Execução Segura de Assinaturas Confiáveis em Documentos Eletrônicos

Júlio da Silva Dias[1*], **Jean Everson Martina**[2]
Ricardo Felipe Custódio[2] , **Daniel Santana de Freitas**[2]

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

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

{jdias,everson,custodio,santana}@inf.ufsc.br

Abstract. *We describe a system able to produce trusted digital signatures in electronic documents even on untrustworthy computational platforms. In our system, all signatures executed by a certain platform are recorded by a trusted third party for comparison in case of dispute. Furthermore, we propose the use of auditable code execution and time restrictions over the whole signing process, thereby collecting evidences in a number that can assure an effective implementation of the security requirement of non-repudiation.*

Resumo. *Propõe-se um sistema para a produção de assinaturas digitais confiáveis em documentos eletrônicos, mesmo sobre plataformas computacionais inseguras. Isto é conseguido com o registro das assinaturas realizadas pelo sistema por uma terceira parte confiável e através de procedimentos de auditoria deste processo como um todo. Em caso de disputa, uma auditoria, com base em evidências fornecidas por uma instrumentação adequada do código utilizado, permite a verificação da corretude de sua execução por comparação formal com o que é esperado e por análise do cumprimento de restrições de tempo ao longo das diversas etapas do processo de assinatura. Com isto, acredita-se que seja possível garantir o atendimento do requisito de segurança irretratabilidade.*

1 Introdução

O uso de documentos eletrônicos apresenta vantagens sobre os documentos em papel, tais como facilidade de administração, cópia, armazenamento e transmissão através de redes de computadores. Porém, sua eficácia jurídica é condicionada a existência de legislação que regule seu uso e de técnicas que garantam um conjunto de requisitos de segurança aos mesmos [EUA, 2000, Brasil, 2001]. Os requisitos mínimos de segurança necessários são: autenticidade, integridade, irretratabilidade e tempestividade das informações. Mecanismos como resumo criptográfico e assinatura digital garantem os requisitos de integridade e autenticidade [Stallings, 2003]. A tempestividade é

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

obtida através do chamado carimbo de tempo (timestamp), o qual pode ser produzido por uma entidade denominada de Protocoladora Digital de Documentos Eletrônicos - PDDE [Pasqual, 2002]. Existe, no entanto, grande preocupação por parte da comunidade científica quanto ao atendimento do requisito da irretratabilidade. Em um primeiro momento a irretratabilidade foi tratada como parte da autenticidade. Contudo, a presença de uma assinatura digital em um documento não é garantia de que a mesma foi realizada com o consentimento do assinante [Balacheff et al., 2001]. Este fato é decorrente do modo como o documento eletrônico é representado e do processo pelo qual uma assinatura digital é obtida. O assinante depende do uso de plataforma computacional para a 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]. Um módulo de hardware seguro apresenta como características principais a inviolabilidade e a garantia da execução do código de acordo com a especificação.

Pesquisas têm sido realizadas com o objetivo de desenvolver mecanismos que garantam a execução segura de código mesmo sobre plataformas inseguras. São trabalhos que não apresentam como requisito uma plataforma segura ou um módulo de hardware seguro e têm como motivação principal a aplicação em agentes móveis. O trabalho de Blum [Blum and Kannan, 1995] busca garantir o correto funcionamento de programas verificando o resultado do processamento para determinadas entradas. A verificação é realizada por um segundo programa que executa na seqüência e verifica se o resultado do primeiro programa executado é correto para a entrada fornecida. Sanders e Tschudin [Sanders and Tschudin, 1998] propõem o uso de funções cifradas, onde uma função P é cifrada utilizando-se uma função E, gerando uma função $E(P)$ que pode ser utilizada para processar uma entrada x, gerando um resultado que pode ser decifrado obtendo-se $P(x)$. Esta abordagem está, entretanto, limitada a poucas aplicações devido a dificuldade de obtenção de funções adequadas. O trabalho de Hohl [Hohl, 1997] propõe a criação de caixas pretas que conteriam o código a ser executado, o qual não poderia ser interpretado facilmente pelo sistema devido ao seu embaralhamento. A impossibilidade de obter um código com a propriedade de caixa preta levou à criação de restrições temporais para a execução do código. A delimitação do tempo total evita que o código possa realizar outras tarefas além da prevista pelo seu criador. Hohl [Hohl, 2000], utiliza verificação de certos estados adotados como referência na validação de sua execução. Vigna [Vigna, 1997], em um trabalho sobre agentes móveis, validou a execução através de registro de eventos produzidos durante a sua execução. O agente, ao migrar, envia o estado atual assinado para que possa ser validado na sua chegada ao novo sistema onde será executado. Monrose [Monrose et al., 1999], através da instrumentação do código a ser executado, determina estados que o sistema deve atingir. Os resultados intermediários são enviados para uma entidade externa que pode validar os estados através de uma nova execução em outro sistema que seria confiável.

A proposta do presente trabalho apresenta características do trabalho de Monrose [Monrose et al., 1999] com relação à instrumentação do código no momento de compilação. O código deve apresentar a capacidade de enviar o estado da máquina local a um elemento central, responsável pela auditoria. Restrições temporais serão aplicadas, evitando que o software em execução possa realizar tarefas que possam comprometer o

resultado da operação. Quando necessário, o código pode enviar o estado da memória de vídeo para que o auditor possa comparar com o estado esperado, podendo paralisar o processamento no caso de execução com resultado fora do esperado.

Com isto, busca-se um sistema de assinatura digital de documentos eletrônicos que permita ao assinante ter acesso efetivo ao conteúdo do documento sendo manipulado. Em caso de dúvida, evidências que permitem a reconstrução do processamento realizado pela plataforma computacional sobre o arquivo de entrada podem ser utilizadas na determinação precisa do ponto em que a plataforma computacional executou operações indesejáveis.

Além de garantir o acesso ao conteúdo real do documento sendo assinado, o sistema proposto permite manter um registro de todas as assinaturas realizadas. O registro permite auditar as assinaturas realizadas, bem como o instante de tempo em que as mesmas foram efetuadas. A auditoria das assinaturas realizadas serve como complemento à auditoria do código descrita anteriormente.

Acredita-se que a utilização de técnicas que garantam a execução confiável dos programas utilizados e a correta identificação visual do conteúdo a ser assinado sejam elementos indispensáveis ao estabelecimento de confiança de um processo de realização de assinaturas digitais.

O uso de documentos eletrônicos é a principal motivação para este trabalho, e na seção 2 é apresentada uma discussão das suas principais características. Na seção 3 é realizado um levantamento dos principais métodos disponíveis atualmente para a obtenção de assinaturas digitais confiáveis. Na seção 4 é apresentado o sistema de assinaturas digitais proposto. Após a apresentação da proposta inicial é discutido na seção 5 um mecanismo de auditoria de código baseado na comparação da execução real dos processos com o que se espera de acordo com uma descrição formal do processo como um todo com base em Redes de Petri temporais. Finalmente na seção 6 os resultados obtidos são discutidos.

2 Documentos Eletrônicos

Um documento eletrônico pode ser definido como uma seqüência de bits cujo conteúdo só pode ser revelado com o auxílio de uma plataforma computacional [Scheibelhofer, 2001]. O uso de plataforma computacional é necessário para que a seqüência de bits seja convertida para um formato apropriado à visualização pelos interessados. O conteúdo será corretamente apresentado ao leitor somente se a plataforma computacional, composta por componentes de hardware e software, executar corretamente as funções necessárias [Balacheff et al., 2001, Balfanz and Felten, 1999]. A propriedade irrefutabilidade está diretamente relacionada com a capacidade do autor ou assinante do documento ter acesso ao conteúdo correto do documento. Uma vez que uma plataforma computacional desonesta pode apresentar ao assinante uma versão modificada do documento por ela armazenado, o assinante pode autorizar a assinatura com conteúdo diferente do desejado, o que compromete a propriedade de irrefutabilidade para uma plataforma sem garantias de segurança.

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. A realização desta função por uma plataforma computacional maliciosa pode levar a resultados inesperados e fraudes. A garantia de que o documento visualizado seja único, independente da plataforma utilizada nesta transformação, e de que seja a expressão fiel do conteúdo proposto pelo assinante, é um problema do processo atual de assinatura digital de documentos eletrônicos. Há estudos que mostram que o formato de representação utilizado pode levar a problemas para a 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].

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

- Gerar pares de chaves assimétricas, assinar, cifrar e decifrar dados;
- Realizar uma inicialização segura de equipamentos através do armazenamento de suas configurações em registradores seguros com a possibilidade de 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 subsistemas 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]. 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.

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 so-

[1] What You See Is What You Sign

bre um meio físico como o papel, esta ligação é realizada através do próprio papel, o qual 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 criptográfico do documento é conhecido como *hash* e representa de forma única o documento. Os mais conhecidos são o MD5 e o SHA-1 [Stallings, 2003]. A chave pública correspondente à 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. 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 a qual pertence a AC que emitiu o certificado do assinante; o segundo é o instante de tempo da realização da assinatura.

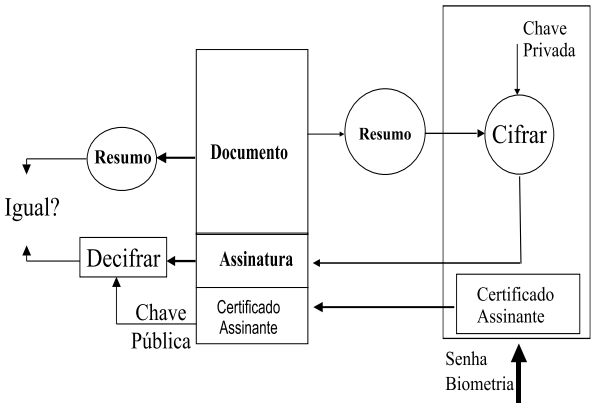

Figura 1: Assinatura Digital Atemporal.

A figura 2 apresenta o esquema de assinatura digital temporal. A hora e a data de assinatura normalmente são estabelecidas 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 evitar isso, a informação temporal deve ser fornecida por uma Protocoladora Digital de Documentos Eletrônicos - PDDE. Neste esquema, primei-

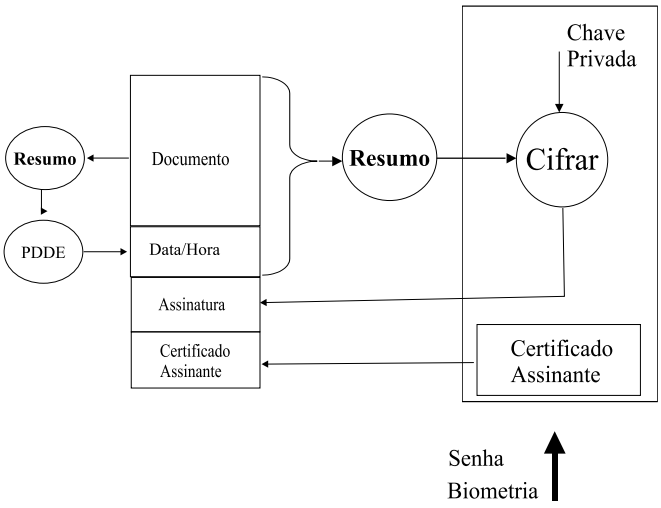

Figura 2: Assinatura Digital Temporal.

ramente é enviado o resumo do documento para a PDDE. O recibo de protocolação é então anexado ao documento e um novo resumo é calculado com base no documento original acrescido do recibo de protocolação. Este novo resumo é cifrado com a chave privada do assinante, obtendo-se a assinatura digital do documento.

A validação da assinatura digital atemporal é realizada no momento da leitura do documento. Se a verificação da assinatura for realizada após o certificado digital do assinante ter sido revogado ou expirado, o resultado será um documento inválido. Isto é devido à 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 protocolação.

Uma política de assinaturas 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 à 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 a 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. Mesmo com a utilização de módulos seguros de hardware ou plataformas computacionais seguras ainda será necessária a realização de processo de auditoria para determinar se efetivamente o sistema está realizando a tarefa para a qual foi projetado de forma eficiente seguindo as especificações estabelecidas pelo projetista.

4 Sistema de Assinatura Segura de Documentos Eletrônicos

Uma proposta preliminar de um sistema que proporciona um maior grau de confiança a uma assinatura digital sem a necessidade de uma plataforma de hardware e software confiável está descrita em [da Silva Dias et al., 2003]. Este grau de confiança seria obtido através da inclusão de elementos que permitiriam ao assinante: visualizar o conteúdo do documento; determinar os tipos de documentos que podem ser assinados; realizar auditoria sobre os documentos.

O sistema apresenta quatro componentes básicos, conforme ilustra a figura 3: o assinador, o gerente 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 manutenção da 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.

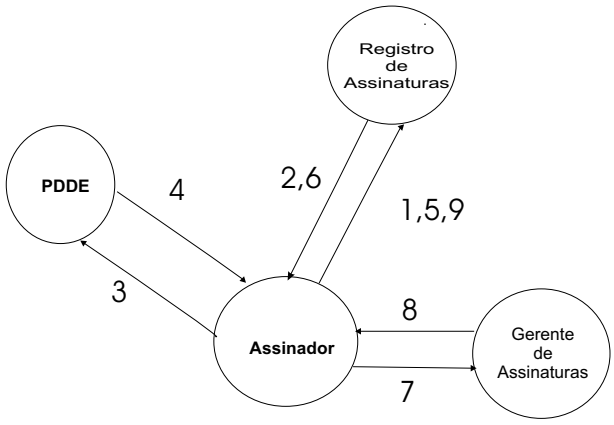

Figura 3: Sistema Proposto.

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 X.509v3 [ITU-T, 1997]. Para o armazenamento das chaves e implementação do gerente de assinaturas, foi adotado o uso de JavaCards [Bieber et al., 2000]. Além de ser um módulo de hardware seguro armazenando a chave privada do assinante de forma confiável, este tipo de cartão permite o carregamento de aplicações, facilitando o desenvolvimento e testes do sistema.

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. O assinador recebe o recibo de protocolação enviado pela PDDE;
5. O recibo de protocolação e o resumo descritivo do documento a ser assinado, são enviados ao registro que os insere no banco de dados de assinaturas;
6. O registro retorna ao assinador uma imagem em formato convencional, gif ou jpeg, 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 esta proposta, pode-se dizer que:

- A inclusão do registro de assinaturas agrega confiança ao processo, com o assinante podendo comprovar a realização ou não de assinaturas com a chave privada sob seu controle;

- A confirmação com uma imagem garante que o assinante tem controle sobre o que está realmente sendo assinado. A imagem produzida por um terceiro dificulta a fraude por parte da plataforma computacional do assinante;
- A inserção da descrição do documento permite verificar se a assinatura atende as políticas de assinatura.

A utilização de uma imagem contendo 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 gerada pelo registro não obedece a um padrão fixo com relação a fonte, tamanho de letra, orientação e forma de escrita, a plataforma computacional não disporia de meios para o reconhecimento do conteúdo da imagem, se desejar realizar qualquer fraude. Esta abordagem introduz uma restrição temporal ao processo. Para o assinador realizar alguma fraude este deve processar a imagem recebida e inserir nesta as informações incorretas. Isto não é viável, uma vez que a ausência de resposta em um curto período de tempo faz com que os demais elementos do sistema, registro de assinatura e gerente de assinatura, sejam impedidos de continuar o processo.

O registro de assinatura introduz um primeiro ponto de auditoria, através do qual o assinante pode identificar os documentos assinados ou não com sua chave privada.

5 Processo de Auditoria

A auditoria do processo de realização de assinaturas digitais apresentado anteriormente agrega maior confiabilidade ao processo tradicional. O presente trabalho busca ampliar o escopo desta auditoria, abrangendo as atividades realizadas pelos componentes distribuídos do sistema e execução do código que realiza cada atividade. Propõe-se um procedimento de auditoria que garanta a exatidão do processo de assinatura como um todo pela reconstrução de cada passo ou etapa de uma assinatura realizada. De forma semelhante à proposta de Monrose [Monrose et al., 1999] o código é instrumentado, criando-se mecanismos que enviam ao auditor informações suficientes para conferência de cada passo do processo de assinatura. A instrumentação do código dos componentes é realizada no momento da compilação, onde o programador deve identificar todas as declarações de métodos e inserir coletores para que o auditor possa obter as informações necessárias ao processo de auditoria. A mesma instrumentação pode ser adicionada em outros pontos que o desenvolvedor da aplicação

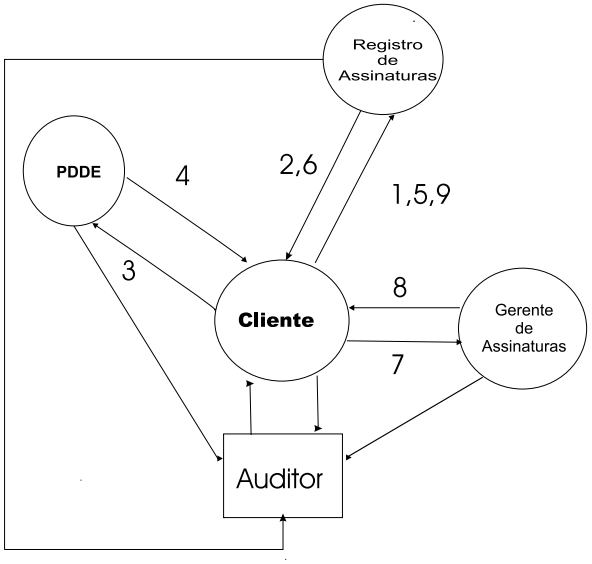

Figura 4: Sistema Proposto com Auditoria de Código Executável.

considerar necessários. No momento da invocação de qualquer método, são salvas todas as entradas necessárias à sua execução assim como as saídas, as quais serão passadas para o auditor, conforme apresentado na figura 4. O coletor é um processo em execução junto ao sistema operacional conforme apresentado na figura 5. Este processo se responsabiliza pela verificação e registro das chamadas realizadas ao sistema pelo processo em execução sendo auditado quando da sua execução. Estes dados, bem como informações temporais coletadas, devem ser suficientes para permitir ao auditor realizar uma validação formal do código executado. O auditor deve conhecer todos os métodos que cada um dos outros componentes executa, podendo, com os dados fornecidos pelos componentes e pelo sistema operacional, validar qualquer função executada pelo sistema, garantindo assim a exatidão da execução, mesmo em plataforma hostil.

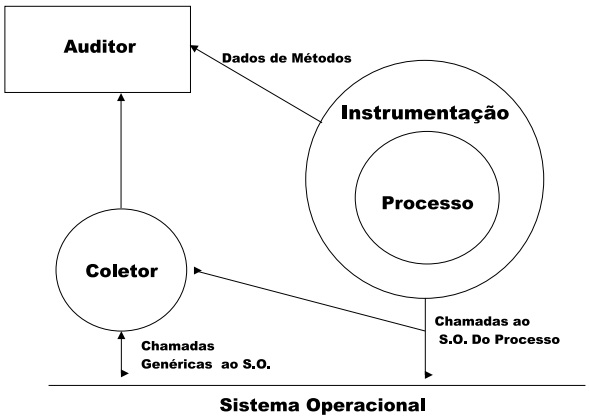

Figura 5: Instrumentação.

O auditor possuí um modelo do sistema com detalhes de todos os estados possíveis dos processos em execução. Os estados são determinados em função das chamadas de métodos realizados bem como das chamadas realizadas ao sistema operacional. O modelo ideal do sistema deve ser desenvolvido em uma etapa anterior à codificação, permitindo o desenvolvimento de código que respeite a especificação do desenvolvedor. Este modelo, por sua vez, deve ser validado para garantir as características desejadas, e posteriormente assinado pelas partes que executaram o processo de validação. Adotou-se a modelagem através de Redes de Petri Lugar/Transição [Murata, 1989, Landwehr, 2001], onde os estados que a rede pode assumir são representados pelas marcações acessíveis. A execução correta do código pode ser avaliada através da análise da seqüência de transições ocorridas para determinada situação. A necessidade de representar os eventos de forma temporal levou à utilização de Redes de Petri temporais, onde a cada transição é associado um par de datas $(\Theta_{min}, \Theta_{max})$, onde Θ_{min} e Θ_{max} especificam o tempo mínimo e máximo para que uma transição seja disparada. A modelagem utilizando Redes de Petri permite representar o processo de assinatura digital com vários graus de abstração, de acordo com o necessário. Pode-se validar um modelo com nível de detalhamento maior com uma quantidade maior de estados ou menor, simplificando a análise. O uso de Redes de Petri temporais permite modelar as restrições temporais impostas ao processo, permitindo ao auditor determinar se o tempo gasto na execução do código é o esperado, inviabilizando ataques que demandem grande esforço computacional. Na figura 6 é apresentado o modelo do sistema de assinaturas confiáveis proposto por [da Silva Dias et al., 2003] com as adaptações apresentadas na seção 4. A figura apresenta todos os estados alcançáveis, incluindo-se estados válidos e inválidos. O modelo mostrado descreve as atividades com alto nível de abstração, não entrando nos detalhes do código em execução. Observa-se na figura que todos os estados de erro ou de exceção estão previstos pelo modelo proposto

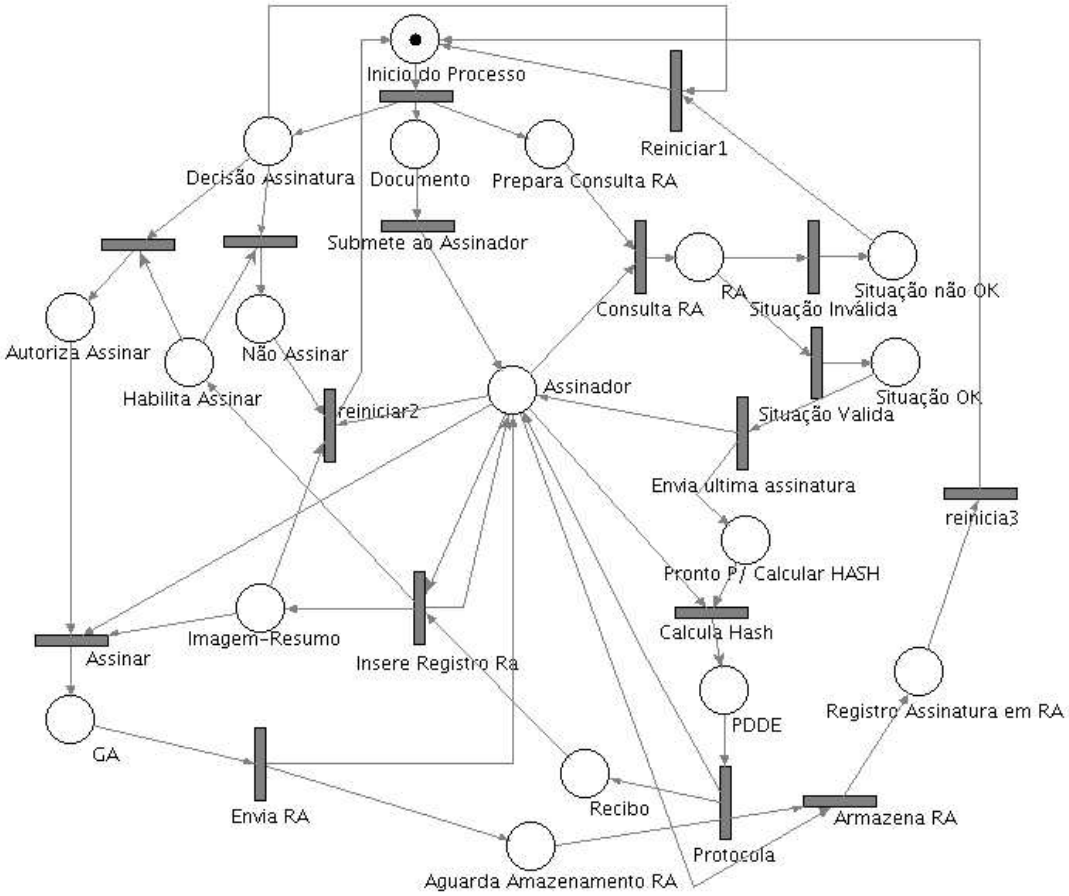

Figura 6: Rede de Petri Geral.

e são alcançáveis. A instrumentação deve ficar localizada nas transições, onde são realizadas chamadas de métodos ou chamadas ao sistema operacional. Observa-se ainda na figura 6 a presença de não-determinismos, como por exemplo no estado *Decisão Assinatura*. Neste caso devem ser fornecidas informações suficientes ao auditor para a resolução do não-determinismo. Finalmente, vale ressaltar que o modelo do código em execução pode ser realizado abrangendo qualquer parte que seja considerada crítica pelo desenvolvedor ou usuário. A inserção de informação temporal pode ser realizada em qualquer ponto, representando as restrições temporais impostas ao processo.

O auditor pode, a qualquer momento, realizar uma simulação com os dados recebidos dos processos sendo auditados. Nesta simulação da execução, os estados atingidos pelos processos devem respeitar os estados possíveis previstos no modelo desenvolvido inicialmente. Qualquer execução que leve um processo a um estado que não é previsto ou proibido vai ser identificada e relatada ao assinante, o qual, com as evidências geradas, pode determinar o elemento responsável pelo problema.

A presença do auditor atende a dois papéis significativos:

- Auditar uma execução específica de um sistema cliente e identificar possíveis fraudes nos métodos usados nos clientes;
- Validar e emitir uma assinatura no processo executado, garantindo que ele foi

completamente auditado por uma terceira parte e não apresentou comportamento anormal.

Os dados coletados durante o processo podem ser armazenados para auditoria posterior, sendo possível a validação do processo por mais de um auditor, garantindo assim maior consistência no processo de auditoria e validação de uma assinatura.

6 Considerações Finais

As assinaturas digitais são realizadas sobre plataformas computacionais que apresentam vulnerabilidades, o que pode gerar dúvida quanto a honestidade do processo de assinatura. A solução para este problema, normalmente proposta na literatura, consiste na adoção de plataformas computacionais seguras. Contudo, estas plataformas não resolvem completamente o problema e apresentam algumas desvantagens: têm custo elevado; não estão disponíveis em larga escala; e necessitam de uma avaliação mais detalhada quanto a privacidade e do possível controle do sistema do usuário por parte dos fabricantes ou outros agentes externos.

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 aumenta a garantia da irrefutabilidade do assinante o qual não poderá negar a assinatura por desconhecimento do conteúdo do documento. O sistema proposto pode ser auditado, fornecendo evidências que confirmam a origem e o interesse do assinante em realizar determinada assinatura.

No entanto, sabe-se que a validação de uma atividade baseada simplesmente na auditoria do resultado final da operação, não garante que o procedimento foi realizado da maneira esperada. É necessário que o processo de assinatura seja controlado durante a produção da assinatura. O sistema proposto estabelece este controle através da auditoria do código em execução.

Com isso, pôde-se de maneira eficiente auditar o código executável obtendo-se, a um custo menor, características de segurança semelhantes às de uma plataforma computacional segura. Uma vez que a auditoria do código é realizada em plataforma computacional externa, esta não produz uma degradação no desempenho dos componentes envolvidos: há uma sobrecarga natural devido ao acréscimo nas mensagens trocadas entre o auditor e os componentes, mas esta sobrecarga não é significativa para a infra-estrutura de redes de computadores existentes.

Finalmente, uma vez que a assinatura é realizada de forma distribuída, a possibilidade de um agente malicioso ter sucesso está diretamente relacionada à capacidade deste agente em obter colaboração de todos os elementos do processo, o que é improvável.

Referências Bibliográficas

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

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.

Bieber, P., Cazin, J., Girard, P., Lanet, J. L., Wiels, V., and Zanon, G. (2000). Checking secure interactions of smart card applets. In *ESORICS*, pages 1–16.

Blum, M. and Kannan, S. (1995). Designing programs that check their work. *Journal of Association of Computing Machinery*, 42(1):269–291.

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

da Silva Dias, J., Custódio, R. F., and de Rolt, C. R. (2003). Assinatura confiável de documentos eletrônicos. In *Wseg 2003*.

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

Hohl, F. (1997). An approach to solve malicious hosts. Technical report, Universidade de Stuttgart.

Hohl, F. (2000). A framework to protect mobile agents by using reference states. In *Proceedings of the 20th International Conference on Distributed Computing Systems (ICDCS 2000)*.

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*.

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security*, 1:3–13.

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

Monrose, F., Wyckoff, P., and Rubin, A. (1999). Distributed execution with remote audit. In *In Proceedings of the 1999 ISOC Network and Distributed System Security Symposium*, pages 103–113.

Murata, T. (1989). Petri nets: Properites, analysis and applicatons. *Proceedings of the IEEE*, 77(4).

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.

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

Sanders, T. and Tschudin, C. (1998). Toward mobile cryptography. In IEEE, editor, *IEEE Symposium on Security and Privacy*.

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. (2003). *Cryptography and Network Security*. Prentice Hall, 3 edition.

Vigna, G. (1997). Protecting mobile agents through tracing. In *In proccedings of the 3rd Workshop on Mobile Object Systems*.