UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Uma ICP baseada em certificados digitais autoassinados

Cristian Thiago Moecke, Ricardo Felipe Custódio

Jonathan Gehard Kohler, Marcelo Carlomagno Carlos

Acadêmico: Matheus Bauer

1. Introdução

- Infraestruturas de Chaves Públicas são uma alternativa já consolidada para fornecer a capacidade de estabelecimento de relações de confiança entre entidades envolvidas em uma transação em meio digital. As ICPs tem sido amplamente utilizadas, por exemplo, no estabelecimento de confiança na navegação em sítios de internet, e mais recentemente tem ganho espaço para a autenticação entre pessoas físicas e jurídicas.

- Entretanto, o crescimento do uso das ICPs nestes novos contextos trouxe a tona uma série de limitações e dificuldades relacionadas à sua implantação e uso. As ICPs foram criadas para serem flexíveis, porém são difíceis de implementar, necessitam de muitos recursos humanos e computacionais para mantê-las e mesmo na presença desses recursos não conseguem prover serviços confiáveis a longo prazo.

- Razões que limitam o crescimento do uso das ICPs:
  - A pequena oferta de serviços que demandam os recursos oferecidos por ICPs;
  - A forma que as ICPs atuais foram projetadas as tornam difíceis de serem implementadas e dificultam a prestação de serviços, tornando-a pouco atrativa diante de outras soluções já existentes;
  - A implantação de uma ICP implica em níveis de segurança muito mais elevados do que os que seriam apropriados ou com boa relação de custo/benefício em muitos contextos.
- A diminuição das dificuldades de implantação e uso, e o menor custo operacional de uma ICP tendem a tornar atraentes os recursos oferecidos por uma ICP.

- Um dos aspectos de maior complexidade em ICPs é a construção e validação de caminho de certificação. Para a validação de um certificado é necessária:

  - a identificação de um caminho de certificados até uma âncora de confiança;
  - a obtenção destes certificados;
  - a validação das respectivas assinaturas digitais e situação de revogação de cada certificado deste caminho.

  A complexidade é maior quanto maior for o tamanho da cadeia de certificação.

- Ainda há mais um ponto de complexidade envolvido. Usualmente uma assinatura digital de um documento eletrônico contém carimbos do tempo para fornecer uma evidência temporal confiável de que a assinatura foi produzida quando o caminho de Certificação era válido.

- Isso é fundamental para documentos eletrônicos cujas assinaturas devem ser verificáveis mesmo após a expiração ou revogação do certificado do signatário e até mesmo da sua cadeia de certificação. Entretanto o carimbo do tempo é, essencialmente, um documento assinado. E desta forma, tem os mesmos problemas e desafios da assinatura digital comum.

- A determinação e a validação do caminho de certificação é a fonte de muitos dos problemas das ICPs. Para a implantação de uma ICP que tratasse adequadamente estes problemas, uma série de soluções tiveram que ser desenvolvidas, que por sua vez aumentaram ainda mais a complexidade da validação dos certificados.

- Além dos problemas já citados, há uma série de limitações de modelo de negócio impostas pela arquitetura tradicional. A hierarquia de ACs, inicialmente concebida para permitir a distribuição geográfica das atividades de emissão de certificados, mostrou-se extremamente cara devido aos custos de operação de cada AC. Para minimizar estes custos, a parte do processo de validação de dados dos titulares dos certificados digitais é repassada para Autoridades de Registro (AR).

- Este artigo propõe um novo modelo de certificação digital, através do uso de certificados digitais autoassinados e a substituição das ACs finais por Autoridades de Validação (AV).

- Quando uma AC emite um certificado, pressupõe-se que ele seja válido por um determinado período do tempo. Entretanto, isso não é correto uma vez que pode ser revogado a qualquer momento. Portanto, é necessária uma prova de que continua válido. Normalmente utilizam-se como prova listas de certificados revogados. Em virtude disso, defendemos que o certificado não deve ser considerado válido quando emitido.

- Assim, não há necessidade do certificado ser emitido por uma autoridade certificadora. Por razões práticas e de simplicidade, propomos que os certificados sejam emitidos por seus titulares, ou seja, autoassinados. Isso quer dizer que não haveria mais uma autoridade certificadora para a emissão dos certificados para o usuário final.

- Propomos ainda que as provas sejam de curta duração, ou vinculadas às assinaturas digitais dos documentos eletrônicos, tornando desnecessário o uso de carimbos do tempo. Isso muda completamente o modelo de certificação e, vários do problemas das ICPs tradicionais deixam de existir, além de tornar a ICP mais flexível e de menor custo de implantação.

2. Modelos de certificação digital e suas dificuldades

- Outras pesquisas tem proposto diferentes abordagens. Todas tentam melhorar o tempo de resposta das consultas a informações de revogação, criar mecanismos mais eficientes de validação, ou até mesmo eliminar a necessidade de revogação de certificados. Entretanto nenhuma das propostas tenta mudar os fundamentos da validação de certificados. O trabalho seguirá uma abordagem diferente, propondo uma nova modelagem de ICP, adequada para assinatura digital de documentos, sem perder a aplicabilidade para autenticação e demais usos de uma ICP tradicional.

3. Invertendo os paradigmas da validação de certificados

- No esquema tradicional de certificação digital, quando um certificado é emitido, ele é assumido como válido por um determinado tempo. Entretanto, certificados digitais podem ser revogados a qualquer momento. Portanto, ele não é válido até que seja obtida uma prova fornecida por uma terceira parte confiável de que ele continua válido. Usualmente usam-se LCRs como prova.

- Então, não é necessário implicar que o certificado seja válido quando emitido. O certificado pode ser emitido sem ser considerado válido e somente quando for necessário busca-se a prova que o torna válido.

- Neste modelo não há caminho de certificação, e todos os problemas relacionados a isso são automaticamente eliminados.

- Nesta proposta, o usuário gera seu próprio certificado autoassinado e realiza uma autenticação segura com uma Autoridade de Registro (AR) para provar sua identidade e posse da chave privada. A AR verifica os dados do certificado e a posse da chave, e os envia para uma terceira parte confiável, denominada de Autoridade de Validação (AV). A AV é responsável por emitir provas, quando solicitado, de que o certificado do usuário é válido num determinado instante de tempo.

- A autenticação segura deve ser feita de forma presencial. Neste modo de autenticação, o usuário precisa ir a uma instalação técnica da AR para se apresentar, provar (através de documentos) que ele é quem alega ser e provar a posse da chave privada. O certificado autoassinado será então assinado pela AR e enviado para uma ou mais Autoridades de Validação.

- Quando recebe uma requisição de verificação de validade, a AV verifica a situação do certificado em questão na sua base de dados e retorna um token, com a situação do certificado. Este token contém a prova de que o certificado é válido por um determinado período de tempo.

3.1. Autenticação

- Para processos de autenticação, o token emitido pela AV apenas prova que o certificado é válido para um determinado (e curto) período. Esta opção pode ser útil para assinaturas de curto prazo e especialmente mecanismos de autenticação. Um único token pode ser utilizado inúmeras vezes para quantas autenticações forem necessárias, sem necessidade de obtenção de mais dados externos pelo verificador.

3.2. Assinaturas de Documentos

- Quando um usuário assina um documento, a aplicação pode encaminhar o certificado, o resumo criptográfico do documento e a assinatura para a AV.

- A AV verifica a validade do certificado e da assinatura, e retorna para a aplicação um token de validação de assinatura. Este token fornece uma prova de validade não apenas do certificado, mas também da assinatura.

3.2.1. Manutenção a longo prazo da assinatura

- Para a conservação da validade de uma assinatura, é necessário obter provas atualizadas emitidas por novas AVs, antes que a prova anterior expire.

- Entretanto, é importante destacar que não é necessário adicionar um novo token, mas sim substituir o antigo. A AV, ao receber um token para ser revalidado, confirma as informações do token antigo e gera um novo token, com as mesmas informações do anterior, mas com sua assinatura.

- No modelo tradicional de ICP, para a conservação de longo prazo de um documento eletrônico, é necessário sempre adicionar novos carimbos do tempo sobre os carimbos do tempo anteriores, antes que estes percam sua validade.

- Cabe destacar que se comprometida a Autoridade de Carimbo do Tempo, todos os carimbos por ela já emitidos tornam-se inválidos, caso não exista um segundo carimbo contraposto ao primeiro. Isto é um problema, pois não há como prever a violação de uma ACT. Essa abordagem leva ao crescimento contínuo do arquivo de assinatura.

- No modelo proposto, a assinatura tem sempre o mesmo tamanho. E também possibilita a atualização de algoritmos de maneira extremamente simples. Os novos tokens podem fazer uso de algoritmos mais seguros e assim manter a confiabilidade da validação mesmo após a quebra dos algoritmos anteriormente usados.

5. Benefícios e Limitações

- A maior limitação da proposta é a mesma de uma Autoridade de Carimbo do Tempo, se uma chave de ACT for comprometida, todos os carimbos do tempo deixam de ser válidos. De igual modo, se uma AV é comprometida, todos tokens por ela emitidos deixam de ser confiáveis.
- Por esta razão, é extremamente importante que as chaves privadas da AV sejam protegidas com segurança apropriada. No caso da violação da chave, a única forma de distinguir entre tokens válidos e inválidos seria com a auditoria da AV. Entretanto, cabe destacar que a manutenção dos tokens, através da substituição destes por novos emitidos por novas AVs, também é bastante simplificado, facilitando a manutenção da verificabilidade da assinatura digital.

6. Considerações Finais

- Este artigo propôs um novo modelo de certificação que visa reduzir a dificuldade de validação de uma assinatura digital. Neste novo modelo foi sugerido que o certificado do usuário deve ser autoassinado, e a Autoridade Certificadora seja substituída por uma Autoridade de Validação. Esta última é responsável pela emissão de tokens que servem como prova de validade do certificado do usuário. Com este token não é mais necessário montar e validar o caminho de certificação do usuário nem utilizar uma Autoridade de Carimbo do Tempo para produzir uma assinatura de longo prazo.
- Os autores veem na evolução da abordagem proposta a possibilidade da solução de diversos problemas do modelo atual de ICP, sem perder a funcionalidade do modelo tradicional.