

# ICP-EDU: unificando as ICPs no âmbito acadêmico.

Wilton Speziali Caldas

Oswaldo Carvalho

Jeroen van de Graaf

Sérgio Novaes

Laboratório de Computação Científica  
Universidade Federal de Minas Gerais  
Avenida Antônio Carlos 6627  
31270-901 Belo Horizonte - MG  
*jvdg@lcc.ufmg.br*

**Resumo:** Neste documento propomos um projeto para unificar as infra-estruturas de chave pública no âmbito acadêmico brasileiro. O objetivo é facilitar o reconhecimento mútuo de certificados X509 emitidos por universidades ou outras organizações acadêmicas, assim facilitando a autenticação, autenticidade, integridade e não-repúdio nas comunicações.

## 1 Introdução

A tecnologia chamada de Infra-Estrutura de Chave Pública (ICP; em inglês *Public Key Infrastructure* ou PKI) objetiva melhorar a segurança digital. Sua adoção é um processo lento por razões diversas como:

- é uma tecnologia complicada, tanto para os técnicos quanto para usuários finais;
- a maioria dos usuários nem se preocupa tanto com a segurança do seu email, e não está disposta a fazer o esforço adicional para usar S/MIME;
- existem grandes interesses comerciais, dificultando a definição de padrões;
- por definir as cadeias de confiança dentro e entre organizações, surgiram atritos entre elas para decidir quem fica com qual responsabilidade.

Hoje o uso principal da ICP é para garantir o URL de um servidor, principalmente em transações comerciais. Também os sistemas de *home banking* utilizam certificados digitais, seja de X509, seja de um formato próprio.

No mundo acadêmico a utilização de ICP está crescendo:

- A intranet da UFMG se baseia no Lotus Notes, que já vem com muitos recursos de segurança embutidos, inclusive uma ICP proprietária. O Notes possibilita também o uso de certificados X509, e a sua emissão já acontecerá em breve.
- A UFSC já tem um Autoridade Certificadora Raiz emitindo certificados para quem tem email no domínio @ufsc.br [1].

- No SINAPAD, o Sistema Nacional de Processamento de Alto Desempenho, os novos *grid computers* adquiridos (e talvez alguns pré-existentes) serão compartilhados entre todos os centros de computação no Brasil. Em princípio um usuário será capaz de submeter um job em qualquer grid computer (sujeito a algumas restrições). O sistema de job scheduling escolhido, chamado Globus, usa certificados digitais para autenticar seus usuários e para transações necessárias a sua utilização, como movimentação de dados automática e conversação entre grids.

O caso do SINAPAD é um exemplo de um recurso compartilhado nacionalmente. Podemos esperar que num futuro próximo surjam muito mais exemplos de sistemas cuja autenticação é feita através de certificados X509, um mecanismo mais robusto que uma mera senha. Por isso achamos o momento oportuno para iniciarmos um projeto de ICP no âmbito acadêmico, estabelecendo algumas diretrizes, e assim facilitar a convergência para uma solução bem-pensada e madura.

## 2 Modelos de confiança

O propósito de uma ICP é aumentar a segurança e confiança digital; ela implementa um modelo (ou hierarquia) de confiança, decidindo quem autentica quem e quem confia em quem. A escolha do modelo de confiança poderia fazer a diferença entre um sucesso ou um fracasso. Apresentamos aqui um resumo sobre modelos de confiança, para detalhes veja por exemplo [3, 4, 2].

Um certificado digital nada mais é que uma assinatura digital num documento com um formato especial. O certificado cria um vínculo entre uma chave pública e a identidade de uma entidade (pessoa, servidor, URL, etc) que possui a chave privada correspondente. O emissor de certificados digitais é chamado uma Autoridade Certificadora (AC). Observe que todo mundo pode atuar como AC, e que as exigências para emitir certificados podem variar muito entre ACs. Ou seja, para se avaliar o significado de um certificado deve-se conhecer a política da AC emissora.

### Modelo hierárquico

Para que um terceiro possa verificar um certificado emitido por uma AC, é necessário que ele possa confiar no certificado da AC. Para resolver isso há duas opções: 1) a AC autoassina sua chave pública criando um certificado e divulgando-o amplamente. Neste caso ela está no topo de hierarquia de confiança e é chamada de AC-Raiz. 2) ela procura uma outra CA-Raiz já bem-conhecida que assina seu certificado. Verifique-se que em ambos os casos um terceiro pode verificar o certificado do usuário. Observe que no primeiro caso temos um modelo "flat": existe uma AC que assina todos certificados, enquanto no segundo caso temos um modelo hierárquico: há uma AC-Raiz e uma AC-Intermediário. Na verdade, não há limite no número de ACs-Intermediário e assim pode se construir hierarquias de confiança mais extensas e complicadas.

Em teoria uma grande hierarquia resolveria todos os problemas de autenticação no mundo, mas na prática há vários problemas: 1) deve-se começar top-down, com conseqüências catastróficas se errar 2) Quem deve assumir o papel de AC-Raiz? A UFMG? A RNP? O governo brasileiro? A ONU?

Na prática várias organizações começam a emitir certificados, atuando como AC-Raiz na sua própria hierarquia, criando várias hierarquias isoladas. Por exemplo, a UFSC e a UFMG já estão emitindo certificados separadamente. A questão é: como juntar estas hierarquias?

## **Certificados cruzados**

Se, por exemplo, a UFSC quiser reconhecer os certificados emitidos pela UFMG, ela pode criar um certificado cruzado, isto é, ela assina o certificado raiz da UFMG. Desta forma, um usuário da UFSC confrontado com um certificado da UFMG vai confiar nele, porque o certificado cruzado é testemunha que a AC-Raiz da UFSC confia em todos certificados emitidos pela UFMG. Normalmente faz-se também o inverso: a UFMG assina o certificado raiz da UFSC, endossando todos os certificados da UFSC.

A grande vantagem deste modelo é que as partes são iguais: entidades autônomas que decidem para cooperar. E se a chave raiz privada de uma entidade for comprometida, o estrago fica limitado na hierarquia onde isto aconteceu; a outra tem apenas que revogar o certificado correspondente.

## **AC-Ponte: um meio-termo**

A situação fica mais complicada se houver mais de duas organizações: com  $N$  organizações todas elas têm que criar certificados cruzados entre si, resultando em  $N(N - 1)$  certificados cruzados. Para resolver isso, existe uma outra topologia: cria-se um AC-Ponte, ou seja, uma AC-Raiz que tem como único objetivo criar certificados cruzados com todas as outras AC-Raiz. Assim, uma AC-Raiz precisa lidar somente com a AC-Ponte. A AC-Ponte tem  $N$  clientes. O custo é que o caminho de verificação aumentou em um nó. Para uma discussão mais ampla sobre as vantagens deste modelo, veja [3] §8.2.2.

## **3 Nossa proposta**

Em essência, a nossa proposta é lançar um projeto para a criação e operação de uma AC-Ponte no âmbito acadêmico. Imaginamos que o próximo passo será a criação de um comitê de especialistas de várias universidades e da RNP. Este comitê deve formular um projeto mais detalhado para solucionar as questões mencionadas neste documento.

## **4 Observações**

1) O relato aqui sobre hierarquias é muito resumido, e existem outras soluções possíveis. Acreditamos que a criação de uma AC-Ponte seja atualmente a melhor solução. Porém, um primeiro ponto do estudo deve priorizar qual é o modelo de confiança desejado no âmbito acadêmico.

2) O ICP-Brasil é uma tentativa do governo federal de definir uma ICP nacional. Ele adotou um modelo estritamente hierárquico, declarando-se a única AC-Raiz do país. Partes interessadas

interpretaram esta atitude como paternalista e resistiram contra este modelo. (Por exemplo, quando o Poder Judiciário quer criar uma AC, ela deve se submeter à ICP-Brasil, gerenciada pelo Poder Executivo?) Muitas partes acreditam que a seguinte solução servirá melhor ao país: i) O Poder Executivo cria uma AC-Raiz para todas as organizações subordinadas a ele. ii) O Poder Executivo cria uma AC-Ponte para juntar todos os órgãos brasileiros com própria AC-Raiz. Na situação atual a relação entre uma AC-Ponte da RNP e a ICP-Brasil torna-se um assunto político e confuso. Mas não há nada que impeça a criação da AC-Ponte proposta aqui, e as experiências adquiridas podem ser valiosas.

3) No caso do SINAPAD, os certificados servem apenas para identificar um usuário, enquanto seus direitos de acesso são gerenciados por mecanismos diferentes, usando LDAP e grupos. Apesar dos certificados X509 conterem campos que poderiam ser usados para estes objetivos também, acreditamos que separar estas funcionalidades proporciona soluções mais simples.

4) As organizações membro da AC-Ponte proposta aqui podem ter políticas diferentes, tanto com relação à emissão de certificados, quanto com relação aos aspectos operacionais (o cuidado empregado na criação das chaves privadas, frequência de atualização de lista de certificados revogados, etc). Seria necessário solucionar este assunto, por exemplo exigindo um nível mínimo que os membros devem satisfazer.

5) Se uma ICP for utilizada para assinaturas digitais de documentos com valor jurídico, seria necessário lidar com a questão de datação (time stamping). Porém, propomos desconsiderar este assunto por enquanto.

6) O nome "ICP-EDU" é provisório; devendo ser substituído por outro.

## Conclusão

Argumentamos que já estão surgindo ICPs isoladas do mundo acadêmico brasileiro, e que unificá-las seria inevitável. A RNP é a entidade "par excellence" para assumir esta responsabilidade.

## Referências

- [1] *Autoridade Certificadora*, <http://ac.labsec.ufsc.br>, acesso 31/03/03.
- [2] Adams, C.; Lloyd, S.; Kent, S. *Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*. New Riders Publishing, ISBN 157870166X, 1999.
- [3] Ignaczak, L. *Um novo modelo de Infra-estrutura de Chaves Públicas para uso no Brasil utilizando aplicativos com o código fonte aberto*. Dissertação de Mestrado em Ciência da Computação. Universidade Federal de Santa Catarina, Florianópolis, 2002.
- [4] Nash, A.; Duane, B.; Brink, D.; Joseph, C. *PKI: Implementing & Managing E-Security*. McGraw-Hill Osborne Media, ISBN 0072131233, 2001.