Assinatura Confiável de Documentos Eletrônicos

Júlio da Silva Dias[2*], Ricardo Felipe Custódio[1] , Carlos Roberto De Rolt[2]

[1]Laboratório de Segurança em Computação – Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900 Florianópolis, SC

[2]Universidade do Estado de Santa Catarina
Av. Madre Benvenuta, 2037 – 88035-001 Florianópolis, SC

jdias@inf.ufsc.br, custodio@inf.ufsc.br, rolt@udesc.br

Abstract. *The intensive use of electronic documents are be possible if new systems that can produce trusted digital signatures were developed. Solutions to produce digital signatures in use today depends on untrustworthy operational platforms leading to untrustworthy signatures. Our main contribution is to develop a model to improve the trust in the process of producing digital signatures. It is also proposed the adoption of Document Revocation Lists (DRL) in order to simplify the document revocation process.*

Resumo. *Propõe-se um sistema para a produção confiável de assinatura digital de documentos eletrônicos, mesmo sobre plataformas computacionais inseguras. O sistema permite a auditoria das assinaturas, fornecendo evidências para garantir ou não a irretratabilidade. Propõe-se ainda a criação da lista de documentos revogados que flexibiliza o uso de documentos eletrônicos. O sistema proposto pode ser implementado sem que sejam necessárias alterações profundas nos mecanismos atualmente utilizados.*

1 Introdução

O interesse no uso de documentos eletrônicos tem se intensificado desde que passou a existir legislação imputando validade legal ao mesmo [EUA, 2000, Brasil, 2001]. Isto só foi possível a partir do desenvolvimento de técnicas que garantem ao documento eletrônico os requisitos mínimos de segurança juridicamente necessários: autenticidade, integridade, irretratabilidade e tempestividade das informações. Mecanismos como resumo criptográfico e assinatura digital garantem os requisitos de integridade e autenticidade [Stinson, 2002, Menezes, 1997]. A tempestividade é obtida através do chamado carimbo de tempo (timestamp). A entidade denominada de Protocolizadora Digital de Documentos Eletrônicos - PDDE [Pasqual, 2002] é utilizada para produzir este carimbo. Existe, no entanto, grande preocupação por parte da comunidade científica quanto ao atendimento do requisito da irretratabilidade. Num primeiro momento a irretratabilidade foi tratada como parte da autenticidade. Contudo, um documento apresentando assinatura digital não é garantia de que a mesma foi realizada com o consentimento do assinante [Balacheff et al., 2001]. Este fato é decorrente do processo indireto pelo qual uma

*Apoiado pela Universidade do Estado de Santa Catarina e CAPES.

assinatura digital é obtida. O assinante depende do uso de plataforma computacional para realização de qualquer assinatura. Com plataformas computacionais não confiáveis o processo de assinatura digital também será não confiável. Na busca de uma solução para este problema vários pesquisadores propõem a adoção de módulos de hardware seguros para agregar confiança ao processo [Balacheff et al., 2001, Balfanz and Felten, 1999].

Hoje em dia, não é recomendável tratar o assunto assinatura digital somente do ponto de vista tecnológico. É importante estudar também os aspectos sociais, culturais e legais relacionados a expressão da vontade do assinante num documento eletrônico [Berbecaru et al., 2000, Marcacini and da Costa, 2001, Rezende, 2002]. Com relação a legislação sobre o uso de assinaturas digitais verifica-se que há dois modelos de leis estabelecidos. O modelo de lei da Uncitral [Uncitral, 1999] e a diretiva da comunidade européia [Europa, 1999] que tratam de forma diferenciada a questão da inversão do ônus da prova quando da utilização de assinatura digital [Austrália et al., 2003]. No modelo de lei da Uncitral fica ao encargo do assinante provar que a assinatura não foi de sua autoria ou foi obtida de forma fraudulenta. Isso faz sentido pois a chave privada deve estar sob a guarda do assinante. Não deveria ser possível uma entidade ou pessoa obter ou utilizar a chave privada de outra entidade. A diretiva européia apresenta uma visão diferente da questão, determinando que a parte interessada deve apresentar evidências de que o assinante efetivamente realizou a assinatura. A legislação brasileira tem maiores semelhanças com o modelo Uncitral, apesar da negativa dos alguns juristas [Marcacini, 2000].

O principal objetivo deste trabalho é propor um sistema de assinatura digital seguro e confiável que permita ao assinante controlar o que efetivamente está sendo assinado bem como registrar as assinaturas realizadas. O registro permitirá ao assinante ou outra entidade interessada, verificar as assinaturas realizadas bem como o instante de tempo em que as mesmas foram efetuadas. Agrega-se desta forma maior confiança ao processo, uma vez que somente as assinaturas efetivamente verificadas e autorizadas pelo assinante serão efetivadas. Propõe-se também a adoção de uma Lista de Documentos Revogados - LDR, onde o autor poderá revogar um documento anteriormente assinado sem a necessidade de revogação de certificados digitais ou emissão de novo documento revogando o anterior. Estas proposições levam ao atendimento do requisito irretratabilidade.

A seção 2 apresenta uma revisão sobre documentos eletrônicos. A seção 3 realiza um levantamento dos principais métodos utilizados na obtenção de assinaturas digitais confiáveis. Na seção 4 é apresentada a proposta do sistema de assinaturas digitais e revogação de documentos eletrônicos. Finalmente a seção 5 apresenta as considerações finais sobre o trabalho desenvolvido.

2 Documentos Eletrônicos

Um documento eletrônico é composto por uma seqüência de bits cujo conteúdo só pode ser revelado com o auxílio de uma plataforma computacional [Scheibelhofer, 2001]. O dispositivo freqüentemente utilizado no processamento e visualização de documentos eletrônicos é o computador com terminal de vídeo. Neste, há um software específico para converter a seqüência de bits em informação a ser exibida no terminal. O conteúdo do documento será corretamente revelado se a plataforma computacional for confiável e o arquivo a ser visualizado apresentar um formato que não permita várias interpretações

por parte do software de visualização [Balacheff et al., 2001, Balfanz and Felten, 1999]

Vários pesquisadores e instituições têm proposto o desenvolvimento de plataformas computacionais seguras. A mais conhecida e discutida é a especificação da Trusted Computing Plataform Alliance (TCPA) [Alliance, 2002], que define um elemento computacional, mais especificamente um processador, capaz de:

- Gerar par de chaves assimétricas, assinar, cifrar e decifrar de dados;
- Realizar uma inicialização segura de equipamentos através do armazenamento de suas configurações em registradores seguros e a posterior comparação para efeitos de verificação;
- Participar de operações de inicialização e gerência para manutenção dos mecanismos de segurança.

A utilização de uma plataforma deste tipo permitiria a conexão segura entre os sub-sistemas da plataforma, mas poderia abrir a possibilidade do controle do sistema por parte dos fabricantes de hardware ou software, tal como somente permitir a execução de determinados tipos de software. Este aspecto que tem sido criticado e é esclarecido em vários documentos apresentados por pesquisadores. *"Procura-se através deste componente proteger os dados de possíveis ataques e não controlar os aplicativos dos usuários"*afirma David Safford da IBM [Safford, 2002]. Há também os que são contra esta iniciativa [Rezende, 2001]. Outra iniciativa que vale destacar é a da Microsoft. Esta tem desenvolvido um sistema que utiliza o conceito de uma plataforma segura buscando apresentar uma série de serviços que as aplicações poderiam utilizar na sua defesa contra código malicioso e vulnerabilidades da plataforma [Microsoft, 2003]. Apesar da polêmica, é sabido que a utilização de uma plataforma segura para execução de aplicativos tornaria o processo de assinatura e leitura de documentos eletrônicos mais confiável. A não utilização de uma plataforma segura deve ser compensada pelo desenvolvimento de outros mecanismos para o real controle da assinatura e leitura dos documentos eletrônicos, que é um dos objetivos deste trabalho.

O documento eletrônico apresenta características específicas que não estão presentes no documento tradicional em papel. No documento em papel tem-se acesso direto ao conteúdo sem auxílio de equipamentos. Os eletrônicos, por sua vez, estão armazenados na forma de um conjunto de bits em algum meio magnético ou ótico. É necessária a transformação da seqüencia de bits formatada segundo algum padrão de representação para um formato mais apropriado à compreensão humana. O documento visualizado deve ser único independente da plataforma e software utilizados nesta transformação e expressar fielmente seu conteúdo de acordo com a vontade do assinante. Há estudos que mostram que o formato de representação utilizado pode levar a problemas para obtenção desta desejável característica [Balacheff et al., 2001, Josang et al., 2002]. Este tem sido um dos problemas apontados no processo de assinatura digital dos documentos eletrônicos. O que se quer é o conceito **o que você assina é o que você vê - WYSIWYS**[1] [Scheibelhofer, 2001].

[1]What You See Is What You Sign

3 Assinatura Digital

A assinatura consiste na expressão da vontade ou do consentimento do assinante em relação ao conteúdo do documento. Deve haver, portanto, uma conexão entre o conteúdo e o assinante. No caso de uma assinatura tradicional sobre um meio físico como o papel, esta ligação é realizada através do próprio papel, que associa o conteúdo à assinatura manuscrita, e do documento de identidade, que associa a assinatura ao assinante. No caso da assinatura digital a ligação entre o conteúdo e o assinante é realizada de maneira indireta através do resumo do documento cifrado com a chave privada de posse exclusiva do assinante. O resumo do documento é conhecido como *hash* e representa de forma única o documento. Os mais conhecidos são o MD5 e o SHA-1 [Stallings, 1998]. A chave pública correspondente a chave privada é utilizada no processo de verificação da assinatura. O certificado digital emitido por uma autoridade certificadora - AC permite que se faça a ligação entre a chave pública e o assinante. Este é o princípio da autenticidade. A integridade no meio papel é garantida pela inexistência de rasuras no próprio papel. No meio digital, esta é verificada comparando-se o resumo do documento com o resumo decifrado com a chave pública do assinante. Este esquema de assinatura digital é conhecido como assinatura atemporal, conforme ilustra a figura 1. Neste esquema não há o registro do instante de tempo da realização da assinatura. Contudo, a confiança num documento assinado de forma digital deve estar ancorada em dois pontos: o primeiro é crer-se na chave pública da AC raiz da cadeia de certificação pertencente a AC que emitiu o certificado do assinante; o segundo é o instante de tempo da realização da assinatura.

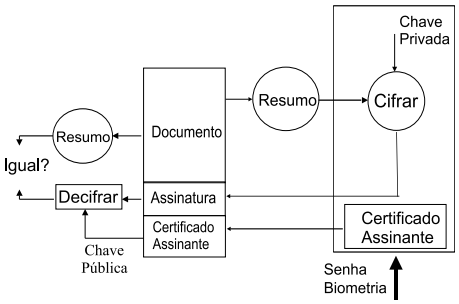

Figura 1: Assinatura Digital Atemporal.

A figura 2 apresenta o esquema de assinatura digital temporal. A hora e a data de assinatura, normalmente é estabelecida pelo assinante no momento da assinatura, considerando o horário da plataforma computacional onde o documento está sendo assinado. Este horário não é confiável, pois não pode ser verificado e poderia ser utilizado de forma maliciosa pelo assinante para realizar assinaturas retroativas no tempo. Para isso a informação temporal deve ser fornecida por uma PDDE. Neste esquema, primeiramente é enviado o resumo do documento para a PDDE. O recibo de protocolização é então anexado ao documento e um novo resumo é calculado com base no documento original adicionado do recibo de protocolização. Este novo resumo é cifrado com a chave privada do assinante, obtendo-se a assinatura digital do documento.

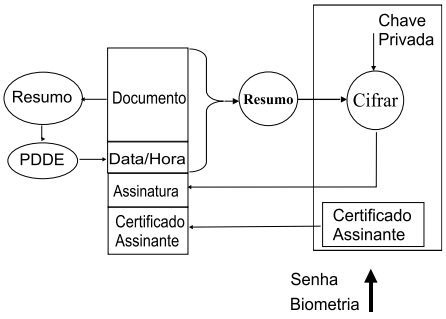

Figura 2: Assinatura Digital Temporal.

A validação da assinatura digital atemporal é realizada no momento da leitura do documento. Se a verificação da assinatura for realizada em um momento, após o certificado digital do assinante ter sido revogado ou expirado, o resultado será um documento inválido. Isto é devido a falta de informação quanto ao instante de tempo em que a assinatura foi efetivamente realizada. Este problema ocorre em várias aplicações. Para o caso da assinatura temporal a validação da assinatura é feita com base no instante de tempo inserido no recibo de protocolização.

Outro ponto que merece ser discutido é a revogação de documentos. Caso uma entidade deseje destruir um documento em papel, esta pode rasgá-lo ou destruí-lo. No caso de um documento digital a entidade pode revogar o certificado invalidando os documentos assinados se for utilizada a assinatura atemporal. No caso de assinatura digital temporal a revogação do certificado não invalida os documentos anteriormente assinados. Uma alternativa seria a emissão de um novo documento invalidando os termos do documento anterior, mas aquele ainda assim continuaria válido. Este seria um problema a ser tratado por um sistema de Gerenciamento Eletrônico de Documentos - GED. Seria interessante todavia, em muitos casos práticos, a revogação de um documento eletrônico com assinatura temporal, de forma individual, sem a necessidade de um sistema de GED.

Uma política de assinatura define um conjunto de regras que devem ser respeitadas para que as assinaturas sejam consideradas válidas. No mundo dos documentos em papel as políticas de assinatura estão muitas vezes implícitas no ambiente ou contexto onde os documentos são utilizados. Como exemplo toma-se a assinatura de um cheque onde sabe-se que este destina-se a promessa de um pagamento. No caso do documento eletrônico a situação é agravada pela separação existente entre o conteúdo e assinatura. A especificação de políticas para realização de assinaturas digitais deve ser considerada. Neste caso devem ser especificados papéis que serão obedecidos na realização de assinaturas digitais. Como exemplo, seja o caso em que, a uma chave privada, foi atribuído o papel de realizar assinaturas digitais para pagamentos com valor abaixo de R$ 50,00. Caso o assinante tente assinar um documento com valor superior a assinatura não deve ser realizada ou não terá validade.

O processo tradicional de assinatura de documentos eletrônicos apresenta inúmeros pontos de vulnerabilidade: o conteúdo a ser assinado não é visualizado de forma confiável; não existe um mecanismo que permita a auditoria sobre os documentos assinados por determinada chave privada; não existe uma política clara que estabeleça as condições para as quais a assinatura de um documento seja confiável; e a revogação de certificados não é adequada à revogação seletiva de documentos.

4 Sistema de Assinatura Segura de Documentos Eletrônicos

Propõe-se um sistema que permita a assinatura com um maior grau de confiança sem a necessidade de uma plataforma de hardware e software confiável. Este grau de confiança é conseguido através da inclusão de elementos que permitam ao assinante: visualizar o conteúdo do documento; determinar os tipos de documentos que podem ser assinados; realizar auditoria sobre os documentos; e revogar o documento sem a necessidade da revogação do certificado digital. O sistema apresenta quatro componentes básicos conforme ilustra a figura 3: o assinador, o ge-

rente de assinaturas, o registro de assinaturas e uma PDDE. O assinador consiste na estrutura necessária para que o assinante tenha acesso aos demais componentes. O gerente de assinaturas é responsável pela realização da assinatura digital, sendo portanto responsável pela chave privada. O registro de assinaturas é responsável pelos históricos sobre assinaturas que o assinante realizou ou tentou realizar. A PDDE responsabiliza-se pela âncora temporal.

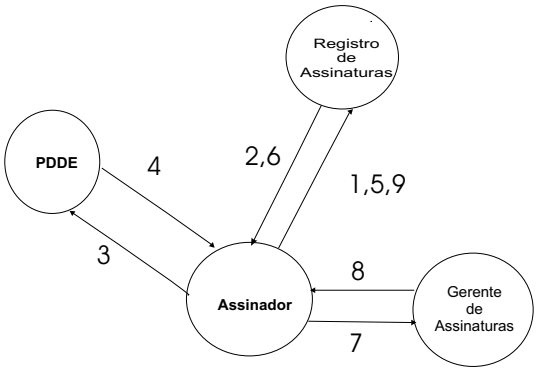

Figura 3: Sistema Proposto.

Inicialmente gera-se um par de chaves e uma política de assinatura. A política deve ser inserida no certificado do assinante na forma de uma extensão.

A assinatura é realizada seguindo as seguintes etapas:

1. O assinante submete o documento ao assinador. Este, antes de iniciar o processo de assinatura, solicita ao registro o estado atual do banco de dados de assinaturas;
2. O registro verifica a consistência dos seus dados e caso não encontre problemas, envia os dados da última assinatura realizada para o assinador;
3. O assinador verifica se os dados estão coerentes e confirma a intenção de realizar uma nova assinatura. Calcula-se o resumo do documento que se deseja assinar, concatena-se uma descrição do mesmo conforme estabelece a política de assinatura e envia-se o resumo destas para a PDDE;
4. A PDDE devolve o recibo de protocolização;
5. O resumo e o recibo de protocolação são enviados ao registro que os insere no banco de dados de assinaturas;
6. O registro retorna ao assinador uma imagem em formato convencional contendo as informações sobre o documento que está sendo assinado, além de um número que identifique a assinatura;
7. O assinante recebe a imagem, verificando se os dados são compatíveis com o documento a ser assinado, autorizando ou não a efetivação da assinatura através do envio do resumo e da imagem ao gerente de assinaturas;
8. O resumo cifrado é retornado ao assinante caso a descrição seja prevista na política estabelecida para aquela chave;
9. O registro recebe o documento assinado e verifica se a assinatura confere com o que foi solicitado.

Comparando-se a forma tradicional de assinatura digital com a presente proposta pode-se dizer que:

- A inclusão do registro de assinaturas agrega confiança ao processo, com o assinante podendo provar a realização ou não de assinaturas com a chave privada sobre seu controle;
- A confirmação utilizando uma imagem, garante que o assinante tenha controle sobre o que esta realmente sendo assinado. A imagem dificulta a fraude por parte da plataforma computacional;

- A inserção da descrição do documento permite verificar se a assinatura atende as políticas de assinatura.

A utilização de uma imagem contento informações sobre o conteúdo do documento a ser assinado garante também que o assinante não poderá refutar a assinatura por não ter tido acesso ao conteúdo do documento. Uma vez que a imagem é gerada pelo registro, não obedecendo a um padrão fixo com relação a fonte, tamanho da letra, orientação e forma de escrita, a plataforma computacional não disporia de meios para o reconhecimento do conteúdo da imagem, se quiser fraudar. O poder de processamento da plataforma computacional do sistema proposto deve ser suficiente somente para realizar as operações de assinatura, não devendo sobrar tempo para um reconhecimento de imagens.

Para a revogação dos documentos, propõe-se a criação de uma LDR aos moldes da lista de certificados revogados existentes em uma Infra-estrutura de Chaves Públicas. O usuário seria responsável por manter atualizada a sua LDR. A localização na forma de uma URI[2] da LDR é inserida no certificado digital do assinante, através do uso de uma extensão X.509v3 [ITU-T, 1997].

5 Considerações Finais

As assinaturas digitais são realizadas sobre plataformas operacionais que apresentam vulnerabilidades, o que permite questionar sua validade. A solução normalmente proposta na literatura consiste na adoção de plataformas computacionais seguras. Estas plataformas resolvem o problema mas apresentam alguns pontos fracos: tem custo elevado e não estão disponíveis em escala; e necessitam uma avaliação mais detalhada, principalmente na questão privacidade e do possível controle por parte dos fabricantes do sistema do usuário.

Foi proposto neste trabalho um sistema confiável para a assinatura digital de documentos eletrônicos sem a necessidade de uma plataforma computacional segura. O sistema faz uso de imagens que permitem ao assinante visualizar o documento eletrônico reduzindo a possibilidade da assinatura de documentos indesejados. Este mecanismo garante a irrefutabilidade do assinante que não poderá negar a assinatura por desconhecimento do conteúdo do documento. O sistema proposto possibilita ainda a auditoria por parte do assinante ou de outros interessados, fornecendo evidências que confirmem a origem e o interesse do assinante em realizar determinada assinatura.

Finalmente é proposta a utilização de uma Lista de Documentos Revogados - LDR que melhora o processo, facilitando o gerenciamento dos documentos por parte dos interessados.

Referências Bibliográficas

Alliance, T. C. P. (2002). Trusted computing plataform alliance: Main specification version 1.1b. http://www.trustedcomputing.org/tcpaasp4/specs.asp.

Austrália, A. M., Caelli, W., and Little, P. (2003). Electronic signatures - understand the past to develop the future. http://www.law.edu.au/unswlj/ecommerce/mccullagh.html.

[2]Uniform Resource Identifier

Balacheff, B., Chen, L., Plaquin, D., and Proudler, G. (2001). A trusted process to digitally sign a document. In *Proceedings of the 2001 Workshop on New Security Paradigms*, pages 79–86. ACM Press.

Balfanz, D. and Felten, E. W. (1999). Hand-held computers can be better smart cards. pages 15–24.

Berbecaru, D., Lioy, A., Maino, F., Mazzocchi, D., and Ramunno, G. (2000). Towards concrete application of electronic signatures. pages 543–561. AICA 2000 Symposium.

Brasil (2001). Medida provisória 2.200-2. Media Provisória que instituíu a ICP-Brasil.

EUA (2000). Electronic signatures in global and national commerce act. http://www.ftc.gov/os/2001/02/esignworkshopfrn.htm.

Europa, P. E. (1999). European directive on electronic signature. http://europa.eu.int/ISPO/ecommerce/legal/digital.html.

ITU-T (1997). The directory: Authentication framework. Recomendation X.509.

Josang, A., Povey, D., and Ho, A. (2002). What you see is not always what you sign. In *Proceedings of the AUUG2002*.

Marcacini, A. T. R. (2000). Documento eletrônico como meio de prova. http://augustomarcacini.cjb.net/textos/docelet2.html.

Marcacini, A. T. R. and da Costa, M. (2001). Criptografia assimétrica, assinaturas digitais e a falácia da ”neutralidade tecnológica”. http://augustomarcacini.cjb.net/textos/neutec.html.

Menezes, P. V. O. S. V. A. (1997). *HandBook of Applied Criptography*. CRC Press, Boca Raton, FL - USA, 1 edition.

Microsoft (2003). Microsoft next-generation secure computing base - technical FAQ. Relatório Técnico sobre NGSCB.

Pasqual, E. S. (2002). Idde - uma infra-estrutura para a datação de documentos eletrônicos. Master’s thesis, Curso de Pós-Graduação em Ciêncioa da Computação da Universidade Federal de Santa Catarina.

Rezende, P. (2002). Sapos piramidais nas guerras virtuais. http://www.observatoriodaimprensa.com.br/artigos/eno201120024.htm.

Rezende, P. A. D. d. (2001). Palavras mágicas sobre entidades certificadoras, assinaturas eletrônicas e projetos de lei. http://www.cbeji.com.br.

Safford, D. (2002). The need for TCPA. Technical report, IBM.

Scheibelhofer, K. (2001). Signing XML documents and the concept of ”what you see is what you sign”. Master’s thesis, Graz University of Technology.

Stallings, W. (1998). *Cryptography and Network Security*. Prentice Hall, 2 edition.

Stinson, D. R. (2002). *Cryptography - Theory and Practice*. Chapnan & Hall, 2 edition.

Uncitral, M. d. L. (1999). Uncitral model law on electronic commerce with guide to enactment. http://www.un.or.at/uncitral/texts/electcom/ml-ec.html.