos pelo comitê do S/MIME são: *Crytographic Message Syntax*, *Message Specification*, *Certificate Handling* e *Certificate Request Syntax*.

**SSL e TLS**

SSL e o emergente TLS, que é baseado no próprio SSL, são os padrões mais importantes para proverem acesso seguro aos Servidores Web. SSL e TLS também são utilizados para segurança em ambiente cliente/servidor numa variedade enorme de aplicações não Web. Ambos recaem num PKI para emissão de certificados para os clientes e sevidores.

**Secure Eletronic Transactions (SET)**

SET facilita o pagamento seguro de cartões de crédito. SET utiliza chaves para a autenticação, confidencialidade e integridade dos dados. O PKI é uma peça crítica para a autenticação das partes envolvidas na transação de pagamento.

**IPSEC**

Define protocolo de encriptação baseado no protocolo IP, e é um dos primeiros protocolos utilizados para implementar uma VPN. IPSEC requer chaves para encriptação e autenticação. Padrões completos para o IPSEC estão surgindo, tendo em vista que o PKI é o jeito mais escalável de gerenciar chaves IPSEC. O uso do IPSEC continua muito limitado. Contudo, a necessidade de se adotar uma solução PKI cresce com o desenvolvimento do próprio IPSEC.

## V. Objetivos no desenvolvimento do PKI

Cinco questões importantes precisam ser consideradas no desenvolvimento do PKI:

- Qual a estratégia de PKI da organização?
- Como a interoperabilidade será alcançada?
- As aplicações são compatíveis com PKI?
- Quantos clientes estarão envolvidos no plano incial de desenvolvimento?
- Quais são os requerimentos do corpo técnico para planejar e desenvolver o projeto?

**Qual a estratégia de PKI da organização?**

A estratégia de PKI tipicamente foca na habilitação de uma aplicação específica ou na consolidação de funções de PKI para múltiplas aplicações.

**Habilitando uma aplicação específica**

Muitas organizações, ainda hoje, não tem aplicações que se baseiem no PKI. Neste caso, a mais pragmática das abordagens, com o investimento mínimo e retorno rápido, o foco fica centrado no desenvolvimento do PKI para uma única aplicação. A experiência ganha com esta aplicação poderá servir de plano para as próximas aplicações a serem desenvolvidas, assim como para um PKI consolidado, o que é muito mais frutífero.

Mesmo quando desenvolvem PKI para uma única aplicação, as organizações tipicamente consideram como eles vão alcançar a interoperabilidade para múltiplas aplicações, ou consolidação do PKI (Veja a próxima questão, Como a interoperabilidade será alcançada?).

**Consolidando as funções do PKI para múltiplas aplicações**

Organizações com diversas aplicações baseadas em PKI podem consolidar a infraestrutura do PKI, afim de aumentar a eficiência no gerenciamento e a redução de custos. Organizações também podem decidir por implementar a infra-estrutura antes e depois as aplicações, caso a sua estratégia consista em desenvolver múltiplas aplicações mais rápido possível. Contudo, implementar um sistema complexo deste tipo sem primeiro resolver os problemas associados com cada aplicação em separado, requer planejamento extra, projeto piloto e muitas vezes uma consultoria externa.

**Como a interoperabilidade é alcançada?**

Existem dois tipos de abordagem para a interoperabilidade:

1. Foco na solução de terceiros (produtos)

2. Foco nos padrões

No passado, os padrões PKI eram tão imaturos que as organizações muitas vezes tinha que focar nos produtos PKI que forneciam a solução para o problema em questão, porém a solução amarrava-se no pacote. Todavia, esta estratégia pode fracassar quando temos como escopo a empresa ou empreendimento como um todo. Companhias diferentes ou unidades de negócios vão necessitar da interoperabilidade, mesmo que eles tenham implementado suas soluções baseados em pacotes de produtos de vendedores diferentes. Padrões PKI, com as especificações PKIX servindo de base, tiveram evolução até o ponto em que as empresas possam planejar utilizá-los como ambiente de trabalho para atingir o nível corporativo de interoperabilidade desejado. Num mercado PKI maturo e expansivo, os padrões proprietários serão cada vez mais escolhidos como método para alcançar a interoperabilidade e a consolidação.

**As aplicações estão preparadas?**

Poucas aplicações estão preparadas para suportar o PKI, em muitos casos as organizações têm duas opções:

Encorajar os vendedores de software a habilitarem suas aplicações ao PKI (*PKI-enable*). Para organizações que somente existem usuários de informática (não existe desenvolvimento) , esta

abordagem é fácil e não requer investimentos iniciais altos. O resultado implica em capacidades PKI que são sutilmente integradas com as aplicações. Porém, o cronograma para a entrega destas características (*PKI-features*) podem não satisfazer as necessidades da organização.

Utilizar a equipe de programadores (prata da casa), ou contratar programadores para desenvolverem o módulo PKI. Este tipo de abordagem leva a resultados que correspondem precisamente às necessidades da empresa e também permite uma integração harmoniosa das funções do PKI com as aplicações internas já existentes. No caso de softwares comerciais, a organização depende das APIs expostas pelo desenvolvedor do software. Isto pode degradar a capacidade de integração do PKI, como também, as necessidades particulares do usuário desta organização. Organizações que pretendem customizar suas aplicações devem avaliar as ferramentas da RSA (*RSA Security enabling-tools*) e servidores PKI, os quais podem reduzir o tempo e custo do projeto.

**Quantos clientes vão desenvolver inicialmente?**

Vendedores podem dizer que o desenvolvimento de milhares ou mesmo dez milhares de clientes PKI, já é um razoável começo. Na realidade, muitas organizações têm projetos pilotos com não mais de poucas centenas – e muitas vezes menos que uma centena – de clientes. Começar pequeno previne o desenvolvimento de milhares de clientes sem ter a certeza de que os primeiros, destas poucas centenas, estão operando corretamente.

**Quais são os requerimentos para a Equipe Técnica?**

De acordo com o grupo de consultoria *Aberdeen*, menos da metade do orçamento para desenvolver uma infra-estrutura de chave pública é atribuído à aquisição de software e hardware. De fato, o pessoal técnico requerido para o planejamento e desenvolvimento representa, tipicamente, o maior custo. Os requerimentos da equipe técnica são buscados dentro da própria empresa ou contratados através de uma firma de consultoria. Geralmente, faz mais sentido ter a equipe interna somente para as necessidades constantes e atividades de rotina. Já as tarefas que necessitam ser executadas uma única vez, podem ser melhor realizadas por um parceiro especializado que as executa de forma mais eficiente, sem o custo de ter que contratar e, posteriormente, dispensar o pessoal.

## VI. Conclusão

A criptografia de chave pública e a certificação digital estão emergindo como habilitadores preferenciais para termos a segurança forte num grande número de aplicações, incluindo email, acesso à internet, VPNs e códigos assinados digitalmente. Um PKI gerencia chaves e certificados para as pessoas, programas e sistemas. Os padrões PKI, tais como as especificações do PKIX, permitem que múltiplos PKIs interoperem e que múltiplas aplicações utilizem um único PKI. Isto torna a consolidação do PKI possível, facilitando um gerenciável e escalável PKI. Para implantar um PKI com sucesso, as organizações devem desenvolver uma estratégia de abordagem, um plano de interoperabilidade, determinar quais e quantas aplicações vão fazer interface com o PKI, mensurar o projeto inicial corretamente e planejar os requisitos da equipe técnica.