Um Panorama sobre Infra-estrutura de Chaves Públicas e Certificados Digitais

Amândio Balcão Filho Antonio Montes
Instituto Nacional de Pesquisas Espaciais – INPE
Laboratório Associado de Computação e Matemática Aplicada – LAC
amandio@lac.inpe.br montes@lac.inpe.br

Resumo

O uso da Internet para realizar negócios e outros serviços, com segurança, só é possível com a utilização de criptografia assimétrica, certificados digitais e uma ICP-Infra-estrutura de Chaves Públicas. São essas tecnologias que garantem a autenticidade, a integridade, o não-repúdio e o sigilo das comunicações.

Abstracts

The use of the Internet to carry out , with security, business and other services are only possible with the use of asymmetric cryptography, digital certificates and a PKI - Public Key Infrastructure. Authenticity, integrity, secrecy and non-repudiation are provided by the use of those technologies.

1. Introdução

Todos aqueles que já realizaram algum comércio ou utilizaram serviços bancários pela Internet fizeram uso de tecnologias associadas à Infra-Estrutura de Chaves Públicas – ICP. Nos últimos três anos o tema ICP tem se mantido entre os tópicos de maior interesse para as grandes corporações e agências governamentais preocupadas com as questões de segurança das transações no mundo virtual [10].

Por ICP entende-se todo um conjunto de equipamentos, softwares, procedimentos, regulamentos e legislação que visam garantir de forma unívoca a ligação entre uma chave criptográfica a uma entidade, seja ela pessoa, serviço, hardware ou software. Essa ligação é conseguida através do uso de uma credencial eletrônica chamada Certificado Digital [2].

Com a grande disponibilidade de acesso a Internet há uma tendência geral a que serviços, comércio e comunicações migrem para o ambiente virtual. À medida que essas aplicações são disponibilizadas as empresas vão mudando seu enfoque sobre segurança. A segurança deve também estar implementada em cada aplicação, onde uma autenticação robusta é prioridade na disponibilização de serviços *on-line*. Parceiros comerciais, empregados terceirizados, bases de dados armazenadas externamente, provedores de serviços e uma gama cada vez maior de pessoas e aplicações penetram o perímetro de nossa rede até alcançar nossas aplicações e serviços, antes disponíveis apenas para a comunidade interna. Não se trata de substituir a segurança conseguida com *firewall*, *proxy*, detectores de intrusão e outros mecanismos, mas sim de acrescentar os serviços de confidencialidade, autenticidade, integridade, não-repúdio e autorização diretamente nas aplicações.

2. Motivação

Como o próprio nome indica, ICP é uma infra-estrutura e quanto menos visível for essa infra-estrutura melhor ela será. Não é à toa que a aplicação que obteve maior sucesso foi o uso de certificados digitais para criar uma conexão segura e identificada com servidores Web, através do protocolo SSL – *Secure Sockets Layer*. A razão para o sucesso dessa aplicação de certificados é porque seu uso é transparente para o usuário final, e todas as funcionalidades estão integradas no navegador que acessa o servidor Web.

Embora já existam diversos pacotes que disponibilizam os componentes de uma ICP, facilitando a criação e gerenciamento dos certificados digitais, é a integração com as aplicações que está mais atrasada e, quando existe, é bastante complicada para o usuário comum. Para facilitar essa integração é preciso que as organizações se preparem para assimilar essa tecnologia.

3. Conceitos de criptografia

Imagine a seguinte situação:

"Um usuário recebe uma mensagem de sua irmã, via correio eletrônico, solicitando que deposite R$ 1.000,00 em sua conta corrente; os dados da conta vêm junto com a mensagem."

Dias depois descobre que sua irmã nunca solicitou tal depósito. Ou seja, foi enganado por não conhecer as vulnerabilidades dos serviços disponíveis via Internet. O

usuário não pode garantir que quem enviou a mensagem é quem diz ser, não havia autenticidade. Não pode garantir que a mensagem não foi modificada, não havia integridade. Não pode garantir que outros não tomaram conhecimento de seu conteúdo, não havia confidencialidade. Não pode evitar que o emissor da mensagem venha a repudiar o envio da mensagem. Todos estes serviços de segurança: confidencialidade, autenticidade, integridade e não-repúdio; são possíveis de serem obtidos utilizando-se as técnicas de criptografia e a infra-estrutura de chaves públicas.

Criptografia, no contexto do mundo virtual, é a ciência que aplica complexas relações matemáticas para aumentar a segurança das transações eletrônicas [6]. Existem duas classes de algoritmos de criptografia, os simétricos e os assimétricos.

3.1. Algoritmos simétricos

Os algoritmos simétricos são muito antigos, já eram conhecidos pelos egípcios [11], e são chamados de simétricos por usarem a mesma chave criptográfica para cifrar e decifrar o texto. Uma comunicação cifrada consta de quatro elementos, o texto original, o algoritmo criptográfico, a chave criptográfica e o texto cifrado.

Os exemplos práticos recomendam que o algoritmo seja de conhecimento público e toda a segurança seja depositada no conhecimento da chave. São considerados seguros os algoritmos que não podem ser quebrados com os recursos do atual estágio da tecnologia de criptoanálise. Uma chave com 128 bits, adequadamente gerada, é considerada segura para o poder computacional atual e por algum tempo ainda.

Existem dois tipos de algoritmos simétricos, os que cifram blocos de dados, utilizados para a troca de mensagens, e os que cifram fluxo de dados, utilizados para a troca de dados que são enviados continuamente de um emissor para um receptor [12]. Como exemplo dos cifradores de blocos temos o DES – *Data Encryption Standard*, 3-DES, RC2 – *Rivest Cypher*, RC5, RC6, Blowfish, IDEA, e o último da família o AES – *Advanced Encryption Standard* [1]. Como exemplo de cifradores de fluxo temos o RC4, que é muito mais rápido que qualquer outro cifrador de blocos e suporta diversos tamanhos de chaves.

Algoritmos simétricos são razoavelmente rápidos, não causam muito impacto na carga dos processadores dos computadores, e os textos cifrados têm aproximadamente o mesmo tamanho do texto original. Ocorrem outros problemas que tornam o uso destes algoritmos bastante complicado. Para cada par de pessoas trocando mensagens é necessária uma chave distinta das demais. Isto faz com que num grupo de 4 pessoas sejam necessárias 4.(4 - 1) = 12 chaves, ou seja o número de chaves cresce com o quadrado do número de participantes. Outra deficiência é a distribuição das chaves. É preciso que os participantes utilizem um canal seguro para procederem à troca de chaves, uma vez que a mesma chave é usada para cifrar e decifrar os textos. Essa situação é agravada pela necessidade da constante renovação das mesmas, pois quanto mais uma chave é utilizada, maiores são as chances de que venha a ser comprometida, comprometendo todas as mensagens por ela cifrada.

O gerenciamento dessas chaves é outro complicador no uso de algoritmos simétricos. O usuário precisa saber qual chave deverá usar para cada participante, e deverá se lembrar qual chave foi utilizada para cifrar cada texto, seu ou de outros, que foi armazenado cifrado. Também deverá se lembrar de excluir a chave correspondente aos textos excluídos. Com algoritmos simétricos também não é possível assinar digitalmente um documento, nem impedir o repúdio.

3.2. Algoritmos assimétricos

Os algoritmos assimétricos são recentes na comunidade acadêmica, surgiram em meados da década de 1970 tendo sido desenvolvidos pela comunidade de inteligência britânica uma década antes [13].

Os algoritmos assimétricos usam um par de chaves matematicamente relacionadas, onde o texto cifrado com uma das chaves somente poderá ser decifrado por seu par. Umas das chaves é chamada de chave privada e deverá ser mantida secreta. A outra, chamada de chave pública, poderá ser de conhecimento público. Também, não deve ser possível derivar a chave privada a partir da chave pública; pelo menos não de forma trivial.

Existem poucos algoritmos assimétricos e geralmente são baseados nos conceitos introduzidos por Whitfield Diffie e Martin Hellman [3] de sistemas de criptografia de chave pública, que permitem cifrar e assinar digitalmente um documento. Com este sistema não é mais necessário o compartilhamento de um segredo, como era necessário compartilhar a chave simétrica no sistema de criptografia simétrico. Toda a comunicação envolve apenas a troca de chaves públicas e nenhum segredo (chaves secretas) é transmitido entre as partes no claro. Portanto, não é preciso confiar na segurança dos meios de comunicação, apenas deve-se garantir a segurança da chave privada e a associação entre a chave pública e a pessoa que a identifica através de um certificado digital.

3.2.1. Características dos algoritmos assimétricos. Em geral são necessárias chaves assimétricas muito mais longas que as simétricas, para obter a mesma resistência à criptoanálise. A comparação entre algoritmos diferentes não é possível de ser feita diretamente comparando-se apenas o comprimento das chaves [9].

Os algoritmos assimétricos mais conhecidos são o RSA, o DSA, o ElGamal e os baseados em curvas

elípticas ECC – *Elliptic Curve Cryptography*. Tanto o RSA, o ElGamal e os ECC são usados para cifrar e assinar, o DSA apenas pode assinar digitalmente.

A questão do gerenciamento das chaves é bastante simplificada, cada usuário precisa apenas se preocupar em manter secreta a sua própria chave privada, todas as demais chaves poderão ser obtidas em um repositório de acesso público. Também está resolvido o problema de distribuição das chaves, uma vez que estas podem ser trocadas através de canais inseguros em ambientes *on-line*.

O processamento de algoritmos assimétricos é computacionalmente intensivo, lento e expande o tamanho do texto cifrado em relação ao texto claro. Uma combinação da criptografia simétrica com a assimétrica e com as funções *hash* será a solução para as comunicações que suportem todas as necessidades de sigilo, integridade, autenticidade e não-repúdio.

3.2.2. Funções hash. Uma função *hash* é uma transformação que dada uma entrada retorna uma seqüência de bits de tamanho fixo, que é chamado o valor *hash* daquela entrada. Quando utilizada em criptografia são necessárias algumas características adicionais como: a entrada pode ser de qualquer tamanho; a saída deve ter um tamanho fixo; deve ser computacionalmente fácil de implementar e rápida no cálculo; deve ser de mão única, ou seja, dada a saída não é possível descobrir a entrada; deve ser livre de colisões, ou seja entradas diferentes não podem produzir saídas iguais; não deve ser possível descobrir nenhuma informação sobre a entrada conhecendo-se a saída.

O valor *hash* representa de forma concisa a mensagem original e é chamado de *message digest* ou *digital fingerprint*. Os algoritmos deste tipo mais conhecidos e testados são o MD2 – *Message Digest 2* – (RF-1319), MD5 - *Message Digest* 5 – (RFC-1321) e SHA-1 – *Secure Hash Algorithm*. O MD2 e o MD5 produzem uma saída com 128 bits de comprimento e são otimizados para processadores de 8 e 32 bits, respectivamente. O SHA-1 produz uma saída de 160 bits e é otimizado para processadores de 32 bits ou mais poderosos. Estes algoritmos são bastante rápidos em calcular o *hash* de grandes textos.

3.2.3. Envelope e assinatura digital. Para enviar uma mensagem assinada e criptografada é necessário que o remetente gere uma chave simétrica que será usada para cifrar o texto claro. Em paralelo passa-se o texto claro por uma função *hash*. A saída da função *hash* é cifrada com a chave privada do remetente, gerando a assinatura do texto. Junta-se o *hash* assinado e a chave simétrica e cifra-se com a chave pública do destinatário, criando o que se chama de envelope digital. Esta última operação é bastante rápida pois tanto a chave simétrica como o *hash* são seqüências de 128 bits cada. Envia-se para o destinatário o texto cifrado pela chave simétrica, criada exclusivamente para esta comunicação, mais o envelope digital.

Dessa forma pudemos aproveitar todas as facilidades da criptografia assimétrica com a rapidez da criptografia simétrica. A gestão da chave simétrica é resolvida sem perder a rapidez de seu uso. Outros protocolos também fazem uso da criptografia de chaves assimétrica para negociar uma chave simétrica que será utilizada apenas numa sessão, sendo renovada a cada nova sessão.

Persiste ainda um problema. Como garantir que a chave pública do remetente é de fato de quem diz ser que é? Um remetente malicioso poderia criar um par de chaves assimétricas em nome de uma pessoa que ele esteja querendo se fazer passar por, e publicar a correspondente chave pública em nome da pessoa personificada. Toda a segurança conseguida desaparece, pois se baseava no fato de que a chave pública e a identidade do remetente estavam univocamente ligadas. Para garantir essa ligação foram criados os certificados digitais. É preciso que o certificado digital seja enviado juntamente com o restante da mensagem, de modo que se possa verificar, no destino, a validade do certificado e se a chave pública do remetente de fato está relacionada ao nome da pessoa que enviou a mensagem.

3.2.4. Certificados digitais. Certificados digitais são como documentos de identidade expedidos por autoridades competentes. Podemos descrever, de forma simplificada, que um certificado digital é um documento que declara que uma particular chave pública pertence a um particular usuário nominado nesse certificado. Todas estas declarações são assinadas com a chave privada da autoridade que faz essa declaração. Para verificar a validade dessa declaração é preciso confiar na correspondente chave pública da autoridade que assinou o certificado. Na seção 4 são descritos os componentes de uma ICP – Infra-estrutura de Chaves Públicas, explicando como gerar e validar os certificados, resolvendo o problema recorrente de confiar numa chave pública final.

4. Conceitos de ICP, modelo PKIX [7]

O grupo de trabalho do IETF – *Internet Engineering Task Force* que desenvolve o modelo PKIX, baseado nas recomendações X.509 da ITU-T – *International Telecommunications Union* [4], tem publicado inúmeras RFCs – Request for Comments [8] descrevendo as principais áreas de suporte deste modelo de arquitetura, que são: perfis de certificados X.509v3 e da LCRv2 - lista de certificados revogados; protocolos de operação; protocolos de gerenciamento; esboço de políticas, PC - Política do Certificado e DPC - Declaração de Práticas de Certificação - DPC; protocolos de validação de

certificados; carimbo de data - *timestamp* e serviços de certificação de dados – *Data Certification Service.*

No sítio http://www.ietf.org/html.charters/pkix-charter.html encontramos uma lista bastante grande de RFCs e *drafts* sobre o modelo PKIX. O documento http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-09.txt é um guia e tutorial para auxiliar no acompanhamento do desenvolvimento desse modelo.

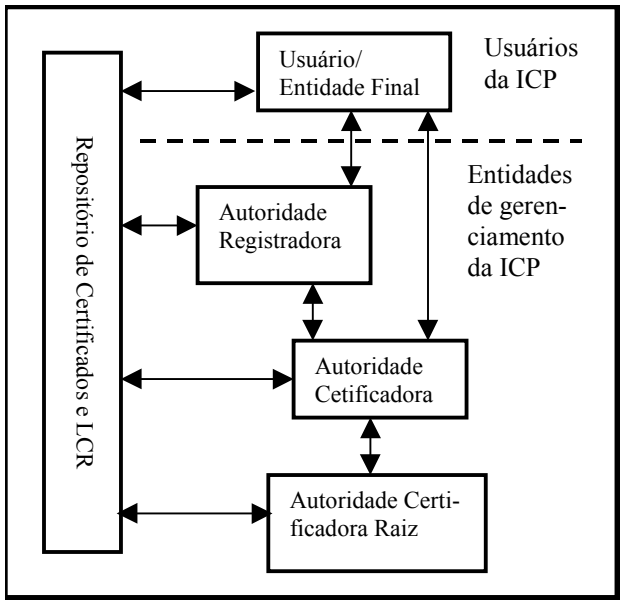

Figura 1 – Componentes de uma ICP modelo PKIX. As setas indicam transações de gerenciamento e operação entre os componentes, através da Internet.

Os perfis dos certificados são uma complexa estrutura de dados com campos de informações básicas e campos opcionais de extensão. São os campos opcionais que dão uma grande flexibilidade a estes certificados, permitindo sua utilização em muitas aplicações em diferentes ambientes. O perfil X.509 v3 é uma descrição de quais conteúdos o certificado obrigatoriamente deve suportar, quais os que pode suportar e quais os que não deve suportar. Da mesma forma é definido o perfil para a Lista de Certificados Revogados – LCR v2. Estas definições e restrições são necessárias para permitir a interoperabilidade entre os diversos implementadores.

Os protocolos de operação fazem uso dos serviços providos pelos protocolos já existentes na Internet como e LDAP - *Lightweight Directory Access Protocol* (RFC-2559) e FTP - *File Transfer Protocol* e HTTP - *Hypertext Transfer Protocol* (RFC-2585), como meio para entregar certificados, distribuir LCRs e trocar mensagens de gerenciamento.

Os protocolos de gerenciamento suportam a comunicação e a transferência de requisição e resposta entre as entidades da ICP. Existem dois tipos de protocolos de gerenciamento, um define o formato da mensagem que será enviada e o segundo define como essa mensagem será transmitida. O formato CRMF – *Certificate Request Message Format* (RFC-2511) descreve os formatos das mensagens para gerenciar as requisições e respostas. Os protocolos CMP – *Certificate Management Protocol* (RFC-2510) e o *CMC – Certificate Management Messages Over CMS (Cryptographic Message Syntax)* (RFC-2797) descrevem dois protocolos para a troca dessas mensagens. No presente estágio de desenvolvimento parece não haver forma de integrar os protocolos CMP e CMC, logo as ICPs deverão implementar estes dois e as entidades finais e os usuários devem escolher um dos protocolos para interagir com a ICP.

A RFC-2527 é um esboço de uma PC - Política do Certificado e de uma DPC - Declaração de Práticas de Certificação. Estes documentos apontam requisitos de segurança como: segurança física das pessoas e equipamentos; procedimentos para identificação dos requisitantes de certificados digitais; políticas de revogação e divulgação de certificados revogados etc. Esta mesma RFC define PC como sendo um conjunto identificado de regras que indica a aplicabilidade de um certificado para uma determinada comunidade ou classe de aplicação com os mesmos requisitos de segurança. Por exemplo, uma particular PC indica que o certificado é aplicável apenas para a autenticação em determinado banco *on-line*.

Quando um certificado é emitido espera-se que seja usado por todo o período de sua validade. Entretanto, diversas circunstâncias podem invalidá-lo antes da expiração de sua validade, como o comprometimento da chave privada associada. Em tais casos a AC – Autoridade Certificadora - revoga o certificado e anuncia essa ação. A forma mais simples de anunciar esses eventos é a AC publicar periodicamente, em um repositório, uma LCR - lista de certificados revogados com a data de publicação, o número de série de todos os certificados revogados por aquela AC e o motivo da revogação de cada um. Essa lista será assinada pela AC de forma a garantir a autenticidade e integridade dela. O repositório normalmente é um diretório baseado no protocolo LDAP (RFC-2559).

Todas as vezes que uma terceira parte (*relying-party*) precisar acreditar em um certificado ela deverá proceder à validação deste, processando uma LCR. Esse processo envolve buscar a lista no repositório apontado no próprio certificado e procurar pelo número de série do certificado em questão, também deverá validar todos os diferentes certificados no caminho de certificação, até o certificado da AC raiz. Há duas outras alternativas em desenvolvimento que provêem serviços de verificação *on-line* do estado dos certificados. Uma é o OCSP – *Online Certificate Status Protocol* definido na RFC-2560. O usuário executa uma consulta através do número de série

do certificado e recebe uma das seguintes respostas: *good, revoked, unknown*. A terceira parte é responsável por continuar a verificação por todo o caminho de certificação até o certificado raiz, esse protocolo não executa esse processo automaticamente. A outra forma é delegar todo o processo de validação do certificado e da cadeia de certificação para um serviço de validação. O cliente solicita o estado de um certificado e esse serviço executa todas as tarefas necessárias para verificar completamente toda a cadeia de certificação. Esse serviço está sendo chamado de SCVP – *Simple Certificate Validation Protocol* [5]. Esse serviço está descrito em um *draft* do grupo de trabalho PKIX muito recente, publicado em junho de 2002. Esse novo protocolo procura resolver diversas deficiências encontradas no OCSP.

O Carimbo de Data e Certificação de Dados são serviços implementados em cima dos providos pela ICP. O serviço de carimbo de data (*timestamp)* (RFC-3161) é provido por uma terceira parte, conhecida como *Time Stamp Autority*, que assina o documento atestando que este existia na data da assinatura. Este serviço fornece suporte para o não-repúdio, pois pode provar que um documento foi assinado antes do comprometimento da chave privada do autor do documento. O serviço de Certificação de Dados (RFC-3029) é a versão digital do cartório de registro de imóveis, onde um documento é atestado como correto e válido. Uma terceira parte verifica a existência e validade de uma determinada assinatura e respectivo certificado em um determinado período de tempo, mesmo depois que o certificado tenha expirado ou sido revogado. Atesta assim que a transação foi válida quando realizada e os dados estão corretos.

4.2. Componentes da ICP

Na figura 1 os diversos blocos representam os vários componentes de uma infra-estrutura de chaves públicas. Os blocos representam entidades que agregam uma série de serviços num mesmo local ou servidor.

O bloco Usuário/Entidades Final representa os detentores dos certificados digitais. Podendo também ser outros usuários ou serviços que acreditam no certificado apresentado por alguém acessando ou se identificando para um sistema, estes são conhecidos como terceira parte (*relying-party*).

O bloco Autoridade Registradora – AR é uma entidade com a responsabilidade de desempenhar tarefas administrativas para o registro dos usuários, tais como: confirmar a identidade do requisitante; validar que o requisitante tem direito aos privilégios requisitados; verificar que o mesmo está de posse da correspondente chave privada associada com o certificado requisitado. As atividades da AR envolvem interações entre os usuários e a ICP no processo de identificação, entrega de certificados e solicitação de revogação de certificados. A AR pode estar localizada fisicamente junto à organização, enquanto a AC pode ser uma empresa contratada para esse fim e a interação entre ambas pode ser feita pela Internet.

O bloco Autoridade Certificadora – AC é uma autoridade que cria e assina certificados digitais, opcionalmente também pode gerar as chaves dos usuários finais. Essa infra-estrutura é responsável pelo gerenciamento dos certificados por ela emitidos, por todo o ciclo de vida destes. Existe também um tipo especial de autoridade certificadora, que é a Autoridade Certificadora Raiz, normalmente uma AC-raiz assina seu próprio certificado. As entidades finais acreditam diretamente na AC-raiz, sem a necessidade de uma terceira parte validando-a. É o caso do certificado da ICP-Brasil [2] que é a AC-raiz para todas as demais ACs que emitem certificados que tenham validade jurídica no Brasil. O certificado de uma AC raiz deve ser obtido de forma segura.

O bloco Repositório de Certificados e LCR é usado para armazenar e dar acesso público aos certificados digitais e LCR - listas de certificados revogados. Normalmente é um diretório tipo LDAP, que são bases de dados especialmente projetadas para facilitar e agilizar a consultas de informações; por exemplo uma lista telefônica. O repositório é um servidor que tem que ter alta disponibilidade pois muitas das operações da ICP e do uso de certificados dependem das informações ali armazenadas [14].

5. Autenticação robusta

Autenticação é o processo de determinar a identidade de alguém com algum nível de certeza, fazer isso a quilômetros de distância é uma tarefa bastante complexa.

Com o aumento do número de sistemas e serviços que os usuários precisam se conectar também aumentou o número de senhas e *usernames* a serem memorizados. Os usuários tomam atitudes que vão desde adotar a mesma senha para todos os sistemas e nunca trocá-las, até colar lembretes debaixo do teclado ou no monitor. Uma saída freqüentemente adotada é o administrador dos sistemas forçar a adoção de senhas não-triviais e obrigar os usuários a trocá-las periodicamente. O custo de gerenciamento então aumenta enormemente, pois os usuários esquecerão as senhas aumentando a carga administrativa. Uma forma mais segura é adotar métodos de autenticação robusta.

Diz-se que uma autenticação é robusta quando envolve dois ou mais fatores. Os três fatores mais comuns são: alguma coisa que o usuário sabe, como senha ou PIN – *Personal Identification Number*; alguma coisa que o usuário tenha, como cartão magnético ou *token*; alguma coisa que o usuário é (biometria), impressão digital ou mapa da retina.

A possibilidade de que os dois fatores venham a ser comprometidos ao mesmo tempo é bem menos provável, tornando o processo de autenticação mais seguro. Caso o cartão do banco seja roubado ou perdido, será preciso também saber a senha para que esse cartão possa ser usado para comprometer a conta do usuário. Essa dificuldade adicional oferece ao usuário um tempo para reagir e solicitar o bloqueio da conta ao administrador do sistema, evitando outros prejuízos.

A dimensão dos prejuízos, o poder computacional crescente, a quantidade de serviços, as responsabilidades sendo transferidas para os usuários finais, exigem mecanismos mais seguros de autenticação e proteção de chaves e senhas. A necessidade de autenticação robusta poderá ser atendida pelas técnicas e tecnologias da ICP e pela adoção de cartões inteligentes para armazenar as chaves privadas. A solução mais segura é a utilização de cartões inteligentes para armazenar a chave privada e o correspondente certificado digital. Para ativar o cartão o usuário terá que entrar com sua senha ou PIN, dessa forma teremos uma autenticação com dois fatores, a senha e a posse do cartão inteligente. As aplicações devem ser construídas de tal forma que não memorizem a senha de ativação do cartão.

Sabemos que qualquer solução de segurança adotada é tão forte quanto o seu elo mais fraco. Na ICP o elo mais fraco é a proteção da chave privada e seu uso adequado. Consequentemente devemos prover uma autenticação robusta do detentor da chave e mecanismos de proteção ao utilizar os serviços de ICP.

6. Considerações finais

Como discorrido ao longo deste trabalho o uso de certificados digitais encontra-se na fase de amadurecimento tecnológico. Superada essa etapa as perspectivas apontam para uma adoção de certificados digitais tão ampla quanto o uso da Internet, onde os serviços e transações passarão a serem feitas de forma mais segura, apoiados por uma infra-estrutura de chaves públicas.

No entanto, persistem inúmeros problemas de interoperabilidade que devem ser resolvidos pela adoção de protocolos não proprietários e amplamente aceitos pelos fornecedores de aplicativos e pacotes de gerenciamento de certificados digitais

Os usuários passarão necessariamente por um processo de aculturamento onde a etapa mais demorada será a aceitação e compreensão das necessidades de uso desta tecnologia e, as organizações deverão investir no desenvolvimento de aplicações que aproveitem os recursos providos pela ICP na melhoria da segurança das transações *on-line*.

Bibliografia:

1. AES. Disponível em: <http://csrc.nist.gov/encryption/aes/>. Acessado em: 06 ago 2002.
2. BRASIL. Medida Provisória nº 2200-2, de 24 de agosto de 2001. *Diário Oficial da União.* Seção 1. 28 ago. 2001.
3. DIFFIE, W.; HELLMAN, M.E.; New directions in cryptography, *IEEE Transactions on Information Theory*. v. 22. 1976. p. 644-654.
4. ITU-T. Draft Revised ITU-T Recommendation X.509 ISO/IEC 9594-8: Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks. version 4. jun. 2000. Disponível em: <http://www.itu.int/itudoc/itu-t/com7/contr/contr5/250-es.html>. Acessado em: 14 ago. 2002.
5. MALPANI, A.; HOUSLEY, R; FREEMAN, T. Simple Certificate Validation Protocol (SCVP): draft-ietf-pkix-scvp-09.txt. jun. 2002. Disponível em: http://www.ietf.org/ internet-drafts/draft-ietf-pkix-scvp-09.txt. Acessado em: 13 ago. 2002.
6. NASH, Andrew; DUANE, William; JOSEPH, Celia; BRINK, Derek. *PKI: Implementing and Managing E-Security*. Califórnia,USA: Osborne/Mc Graw Hill, 2001.
7. PKIX working group. Disponível em: <http://www.ietf.org/html.charters/pkix-charter.html> . Acessado em: 09 de ago. 2002.
8. RFC-____. Todas as RFCs estão disponíveis em: <http://www.ietf.org/ rfc/rfc____.txt>. Acessado em: 14 ago. 2002.
9. RSA Laboratories Bulletin nº 13, abr. 2000. A Cost-Based Security Analysis of Symmetric and Asymmentric Key Lengths. revisado em nov. 2001. Disponível em: < http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html>. Acessado em: 08 ago. 2002.
10. SANS. *PKY: Why hans´t it taken off?*. Disponível em: <http://www.101.com/solutions/security/article.asp?ArticleID=574>. Acessado em: 06 ago. 2002.
11. SCHNEIER, Bruce. *Secrets and lies*, Jonh Wiley & Sons, Inc. 2001. cap. 6.
12. SCHNEIER, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc.. 1995. 2ª edição. ISBN: 0-471-11709-9
13. SINGH, Simon. *The Code Book: The Secret History of Codes and Code-Breaking.* <http://www.simonsingh.com/bookshop.htm>.
14. WILCOX, Mark. *Implementing LDAP*. Birmingham, UK: Wrox Press, 1999.