Curso de Tecnologia em Redes de Computadores
Disciplina: Tópicos Avançados II – 5º período
Professor: José Maurício S. Pinheiro

AULA 3: Políticas e Declaração de Práticas de Certificação

A certificação digital nas organizações é baseada na especificação RFC 2527 - Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Framework*. São oito os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo quatro relacionados com assinatura digital e quatro com sigilo.

Políticas de Certificação (PC)

Qualquer organização, independente do porte que tenha, pode criar uma ICP. Se uma empresa, por exemplo, criou uma política de uso de certificados digitais para garantir a segurança na troca de informações entre a matriz e filiais, não vai ser necessário pedir tais certificados a uma AC controlada pela ICP-Brasil. A própria empresa pode criar a ICP e fazer com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus usuários.

Todavia, a organização é responsável por sua ICP e deve elaborar um documento contendo suas Políticas de Certificação (PC) de forma a facilitar o entendimento do processo como um todo por seus usuários. Este documento detalha todas as políticas instituídas pela organização para garantir a segurança do processo de emissão e manutenção dos certificados emitidos.

As Políticas de Certificação descrevem o papel de cada componente dentro da ICP, as responsabilidades assumidas pelos seus usuários para a requisição e uso dos certificados digitais, além da manutenção do par de chaves de responsabilidade dos usuários. Elas devem abranger desde a solicitação do certificado, até a sua expiração ou revogação. Entretanto, as políticas de certificação não declaram os detalhes operacionais, pois estes podem ser alterados ao longo do tempo.

Declaração de Práticas de Certificação (DPC)

Os certificados digitais possuem validade devido à evolução dos dispositivos de processamento. A validade dos certificados para usuários finais varia de 1 a 3 anos. Os certificados das autoridades certificadoras podem variar de 3 a 20 anos. Sempre que o certificado digital é renovado geralmente trocam-se os pares de chaves. Também há a possibilidade dos certificados expirarem antes do seu prazo de validade, através da revogação. Estas informações são documentadas na Declaração de Práticas de Certificação (DPC) de cada Autoridade Certificadora.

Na DPC é especificado detalhadamente como que cada componente de uma ICP elabora a Política de Certificação. A DPC declara a PC associada e especifica os mecanismos e procedimentos utilizados para alcançar as políticas de segurança.

Uma DPC pode informar os aplicativos utilizados e os procedimentos de utilização do aplicativo. Ela deve detalhar informações suficientes para comprovar que todas as políticas serão satisfeitas através de procedimentos e ferramentas. O caminho para a DPC de um certificado digital pode estar armazenado na extensão “Política de Certificado”.

Listas de Certificados Revogados (LCR)

As Listas de Certificados Revogados (LCR) podem ser definidas como uma estrutura de dados assinada por uma AC contendo a lista de certificados que não devem ser considerados válidos.

Embora um certificado digital possua uma data para sua expiração, algumas vezes é necessário que sua validade seja negada antes do término deste prazo. Assim, um certificado pode ser revogado e, a partir deste momento, ele constará em uma lista de certificados inválidos.

Uma forma de distribuição da lista de certificados revogados é através de página web. O local onde a lista de certificados revogados encontra- se é adicionado em uma extensão do certificado digital, conforme mostra o exemplo da Figura 1.

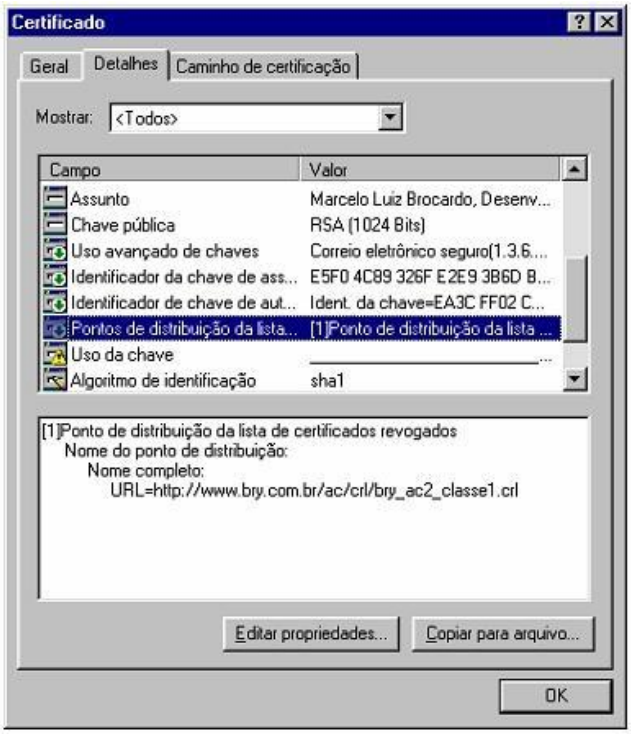

Figura 1 - Exemplo de LCR

As LCR's também seguem a recomendação X.509 do ITU-T. Uma LCR é formada pelo seguinte conjunto de campos:

- **Versão** - Indica a versão da LCR. Esse campo é opcional e, se não constar, sua versão é 1. Isto porque o campo não havia sido definido na versão 1 da recomendação X.509;
- **Assinatura** - Identificação do algoritmo utilizado na assinatura digital da LCR;
- **Emissor -** Dados que identificam o emissor da LCR;
- **Data de efetivação -** Data e hora de emissão da LCR;
- **Próxima Atualização** - Data e hora que uma nova atualização desta LCR deve ser emitida;
- **Certificados Revogados** - Lista contendo os números seriais de todos os certificados digitais revogados. Cada certificado revogado pode conter uma extensão indicando a razão da sua revogação.

Um Certificado Digital pode ser revogado pelos seguintes motivos:

- **Comprometimento da Chave Privada do Certificado** - Indica que a chave privada do usuário pode estar comprometida, tornando o certificado do usuário não-confiável;
- **Comprometimento da Chave Privada da AC** - A chave privada da AC que emitiu o certificado pode estar comprometida, com isto não se deve mais confiar nos certificados emitidos por ela;
- **Mudança de Filiação** - Alguma informação do sujeito contida no certificado foi alterada e assim, um novo certificado deve ser emitido;
- **Atualização** - Indica que o certificado foi atualizado;
- **Cancelamento da Operação** - O certificado não será mais utilizado para o propósito ao qual ele foi emitido;
- **Suspensão Temporária** - Indica que o certificado está, temporariamente, incluído na LCR. Atribuindo esta suspensão ao certificado, ele poderá ser retirado da LCR após um período de tempo ou definitivamente revogado;
- **Não-Específico** - O certificado consta na LCR por algum motivo diferente dos apresentados acima;

Deveres e Obrigações

Para a emissão dos certificados, as Autoridades Certificadoras (AC's) possuem deveres e obrigações que são descritos na DPC. A DPC dever ser pública, para permitir que as pessoas possam saber como foi emitido o certificado digital.

Entre as atividades de uma AC, a mais importante é verificar a identidade da pessoa ou da entidade antes da emissão do certificado digital. O certificado digital emitido deve conter informações confiáveis que permitam a verificação da identidade do seu titular. Por estes motivos, quanto melhor

definidos e mais abrangentes os procedimentos adotados por uma AC, maior sua confiabilidade.

O cumprimento dos procedimentos é auditado e fiscalizado, envolvendo, por exemplo, exame de documentos, de instalações técnicas e dos sistemas envolvidos no serviço de certificação, bem como seu próprio pessoal. A não concordância com as regras acarreta em aplicações de penalidades, que podem ser inclusive o descredenciamento. As AC's credenciadas são incorporadas à estrutura hierárquica da ICP-Brasil e representam a garantia de atendimento dos critérios estabelecidos em prol da segurança de suas chaves privadas.

Validade do Certificado

O certificado digital, diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, possui um período de validade. Só é possível assinar um documento enquanto o certificado é válido. É possível, no entanto, conferir as assinaturas realizadas mesmo após o certificado expirar.

O certificado digital pode ser revogado antes do período definido para expirar. As solicitações de revogação devem ser encaminhadas à AC que emitiu o certificado ou para quem foi designada essa tarefa. As justificativas podem ser por diversos fatores como comprometimento da chave privada, alterações de dados do certificado ou qualquer outro motivo.

A AC, ao receber e analisar o pedido adiciona o número de série do certificado a um documento assinado chamado Lista de Certificados Revogados (LCR) e a publica. O local de publicação das LCR's está declarado na DPC da AC que emitiu o certificado, e em muitos casos o próprio certificado possui um campo com apontador para um endereço WEB que contém o arquivo com a LCR. As LCR's são publicadas de acordo com a periodicidade definida pela AC. Essas listas são públicas e podem ser consultadas a qualquer momento para verificar se um certificado permanece válido ou não.

Após a revogação ou expiração do certificado, todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se houver uma forma de garantir que esta operação foi realizada durante o período de validade do certificado.

Carimbo de Tempo

Existem técnicas para atribuir a indicação de tempo a um documento, chamadas carimbo de tempo (time stamp). Estes carimbos adicionam uma data e hora à assinatura, permitindo determinar quando o documento foi assinado. O usuário pode solicitar a renovação do certificado para a AC após a perda de validade deste. A Resolução nº 16 da MP 2200-2, deu ao Observatório Nacional a responsabilidade pelo fornecimento da "hora oficial" a ser utilizado por todas as entidades integrantes da ICP-Brasil, de modo a

atuarem de forma sincronizada, elemento vital para a plena utilização das assinaturas digitais, pois permite a marcação do exato momento em que um documento eletrônico foi assinado.

O carimbo de tempo é um processo matemático público (que utiliza os mesmos modelos da assinatura eletrônica) em que são utilizados certificados digitais e uma terceira parte confiável (uma entidade que não faz parte das entidades que apresentam propostas nem da entidade adjudicante) que garante a data e hora em que determinada ação foi realizada. Assim, o Carimbo de Tempo é uma certidão digital com referência temporal que permite atestar a existência de um documento eletrônico em determinado instante de tempo. É uma solução necessária para garantir aos documentos digitais uma segurança equivalente àquela existente em documentos de papel.

Na solicitação, o usuário pode manter os dados do certificado e até mesmo o par de chaves, se a chave privada não tiver sido comprometida. Mas, por que não emitir os certificados sem data final de validade? Porque a cada renovação da validade do certificado renova-se também a relação de confiança entre seu titular e a AC.

Essa renovação pode ser necessária para a substituição da chave privada por outra tecnologicamente mais avançada ou devido a possíveis mudanças ocorridas nos dados do usuário. Essas alterações têm como objetivo tornar mais robusta a segurança em relação às técnicas de certificação e às informações contidas no certificado.

O Carimbo do Tempo é também uma ferramenta importante para garantir a validade de assinaturas digitais e desta forma atestar com segurança a identidade de um indivíduo no universo digital. Para ter validade, a assinatura digital precisa estar ligada a um certificado digital válido. Como os certificados digitais possuem validades pré-definidas, no momento em que são gerados, é necessária uma referência temporal para determinar se a assinatura foi produzida enquanto o certificado era válido.

Renovação e Revogação de Certificado

Conforme determina a legislação vigente, o certificado de servidor web ICP-Brasil não pode ser renovado pela internet. Entretanto, é possível renovar um e-CPF sem a presença do titular uma única vez. O pedido de renovação de um certificado digital deverá ser feito dentro do período de validade do certificado e o usuário deverá solicitar, usando sua assinatura eletrônica, junto à autoridade certificadora credenciada, a renovação do certificado.

Para renovar um Certificado Digital é obrigatório cumprir o prazo determinado de 30 dias ou menos para expiração do Certificado (é possivel ver a validade através do gerenciador de Certificados do browser). É importante lembrar que não é possível renovar um certificado digital após a data de expiração. Neste caso, é necessário fazer um novo pedido a AC portando toda a documentação necessária.

A revogação de certificados é o ato de tornar certificados inválidos antes de sua expiração natural e as aplicações que verificam o estado do certificado quanto à sua validade podem requisitar maiores informações a respeito do

motivo da revogação consultando a lista de revogação e decidir que ações tomar. Para revogar o certificado digital, o usuário deverá contatar a Autoridade Certificadora, emissora do Certificado Digital e seguir os procedimentos solicitados por esta.

É importante notar que apenas revogar certificados não é o bastante para disponibilizar a informação para as aplicações. É necessário criar e publicar a Lista de Certificados Revogados.

Verificando a Validade do Certificado

O certificado digital geralmente é armazenado em sistema de arquivos, mas também a possibilidade de ser armazenada em repositório físico como Token ou Smart-Cards. O exemplo da Figura 2 mostra como verificar os certificados em instalados num computador que utilize como browser o Internet Explorer.

No menu "Ferramentas" selecionar o item "Opções da Internet".

Figura 2 - Verificando os certificados instalados

Entre as "abas" que aparecem clicar em "Conteúdo" e surgirá o item denominado "Certificados". Ao clicar neste botão, irá aparecer uma tela com várias "abas", estas que destacam o os tipos de certificados.

Para obter maiores informações a respeito de um determinado certificado digital, basta selecionar o certificado desejado e, em seguida, clicar em “Exibir”, no canto inferior direito ou efetuar um duplo clique (Figura 3).

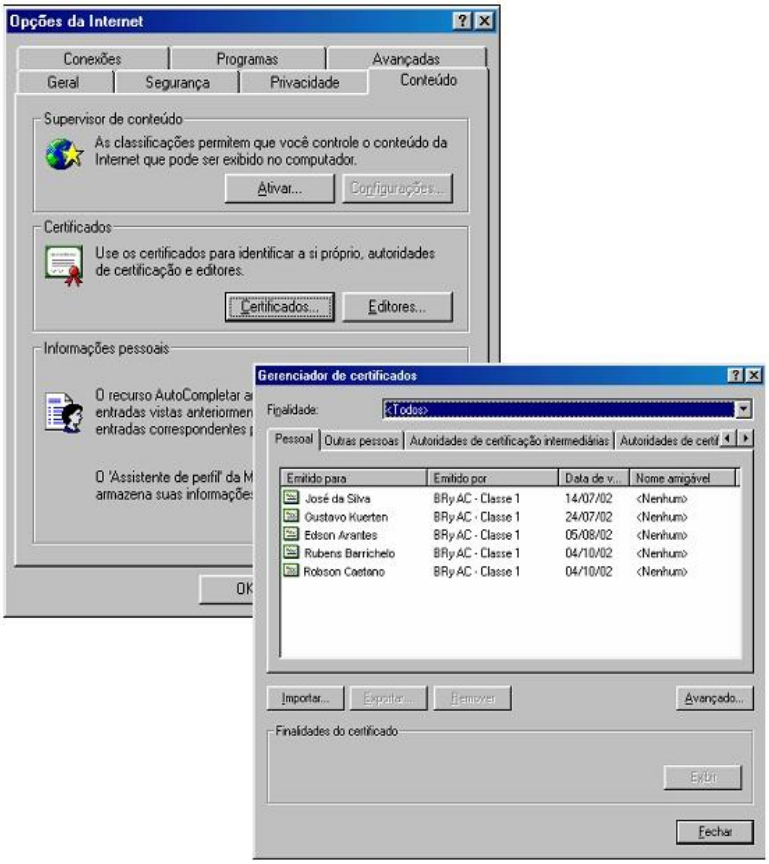

Figura 3 - Informações do Certificado

Ao clicar na "aba" "Detalhes" poderá visualizar várias informações como tamanho da chave, a validade, entre outras, e na "aba" "Caminho de Certificação" (Figura 4), pode-se ver o caminho que o certificado passou para chegar a seu computador desde a Autoridade Certificadora Raiz.

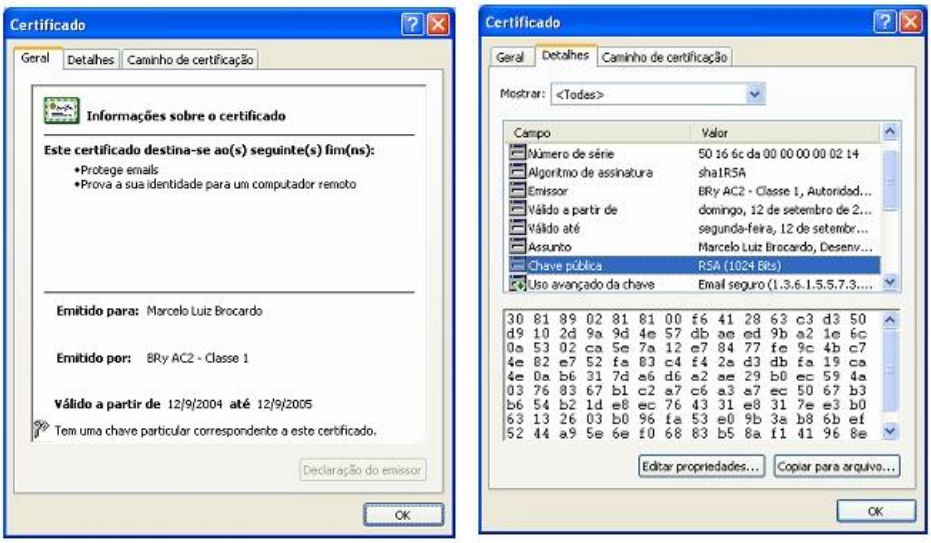

Figura 4 - Caminho da certificação