14 – Dezembro de 1999

Segurança em aplicações Public Key Infrastruture ready

Abrimos o jornal e eis que temos mais uma nova tecnologia. Essa cena é uma constante no ambiente corporativo, afinal, é preciso evoluir e solucionar os antigos e novos problemas.

Public Key Infrastruture é um bom exemplo de tecnologia recém-nascida. PKI ou Infra-estrutura de chaves públicas, consiste de serviços, protocolos e aplicações, usados para o gerenciamento de chaves públicas e certificados, que provê serviços de criptografia de chave pública e assinatura digital, permitindo a interação segura entre usuários e aplicações.

Serviços às aplicações oferecidos por uma solução PKI

- Registro de chaves com a emissão de um novo certificado para uma chave pública
- Revogação ou cancelamento de certificados
- Obtenção de chaves públicas de uma Autoridade Certificadora
- Validação de confiança, determinando se o certificado é válido e a quais operações ele está autorizado

Formada basicamente por *software*, as soluções de PKI podem ser instaladas na maioria dos servidores existentes no mercado: Windows NT, Novell Netware, Solaris, HP-UX, AIX, Macintosh OS etc. Contudo, ainda existem iniciativas com soluções que suportam *hardwares* próprios de criptografia para a geração das chaves e emissão dos certificados.

Componentes de uma solução PKI

- Autoridade Certificadora (CA)
- Autoridade Registradora (RA), opcional
- Diretório

CA, acrônimo para *Certification Authority*, ou Autoridade Certificadora, é uma entidade representada por pessoas, processos e ferramentas, usada na emissão de certificados digitais que, de uma forma segura, associa o nome da entidade (usuário, máquina etc) ao seu par de chaves.
Ela age como um agente da segurança, desta forma, se os usuários confiam em uma CA e em sua política de emissão e gerenciamento de certificados, eles confiam nos certificados emitidos pela CA. Isso é o que chamamos de *third-party trust*, ou confiança em uma terceira parte ou entidade.

O Diretório, por sua vez, pode ser entendido como um local de armazenamento – repositório – dos certificados e das listas de revogação emitidos por uma CA.

Benefícios de uma solução PKI

- Autenticação: como identificar os usuários e máquinas

- Controle de Acesso: como controlar quem acessa as informações e realiza as transações
- Confidencialidade e Privacidade: como ter certeza de que a comunicação é privada mesmo via Internet
- Integridade: como garantir que a informação não será alterada
- Não-repúdio: como prover um método digital de assinatura das informações e transações

O conceito é inovador e vem para expandir a esfera da segurança até às aplicações. Contudo é preciso definir as necessidades com clareza, para só então especificar uma solução PKI.

Em tempo...cabe um agradecimento aos especialistas em segurança da informação Marlon Dias e Marcelo Duarte, que subsidiaram este artigo com informações técnicas mais aprofundadas sobre esta promissora tecnologia.

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Coordenador de Segmento de Mercado e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br