23 – Setembro de 2000

Quebrando o protocolo da coluna, abro espaço especial nesta edição para um especialista de Segurança da Informação que com indiscutível competência conseguiu tornar um assunto antes complexo e ininteligível para os mortais, fácil e de leitura agradável. Diante disso, não pude me render e deixar de beneficiar o leitor com um eficiente esclarecimento sobre a promissora tecnologia PKI – Public Key Infrastructure.

PKI: a chave para segurança no e-commerce

Para viabilizar o comércio eletrônico em todo o seu potencial necessitamos de segurança que permita, usuários, empresas, provedores e operadoras de comunicação, confiar na Internet para realizar sem medo transações comerciais e financeiras. Entre os requisitos funcionais desta segurança estão cinco aspectos básicos que são considerados fundamentais:

1) Confidencialidade - Certamente nenhum de nós vai querer que alguém leia nossa correspondência de negócios ou que veja o valor das compras que fizemos sem o nosso consentimento. Privacidade e discrição são fundamentais em qualquer negócio;
2) Autenticação - Queremos saber qual a real origem das informações que recebemos e, mais ainda, não aceitamos a hipótese de alguém acessar nossa conta bancária e começar a fazer retiradas;
3) Integridade - Mais do que ter certeza da origem das informações, queremos confiar que nenhuma delas foi alterada no caminho. Não gostaríamos de descobrir mais tarde que um valor ou número crucial não era bem aquele que recebemos.
4) Não repúdio - Igualmente não queremos que ninguém que nos faça uma encomenda e depois diga que não foi o autor do pedido, sem que consigamos provar quem fez a operação;
5) Autorização - Certamente o banco em que temos conta não nos quer movimentando somas acima de nosso saldo ou realizando operações com produtos que não possuímos.

A solução destes problemas é a base da tecnologia de PKI (Public Key Infrastructure) para a segurança de comércio eletrônico. Fazendo uso de um sistema de certificados e chaves, em conjunto com diversos algoritmos, as aplicações de PKI conseguem assegurar os cinco requisitos descritos acima de uma maneira difícil de ser fraudada e que se apresenta de forma transparente para o usuário. Estes dois pontos, transparência aliada à forte base técnica de seus mecanismos, denotam o ponto forte desta tecnologia: o aspecto de infra-estrutura contido no "I" de seu nome. Afinal de contas, nenhum de nós tem que se dar conta do emaranhado de linhas de transmissão e usinas que estão por trás da rede elétrica cada vez que ligamos uma televisão à tomada. Assim também deveria ser o comércio eletrônico pela Internet.
De forma simplificada, em uma PKI certificados digitais são emitidos por uma Autoridade Certificadora para cada usuário ou equipamento envolvido. Com estes certificados, são gerados pares de chaves constituídos por uma chave pública e uma privada. Os algoritmos utilizados permitem que aquilo que foi criptografado com a chave pública só possa ser aberto pela chave privada, e vice-versa. Desta forma, tudo que é público é colocado à

disposição num diretório onde se tenham acesso às informações de todos, e tudo que é privado é mantido em segredo pelo usuário, quer seja criptografado no disco de seu computador, dentro de um smartcard ou em um servidor na rede.
Os certificados digitais contêm informações sobre a Autoridade Certificadora que os emitiu, e neste ponto se tornam primordiais aspectos de política e de confiança. Na política de certificação estabelecem-se os requisitos mínimos para a concessão de um certificado para um indivíduo ou equipamento, que, em última instância, vão determinar a percepção externa de confiança naquele certificado. Isto é análogo ao que ocorre na vida real com a documentação, por exemplo. Um gerente de banco certamente irá confiar mais em nossa carteira de identidade do que em uma carteira de clube ou associação no momento da abertura de uma conta.
Mais importantes que os certificados em si, e pelo menos tão importantes como o processo de validação dos usuários para a certificação, as aplicações preparadas para a utilização de PKI são essenciais para a ampliação do seu escopo de uso e para a transparência de operação para os usuários. São elas que fazem a diferença na sua implementação em comércio eletrônico.
No contexto de negócios via Web, certificados estariam presentes nos servidores e nos clientes em conjunto com aplicações que permitem a autenticação mútua entre eles, controle de autorizações, criptografia de sessão de comunicação e de objetos, assinatura digital - que garante também a integridade do conteúdo assinado - e suporte à contestação de repúdio de transações. Na prática, isto representa desde soluções mais simples, sem software cliente mas com toda a carga de operação dos certificados e de decisão de confiança sob a responsabilidade do usuário, até soluções mais completas em que toda a administração do certificado é feita de forma automatizada, transparente para o usuário, e toda a questão de confiança é definida em política centralizada, adaptada a cada tipo de operação de maneira consistente.
A iminente migração do comércio eletrônico para o telefone celular, viabilizada pela adoção do protocolo WAP (wireless application protocol) como padrão de facto para o acesso Internet em celulares, traz à tona os mesmos cinco requisitos citados no início do artigo. Neste novo contexto, o grande desafio é atender todas as cinco funcionalidades dentro das características restritas, em tamanho, memória e poder de processamento, dos aparelhos celulares. A implantação de PKI neste ambiente para solucionar estes problemas, no entanto, esbarra ainda em questões técnicas e na relativa imaturidade do protocolo WAP.
Atualmente os servidores e gateways WAP disponíveis no mercado seguem a versão 1.1 do protocolo, o que possibilita o uso de certificados digitais nos servidores e gateways. Isto possibilita sua autenticação (lado servidor) e o estabelecimento de comunicação criptografada entre o servidor e os micro-browsers instalados nos telefone através do protocolo WTLS (Wireless Transport Layer Security), análogo ao SSL utilizado de forma similar entre servidores e browsers Web. Neste caso, ficam ainda comprometidos autenticação do usuário, assinatura digital, autorização e não-repúdio, todos dependentes do certificado cliente.
Existe ainda uma limitação adicional em relação aos gateways WAP: apesar de sua utilização permitir que telefones WAP se conectem a versões simplificadas dos web sites existentes, eles trazem consigo um problema intermediário, que ocorre entre sua comunicação com o telefone e com o servidor Web. Por um breve momento na memória, o gateway decriptografa o que foi transmitido por um e criptografa em um protocolo

diferente (WTLS para o telefone e SSL para o servidor Web) para enviar para o outro. Esta vulnerabilidade pode ser explorada se o gateway não estiver devidamente protegido. No futuro, isto deverá ser solucionado através de aplicações que realizem a criptografia do conteúdo independentemente do WTLS e do SSL, ou de servidores de aplicações que utilizam todo o stack do protocolo WAP, e não mais dependam de gateways.

Na versão 1.2, já definida mas com produtos ainda em protótipo, o protocolo WAP poderá certificar também usuários dos telefones. Entretanto, a forma de armazenamento do certificado digital no lado cliente é ainda tema de discussão. Nos telefones no padrão europeu GSM, recentemente adotado para a banda C no Brasil, este problema é resolvido com os cartões WIM (Wireless Identity Modules), similares aos SIM (Subscriber Identity Modules) utilizados atualmente para identificação do assinante. A questão se acirra quando se consideram os telefones CDMA e TDMA, este último grupo ainda sem suporte para WAP, utilizados pelas atuais operadoras de banda A e B.

A alternativa para armazenagem do certificado no telefone seria sua manutenção na rede, criptografado, de forma similar a algumas aplicações de PKI para a web. A limitação desta solução é a dependência de um software cliente, ou applet, rodando no telefone celular para permitir a recuperação e utilização segura do certificado para autenticação e assinatura digital. A linguagem que deverá permitir isto, o WMLScript, só está prevista para ser definida na versão 1.3 do protocolo WAP.

Apesar das constantes analogias com a Web, o mercado WAP possui características peculiares que deverão demandar não apenas novos modelo de negócios, mas também tecnologias específicas. O curto ciclo de vida dos telefones celulares quando comparado ao dos computadores, e a iminência constante de novas tecnologias, demanda das empresas a criação soluções em uma velocidade muito grande. É possível que muitas soluções proprietárias cheguem ao mercado antes de haver consenso sobre padrões.

Por outro lado, devido à maturidade atual dos produtos de PKI para a Internet tradicional e o estado avançado de algumas proposições existentes no mercado para a solução de seus problemas no mundo sem fio, a tecnologia de PKI deverá se firmar como a infra-estrutura de segurança também para o mobile e-commerce. Tudo isto de maneira simples e transparente para o usuário, como o comércio eletrônico tem que ser.

Ivan Alcoforado *é Gerente de produtos PKI da Módulo Security Solutions.*
ialcofor@modulo.com.br

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Gerente de Produto e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br