UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA - DAELN
ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO
E COMUNICAÇÃO

CAIO NOGARA ANDREATTA

ANÁLISE DE SOLUÇÃO GENÉRICA PARA ASSINATURA DIGITAL DE DOCUMENTOS - estudo de caso

MONOGRAFIA

CURITIBA

2014

CAIO NOGARA ANDREATTA

ANÁLISE DE SOLUÇÃO GENÉRICA PARA ASSINATURA DIGITAL DE DOCUMENTOS - estudo de caso

Monografia apresentada ao Curso de Especialização em Gestão de Tecnologia da Informação e Comunicação do Departamento Acadêmico de Eletrônica - DAELN da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de Especialista.

Orientador: Prof. M.Sc. Christian Carlos Souza Mendes

CURITIBA

2014

AGRADECIMENTOS

Primeiramente gostaria de agradecer aos meus familiares. Minha namorada Hannah, por ter lido e relido meus textos, mesmo sendo assunto tão diferente do de sua área profissional. Minha irmã Giuliana, por ter dado sugestões de construção do trabalho e por ter me incentivado jogando video-game enquanto eu quase desistia e ia jogar junto. Minha mãe Márcia, pelos muitos finais de semana em que não pude visitá-la para poder aproveitar o longo período de concentração que estes intervalos do meu trabalho permitiam. Meu pai Mario, por ter respeitado meus horários de estudo e me incentivado a terminar o curso.

Gostaria de agradecer aos meu professores GETIC, com quem pude aprender e aperfeiçoar meus conhecimentos durante estes quase dois anos, além de poder ter aprendido com suas experiência profissionais e de vida. Em especial, ao coordenador Alexandre Miziara, por sua dedicação e prontidão em todas as vezes que foi solicitado; ao secretário de curso Reneudo, pela disposição em ajudar e de responder a todos os e-mails da turma; e ao meu coordenador Christian Mendes, pela disposição em conversar e aceitar meu trabalho e pela paciência na orientação.

Gostaria de agradecer aos meus colegas por esta jornada de aprendizado por que passamos juntos e por todas as experiências trocadas durante o curso. Em especial, gostaria de agradecer aos amigos Gastão e Johannes pela força nas horas difíceis e pela parceria nos trabalhos, sempre proveitosas e produtivas.

Gostaria, ainda, de agradecer ao meu colega de trabalho Dáltoni, pela sugestão de tema para a monografia que, apesar de estar bem na minha frente, não me era tão evidente naquele momento de dúvidas. Aos meus diretores Luciano, Omar e João Miranda por me autorizarem a divulgar informações privativas de nossa Secretaria, confiando no trabalho que seria feito.

RESUMO

ANDREATTA, Caio N.. ANÁLISE DE SOLUÇÃO GENÉRICA PARA ASSINATURA DIGITAL DE DOCUMENTOS - estudo de caso. 71 f. Monografia – Especialização em Gestão de Tecnologia da Informação e Comunicação, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

A utilização da assinatura digital vem ganhando bastante espaço desde sua regulamentação no ano de 2001, em que foram instituídos órgãos reguladores, fiscalizadores e executores das políticas estabelecidas. Vários órgãos do governo, a fim de acompanhar o desenvolvimento tecnológico e proporcionar ao público serviços eficientes e seguros, iniciaram o desenvolvimento de projetos de assinatura digital. É o caso do projeto em análise neste Estudo de Caso, que foi desenvolvido no Tribunal Regional do Trabalho da 9ª Região - Paraná, para suprir uma solicitação realizada pela Corregedoria deste mesmo órgão. A solução foi desenvolvida para ser implantada no sistema de Atas de Correição foi planejada para ser posteriormente adotada por outros sistemas do próprio órgão, como medida de segurança, tanto para o próprio Tribunal quanto para o público.

O objetivo deste Estudo é apresentar como foi desenvolvida a solução, quais os recursos que foram necessários e quais as dificuldades e problemas encontrados, proporcionando uma visão concreta daquilo que várias teorias e bibliografias reconhecidas de Segurança da Informação apresentam.

A metodologia adotada baseou-se no levantamento da bibliografia atual acerca do tema assinatura digital, de legislações de outros países que já estabeleceram infraestruturas para o uso de certificados digitais; bem como baseou-se na análise da documentação de projeto que foi elaborada durante o desenvolvimento, armazenada em um repositório próprio do órgão. Os documentos utilizados foram o próprio código-fonte desenvolvido, *Status Reports*, Casos de Uso e Casos de Teste, Plano Integrado de Projeto, entre outros.

Como resultados, observou-se algumas debilidades no sistema desenvolvido que podem levantar questionamentos acerta da legitimidade da solução, como é o caso de formatos de arquivo HTML e PDF que utilizam referências externas ao documento assinado. Foi identificada uma responsabilidade desnecessária, assumida pela solução, que é a conversão entre formatos de arquivos. Outras melhorias foram identificadas e sugeridas.

Além de trazer ao meio acadêmico os resultados concretos que tais teorias permitiram, este Estudo pretende apresentar a experiência de projeto adquirida para que interessados tenham um ponto de partida, podendo adotar as inovações trazidas pela solução, assim como preparar-se antecipadamente para problemas semelhantes.

Palavras-chave: assinatura digital, projeto órgão público, solução genérica

ABSTRACT

ANDREATTA, Caio N.. ANALYSIS OF A GENERIC SOLUTION FOR DIGITAL SIGNATURE - case study. 71 f. Monografia – Especialização em Gestão de Tecnologia da Informação e Comunicação, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Digital signature has gained space since its regulation in 2001, when it instituted regulatory, supervisory and executing agencies of the established policies. Many government agencies, in order to keep up with the technological development and to provide eficient and safe services to the public, started projects to implement digital signature. This Case Study analyzes one of these implementations, developed in Tribunal Regional do Trabalho da 9ª Região - Paraná, built to answer the request made by the Corregedoria of the same agency. The developed solution was firstly built to be adopted by the Atas de Correição system, but was also planed to be adopted by other systems, as a security measure for both the Tribunal and the public.

The objective is to present the developed solution, what resources were needed and what dificulties and problems were found, providing a concrete vision of what are present among many Security Information theories and known bibliographies.

The methodology adopted relied on the currently known bibliography about digital signature, legislation in other countries that already set the digital certificate infrastructure, as well as on the analysis of project documents that were made during the development and stored in the agency repository. The documents used in the analysis are the source code, Status Reports, Use Cases and Test Cases, Integrated Project Plan, and others.

As result, there was some weaknesses on the built system that might raise questions about its legitimacy, as stated on the use of HTML and PDF file formats using external references. One unnecessary responsibility assumed by the system was identified, that is the file format conversion. There were some improvements identified and suggested.

In additionto bringing to the academia concrete results that such theories allowed, this study aims to present the experience gained from the project so that interested parties may have a starting point, and may adopt the innovations brought by the solution, as well as prepare in advance for similar problems.

Keywords: digital signature, public agency project, generic solution

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AC	Autoridade Certificadora
ACT	Autoridade Certificadora do Tempo
AR	Autoridade de Registro
CAS	*Central Authentication Service*
CNJ	Conselho Nacional de Justiça
CRC	*Cyclic Redundancy Check*
CRL	*Certificate Revocation List*
CSJT	Conselho Superior da Justiça do Trabalho
CTA	Controle de Tramitação Administrativa
DTO	*Data Transfer Objects*
FDA	*Food and Drugs Administration*
FK	*Foreign key*
HMAC	*Hash-based Message Authentication Code*
ICP	Infraestrutura de Chaves Públicas
ISO	*International Organization for Standardization*
ITI	Instituto Nacional de Tecnologia da Informação
ITU-T	*International Telecommunication Union - Telecommunications*
JAR	*Java Archive*
JVM	*Java Virtual Machine*
LCR	Lista de Certificados Revogados
MAC	*Message Authentication Code*
MIME	*Multipurpose Internet Mail Extension*
MP	Medida Provisória
OAB	Ordem dos Advogados do Brasil
PDDE	Protocoladora Digital de Documentos Eletrônicos
PIP	Plano Integrado de Projeto
PJe	Processo Judicial Eletrônico
PKCS	*Private-Key Cryptography Standards*
PK	*Primary Key*
PKI	*Public Key Infrastructure*
SDSTI	Secretaria de Desenvolvimento de Soluções em Tecnologia da Informação
TRT4	Tribunal Regional do Trabalho da 4ª Região - Rio Grande do Sul
TRT9	Tribunal Regional do Trabalho da 9ª Região - Paraná
TST	Tribunal Superior do Trabalho
TTP	*Trusted Third Party*
XML	*Extensible Markup Language*

SUMÁRIO

1 INTRODUÇÃO

Após a regulamentação da Assinatura Digital no Brasil em 2001, o desenvolvimento de soluções ou adaptações desta funcionalidade ganhou espaço no governo, principalmente pelo compromisso do Estado com os princípios da celeridade, acessibilidade, economia, sustentabilidade e eficiência alinhados ao interesse público.

No Poder Judiciário, uma iniciativa realizada pelo Conselho Nacional de Justiça (CNJ), em pareceria com os Tribunais e a Ordem dos Advogados do Brasil (OAB), conduziu o desenvolvimento do Processo Judicial eletrônico (PJe), com o principal objetivo de automatizar a prática de atos processuais, permitindo o acompanhamento de processos independentemente do âmbito jurisdicional do mesmo (JUSTIçA, 2014b). O lançamento oficial do projeto foi realizado no dia 21 de junho de 2011, sendo adotado por diversos Tribunais em todo o país.

A Justiça do Trabalho, em particular, foi completamente envolvida no projeto a partir do Termo de Acordo de Cooperação Técnica nº 51/2010 entre o CNJ, o Tribunal Superior do Trabalho (TST) e o Conselho Superior da Justiça do Trabalho (CSJT), aderindo ao PJe; e a partir do Acordo de Cooperação Técnica nº 01/2010, assinado pelo TST, pelo CSJT e por todos os 24 Tribunais Regionais do Trabalho (TRABALHO, 2014). Desta forma, toda a Justiça do Trabalho, diferentemente da Justiça Federal e da Eleitoral (cuja implantação está sendo gradual), iniciou a implantação do PJe-JT, um sistema derivado e dependente do PJe que o adequou às peculiaridades da justiça trabalhista.

Por se tratarem de sistemas que lidam com documentos envolvidos em processos judiciais, a confiabilidade de todos os processos resta na capacidade de se garantir a autoria de cada documento, tramitação, entre outros, como é evidenciado no trecho a seguir, extraído de informativo divulgado pelo CNJ (JUSTIçA, 2014a).

> A tramitação de processos judicias por meio do Processo Judicial Eletrônico (PJe) exige a certificação digital de advogados, magistrados e servidores de Tribunais. O mecanismo garante proteção a dados confidenciais fornecidos em ações judiciais e aos atos realizados no âmbito do Poder Judiciário e evita fraudes possíveis de serem cometidas com a violação de informações confiadas ao Judiciário para a resolução de

litígios. (JUSTIçA, 2014a)

Concomitantemente ao desenvolvimento de soluções para os sistemas judiciais, as áreas administrativas de cada Órgão viram a possibilidade de aproveitar a Assinatura Digital como mecanismo de segurança para seus documentos. Tendo em vista que o desenvolvimento do PJe foi centralizado, os Órgãos que tiveram interesse iniciaram, individualmente, o desenvolvimento de uma solução para Assinatura Digital no âmbito administrativo.

O presente Estudo de Caso analisa a solução desenvolvida no Tribunal Regional do Trabalho da 9ª Região - Paraná (TRT9) pela Secretaria de Desenvolvimento de Soluções em Tecnologia da Informação (SDSTI) solicitada pela Corregedoria deste mesmo Órgão. O projeto desenvolvido teve por objetivo atender à solicitação, mas também preparar uma solução genérica o suficiente para que fosse possível reutilizá-la em outros sistemas administrativos futuramente.

A análise se faz necessária, pois relatar as dificuldades encontradas no projeto pode favorecer futuras implementações, evitando certas decisões ou adotando as que se mostraram bem sucedidas.

Como justificativa para este estudo de caso, pode-se citar o compartilhamento da solução desenvolvida para que outros interessados (até mesmo outros Órgãos de mesma ou diferente esfera) possam tomá-la como ponto de partida; aproveitarem-se dos aprimoramentos implantados; ou, ainda, aprimorar as funcionalidades construídas. Tendo em vista a pouca divulgação de estudos semelhantes nos meios acadêmicos, incentivar o compartilhamento de experiências.

Uma segunda justificativa é a extensão da documentação acerca do projeto desenvolvido, para que futuros interessados (deste mesmo Órgão ou de outros) possam entender a solução desenvolvida sem que para isso precisem analisar todo o código fonte (como por exemplo, analistas de negócio, analistas de arquitetura, entre outros).

Como terceira justificativa, o presente estudo de caso busca realizar uma análise crítica na perspectiva de decisões de projeto, quais favoreceram e quais dificultaram adaptações posteriores, para que outras implementações possam economizar tempo de análise tomando como subsídio uma implementação já realizada.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

- Apresentar a documentação de projeto, a arquitetura do sistema, os resultados e as dificuldades encontradas no desenvolvimento de software específico para assinatura digital de documentos em um órgão público.

1.1.2 OBJETIVOS ESPECÍFICOS

- apresentar os requisitos levantados e as restrições do projeto;
- apresentar a arquitetura projetada;
- apresentar as funcionalidades desenvolvidas;
- apresentar as dificuldades conceituais de segurança da informação do projeto;
- realizar um levantamento de melhorias para implementações futuras.

2 FUNDAMENTAÇÃO TEÓRICA

> "A digital signature is a hash value that has been encrypted with de sender's private key." (HARRIS, 2005)

Esta é a definição de Assinatura Digital dada por Shon Harris em seu livro e guia de estudos (HARRIS, 2005) para a certificação CISSP, bastante conhecida pelos profissionais de Segurança da Informação de todo o mundo.

A versão em português poderia ser dada da seguinte forma: uma assinatura digital é um valor *hash* que foi criptografado com a chave privada do remetente.

Para aqueles que desconhecem os assuntos a que várias das palavras utilizadas nesta definição se referem, é difícil entender. Mas isso é perfeitamente aceitável para qualquer que fosse o assunto ou área profissional em análise.

Já para aqueles que conhecem, pelo menos em parte os conteúdos, esta definição é análoga a se dizer que "celular é um aparelho móvel utilizado para realizar ligações telefônicas, enviar mensagens e entrar na internet", ou seja, praticamente cada palavra representa uma gama de conhecimentos que podem passar despercebidos sem a devida atenção.

Esta definição pode ser prematuramente reconhecida como simplista, ou até mesmo incompleta. No entanto, as principais ideias por trás da Assinatura Digital foram conectadas e apresentadas.

Este capítulo busca trazer a foco muitas dessas "principais ideias", clarificá-las e fornecê-las como subsídio para a análise crítica que será realizada sobre o projeto deste Estudo de Caso.

2.1 ANÁLISE PRELIMINAR

Analisando-se os elementos presentes na definição dada no início deste capítulo, as seguintes explicitações se fazem pertinentes.

Primeiramente, pode-se observar que existe um remetente, o que implica em uma comunicação e necessariamente em um ou mais destinatários.

O remetente, de sua parte, deseja garantir que sua mensagem se mantenha íntegra, inalterada, até seu recebimento pelos destinatários. Para tanto, a mensagem é submetida a um algoritmo *hash*, cujo resultado, chamado na definição de valor *hash*, é criptografado e finalmente anexado à mensagem.

Infere-se, também, que a criptografia utilizada é do tipo assimétrica (que possui uma chave pública e outra privada) e que seu emprego tem o objetivo de garantir a autoria da mensagem e não a confidencialidade dela, uma vez que a chave utilizada foi a privada.

Os destinatários, por outro lado, desejam ter certeza tanto da integridade quanto da autoria da mensagem, bem como a garantia de que nenhum mal intencionado tenha tentado enviar uma mensagem em nome de outra pessoa. Desta forma, a chave pública do remetente é necessária para que os destinatários verifiquem a integridade e a autoria da mensagem, assim como é necessário um sistema que garanta chaves privadas únicas e secretas.

Nesta estrutura aparentemente simples, surgem diversas necessidades, inclusive de padronização, a fim de garantir que remetentes e destinatários dialoguem baseando-se no mesmo idioma.

Surge neste cenário uma entidade chamada de terceiro confiável, que é um elemento externo à comunicação em que ambas as partes confiam e consultam. Este terceiro confiável é responsável por, entre outras atribuições, criar certificados que garantam a identidade dos usuários; garantir que a criação das chaves pública e privada sejam realizadas pelos próprios usuários; divulgar o certificado (contendo a chave pública e informações verdadeiras de seu respectivo proprietário) para toda a comunidade; e informar para a comunidade todas as chaves sob seus cuidados que foram revogadas, ou seja, que não devem ser consideradas válidas.

Todo este sistema, por garantir que as chaves privadas, únicas e secretas, estão associadas a uma identidade única e válida, permite que a autoria seja irrefutável, ou seja, o autor da mensagem não pode negar sua autoria. O não-repúdio, desta forma, confere validade jurídica à assinatura digital, tendo o mesmo valor jurídico que a assinatura física, à caneta.

Nas últimas décadas, vários países estabeleceram diretrizes, normas e leis a fim de regulamentar a utilização de assinatura em meio eletrônico, sua validade jurídica e efeitos legais decorrentes, bem como os requisitos e elementos necessários para sua implementação e utilização.

Das finalidades mais diversas para esta ferramenta, pode-se incluir o envio de corres-

pondências por meio digital, envio de documentos oficiais, intimações e até mesmo processos judiciais completos, decisões e acórdãos.

De maneira mais ampla, os benefícios da assinatura em meio eletrônico incluem a celeridade no trâmite de documentos, o ganho de produtividade, a economia de material e a segurança.

Na lei canadense relacionada à privacidade de dados, o conceito de Assinatura Eletrônica é definido no *Personal Information Protection and Eletronic Documents Act*, transcrito a seguir.

> ""electronic signature" means a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document." (CANADA, 2000)

Além disso, a mesma lei define o que vem a ser Assinatura Eletrônica Segura, aquilo que efetivamente possui valor legal, e seus requisitos de implementação, cuja transcrição encontra-se abaixo.

> - (a) the electronic signature resulting from the use by a person of the technology or process is unique to the person;
> - (b) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;
> - (c) the technology or process can be used to identify the person using the technology or process; and
> - (d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document. (CANADA, 2000)

Na legislação estadounidense existem definições em diferentes leis, como na seção 106 da *Eletronic Signatures in Global and National Commerce Act*, lei que facilitou o uso de registros e assinaturas eletrônicas no comércio nacional ou internacional. A definição encontra-se transcrita abaixo.

> " Electronic signature.–The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." (GOVERNMENT, 2000)

Outra lei estadounidense que define Assinatura Eletrônica é o *Government Paperwork Elimination Act*, cujo objetivo é a substituição do uso de papel por formatos eletrônicos, exigindo que as agências federais, quando factível, utilizem formulários e assinaturas em meio eletrônico.

> "Electronic signature.–The term "electronic signature" means a method of signing an electronic message that–
>
> - (A) identifies and authenticates a particular person as the source of the electronic message; and
> - (B) indicates such person's approval of the information contained in the electronic message.
>
> (GOVERNMENT, 1999)

No *Code of Federal Regulations*, em seu Título 21 (Title 21 - *Food and Drugs*), a agência nacional estadounidense *Food and Drugs Administration* - FDA, define tanto Assinatura Eletrônica, quanto Assinatura Digital.

> "Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." (GOVERNMENT, 2011)
>
> "Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified." (GOVERNMENT, 2011)

Estas definições, como pode-se evidenciar, convergem para um significado único, bem esclarecido no documento "Visão Geral Sobre Assinaturas Digitais na ICP-Brasil" (ITI, 2012), do Instituto Nacional de Tecnologia da Informação - ITI. Assinatura Eletrônica, de modo geral:

> "representa um conjunto de dados, no formato eletrônico, que é anexado ou logicamente associado a um outro conjunto de dados, também no formato eletrônico, para conferir-lhe autenticidade ou autoria." (ITI, 2012)

Embora haja semelhança, é equívoca a substituição de Assinatura Eletrônica por Assinatura Digital. Como já evidenciado anteriormente na legislação estrangeira, a exemplo da canadense e da estadounidense, Assinatura Digital é espécie do gênero Assinatura Eletrônica, pois diz respeito a um subconjunto da Assinatura Eletrônica em particular, qual seja, aquela que envolve um par de chaves criptográficas associado a um certificado digital.

2.1.1 PROPRIEDADES DE SEGURANÇA

Na Segurança da Informação existem diversas propriedades ou atributos que sintetizam objetivos que determinada aplicação deseja alcançar, desde os fundamentais, confidencialidade, integridade e disponibilidade, até outros tão importantes quanto, como autenticidade, não-repúdio, auditabilidade.

Tratando-se de Assinatura Digital, as principais propriedades de segurança necessárias à confiabilidade de toda a infraestrutura envolvida são: integridade, autenticidade, não-repúdio e, em determinados casos, confidencialidade (NIST, 2001) (COMMERCE, 2013) (HARRIS, 2005) (STALLINGS, 2010).

A integridade diz respeito à garantia de que a mensagem original não foi alterada após sua assinatura digital. Desta forma, os destinatários podem, sempre que necessário, verificar se a mensagem recebida é exatamente igual à original (NIST, 2001).

A autenticidade é a garantia de autoria, ou seja, é a propriedade que permite aos destinatários terem certeza do autor daquele documento (NIST, 2001) (STALLINGS, 2010) (HARRIS, 2005).

A terceira propriedade, o não-repúdio, está diretamente relacionada à autenticidade, pois na medida em que se pode garantir que somente uma identidade está relacionada à uma chave privada, não há como o autor negar a autoria de determinado documento cuja assinatura digital esteja relacionada à sua chave pública (NIST, 2001) (STALLINGS, 2010) (HARRIS, 2005) (COMMERCE, 2013).

A última propriedade, a confidencialidade, garante que a mensagem se manterá restrita, exceto apenas para os destinatários de interesse. Isto quer dizer que somente os destinatários de interesse poderão visualizar a mensagem original, os demais não terão acesso (NIST, 2001), (HARRIS, 2005).

2.2 MECANISMOS DE SEGURANÇA

Mecanismos de segurança são algoritmos que foram projetados para fornecer ao usuário algumas ou várias das propriedades de segurança, de acordo com a necessidade de cada aplicação.

2.2.1 MECANISMOS NÃO-CRIPTOGRÁFICOS

Existem diversos mecanismos que fornecem propriedades de segurança sem a utilização de algoritmos criptográficos. Entre eles, tem-se:

Bits de paridade: são bits adicionais à mensagem transmitida cuja finalidade é assegurar que o número de 0s (ou 1s) da mensagem é par. Apesar de ser um mecanismo bastante simples, que não protege a mensagem de alguém mal intencionado, ou de erros acidentais múltiplos, ele visa garantir a integridade da mensagem em canais ruidosos (NIST, 2001).

Verificação de redundância cíclica (*Cyclic Redundancy Check* - CRC): Semelhante aos bits de paridade, os CRCs possuem tamanho fixo e são calculados sobre toda a mensagem. Desta forma, o destinatário pode efetuar o mesmo cálculo sobre a mensagem e comparar os CRCs para verificar a integridade. Assim como os bits de paridade, os CRCs visam garantir a integridade da mensagem, sem se preocuparem com modificações intencionais (NIST, 2001) (STALLINGS, 2010).

Assinatura digitalizada: é a digitalização de uma assinatura manuscrita. Ela não garante nenhuma propriedade de segurança, uma vez que ela pode ser inserida em qualquer documento por qualquer pessoa, sem o consentimento do proprietário.

PINs e senhas: número de identificação pessoal (Personal Identification Number - PIN) e senhas visam garantir a autenticidade, ou seja, assegurar que determinado acesso é autêntico. Apesar disso, estes mecanismos não permitem o não-repúdio, uma vez que mais de uma pessoa pode saber o PIN ou a senha (STALLINGS, 2010).

Biometria: é a análise de determinado atributo físico ou comportamento com a finalidade de se identificar o indivíduo. Por exemplo, análise de digitais, íris, entre outros. Dentre os problemas deste mecanismo estão os falsos positivos, falsos negativos, aceitação dos usuários, custo e conveniência (STALLINGS, 2010).

A Tabela 1 apresenta quais propriedades são alcançadas pelos mecanismos acima descritos. Pode-se notar a fragilidade intrínseca a cada uma (que pode ser completamente aceitável, dependendo da aplicação), uma vez que, não fornecendo algumas das propriedades, uma identidade pode ser forjada ou a autoria pode ser questionada e até mesmo negada.

A Assinatura Digital em geral, por requerer garantias de confidencialidade e não-repúdio, exige a utilização de mecanismos criptográficos (NIST, 2001).

Tabela 1: Mecanismos não criptográficos e propriedades de segurança alcançáveis.

Mecanismo	Integridade	Confidencialidade	Autenticidade	Não-repúdio
Bits de paridade	Sim	Não	Não	Não
CRC	Sim	Não	Não	Não
Assinatura Digitalizada	Não	Não	Não	Não
PIN e senha	Não	Não	Sim	Não
Biometria	Não	Não	Sim	Não

Adaptado de (NIST, 2001)

2.2.2 MECANISMOS CRIPTOGRÁFICOS

A Criptografia é um campo da matemática que estuda a transformação de dados (ou codificação e decodificação) com a finalidade de fornecer alguma ou várias das propriedades de segurança mencionadas. Ela é um método de armazenamento e transmissão de dados de forma que apenas os destinatários de interesse possam ler e processar os dados. É considerada, também, uma forma eficaz de proteger informações confidenciais, pois elas são armazenadas em mídias ou transmitidas em redes não confiáveis (HARRIS, 2005).

Estes mecanismos baseiam-se na utilização de chaves, que nada mais são do que sequências de bits. Eles podem ser divididos em algoritmos simétricos e assimétricos.

2.2.2.1 ALGORITMOS SIMÉTRICOS

Os algoritmos simétricos utilizam apenas uma chave. Por esta razão, ela é conhecida como chave secreta, pois é utilizada tanto para codificar quanto para decodificar mensagens.

Apesar de garantir confidencialidade, algoritmos simétricos não garantem autenticidade e não-repúdio, uma vez que a senha deve ser compartilhada entre as pessoas ou entidades de interesse para que haja troca de mensagens criptografadas (HARRIS, 2005) (STALLINGS, 2010).

A Figura 1 mostra como é estabelecida a comunicação entre as partes. Uma das partes, de posse da chave, criptografa a mensagem e envia o resultado para os destinatários de interesse. Ao receber, cada um deve utilizar a mesma chave (utilizada para codificar) para decodificar e ler a mensagem original. Pode-se notar que um dos destinatários não possui a chave de criptografia e, desta forma, nada poderá fazer com a mensagem, pois não conseguirá saber o conteúdo original.

Além de serem utilizados para garantir a confidencialidade de dados, algoritmos simétricos podem ser utilizados para autenticar a integridade e a origem de dados. Para tanto, o

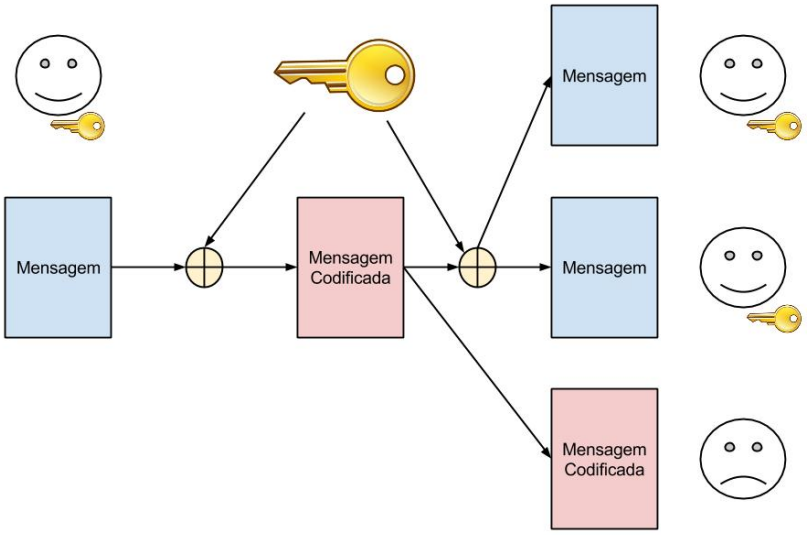


Figura 1: Comunicação utilizando algoritmo simétrico de criptografia.
Fonte: Autoria própria.

remetente usa a chave para criptografar a mensagem e, ao invés de enviar a mensagem codificada, envia a mensagem original e parte da mensagem codificada, como pode ser visto na Figura 2. Esta parte é chamada de código de autenticação de mensagem (*Message Authentication Code* - MAC).

O envio de parte da mensagem codificada cumpre dois objetivos principais. O primeiro, é evitar que algum intruso consiga descobrir a chave secreta a partir das mensagens original e codificada. O segundo, é economizar o volume de dados transferidos, pois, caso houvesse o envio completo da mensagem codificada, em todas as vezes o dobro de dados seria enviado (STALLINGS, 2010) (HARRIS, 2005). Além disso, o objetivo nesta utilização é garantir a integridade e não a confidencialidade, caso em que apenas a mensagem codificada seria enviada, como já exposto.

O destinatário quando receber a mensagem poderá verificar se houve alguma alteração realizando a codificação da mensagem recebida e comparando o trecho correspondente com o MAC recebido. Além disso, o destinatário tem a garantia que a mensagem é originada de determinado remetente, pois somente eles conhecem a chave secreta. Embora haja esta garantia, o não-repúdio não é alcançado, pois o remetente pode negar ser o autor, atribuindo a autoria à outra parte que também conhece a chave secreta.

É de se notar, ainda que aparentemente destoantes, que os atributos podem ser utili-

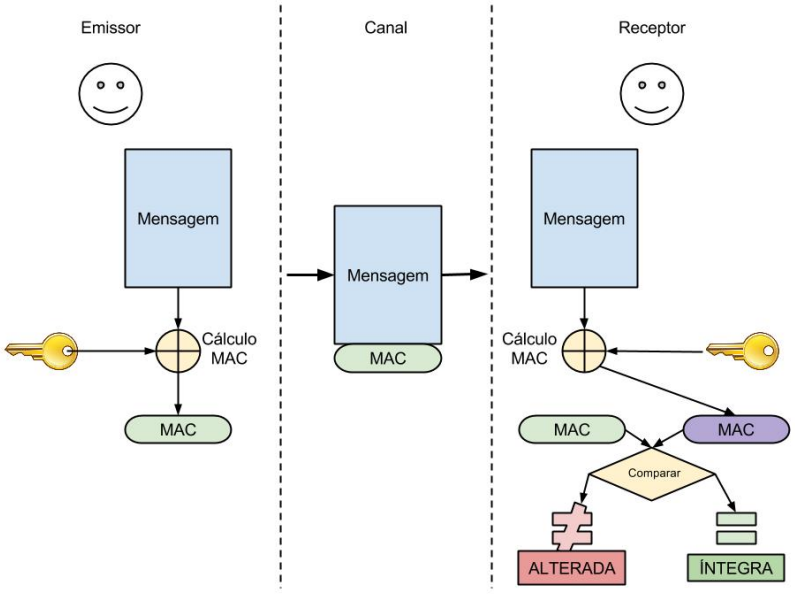


Figura 2: Algoritmo simétrico utilizado para garantir integridade e origem de dados.
Fonte: Autoria própria.

zados em conjunto, ou seja, pode-se alcançar tanto a confidencialidade quanto a garantia de integridade e autoria. Basta que a mensagem seja primeiramente codificada e que o MAC seja calculado sobre o resultado da codificação, como pode ser observado na Figura 3.

Uma das dificuldades na utilização de algoritmos simétricos é o gerenciamento das chaves. Como ambas as partes precisam conhecer a chave secreta, é necessária uma maneira segura de compartilhá-la. Outra questão envolvida neste gerenciamento é a quantidade de chaves utilizadas, dependendo do tamanho da comunidade, cada pessoa ou entidade precisa manter uma chave para cada comunicação estabelecida, o que pode tornar-se uma tarefa pouco prática (HARRIS, 2005) (NIST, 2001) (STALLINGS, 2010).

Neste cenário, o terceiro confiável (*Trusted Third Party* - TTP) pode surgir como solução para este gerenciamento de chaves. Como ambas as partes confiam neste TTP, a princípio, basta que cada pessoa ou entidade saiba a chave secreta do TTP, utilizando-a para estabelecer a comunicação com ele e, assim, obter as chaves secretas de destinatários de interesse, apenas quando for conveniente.

2.2.2.2 FUNÇÕES *HASH*

As funções de embaralhamento, funções de resumo criptográfico, ou Funções *Hash*, são algoritmos criptográficos cuja finalidade é calcular uma impressão digital dos dados de

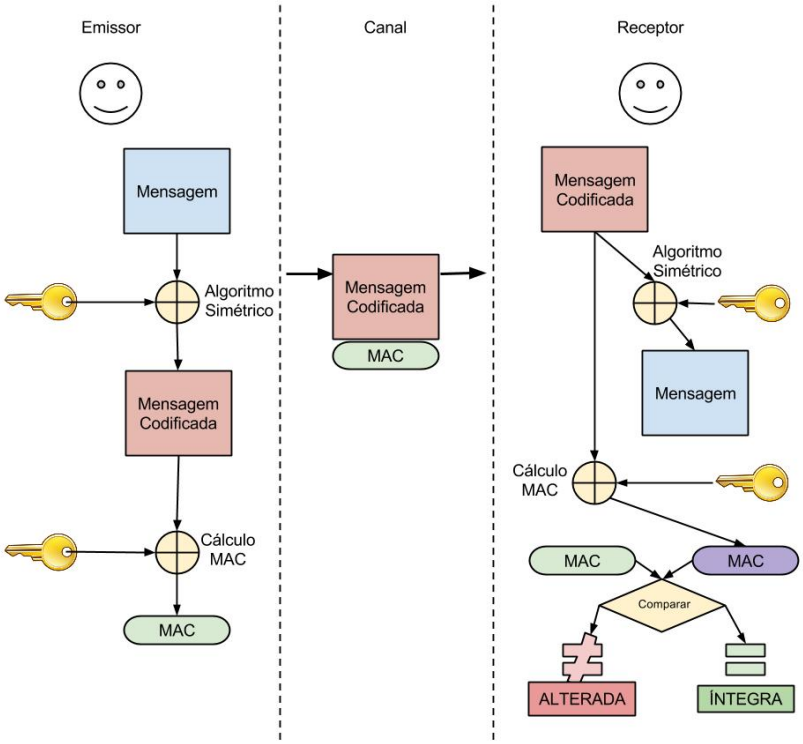


Figura 3: Algoritmo simétrico utilizado para garantir integridade e origem de dados. Fonte: Autoria própria.

interesse (NIST, 2001). Estas funções criam uma representação única (também chamada de resumo ou valor *hash*) de tamanho fixo a partir de dados de tamanhos variáveis, sendo impossível reconstruí-los apenas com esta representação (STALLINGS, 2010). Por este motivo, estas funções também são chamadas de *one-way*, ou seja, unidirecional.

Outra garantia das Funções *Hash* é a resistência à colisões, ou seja, computacionalmente, é impossível de se encontrar um mesmo valor *hash* a partir de duas sequências de dados diferentes (COMMERCE, 2013). Essa garantia é essencial para se evitar que um intruso troque uma mensagem original, ou parte dela, por outra sem que essa violação de integridade seja detectada.

As Funções *Hash* proporcionam integridade, uma vez que qualquer alteração, intencional ou acidental, implica em uma mudança significativa em seu resultado. Este efeito, conhecido como Efeito Avalanche, é uma das propriedades destas funções (WIKIPEDIA, 2014b).

Estas funções, por si próprias, não garantem a autoria de dados, pois não utilizam chaves secretas. Apesar disso, é possível, assim como o MAC dos algoritmos simétricos, utilizar este mecanismo com a finalidade de garantir-se a autoria. Primeiramente, a mensagem original

é codificada. Em seguida, o resultado é processado por uma Função *Hash* e seu conteúdo é enviado anexo à mensagem original.

O valor *hash* calculado é chamado de código de autenticação de mensagens baseado em funções *hash* (*Hash-based Message Authentication Code* - HMAC) e nada mais é que a especialização do MAC utilizando funções *hash*.

2.2.2.3 ALGORITMOS ASSIMÉTRICOS

Os mecanismos assimétricos, por sua vez, utilizam duas chaves para cada pessoa/entidade: uma pública, de conhecimento público, e outra privada, pessoal e secreta (STALLINGS, 2010). As chaves são altamente dependentes uma da outra, pois quando uma é utilizada para codificar, somente a outra pode decodificar mensagens. Embora haja esta dependência, os algoritmos buscam garantir que seja impossível reconstruir uma das chaves a partir da outra (STALLINGS, 2010).

A utilização de duas chaves permite alcançar autenticidade e não-repúdio quando o remetente codifica sua mensagem utilizando sua chave privada. Desta forma, a mensagem pode ser decodificada por qualquer outra entidade utilizando a chave pública do remetente. Isso implica dizer que a mensagem foi, necessariamente, codificada pela entidade associada à chave pública utilizando sua chave privada, pois há a garantida de que as chaves se relacionam exclusivamente.

Os algoritmos assimétricos permitem, ainda, alcançar a confidencialidade quando o remetente, de posse da chave pública de um destinatário de interesse, codifica sua mensagem com esta chave (HARRIS, 2005). Somente o destinatário, utilizando sua chave privada, pode decodificar a mensagem recebida.

Em relação ao desempenho, algoritmos assimétricos tendem a ser piores que algoritmos simétricos, pois as chaves precisam ser maiores, em comparação, assim como mais turnos de codificação/decodificação são necessários para cada operação (HARRIS, 2005). Esta, assim como a possibilidade de se utilizar duas chaves, são as principais razões que direcionam o uso deste tipo de algoritmo, que são: transporte de chaves, acordo de chaves, assinaturas digitais.

Aproveitando-se do fato que algoritmos simétricos são mais rápidos, algoritmos assimétricos podem ser utilizados para suprir a dificuldade encontrada no compartilhamento de chaves secretas (STALLINGS, 2010). Desta forma, chaves de algoritmos simétricos podem ser compartilhadas, ou seja, transportadas, se forem codificadas com a chave pública (assimétrica) do destinatário de interesse. Enviada a chave simétrica de forma segura, apenas ela precisa ser

utilizada na troca das demais mensagens entre as partes.

O acordo de chaves diz respeito à uma propriedade alcançada, entre outros, pelo algoritmo assimétrico Diffie-Hellman. Este algoritmo assegura que, dados dois pares de chaves assimétricas, a combinação entre a chave privada de A com a chave pública de B gera a mesma combinação que a chave privada de B com a chave pública de A, ou seja, a combinação representa uma chave simétrica construída com base em chaves assimétricas e que só pode ser reconstruída por cada parte com sua chave privada (STALLINGS, 2010).

O último uso mencionado, a Assinatura Digital, tema central deste Estudo de Caso, será abordado em profundidade na seção seguinte.

2.2.2.4 ASSINATURA DIGITAL

Vários conceitos de Assinatura Digital foram apresentados no início deste capítulo. Faz-se necessário, neste momento, apresentar seu funcionamento e as implicações e requisitos de seu uso.

A Figura 4, a seguir, apresenta de forma simplificada o processo de assinatura de um documento. O documento original é submetido à uma função *hash*, ou resumo criptográfico, gerando a impressão digital do documento, ou seja, seu valor *hash*. Em seguida, este valor é codificado com a chave privada do assinante, resultando na assinatura propriamente dita. O documento final é composto pelo documento original e pela sequência de bits da assinatura.

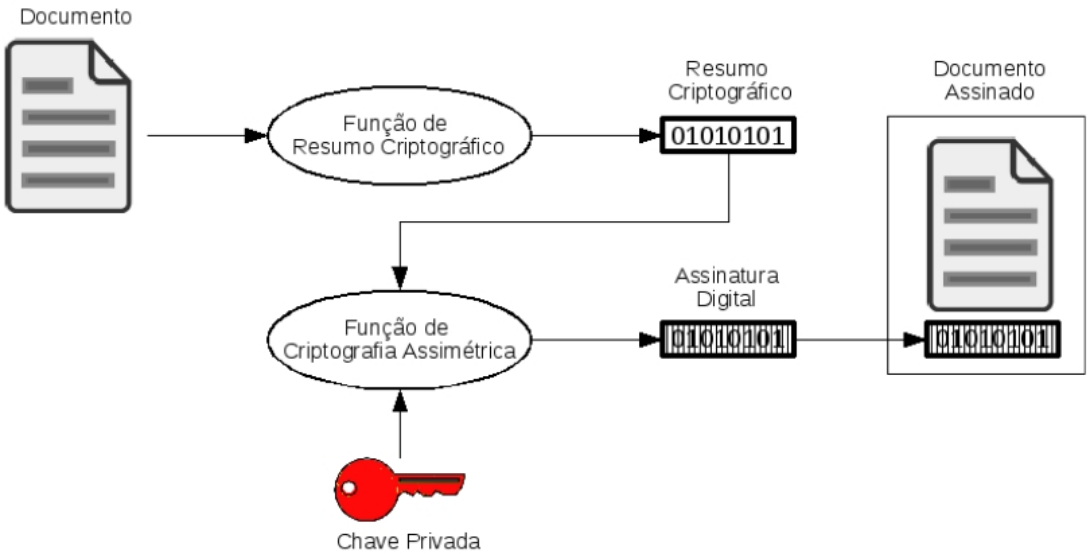


Figura 4: Passos para criar uma assinatura digital.

Fonte: (ITI, 2012)

Os destinatários, ou interessados neste documento, podem, a qualquer momento, realizar o processo inverso para verificarem se o autor do documento é aquele cuja identidade está associada à chave pública correspondente e se o conteúdo manteve-se íntegro. Este processo é apresentado na Figura 5.

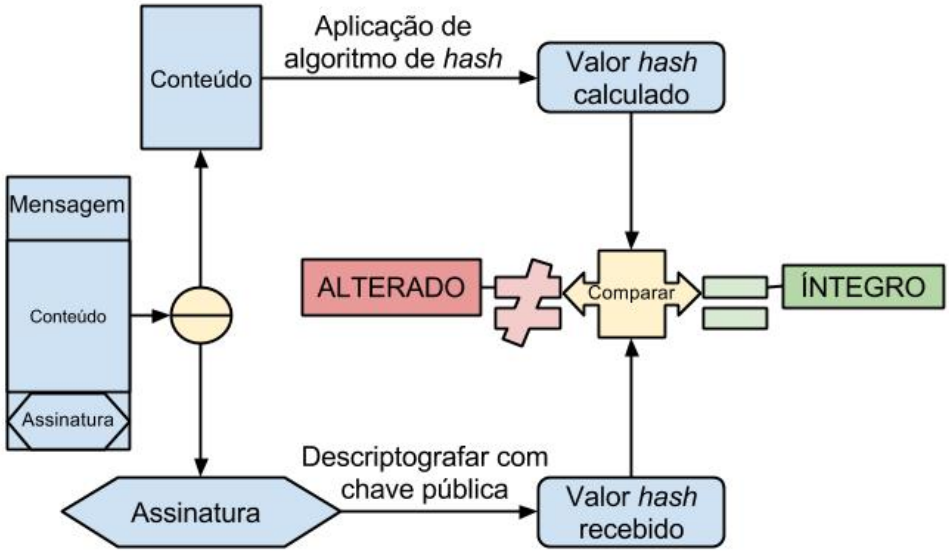


Figura 5: Passos para verificar uma assinatura digital.

Fonte: Autoria própria.

A Tabela 2 apresenta de forma resumida uma comparação entre os mecanismos de segurança até aqui apresentados.

Tabela 2: Mecanismos e propriedades.

Mecanismo		Integ.	Confid.	Autent.	Não-repúdio	Dist. de Chaves
Criptografia de chave simétrica	Encriptação	Não	Sim	Não	Não	Não
	MAC	Sim	Não	Sim	Não	Não
	Transporte de Chaves	Não	Não	Não	Não	Sim [1]
Funções *Hash* seguras	Message Digest	Sim	Não	Não	Não	Não
	HMAC	Sim	Não	Sim	Não	Não
Criptografia Assimétrica	Assinatura Digital	Sim	Não	Sim	Sim [2]	Não
	Transporte de Chaves	Não	Não	Não	Não	Sim
	Acordo de Chaves	Não	Não	Sim	Não	Sim

Adaptado de (NIST, 2001)

[1] Desde que com TTP.

[2] Requer inicialização isolada ou um TTP.

A assinatura digital deve possuir as seguintes propriedades (STALLINGS, 2010). Deve verificar o autor, a data e a hora da assinatura; deve autenticar o conteúdo no instante de tempo da realização da assinatura; deve ser verificável por terceiros, para resolver disputas (STALLINGS, 2010).

Como requisito para a assinatura digital, tem-se (adaptado de (STALLINGS, 2010)):

- a assinatura deve ser um padrão de *bits* dependentes da mensagem sendo assinada;
- a assinatura deve usar alguma informação única do assinante para prevenir falsificações ou negações de autoria;
- deve ser relativamente simples produzir uma assinatura digital;
- deve ser relativamente fácil reconhecer e verificar uma assinatura digital;
- deve ser computacionalmente impossível forjar uma assinatura digital, tanto construindo uma nova mensagem para uma assinatura digital existente, quanto construindo uma assinatura digital fraudulenta dada uma mensagem;
- deve ser funcional e prático armazenar cópia de uma assinatura digital.

A validade de toda a assinatura digital reside na proteção que deve ser conferida à chave privada do titular e no carimbo de tempo da assinatura. Por estas razões, a resposta para as ameaças decorrentes aceita universalmente é pelo uso de certificados digitais e autoridades certificadoras (STALLINGS, 2010). A composição de todos os elementos envolvidos, regras, padrões, entre outros, forma o que é conhecido como Infraestrutura de Chaves Públicas.

2.3 INFRAESTRUTURA DE CHAVES PÚBLICAS

Infraestrutura de Chaves Públicas (ICP ou *Public Key Infrastructure* - PKI) é um *framework* estabelecido para criar, manter e revogar Certificados de Chave Pública, consistindo em programas, formatos de dados, protocolos, políticas, mecanismos criptográficos, entre outros (HARRIS, 2005) (COMMERCE, 2013).

De acordo com (IETF, 2000), o Glossário de Segurança da Internet, ICP (ou PKI) é:

"Public-Key Infrastructure (PKI)

> - (I) A system of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
> - (O) PKIX usage: The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography."

É de se notar que existem muitas entidades, pessoas, regulamentos, padrões e leis envolvidas nesta Infraestrutura. Alguns dos principais componentes de uma ICP são explicados a seguir.

Usuário são pessoas e entidades (empresas, órgãos do governo, entre outros) que desejam ser reconhecidos digitalmente, ou que desejam reconhecer terceiros de forma segura por meio de certificados digitais (NIST, 2001).

Chaves são as chaves criptográficas (pública e privada) geradas pela AC e associadas a uma identidade, criando um certificado digital (STALLINGS, 2010) (NIST, 2001).

Certificado é a composição de informações e uma chave pública que identificam de forma única o proprietário das informações. Todo o conjunto de informações é assinado por uma AC. O padrão definido é o X.509 e está atualmente na versão 3. Ele estabelece os campos de informação necessários, quais são obrigatórios, quais são opcionais, entre outras informações (mais detalhes na Seção 2.3.2) (NIST, 2001) (STALLINGS, 2010).

O certificado digital, uma vez emitido, passa a ser de posse do usuário titular e seu conteúdo não é alterado. A AC, de certa forma, perde o controle sobre o certificado e a maneira para contornar essa insegurança é emitir as LCR (descrição abaixo).

Autoridade de Registro (AR) é a entidade que intermedeia a relação entre usuários e AC. É responsável por verificar a validade das informações fornecidas por usuários e requisitar a criação de certificados para usuários. Ela atua como filtro para que somente as informações válidas sejam analisadas por uma AC. Importante ressaltar que AR não emite certificados.

Autoridade Certificadora (AC) é uma TTP, ou seja, é uma entidade confiável responsável por emitir, manter e revogar certificados digitais. Depois que as informações são verificadas por uma AR, o certificado é gerado. O certificado gerado deve ser assinado pela AC, ou seja, a AC garante que as informações são válidas e que estão efetivamente associadas à determinada chave pública, também contida no certificado. A AC é consultada sempre

que alguém deseja saber se um certificado é válido e se a chave pública informada é propriedade da identidade que alega possuí-la.

A AC, ainda, publica listas de certificados revogados (LCR ou *Certificate Revocation Lists* - CRL) periodicamente, para que qualquer pessoa ou entidade possa verificar a validade do certificado com quem está negociando.

Carimbo de Tempo é o registro de data e hora associado a uma assinatura ou certificado digital. Uma importante entidade da infraestrutura é uma fonte confiável de Carimbo de Tempo. Fonte confiável implica em um sistema seguro, ou seja, que garanta que Carimbos de Tempo criados em momentos diferentes sejam comparados sem que haja a menor dúvida de sua validade.

Uma função do Carimbo de Tempo é a de servir como evidência de que uma informação digital existia numa determinada data e hora no passado (ITI, 2014c). Além disso, Carimbos de Tempo permitem que certificados digitais sejam aceitos ou rejeitados com base em sua data de validade.

Uma característica que pode ser de fundamental importância em disputas futuras é a de que, mesmo que a chave privada de um certificado seja exposta, o Carimbo de Tempo pode garantir que uma assinatura digital permanece válida (WIKIPEDIA, 2014c).

As entidades responsáveis por fornecer Carimbos de Tempo são conhecidas como Protocoladoras Digitais de Documentos Eletrônicos - PDDE, ou também Autoridade Certificadora de Tempo, como será visto mais adiante.

2.3.1 ARQUITETURAS

Existem duas arquiteturas tradicionalmente conhecidas de ICP, a Hierárquica (em inglês *hierarchical*) e a em Malha (*Mesh*).

A infraestrutura que segue a arquitetura Hierárquica tem o formato apresentado na Figura 6 (a). Nesta arquitetura, uma AC Raiz emite certificados para AC abaixo dela (ou diretamente para usuários finais), que por sua vez podem emitir certificados para outras AC e usuários (NIST, 2001). Como será visto adiante, a arquitetura adotada no Brasil é do tipo hierárquica, porem não permite que a AC Raiz emita certificados diretamente para usuários finais (ITI, 2014a).

A arquitetura em Malha, apresentada na Figura 6 (b), não possui uma AC Raiz. As AC emitem certificados para outras AC que emitem certificados em retorno, formando uma malha de confiança (NIST, 2001).

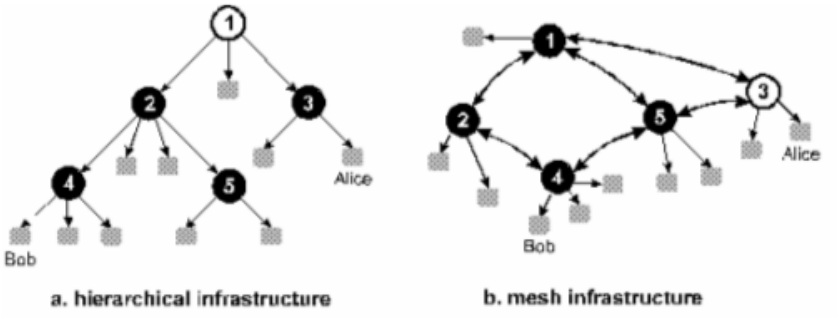


Figura 6: Arquiteturas de ICP Hierárquica e em Malha.
Fonte: (NIST, 2001)

Ainda, é possível formar vínculos entre diferentes ICP por meio de ligações chamadas pontes (ou *bridges*), independentemente da arquitetura adotada por cada ICP. Isto permite, por exemplo, que um certificado emitido no âmbito de uma ICP de outro país seja aceito dentro da ICP-Brasil, caso haja uma ponte entre a AC Raiz brasileira e a AC desta ICP externa (podendo ser Raiz ou não).

Em decorrência das conexões entre as AC, particularmente na arquitetura Hierárquica, o certificado de um usuário final é assegurado por uma AC, que por sua vez tem o seu certificado assegurado por AC hierarquicamente superiores até chegar na AC Raiz. Este caminho de certificados, onde os hierarquicamente superiores garantem a validade dos imediatamente inferiores é chamado de Cadeia de Certificados, ou Cadeia de Certificação.

Supondo que a entidade 1 da Figura 6 (a) seja a AC Raiz, o certificado de Bob foi emitido e assinado pela entidade 4, que por sua vez foi emitido e assinado pela entidade 2, que por sua vez foi emitido e assinado pela AC Raiz 1. Isso significa que ao se verificar o certificado de Bob, os certificados da cadeia também devem ser verificados até que a AC Raiz seja alcançada, pois esta entidade é garantidamente confiável (as intermediárias podem eventualmente terem seus certificados revogados).

2.3.2 PADRÃO X.509 E FORMATO PKCS #12

X.509 é um padrão ITU-T (ITU, 2012), mantido pela divisão de telecomunicações do *International Telecommunication Union* - (ITU), uma entidade internacional cuja missão é elaborar recomendações de padrões internacionais para todos os campos da telecomunicação.

As recomendações decorrentes do padrão X.509 especificam formatos para certificados de chave pública, listas de certificados revogados (LCRs), certificados de atributos e algo-

ritmos de validação de cadeia de certificado (ITU, 2012).

O certificado apresentado a seguir exemplifica o formato X.509 para certificados de chave pública (WIKIPEDIA, 2014f).

Código 2.1: Exemplo de Certificado X.509. Fonte: (WIKIPEDIA, 2014f)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting
            cc, OU=Certification Services Division, CN=Thawte Server CA
           /emailAddress=server-certs@thawte.com
        Validity:
            Not Before: Aug  1 00:00:00 1996 GMT
            Not After: Dec 31 23:59:59 2020 GMT
        Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
           Consulting cc, OU=Certification Services Division, CN=Thawte
            Server CA/emailAddress=server-certs@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
    00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:68:75:47:a2:aa:c2:
    da:84:25:fc:a8:f4:47:51:da:85:b5:20:74:94:86:1e:0f:75:c9:e9:08:
    61:f5:06:6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:6a:0c:44:
    38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:29:b6:2f:49:c8:3b:d4:27:04:
    25:10:97:2f:e7:90:6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
    5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:3a:c2:b5:66:22:12:
    d6:87:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA: TRUE
Signature Algorithm: md5WithRSAEncryption
    07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:a8:6f:49:
    1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:3e:59:43:7d:4f:95:
    3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:4e:4e:9e:40:db:a8:cc:32:74:
    b9:6f:0d:c6:e3:b3:44:0b:d9:8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:
    28:9a:5a:3c:d5:b5:e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:
    a9:da:b9:b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
    70:47
```

O certificado X.509 possui campos fixos e campos opcionais, ou extensões. As extensões surgiram apenas na versão 3 do X.509, de modo que só podem ser utilizadas se no campo versão (*Version*) constar o valor 3 (IETF, 2008). A linha 4 apresenta um número serial que deve ser único no âmbito de cada AC emissora.

O certificado apresentado acima é um exemplo de certificado autoassinado, ou seja, o emissor (*Issuer*, linha 6) é o mesmo que o usuário titular (*Subject*, linha 10). Uma eventual verificação do certificado e sua cadeia chegaria no próprio certificado, por isso é chamado de autoassinado. Ainda nestes campos, é possível observar subcampos que caracterizam e detalham a origem do emissor e do usuário titular. Como exemplo, pode-se citar os subcampos C, ST, L, O, OU que representam respectivamente informações sobre código de país segundo a ISO3166, estado ou província, localidade (normalmente cidade), organização (nome da empresa), divisão ou unidade da empresa (IETF, 2008).

O campo da linha 7, validade (*Validity*), apresenta o período de validade do certificado, que é delimitado por uma data inicial "não válido antes de" (*Not Before*) e outra data final "não válido depois de" (*Not After*). Estes valores devem ser utilizados pelas aplicações para aceitar ou não determinado certificado.

Na linha 11 estão presentes informações acerta da chave pública do usuário titular como o algoritmo utilizado para gerar a chave (linha 12, neste caso o campo indica a utilização de criptografia RSA), a especificação da chave pública (linha 13) e a chave pública propriamente dita de 1024 bits (linha 14).

Por fim, o certificado apresenta informações acerta da assinatura do próprio certificado pela autoridade emissora. A linha 26 apresenta qual o algoritmo utilizado para realizar a assinatura do certificado e a partir da linha 27 é apresentada a assinatura, contendo 1024 bits.

Pode-se notar que no certificado X.509 não há nenhuma menção à chave privada do titular, necessária para assinar documentos. Esta chave é codificada com uma chave simétrica de conhecimento do titular (utilizada como senha) e encapsulada, juntamente com seu certificado e os certificados de sua cadeia, em um arquivo no formato PKCS #12 (WIKIPEDIA, 2014e) (LABORATORIES, 1999). Este arquivo é armazenado em um *token* USB (a Figura 7 apresenta um dos modelos), que deve ficar em posse do titular do certificado. A chave privada é acessada somente por meio da senha, isto quer dizer que o titular só pode realizar assinaturas se informar esta senha. Caso contrário, o *driver* do sistema operacional não pode decodificar a chave privada e fornecê-la à aplicação solicitante.

Figura 7: Token USB contendo arquivo PKCS #12.
Fonte: (SAFENET, 2014)

2.3.3 LISTAS DE CERTIFICADOS REVOGADOS - LCR

Apesar de os certificados X.509 possuírem data de validade, eles podem se tornar não confiáveis antes desta data por diversos motivos, como por exemplo, extravio, perda, furto, exposição da senha, entre outros. O mecanismo para fornecer um *status* atualizado dos certificados emitidos por uma AC é a Lista de Certificados Revogados, periodicamente divulgada publicamente. Esta lista, assim como os certificados emitidos pela AC, é assinada pela entidade com a finalidade de atestar a autenticidade da LCR divulgada.

O padrão, como já mencionado, é o X.509. Um exemplo neste padrão pode ser observado a seguir.

Código 2.2: Exemplo de Lista de Certificados Revogados X.509. Fonte: (ITI, 2014b)

```
Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=BR/O=ICP-Brasil/OU=Instituto Nacional de Tecnologia da
            Informacao - ITI/CN=Autoridade Certificadora Raiz Brasileira v1
        Last Update: Aug 20 13:39:41 2014 GMT
        Next Update: Nov 18 13:39:41 2014 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:42:B2:2C:5C:74:01:07:BE:9B:FF:
                      55:33:3B:EE:29:BB:5D:91:BF:06
            X509v3 CRL Number:
                30
Revoked Certificates:
    Serial Number: 07
        Revocation Date: Jun 12 19:09:32 2009 GMT
    Serial Number: 0B
```

```
17          Revocation Date: Dec 23 17:36:36 2010 GMT
18      Signature Algorithm: sha1WithRSAEncryption
19          72:32:08:e8:c9:50:0e:aa:75:46:37:f3:45:f7:f9:11:80:7d:
20          27:04:ef:13:73:1f:33:43:eb:6e:fa:52:40:52:00:d2:1d:c1:
21          a0:30:73:9a:c7:3a:fa:d4:1f:7b:63:61:8d:0e:ab:73:84:a7:
22          c4:0c:0f:e2:fd:75:aa:e2:18:ea:f7:45:07:50:e9:bd:e0:ca:
23          03:94:27:ad:d3:e8:ce:99:aa:43:41:a4:ab:f1:7c:46:e9:6c:
24          e0:49:ca:66:fa:f2:c5:fe:f9:1f:6a:b2:9d:86:47:94:63:78:
25          6d:af:05:fc:f7:dd:e9:10:1c:3d:8d:e9:83:fd:4d:3c:a9:d1:
26          b4:37:da:b5:9b:a7:43:5a:ac:82:4d:de:b2:16:1f:34:7e:cd:
27          a3:ad:36:61:eb:71:c0:17:12:38:f7:40:6a:e0:83:09:7f:5d:
28          86:4b:29:8a:4f:96:1c:5e:07:93:95:88:1c:1e:90:04:79:29:
29          7b:b6:cf:b1:24:80:68:11:ed:a7:cf:97:da:31:bf:fd:dc:34:
30          f5:b2:44:4a:2d:fe:d9:0b:11:3a:ab:15:3b:58:91:83:73:43:
31          81:e4:92:41:4a:34:c0:c6:4c:cd:c9:d0:c5:14:1f:89:ba:5f:
32          16:6a:10:01:31:c5:75:48:be:34:b7:a4:98:d3:b9:0b:30:fc:
33          ff:27:21:88
```

O primeiro campo indica a versão (*Version*) utilizada pela LCR, que neste caso é a versão 2.

Na linha 4 consta o emissor (*Issuer*) desta lista e os campos de detalhamento. As linhas 5 e 6 indicam, respectivamente, os Carimbos de Tempo da data de emissão desta LCR e da data de emissão da próxima lista a ser emitida.

A partir da linha 13 pode ser observada a lista de certificados revogados. Os certificados são indicados pelo seu número serial (*Serial Number*), que é único no âmbito de cada AC. Outra informação associada a cada certificado revogado é a data de revogação (*Revocation Date*). Esta informação é importante pois o titular pode demorar a informar para a autoridade certificadora o problema acontecido com seu certificado.

Por fim, o campo de assinatura (*Signature Algorithm*) indica o algoritmo utilizado pelo emissor para assinar a LCR e a assinatura propriamente dita, que neste caso contém 4096 bits.

2.4 ICP-BRASIL

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) foi instituída pela Medida Provisória (MP) Nº2200-2, de 24 de agosto de 2001. Em seu artigo 1º são definidos os objetivos desta entidade, como pode ser observado a seguir.

> "Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras." (REPúBLICA, 2001)

É de se notar a validade jurídica envolvida que foi garantida aos documentos em forma eletrônica a partir da instituição da ICP-Brasil. Esta garantia permite que assinaturas digitais tenham legalmente a mesma validade jurídica que assinaturas físicas.

A MP 2200-2 estabelece que a ICP-Brasil é composta por uma autoridade gestora, cuja função é exercida pelo Comitê Gestor da ICP-Brasil vinculado à Casa Civil da Presidência da República, sendo composto por representantes da sociedade civil, representantes de órgãos públicos (como Ministérios da Justiça, da Fazenda, da Ciência e Tecnologia, entre outros) e integrantes de setores interessados, designados pelo Presidente da República (REPúBLICA, 2001).

Também compõe a ICP-Brasil a cadeia de autoridades certificadoras, sendo esta composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Além da composição, a MP estabelece as competências do Comitê Gestor, da AC Raiz, das ACs e das ARs; transforma o Instituto de Tecnologia da Informação - ITI em autarquia federal vinculada ao Ministério da Ciência e Tecnologia, delegando-lhe a função de AC Raiz da ICP-Brasil (REPúBLICA, 2001).

Compete ao Comitê Gestor coordenar o funcionamento da ICP-Brasil; estabelecer políticas, critérios e normas técnicas para o credenciamento das ACs e das ARs; estabelecer a política de certificação e as regras operacionais da AC Raiz; homologar, auditar e fiscalizar a AC Raiz; formulação de políticas de certificados e e regras operacionais das ACs e das ARs; entre outros.

Entre as competências da AC Raiz pode-se destacar a emissão, expedição, distribuição, revogação e gerenciamento dos certificados das ACs de nível imediatamente subsequente ao seu; o gerenciamento da lista de certificados emitidos, revogados e vencidos; a execução de atividades de fiscalização e auditoria das ACs e das ARs e dos prestadores de serviço habilitados.

Interessante ressaltar o artigo e 6º e seu Parágrafo Único. Este artigo estabelece as competências da AC, como, por exemplo, a emissão de certificados para usuários finais. Apensar dessa possibilidade, o Parágrafo Único estabelece que quem gera o par de chaves criptográficas é o próprio titular e sua chave privada é de seu exclusivo controle, uso e conheci-

mento, ou seja, nenhuma entidade da cadeia de certificação tem conhecimento desta chave. Esta medida visa garantir que nenhuma falha ou vazamento de informações de algum componente da cadeia comprometa a integridade de toda a infraestrutura. Além disso, esta medida garante que somente o titular possui conhecimento do par de chaves criptográficas, requisito essencial ao não-repúdio.

> "Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.
>
> Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento." (REPúBLICA, 2001)

Além destas entidades, existe, no âmbito da ICP-Brasil, a Autoridade Certificadora do Tempo - ACT. Os usuários de serviços de Carimbo de Tempo confiam nesta entidade para obter Carimbos de Tempo. Por ser uma entidade confiável, o Carimbo de Tempo assegura a existência de uma assinatura digital em determinado período (ITI, 2014a).

O modelo adotado pelo Brasil foi o de certificação com raiz única, de forma que as demais entidades que desejarem se tornar uma AC, devem ser autorizadas e certificadas pelo ITI, por ser a AC Raiz (ITI, 2014a).

3 METODOLOGIA DE PESQUISA

A presente monografia foi elaborada a partir do levantamento da bibliografia acerca do assunto Assinatura Digital. Além disso, foi evidenciado em legislações vigentes, tanto no Brasil quanto em outros países, o domínio atual e os resultados obtidos da aplicação real da teoria envolvida. Por se tratar de um Estudo de Caso, a metodologia qualitativa foi realizada a partir da análise de toda a documentação gerada pelo projeto e pelo produto em si (códigos-fonte).

O caso concreto foi apresentado com base na análise destes documentos (códigos-fonte e artefatos de projeto) disponíveis em repositório do TRT9 (documentação técnica e de negócios), tornando possível estabelecer relação com a teoria apresentada e posterior avaliação do projeto desenvolvido.

A análise teve como objetivo delinear possíveis deficiências presentes no projeto passíveis de melhorias, bem como elencar questionamentos e sugestões para manutenções futuras. De forma mais ampla, a análise objetivou trazer ao debate acadêmico as dificuldades encontradas na aplicação da teoria, bem como divulgar a outros interessados a experiência adquirida e presente no projeto.

Esta análise documental foi devidamente autorizada pela chefia da Secretaria responsável pelo Projeto da Assinatura Digital.

4 ESTUDO DE CASO

4.1 A EMPRESA

O presente Estudo de Caso apresenta o Projeto Assinatura Eletrônica de Atas de Correição, desenvolvido no Tribunal Regional do Trabalho da 9ª Região - Paraná pela Secretaria de Desenvolvimento de Soluções em Tecnologia da Informação, com início em 26 de março de 2012.

Diante das funcionalidades proporcionadas pela Assinatura Digital no PJe e em outros sistemas desenvolvidos pelo próprio TRT9 e já utilizados pela área fim (e.g., Gabinete Juiz, e-REC, e-Gab), percebeu-se a possibilidade e a importância de se utilizar ferramenta semelhante para documentos de âmbito administrativo.

4.2 OBJETIVOS

Inicialmente solicitado pela Corregedoria do TRT9, o projeto contemplou em seus objetivos a possibilidade de se reutilizar em outros sistemas administrativos a solução desenvolvida, como pode ser observado no objetivo específico a seguir, extraído do documento Plano Integrado de Projeto (PIP).

> Desenvolver uma solução para Assinatura Digital de Atas de Correição, com toda a infraestrutura de desenvolvimento preparada para demais tipos de documentos administrativos (TRT9, 2012a).

Algumas das premissas deste mesmo documento reafirmam a previsão de reutilização da solução, como pode ser observado a seguir.

> A solução será a mais genérica possível, atendendo a necessidade imediata da Corregedoria e viabilizando o desenvolvimento de necessidades futuras análogas do TRT9 (TRT9, 2012a).

> O desenvolvimento da solução para Assinatura Digital de outros tipos de documentos administrativos se dará sob demanda e priorizada pelo Comitê de Informática do TRT9.

4.3 ESCOPO

O escopo, como registrado em vários dos documentos de projeto, é o desenvolvimento de uma solução de Assinatura Digital para o sistema administrativo de Atas de Correição, utilizado pela Corregedoria do TRT9, tendo em vista sua reutilização em outros sistemas administrativos.

O PIP apresenta alguns itens relacionados ao escopo do projeto, apresentado na íntegra a seguir (TRT9, 2012a).

1. Componente reutilizável de assinatura digital genérica na *web* para documentos administrativos do TRT9.
2. Componente para geração do número localizador de documentos administrativos.
3. Interface *web* para localizar e apresentar os documentos de Atas de Correição através do número Localizador. Essa interface *web* estará disponível para acesso externo e interno.
4. Interface para impressão de Atas de Correição assinados digitalmente.

Em relação ao formato de arquivo passível de ser assinado, embora a arquitetura tenha sido projetada para assinar qualquer tipo de documento, foi definido que neste projeto apenas arquivos no formato HTML seriam assinados, em função da necessidade apresentada pela Corregedoria, que utiliza documentos neste formato.

Outra restrição de escopo refere-se ao número de assinaturas sobre um mesmo documento. Apesar de a arquitetura prever esta possibilidade, ela não foi implementada neste momento em função da necessidade específica deste projeto. Desta forma, foi definido que apenas uma assinatura seria realizada por documento.

4.4 DESENVOLVIMENTO DA SOLUÇÃO

4.4.1 REQUISITOS

Os requisitos funcionais e não-funcionais foram levantados com base na análise do código-fonte e nos documentos de projeto, como por exemplo, o PIP, a Especificação dos Casos

de Teste e os *Status Reports*. Os requisitos levantados nos Casos de Uso serão apresentados na seção 4.4.2.

4.4.1.1 REQUISITOS FUNCIONAIS

- que o sistema seja preparado para possibilitar assinatura de diversos formatos de arquivo;
- que o sistema seja preparado para suportar múltiplas assinaturas;
- que em toda consulta de documentos assinados as informações do usuário sejam registradas;
- que seja possível utilizar a parte cliente de forma *web*, por meio de um navegador, ou local;
- que seja possível cancelar assinaturas realizadas;
- que seja possível realizar assinatura em bloco (ou batelada).

4.4.1.2 REQUISITOS NÃO-FUNCIONAIS

- que a parte cliente (arquivo JAR) seja pequena o suficiente para que o carregamento *web* exija o mínimo de download possível;
- que seja possível baixar o documento assinado, mesmo por usuários externos ao TRT9 (internet);
- que seja possível controlar o volume de dados de documentos assinados no banco de dados, sem prejudicar eventuais consultas;
- que o sistema seja genérico o suficiente para poder ser incluído em outros sistemas administrativos;
- que o sistema seja modular o suficiente para comportar o uso dos outros sistemas administrativos sem precisar sofrer alterações significativas, causando mudanças em cascata;

4.4.2 CASOS DE USO

Nos documentos de Especificação de Caso de Uso constam quatro casos, todos transcritos na íntegra no Anexo A. A lista abaixo contempla o nome dos casos de uso, a respectiva descrição e os respectivos requisitos elicitados, todas informações obtidas dos mencionados documentos de projeto.

UCS_01_ASSINAR_DOCUMENTO Este caso de uso é utilizado na assinatura de documentos.

- Requisitos Funcionais:
  - A tarja de ser igual a do modelo fornecido (ver Figura 14 no Anexo A).
  - Somente terá permissão para assinar um magistrado com perfil de corregedor.
  - O usuário logado poderá não ser o mesmo que assinará a ata.
  - O programa atual de "Edição de Ata" será alterado para não apresentar ao final do texto o nome do Corregedor(a) e os dois quadros de conferência.
  - O programa atual será alterado para solicitar confirmação na opção "Excluir".
  - O programa atual será alterado para não ter mais a opção de "Publicação", conforme figura apresentada.
  - O programa atual será alterado incluindo-se um filtro para apresentar somente as "Atas em aberto" ou "Todas as atas".
- Requisitos Não-Funcionais:
  - A assinatura da ata poderá ser realizada de qualquer lugar com acesso ao ambiente *web* do TRT9.

UCS_02_LOCALIZAR_DOCUMENTO_ASSINADO Este caso de uso é utilizado na localização de documentos assinados.

- Nenhum requisito apresentado.

UCS_03_CANCELAR_ASSINATURA Este caso de uso é utilizado na assinatura de documentos.

- Requisitos Funcionais:
  - Todos os casos de cancelamento de assinatura devem ser registrados em Log.
- Requisitos Não-Funcionais:
  - Cancelar de qualquer lugar (não necessariamente de dentro da rede do TRT9).

UCS_04_EXIBIR_PDF Este caso de uso é utilizado na assinatura de documentos.

- Nenhum requisito apresentado.

4.4.3 RECURSOS HUMANOS

A Tabela 3 apresenta os papéis e o número de pessoas envolvidas no projeto.

Tabela 3: Equipe mobilizada para o projeto.

Papel	Quantidade
Patrocinador do Projeto	1
Gerente Funcional	1
Gerente do Projeto	1
Analista de Negócio	3
Desenvolvedor	4
Configuração de Ambiente	1

Fonte: Adaptada de (TRT9, 2012a).

4.5 CRONOGRAMA

A Tabela 4 a seguir, extraída do *Status Report* 5 do projeto (TRT9, 2012c) (sendo esta versão 5 a última deste documento), apresenta os marcos e entregas inicialmente planejados e respectivas data final planejada, data início realizada e data final realizada.

Tabela 4: Cronograma do Projeto

Entrega/Marco	Dt. Final Planejada	Dt. Início Realizada	Dt. Final Realizada
Aprovação e *kickoff* do projeto	18/04/2012	18/04/2012	18/04/2012
Desenvolvimento Protótipo	03/05/2012	19/04/2012	10/05/2012
Requisitos	02/05/2012	19/04/2012	10/05/2012
Desenvolvimento Assinatura	01/06/2012	07/05/2012	08/06/2012
Desenvolvimento Localizador	01/06/2012	07/05/2012	08/06/2012
Desenvolvimento Applet	01/06/2012	08/05/2012	08/06/2012
Alteração interface Atas	01/06/2012	29/05/2012	08/06/2012
Alfa testes internos integração	11/06/2012	11/06/2012	14/06/2012
Melhorias e Correções	15/06/2012	15/06/2012	19/06/2012
Semana de Homologação	18/06/2012	15/06/2012	29/06/2012
Entrada em Produção	11/06/2012	11/06/2012	04/07/2012

Fonte: (TRT9, 2012c).

O cronograma precisou ser replanejado, entre outros motivos apresentados no *Status Report* 5, pelo treinamento que parte da equipe participou, inicialmente não previsto; substituição do Gerente de Configuração, também não prevista; dificuldades técnicas encontradas durante o desenvolvimento; necessidade de testes mais apurados de integração (TRT9, 2012c).

4.6 RISCOS

Os riscos foram incluídos a partir do *Status Report* 2 (TRT9, 2012b), do dia 5 de maio. Os principais riscos levantados e respectivas respostas são apresentados a seguir.

Risco surgimento de novas tecnologias, inovação.

Resposta minimizar a utilização de tecnologias pouco conhecidas pelo pessoal da SDSTI.

Risco indisponibilidade de integrantes da equipe (férias, alocação em outros projetos, saída de integrante do órgão).

Resposta risco assumido pela secretaria SDSTI.

4.7 ARQUITETURA

Para o desenvolvimento da solução foi estabelecida a linguagem de programação Java e o banco de dados Oracle.

A arquitetura é constituída de duas partes que se comunicam. A primeira, a parte cliente, é um arquivo Java executável (JAR) que pode ser utilizado tanto de maneira local por uma aplicação (instalada na máquina do usuário), quanto de maneira *web*, por meio de um navegador.

A segunda parte, do lado do servidor, consiste em um *Web Service* construído também em Java, com duas funções principais, apresentadas resumidamente a seguir.

Localizador É o *Web Service* disponibilizado que permite, a qualquer pessoa de posse de um número localizador, obter o documento assinado. A finalidade deste serviço é permitir que uma pessoa verifique que um documento previamente recebido é autêntico e manteve-se íntegro.

Assinador Esta funcionalidade é chamada pela parte cliente quando o usuário deseja assinar determinado documento.

A arquitetura do banco de dados do esquema ASSINATURA foi construída conforme a estrutura apresentada na Figura 8. A única alteração no esquema de banco de dados do sistema administrativo necessária, a princípio, ao se adotar a assinatura digital, é a criação de um campo de chave estrangeira (*Foreign Key* - FK) na tabela de documentos deste sistema que

deve apontar para o campo COD_LOCALIZADOR da tabela DTT_OBJETO_ASSINADO. Este campo é atualizado pelo próprio esquema ASSINATURA quando um documento é assinado, de modo que a aplicação final (o sistema administrativo) não necessita se preocupar com isso, apenas em conceder o devido acesso para a operação *UPDATE* deste campo.

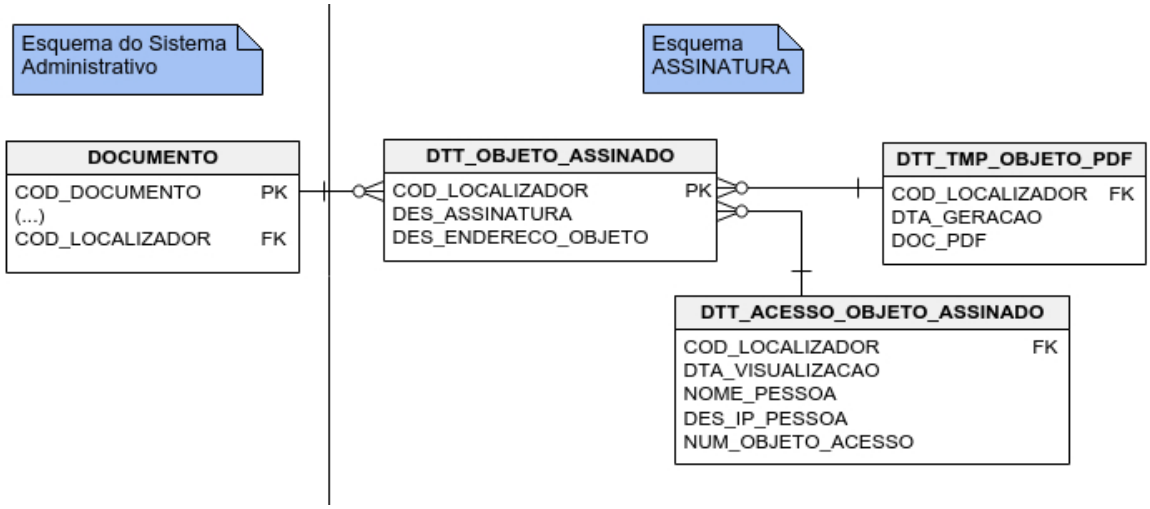


Figura 8: Estrutura do Banco de Dados.

Fonte: Autoria própria.

Sobre a arquitetura do servidor *web*, os *Web Services* desenvolvidos pelo TRT9 são hospedados sob o domínio https://www.trt9.jus.br. O Localizador, por exemplo, fica hospedado no endereço *web* https://www.trt9.jus.br/AssinaturaEletronica/. Este domínio utiliza o serviço central de autenticação, conhecido por sua sigla CAS (*Central Authentication Service*). Este serviço permite autenticação do tipo *Single Sign-On*, ou seja, é necessária apenas uma autenticação para ter acesso à todos os serviços disponibilizados pela empresa que o utiliza (FUNDATION, 2014).

Já a *Intranet*, onde ficam hospedadas a maior parte das aplicações administrativas (inclusive as Atas de Correição), fica localizada sob o domínio https://intranet.trt9.jus.br. Ao contrário do domínio www, o domínio *Intranet* não utiliza o CAS. A autenticação é realizada por meio do *Oracle Fusion Middleware*, um sistema do mesmo desenvolvedor do banco de dados em uso no TRT9.

O diagrama de sequência apresentado na Figura 9 mostra as interações entre o usuário, os servidores *web* e o banco de dados.

Tomando como exemplo a implementação da assinatura digital no sistema de Atas de Correição, o Usuário (Figura 9) acessa uma página *web* hospedada no domínio *Intranet*. Como resposta, o servidor retorna a página HTML para o navegador do usuário informando que alguns

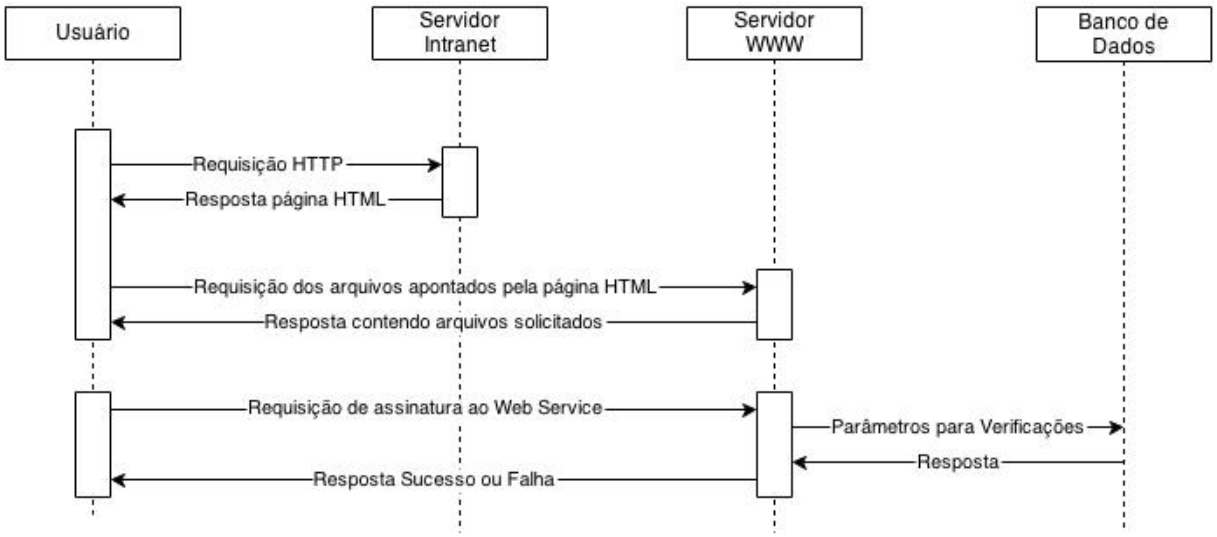


Figura 9: Diagrama de Sequência - Interação entre o usuário, servidores *web* e banco de dados.
Fonte: Autoria própria.

arquivos adicionais (incluindo o arquivo JAR) devem ser obtidos no domínio *www*. O navegador do usuário realiza a requisição dos arquivos, que ficam à disposição para ações do usuário.

Caso o usuário realize um pedido de assinatura, ação indicada na parte de baixo da Figura 9, a solicitação, originada do arquivo JAR, é encaminhada para o *Web Service* localizado no domínio *www*. O *Web Service*, por sua vez, realiza verificações (ver seção 4.7.3.2 para maiores detalhes) no banco de dados. Não havendo erro nem restrições a assinatura é armazenada. Seja qual for o resultado, uma mensagem é repassada ao usuário.

A hospedagem dos arquivos adicionais no mesmo servidor *web* do *Web Service* se deve à arquitetura de projeto Java adotada. Nela, os arquivos adicionais, assim como o arquivo JAR, são incluídos como *resources* no *Web Service*. Neste projeto da Assinatura Digital são quatro os arquivos adicionais. O primeiro deles, assina.js, é um arquivo *Javascript* que realiza tanto a requisição do arquivo JAR que se comunicará com o *Web Service* quanto a *interface* entre o navegador *web* e este JAR. Os outros três arquivos são da biblioteca JQuery, utilizada pelo assina.js.

4.7.1 CLIENTE

Tendo em vista o objetivo de fornecer uma solução genérica, o JAR, como já apresentado, foi desenvolvido para poder ser utilizado em aplicações *web* e em aplicações *standalone* (instaladas no computador).

Para se comunicar com o servidor, o JAR necessita três parâmetros, explicados a seguir.

4.7.1.1 CERTIFICADO

Um dos parâmetros que a parte cliente deve enviar para o *Web Service* consiste no certificado do usuário. Este certificado, que está no formato X.509, é obtido por meio de uma biblioteca Java desenvolvida pelo Tribunal Regional do Trabalho da 4ª Região - Rio Grande do Sul (TRT4), chamada Assinejus. Esta biblioteca realiza a *interface* com o sistema operacional, fornecendo para a aplicação cliente um objeto Java contendo as informações presentes no certificado. Além disso, uma das funções mais importantes desta biblioteca é a realização da assinatura propriamente dita, em que a chave secreta contida no *token* do usuário será combinada com o valor *hash* de cada documento a ser assinado.

Importante ressaltar que a assinatura é realizada na parte cliente, ou seja, a chave privada do usuário não trafega junto com os demais parâmetros pela internet. Apenas a chave pública, junto com as demais informações contidas no certificado que são de conhecimento público (disponibilizadas pelas Autoridades Certificadoras), são enviadas por meio deste parâmetro.

4.7.1.2 LISTA DE DOCUMENTOS

Esta lista contém o caminho, dentro do banco de dados, até cada um dos documentos que o cliente deseja assinar. Este modelo de localização também visa ao objetivo de solução genérica, de acordo com o requisito de projeto. Para que o esquema de banco de dados ASSINATURA possa acessar os documentos em outros esquemas, as devidas permissões devem ser concedidas.

A lista tem o formato XML apresentado no Código 4.1. Ela deve possuir um ou mais objetos, ordenados a partir do <num_sequencial> = 1. Para cada objeto, deve ser informado o esquema de banco de dados, a tabela, a coluna contendo o documento, o nome do objeto e o respectivo tipo MIME do arquivo. Além disso, para localizar na tabela o documento desejado, deve-se informar a chave primária (ou *Primary Key* PK) que identifica unicamente o respectivo documento.

Há suporte, como pode ser observado, para tabelas em que a chave primária seja composta. Neste caso, cada item <pk> da chave deve ser informado dentro do item <lista_de_pk>,com o respectivo nome da coluna e valor da chave.

Código 4.1: Lista de documentos

```
<?xml version = \"1.0\" encoding=\"ISO-8859-1\"?>
<objeto>
    <num_sequencial>1</num_sequencial>
    <schema>egestao</schema>
    <tabela>correicao_ata_info</tabela>
    <coluna>des_texto_completo</coluna>
    <nome_objeto>Ata1.doc</nome_objeto>
    <mime_type>application/msword</mime_type>
    <lista_de_pk>
        <pk>
            <nome_pk>cod_ata</nome_pk>
            <valor_pk>1422</valor_pk>
        </pk>
    </lista_de_pk>
</objeto>
```

Com esta lista de documentos é possível realizar assinaturas em bloco, ou seja, é possível assinar um conjunto de documentos de uma vez só.

4.7.1.3 LISTA DE ASSINATURA

Esta lista, também construída pela aplicação na parte cliente, é um objeto List do pacote padrão Java java.util constituído por objetos da classe TransporteAssinaturaDTO. Esta classe, como nota-se no nome, segue o padrão de Objetos para Transferência de Dados (*Data Transfer Objects* - DTO) (FOWLER, 2004), ou seja, é um objeto utilizado para chamadas remotas, como é o caso da chamada ao *Web Service* pelo cliente.

Cada objeto da lista representa uma assinatura e contém os seguintes dados.

- Número de identificação, correspondente ao <num_sequencial> da Lista de Documentos.
- Valor *hash* calculado pelo banco de dados para cada documento a ser assinado no momento em que o usuário realiza a assinatura. Desta forma, o usuário, ao assinar, concorda com determinado "estado" do documento.
- A assinatura que foi calculada pela biblioteca Assinejus a partir da chave privada do usuário, da senha (PIN) digitada e do valor *hash* (mesmo valor do item anterior). Antes

de criar as assinaturas, o PIN informado pelo usuário é verificado. Caso seja incorreto, não ocorre a comunicação com o *Web Service*.

4.7.2 DOCUMENTO ASSINADO

O documento assinado é um documento diferente do original, sendo cada um armazenado em um local diferente. Vários sistemas armazenam documentos, cada um a sua maneira, em diferentes esquemas ou tabelas. Tendo em vista a possibilidade de atender vários destes sistemas, o esquema ASSINATURA concentra os documentos assinados, enquanto que os originais permanecem a cargo de cada sistema, ou seja, quase nenhuma adaptação necessita ser realizada nestes sistemas.

Para evitar armazenar informações redundantes, foi projetada uma maneira de se economizar espaço do banco de dados. Desta forma, apenas as informações relevantes são armazenadas, como a assinatura (sequência de *bits*), o caminho até o documento original e o código localizador.

As assinaturas válidas são armazenadas no banco de dados na tabela DTT_OBJETO_ASSINADO do esquema ASSINATURA. Esta tabela possui os três campos mencionados acima, detalhados a seguir.

COD_LOCALIZADOR O código localizador é a chave primária da tabela. É uma *string* de 32 caracteres utilizada por qualquer pessoa que queira realizar uma consulta no Localizador, descrito na próxima seção.

DES_ASSINATURA Este campo armazena um objeto TransporteAssinaturaDTO que, como explicado anteriormente, contém um número identificador, o valor *hash* do documento assinado e a assinatura propriamente dita. Há apenas uma diferença deste objeto para aquele recebido pelo *Web Service* do cliente. No *Web Service*, a lista de caminhos para alcançar cada documento dentro do banco de dados é enviada como um parâmetro independente da lista de objetos TransporteAssinaturaDTO. No momento de gravação no banco de dados, entretanto, cada objeto TransporteAssinaturaDTO é atualizado para armazenar seu respectivo caminho até o documento original.

DES_ENDERECO_OBJETO Armazena o arquivo XML que indica o caminho, dentro do banco de dados, até o documento original (semelhante ao XML descrito na seção 4.7.1.2).

O documento final não é armazenado de forma permanente. Ele é montado apenas quando ocorre uma consulta ao Localizador, sendo armazenado na tabela

DTT_TMP_OBJETO_PDF. Esta tabela contém três campos, descritos a seguir.

COD_LOCALIZADOR É a chave estrangeira, aponta para um objeto da tabela DTT_OBJETO_ASSINADO.

DTA_GERACAO Informa a data em que este documento assinado foi montado.

DOC_PDF É o documento PDF contendo a tarja de assinatura.

Uma vez montado o documento assinado, ele permanece na tabela temporária indefinidamente. Quando desejado, os registros desta tabela temporária podem ser excluídos sem nenhum prejuízo para a assinatura, uma vez que as informações essenciais ficam armazenadas em tabela própria. Assim que uma nova consulta for realizada, um novo documento será montado e armazenado nesta tabela, caso não exista.

A forma do documento assinado pode ser observada na Figura 10, à direita. O documento é montado a partir de uma redução do documento original (à esquerda) e de uma tarja sobreposta ao rodapé de todas as páginas. Esta tarja informa todos os assinantes daquele documento, as respectivas datas de assinatura e o código localizador, para que a pessoa que recebê-lo possa validá-lo no Localizador.

4.7.3 SERVIDOR

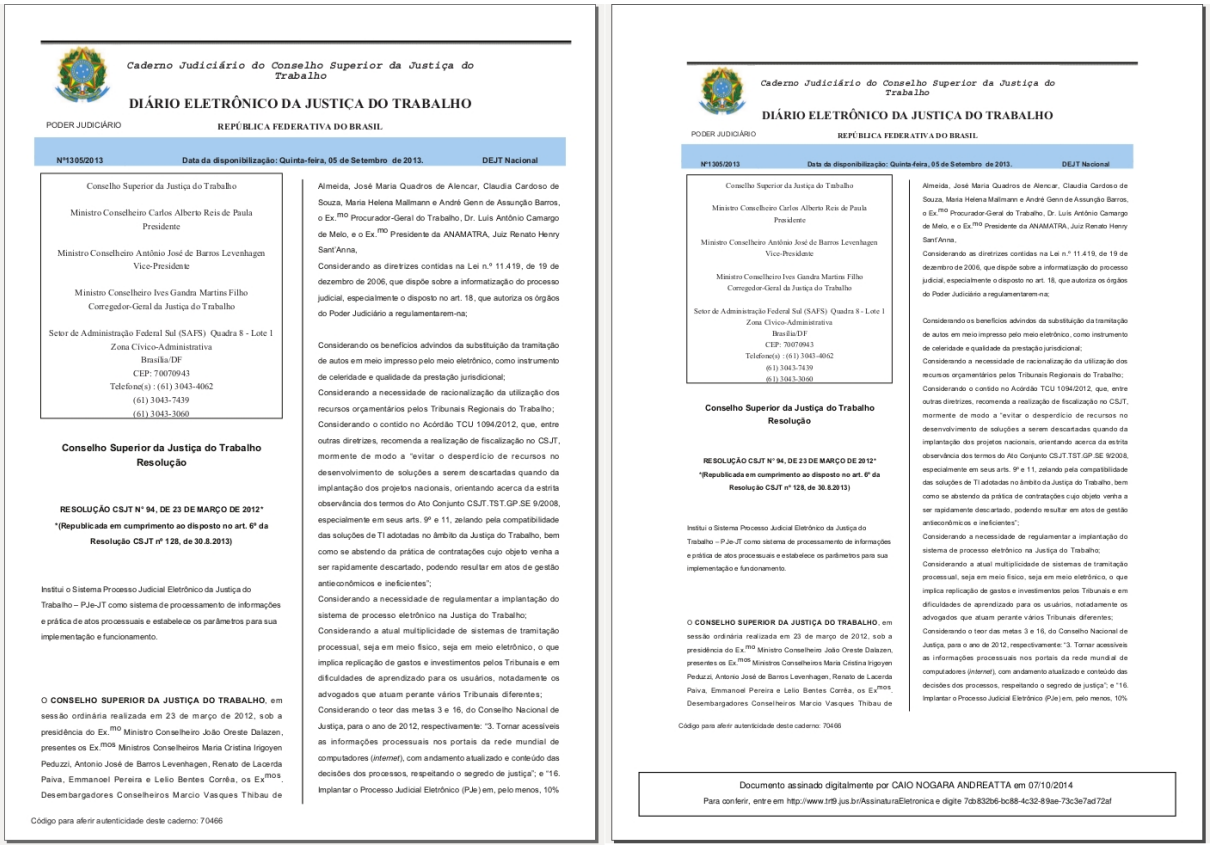
O lado servidor, como já apresentado, contém os serviços Localizador e Assinador, analisados nas seções seguintes.

4.7.3.1 LOCALIZADOR

Uma das finalidades fundamentais da Assinatura Digital é permitir que qualquer pessoa de posse de um documento digitalmente assinado possa verificar a autenticidade e a integridade deste documento. Em vista disso, o Localizador é um *Web Service* Java disponibilizado de forma pública em um sítio na *Internet* para que, ao informar um código localizador, a pessoa tenha acesso ao documento assinado, podendo comparar ambos os documentos.

Como explicado na seção 4.7.2, caso o documento assinado não exista, ele será criado no momento da consulta e será armazenado na tabela temporária.

Além das duas tabelas mencionadas, existe ainda uma terceira tabela no esquema ASSINATURA que armazena dados do usuário que realiza uma consulta no Localizador. A tabela



Caderno Judiciário do Conselho Superior da Justiça do Trabalho

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO — REPÚBLICA FEDERATIVA DO BRASIL

Nº1305/2013 — Data da disponibilização: Quinta-feira, 05 de Setembro de 2013. — DEJT Nacional

Conselho Superior da Justiça do Trabalho

Ministro Conselheiro Carlos Alberto Reis de Paula
Presidente

Ministro Conselheiro Antônio José de Barros Levenhagen
Vice-Presidente

Ministro Conselheiro Ives Gandra Martins Filho
Corregedor-Geral da Justiça do Trabalho

Setor de Administração Federal Sul (SAFS) Quadra 8 - Lote 1
Zona Cívico-Administrativa
Brasília/DF
CEP: 70070943
Telefone(s) : (61) 3043-4062
(61) 3043-7439
(61) 3043-3060

Conselho Superior da Justiça do Trabalho
Resolução

RESOLUÇÃO CSJT Nº 94, DE 23 DE MARÇO DE 2012*
***(Republicada em cumprimento ao disposto no art. 6º da Resolução CSJT nº 128, de 30.8.2013)**

Institui o Sistema Processo Judicial Eletrônico da Justiça do Trabalho – PJe-JT como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento.

O **CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO**, em sessão ordinária realizada em 23 de março de 2012, sob a presidência do Ex.mo Ministro Conselheiro João Oreste Dalazen, presentes os Ex.mos Ministros Conselheiros Maria Cristina Irigoyen Peduzzi, Antonio José de Barros Levenhagen, Renato de Lacerda Paiva, Emmanoel Pereira e Lelio Bentes Corrêa, os Ex.mos Desembargadores Conselheiros Marcio Vasques Thibau de Almeida, José Maria Quadros de Alencar, Claudia Cardoso de Souza, Maria Helena Mallmann e André Genn de Assunção Barros, o Ex.mo Procurador-Geral do Trabalho, Dr. Luis Antônio Camargo de Melo, e o Ex.mo Presidente da ANAMATRA, Juiz Renato Henry Sant'Anna,

Considerando as diretrizes contidas na Lei n.º 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, especialmente o disposto no art. 18, que autoriza os órgãos do Poder Judiciário a regulamentarem-na;

Considerando os benefícios advindos da substituição da tramitação de autos em meio impresso pelo meio eletrônico, como instrumento de celeridade e qualidade da prestação jurisdicional;

Considerando a necessidade de racionalização da utilização dos recursos orçamentários pelos Tribunais Regionais do Trabalho;

Considerando o contido no Acórdão TCU 1094/2012, que, entre outras diretrizes, recomenda a realização de fiscalização no CSJT, mormente de modo a "evitar o desperdício de recursos no desenvolvimento de soluções a serem descartadas quando da implantação dos projetos nacionais, orientando acerca da estrita observância dos termos do Ato Conjunto CSJT.TST.GP.SE 9/2008, especialmente em seus arts. 9º e 11, zelando pela compatibilidade das soluções de TI adotadas no âmbito da Justiça do Trabalho, bem como se abstendo da prática de contratações cujo objeto venha a ser rapidamente descartado, podendo resultar em atos de gestão antieconômicos e ineficientes";

Considerando a necessidade de regulamentar a implantação do sistema de processo eletrônico na Justiça do Trabalho;

Considerando a atual multiplicidade de sistemas de tramitação processual, seja em meio físico, seja em meio eletrônico, o que implica replicação de gastos e investimentos pelos Tribunais e em dificuldades de aprendizado para os usuários, notadamente os advogados que atuam perante vários Tribunais diferentes;

Considerando o teor das metas 3 e 16, do Conselho Nacional de Justiça, para o ano de 2012, respectivamente: "3. Tornar acessíveis as informações processuais nos portais da rede mundial de computadores (*internet*), com andamento atualizado e conteúdo das decisões dos processos, respeitando o segredo de justiça"; e "16. Implantar o Processo Judicial Eletrônico (PJe) em, pelo menos, 10%

Código para aferir autenticidade deste caderno: 70466

Documento assinado digitalmente por CAIO NOGARA ANDREATTA em 07/10/2014
Para conferir, entre em http://www.trt9.jus.br/AssinaturaEletronica e digite 7cb832b6-bc88-4c32-89ae-73c3e7ad72af

Figura 10: Forma do documento assinado.

Fonte: Autoria própria.

DTT_ACESSO_OBJETO_ASSINADO registra todos os acessos realizados por meio do Localizador. Os dados que são salvos estão descritos a seguir.

COD_LOCALIZADOR Código localizador do objeto assinado.

DTA_VISUALIZACAO Data em que houve a consulta ao objeto.

NOM_PESSOA Nome da pessoa que visualizou, caso esteja logada no sistema.

DES_IP_PESSOA Endereço IP do usuário que realiza a consulta.

NUM_OBJETO_ACESSO Número interno do acesso.

A relação entre Objetos e Acessos é de um-para-muitos, ou seja, para cada Objeto pode existir zero ou vários Acessos realizados.

Este registro tem por finalidade fornecer um critério adicional de segurança, pois estas informações podem ser úteis em eventuais disputas de autoria.

De acordo com o escopo do projeto, apenas arquivos do tipo HTML podem ser assinados. Para facilitar a visualização destes arquivos e para que fosse possível sobrepor a tarja com informações acerca da assinatura, o formato de arquivo PDF foi adotado como sendo o formato do documento assinado, ou seja, o documento final é um PDF gerado a partir da conversão do documento HTML para PDF e posterior adição da tarja. Foi utilizada a versão gratuita da biblioteca Java iText (ITEXT, 2014) para realizar as conversões HTML e manipulações de arquivos PDF.

Um exemplo deste processo pode ser observado na Figura 11. À esquerda, pode-se observar o documento original, visualizado por meio de um navegador *web*. O documento assinado no formato PDF é mostrado à direita.

Figura 11: Documento original HTML e documento assinado PDF resultante.
Fonte: Autoria própria.

4.7.3.2 ASSINADOR

Este serviço é requisitado pela parte cliente, recebendo os parâmetros que foram descritos anteriormente. Em síntese, o Assinador recebe um conjunto de dados do certificado do assinante; uma lista de localização de documentos; e uma lista de assinaturas, contendo também o valor *hash* utilizado na correspondente assinatura.

De posse destes parâmetros, o servidor realiza, para cada item da lista de localização de documentos, uma sequência de verificações para aceitar ou recusar o pedido de assinatura.

A primeira verificação é de permissão de assinatura. Essa verificação é realizada pela função FNC_PODE_ASSINAR_OBJETO do esquema ASSINATURA e toma como parâmetros o nome do usuário (contido no certificado recebido) e a localização do documento, também recebida pelo Assinador. Caso o usuário tenha permissão para assinar documentos da tabela indicada pelo parâmetro de localização de documentos, as verificações prosseguem. Caso contrário, é retornado erro para o usuário informando a restrição.

Não havendo erro, o servidor adquire a cadeia de certificados realizando consulta a uma Autoridade Certificadora, a partir dos dados contidos no certificado do usuário. Em seguida, são requisitadas LCR. O próximo passo é gerar um carimbo de tempo, obtido de uma consulta a uma PDDE de confiança, e adicioná-lo à assinatura, junto com a cadeia de certificados e as LCR. O objeto resultante é verificado pela biblioteca Assinejus. Caso a assinatura seja válida, uma mensagem de confirmação é retornada ao usuário, caso contrário, uma mensagem de erro é retornada informando em que parte da verificação houve falha.

Dentre as verificações realizadas, pode-se citar:

- comparação entre os valores *hash* recebido e calculado (que devem ser idênticos);
- verificação do carimbo de tempo em relação ao período de validade do certificado;
- verificação das LCR, se o certificado consta em alguma delas;
- verificação do certificado recebido, a partir da chave pública da Autoridade Certificadora indicada pelo próprio certificado; entre outras.

Após os processos de verificação, os dados da assinatura são salvos na tabela DTT_OBJETO_ASSINADO, como explicado na seção 4.7.2.

5 RESULTADOS

5.1 IMPLANTAÇÃO

A Assinatura Digital foi primeiramente implantada no sistema de Atas de Correição. Posteriormente, foi incluído no sistema de Oficiais de Justiça e no sistema de Controle de Tramitação Administrativa - CTA.

Nesta primeira implantação, as seguintes fases foram seguidas.

- Adaptação da tabela de documentos, para incluir o campo do código localizador e concessão de permissão ao esquema ASSINATURA para poder atualizá-lo.
- Adaptação da função FNC_PODE_ASSINAR_OBJETO do esquema ASSINATURA para conceder as devidas permissões de assinatura.
- Adaptação da página *web* que apresenta a lista de documentos passíveis de assinatura com adição de botões de ação (assinar, cancelar assinatura, entre outros) e *links* para *download* dos documentos assinados.
- Criação de referências, nesta mesma página, aos arquivos adicionais hospedados como recursos no *Web Service* (javascripts e arquivos de estilo) que devem ser carregados na requisição da página pelo navegador do usuário.

Estes passos foram os essenciais para a implantação da Assinatura Digital nas Atas de Correição e devem servir de base para as posteriores. Evidentemente que adaptações adicionais devem ser realizadas dependendo das restrições de negócio.

A implantação foi bem sucedida e ocorreu dentro do cronograma previsto.

5.2 PROBLEMAS ENCONTRADOS

O primeiro problema detectado, que trouxe dificuldade de aceitação do projeto pelos usuários das Atas de Correição, foi a conversão HTML para PDF. Apesar de a biblioteca iText

ser bastante estável, a formatação nem sempre é fiel ao documento original. Este problema ficou bem evidente na Figura 11, em que surgiu uma linha em branco no cabeçalho.

Outros problemas de formatação ocorreram na utilização de partes do texto em negrito, alinhamento de texto, tamanho de fonte, entre outros. A Figura 12 apresenta alguns destes erros. No documento à direita, em sua parte superior, algumas linhas de texto perderam a formatação em negrito. Já sua parte inferior, ainda à direita, é possível notar a perda do alinhamento das primeiras linhas de cada parágrafo, comparando-se com o documento original à esquerda. Apesar de ser incomum a ocorrência de tais erros, é facilmente percebida pelo usuário, que deseja fidelidade entre os documentos.

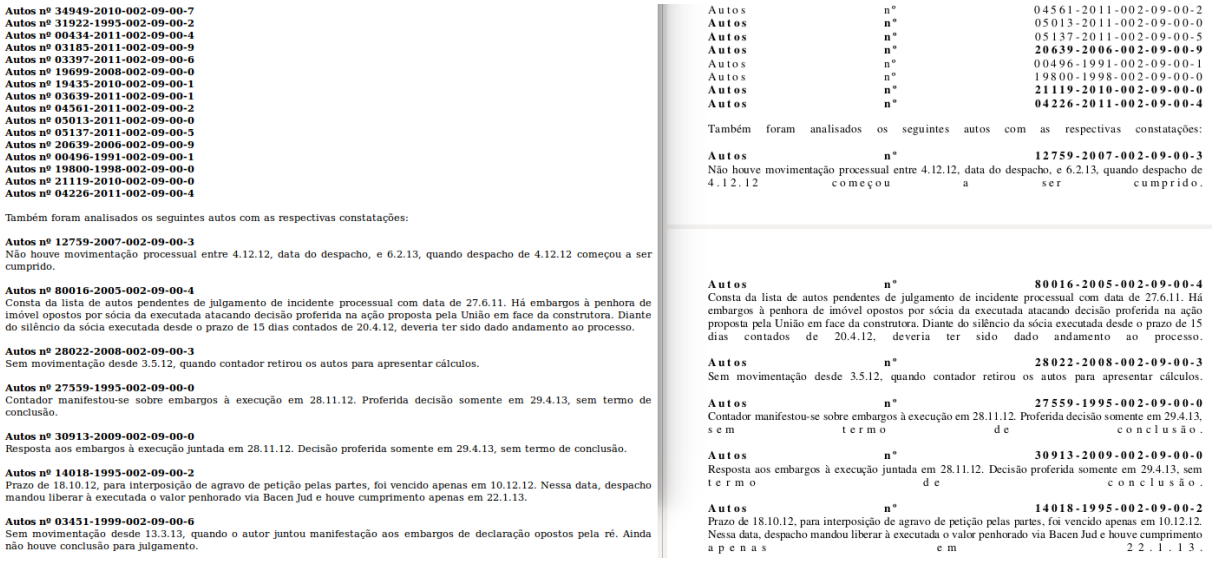


Figura 12: Problemas na conversão HTML (à esquerda) para PDF (à direita).
Fonte: Autoria própria.

Outro problema decorrente do uso de texto no formato HTML são as imagens utilizadas. Em um texto HTML, as imagens são referenciadas pelo marcador <img>, cuja URL é indicada pelo elemento *src* (e.g., <img src="http://www.endereco.com.br/imagem.jpg">). Grande parte dos editores de texto HTML utilizados nos sistemas administrativos permitem a utilização de imagens, desde que elas sejam disponibilizadas em uma pasta padrão no domínio do TRT9 (atualmente, só o Brasão da República está disponível).

A falha reside justamente na utilização de referências, pois o documento considerado para a assinatura digital, a princípio, é apenas o texto contido no documento HTML, e não os arquivos apontados por ele (como as imagens). Supondo que a imagem seja alterada, porém permaneça com o mesmo nome de arquivo e localização no servidor, o valor *hash* calculado do documento será o mesmo, pois o texto de referência à imagem continua o mesmo. Apesar de

ser um ambiente bastante controlado, em que o usuário não pode criar outras imagens e que, atualmente, apenas uma imagem seja utilizada, esta é uma falha que pode ser indetectável, caso alguém mal intencionado produza uma imagem com conteúdo suficientemente convincente.

O documento HTML original permanece vulnerável mesmo depois de assinado, pois o documento PDF contendo a assinatura (tarja) é apenas temporário, como explicado na seção 4.7.2.

A tarja foi a opção escolhida para não gerar uma quebra de paradigma muito grande para os usuários, já acostumados com outros sistemas (o próprio PJe, por exemplo) que utilizam tarjas sobrepostas ao documento original reduzido (observar redução resultante na Figura 10). Toda esta manipulação feita sobre o documento original pode suscitar questionamentos sobre a integridade do sistema de Assinatura Digital.

Do ponto de vista do usuário, é correto forçá-lo a confiar cegamente no sistema que manipula seu arquivo? Do ponto de vista do sistema, é correto realizar estas manipulações, fornecendo um documento que não é realmente o documento assinado?

Um dos efeitos colaterais da utilização desta redução e posterior sobreposição de tarja pode ser constatada na Figura 13. Este documento foi originalmente gerado como HTML e assinado. O documento PDF resultante foi inserido no sistema como se fosse um novo documento e assinado novamente. Este processo foi repetido sucessivas vezes, até que este documento anômalo fosse obtido.

Apesar de ser algo aparentemente esdrúxulo, o sistema não é capaz de reconhecer este tipo de documento no momento da assinatura, ou seja, não há, a princípio, como evitar que usuários façam este tipo de uso indevido, até mesmo para alcançar uma possível assinatura de múltiplos usuários em um sistema que eventualmente a restringe.

O sistema de Assinatura Digital foi projetado prevendo-se o uso de variados formatos de arquivo (.doc, .xls, .docx, entre outros). Contudo, nem todo arquivo pode ser convertido para PDF para posterior adição de tarja, como é o caso de planilhas de cálculo. O sistema de Assinatura Digital permite que seja criada uma lógica individual para cada formato, porém isso pode gerar uma despadronização. Deve-se converter para PDF tudo o que for possível para aplicar a tarja e o que não for, emitir recibo externo? Deve-se emitir recibo para qualquer tipo de arquivo, mesmo os que possam ser convertidos, considerando-se o impacto na comunidade de usuários?

Além destas questões mais próximas da área de negócios, foram constatadas três dificuldades técnicas. A primeira diz respeito à arquitetura dos servidores *web* do TRT9. No

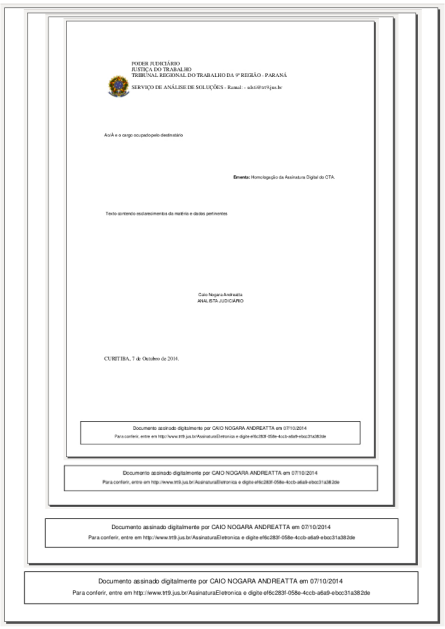


Figura 13: Efeito colateral de sucessivas assinaturas.
Fonte: Autoria própria.

domínio *www*, como já mencionado, ocorre autenticação por meio do CAS. Neste domínio ficam hospedados os *Web Services*, inclusive seus arquivos adicionais (*resources*). Por outro lado, os sistemas administrativos, a exemplo do sistema de Atas de Correição, são hospedados em outro domínio que não utiliza o CAS.

Em função das outras aplicações e serviços hospedados no domínio *www*, uma das configurações do CAS (o item *SSLVerifyClient*) exige que o usuário que esteja se conectando por meio do protocolo HTTPS e que esteja com seu *token* conectado em sua máquina seja identificado, ou seja, é solicitada a senha do *token* ao tentar acessar alguma página hospedada no domínio *www*.

Por esta configuração, quando o usuário acessa um sistema administrativo hospedado no domínio *Intranet* para tentar assinar um documento, os arquivos adicionais são baixados do domínio *www*, pois estão hospedados como recursos do *Web Service*. Neste momento em que eles são requisitados, para cada arquivo adicional é solicitada a senha do *token* do usuário, desde que ele esteja conectado no computador. Isso causa alguns problemas na usabilidade.

Primeiramente, para assinar um único documento o usuário acaba precisando digitar cinco vezes sua senha, uma para cada arquivo adicional e uma para a efetiva assinatura. Uma solução é remover o *token*, carregar a página da assinatura com os arquivos adicionais e depois

conectar o *token* novamente. Apesar de solucionar o problema, não é uma solução razoável, tendo em vista que vários documentos podem precisar ser assinados. Retirar e recolocar o *token* para cada um deles apenas dificulta o uso do sistema, fazendo o usuário perder muito tempo.

Outra solução para evitar solicitações múltiplas de senhas é requisitar os arquivos adicionais por meio do protocolo HTTP, ao invés do protocolo HTTPS. Esta solução funciona em versões anteriores dos principais navegadores, pois o carregamento de arquivos adicionais com HTTP em uma página HTTPS causa uma falha de segurança conhecida como *Cross-Site Scripting* (WIKIPEDIA, 2014a). Por esta razão, as versões mais atuais dos navegadores *web* bloqueiam qualquer tentativa de carregar, em uma página HTTPS, arquivos adicionais hospedados em um endereço HTTP. Para que seja possível utilizar esta solução, chega-se a um impasse: utilizar navegadores antigos e talvez desatualizados ou não carregar os arquivos, desta forma não permitindo a assinatura?

Uma alternativa seria hospedar uma cópia destes arquivos adicionais no mesmo domínio do sistema administrativo, ou seja, no domínio *Intranet* e criar as respectivas referências no lugar das referências aos recursos do *Web Service* (hospedados no domínio *www*, como explicado anteriormente). Um cuidado adicional durante a manutenção do sistema de Assinatura Digital seria o de manter estas cópias sempre atualizadas.

O segundo problema técnico decorre da versão Java do computador do usuário e da assinatura de código que deve ser realizada no arquivo JAR. A máquina virtual Java - JVM instalada no computador do usuário, depois de o navegador *web* baixar o JAR, verifica se o arquivo foi assinado com um certificado válido. A política de execução deste arquivo sofreu algumas alterações nas últimas atualizações da versão 7, o que exigiu manutenções emergenciais do sistema de Assinatura Digital.

Até a atualização 10 (Java 7u10), a política de segurança Java permitia a execução de código não assinado, apenas pedindo a confirmação do usuário (ORACLE, 2014a). Na atualização 7u10, foram implementados níveis de segurança, permitindo ao usuário alterar entre os níveis baixo, médio e alto. No nível baixo, ocorria o mesmo que nas versões anteriores, ou seja, antes de executar algum arquivo Java, a confirmação do usuário era solicitada. A partir do nível médio, as aplicações que não atendessem à política de segurança Java, ou seja, que não estivessem assinadas com um certificado válido, eram automaticamente bloqueadas (ORACLE, 2014a).

Na atualização 51 (Java 7u51) a execução de código não assinado, assinado com um certificado expirado, ou que não tenha algum atributo de segurança, é completamente bloqueada

(ORACLE, 2014b), ou seja, alterar o nível de segurança Java não possibilita sua execução.

A versão Java homologada para uso nos computadores do TRT9 é a versão 7 atualização 6. Realizando-se testes com atualizações mais recentes, descobriu-se que o certificado do arquivo JAR estava expirado e poderia causar problemas e até mesmo indisponibilidade da Assinatura Digital. Procedeu-se, desta forma, para nova assinatura de código para adequá-lo às novas políticas de segurança Java.

O terceiro questionamento técnico se deve ao formato de arquivo PDF, notório por ter certas debilidades na preservação de documentos, visto que possui referências externas semelhantes ao formato HTML (WIKIPEDIA, 2014d). Com vistas à preservação por longos períodos de tempo, foi desenvolvido um padrão ISO chamado PDF/A, em que estas referências externas devem ser embutidas no próprio documento (WIKIPEDIA, 2014d). Diante disso, deve-se conscientizar os usuários sobre o uso do PDF/A e abolir o PDF simples do sistema? Como adaptar os arquivos PDF já existentes no sistema?

5.3 MELHORIAS FUTURAS

As melhorias futuras podem ser divididas em dois grupos, as essenciais e as opcionais. Dentre as essenciais, é necessária uma avaliação sobre a manipulação dos arquivos originais, transformando-os em arquivos PDF. Uma solução que também facilitaria e padronizaria a assinatura de outros formatos de arquivo seria a utilização de arquivos de recibo com os dados da assinatura, ainda que seja uma quebra de paradigma para os usuários. Este recibo, de certa forma, retira a responsabilidade que o sistema de Assinatura Digital atualmente possui de manter a integridade e autenticidade do arquivo original ao convertê-lo para outro formato, como é o caso da conversão HTML para PDF em que parte da formatação é alterada. Além disso, haveria o benefício de economia de manutenções do sistema, uma vez que cada novo problema de formatação deve ser resolvido de forma particular, sem a garantia de que outros deixarão de surgir.

Em relação ao serviço de autenticação diferenciado entre os domínios utilizados, a alternativa de utilizar cópias dos arquivos adicionais se mostra uma solução razoável, tendo em vista que muitas aplicações dependem do respectivo serviço de autenticação e a modificação de algum destes serviços, a fim de evitar a solicitação múltipla de senha, pode implicar em uma manutenção generalizada dos demais sistemas para adequá-los à nova autenticação. Isto demandaria tempo e recursos, o que a simples cópia pode evitar.

Como melhoria opcional, pode-se citar a finalização da implementação de assinaturas

múltiplas, até mesmo antes da manifestação de interesse dos usuários. Outra melhoria opcional seria finalizar a implementação de outros formatos de arquivo, que ainda estão restritos ao HTML e ao PDF.

Assim como ocorre nos documentos HTML e PDF, as referências externas devem ser avaliadas em maior profundidade, tendo em vista o período de existência que estes arquivos porventura devam possuir (preservação dos documentos), bem como as possíveis falhas de segurança decorrentes. Alguns questionamentos que deveriam acompanhar a discussão são: deveria ser função do sistema garantir que estes arquivos com referências externas sejam acessíveis daqui a dez, vinte ou mais anos? Deveria ser permitido utilizar arquivos que possuem referências externas? Qual a validade de tais documentos?

Dada a utilização quase que unânime de editores e arquivos HTML pelos sistemas administrativos, proibir sua assinatura atualmente não é uma solução viável, de forma que deve haver uma solução diferente da proibição, ainda que de difícil concepção atualmente.

5.4 CONSIDERAÇÕES FINAIS

A Tecnologia da Informação é uma área em constante evolução e o desenvolvimento e posterior manutenção de sistemas devem ser vistos da mesma maneira, ou seja, não devem ser estáticos, finitos. Partindo-se deste ponto de vista, um dos objetivos deve ser a pró-atividade, em que problemas são identificados de forma preventiva e controlada e a solução disponibilizada para o usuário antes mesmo de ele encontrar tais problemas.

O presente Estudo de Caso buscou, de certa forma, colaborar com a manutenção preventiva do sistema de Assinatura Digital, levantando questionamentos e sugerindo alternativas antecipadamente a situações emergenciais ou demandas urgentes de usuários.

Apesar das questões apresentadas, as implantações posteriores foram, também, bem sucedidas, evidenciando a qualidade da solução desenvolvida, sua robustez e genericidade, objetivos essenciais do projeto.

A implantação da Assinatura Digital é de grande importância no âmbito de um órgão público, seja em seus sistemas voltados para a área fim, seja para os sistemas administrativos. Tendo em vista que estes sistemas contemplam desde documentos de Processos Administrativos Disciplinares (que envolvem as carreiras de servidores), documentos utilizados para gerenciar o orçamento do próprio órgão, pagamentos, até processos licitatórios, a segurança necessária e a garantia fornecida pela assinatura digital aos documentos envolvidos é evidente, pois a forja de qualquer um deles pode causar prejuízos ao Erário e até mesmo aos próprios servidores, sem

que a devida autoria seja identificada.

ANEXO A – CASOS DE USO

A.1 UCS_01_ASSINAR_DOCUMENTO

Este caso de uso é utilizado na assinatura de documentos.

A.1.1 ATOR

Magistrado(a) Corregedor(a).

A.1.2 REQUISITOS FUNCIONAIS

- A tarja deve ser igual a do modelo abaixo (Figura 14).
- Somente terá permissão para assinar um magistrado com perfil de corregedor.
- O usuário logado poderá não ser o mesmo que assinará a ata.
- O programa atual de “Edição de Ata” será alterado para não apresentar ao final do texto, o nome do Corregedor e os dois quadros de conferência.
- O programa atual será alterado para solicitar confirmação na opção “Excluir”.
- O programa atual será alterado para não ter mais a opção de “Publicação”, conforme figura apresentada.
- O programa atual será alterado incluindo-se um filtro para apresentar somente as “Atas em aberto” ou “Todas as atas”.

A.1.3 REQUISITOS NÃO FUNCIONAIS

- A assinatura da ata poderá ser realizada de qualquer lugar com acesso ao ambiente *web* do TRT9.

AUTORIA

Documento assinado com cerificado digital por Abreu Mota em 23/04/2012

Confira a autenticidade no sítio www.trt9.jus.br/processoeletronico – Código: 4M2C-R118-2918-7741

Figura 14: Modelo da tarja de assinatura.

Fonte: (TRT9, 2012d).

A.1.4 PRÉ-CONDIÇÕES

- A Ata de Correição deve estar finalizada e pronta para ser assinada.

A.1.5 FLUXO DE EVENTOS

A.1.5.1 FLUXO PRINCIPAL

1. Ator: Este caso de uso é iniciado quando o Ator acionar, através da Tela de Ata de Correição, o botão "Assinar" (Figura 15).

Figura 15: Tela de Atas de Correição - Detalhe para o botão "Assinar".

Fonte: (TRT9, 2012d).

2. Sistema: Exibe uma janela para obter os dados do certificado digital contidos no *token* do ator que irá assinar a Ata (Figura 16).

3. Ator: Insere o *token*, digita seu PIN e clica no botão "OK".

4. Sistema: Obtém os dados de identificação do *token* e o conteúdo da ata e gera o documento assinado em formato PDF e salva na base de dados.

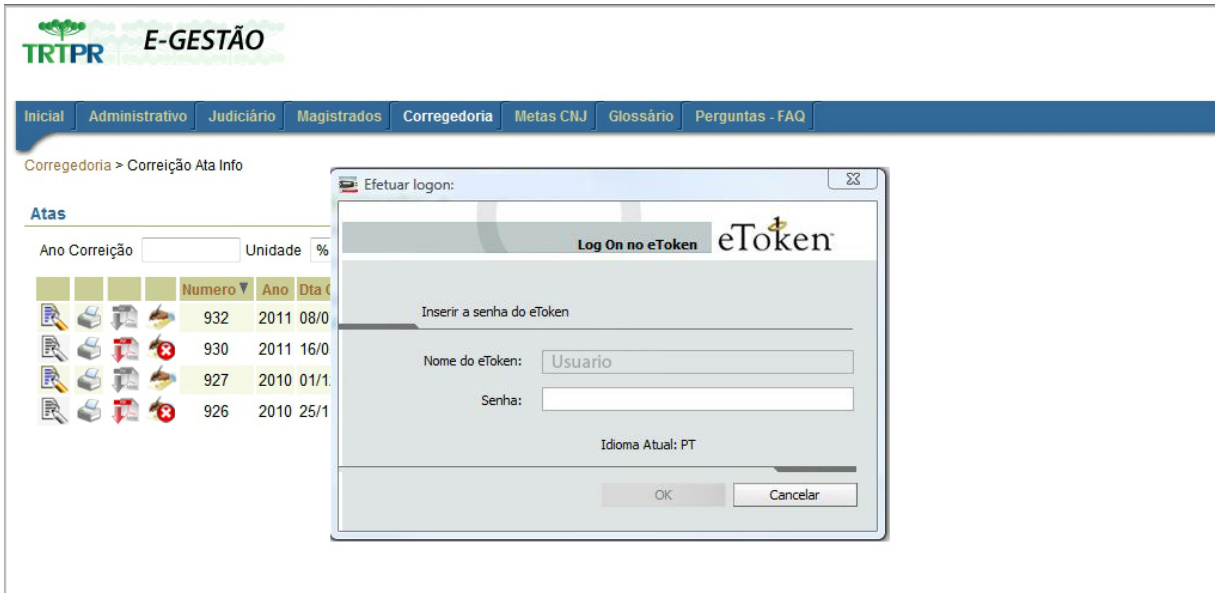


Figura 16: Tela de Atas de Correição - Dados e senha do certificado do Ator.

Fonte: (TRT9, 2012d).

5. Sistema: Exibe a mensagem “Documento assinado com sucesso” (Figura 17).

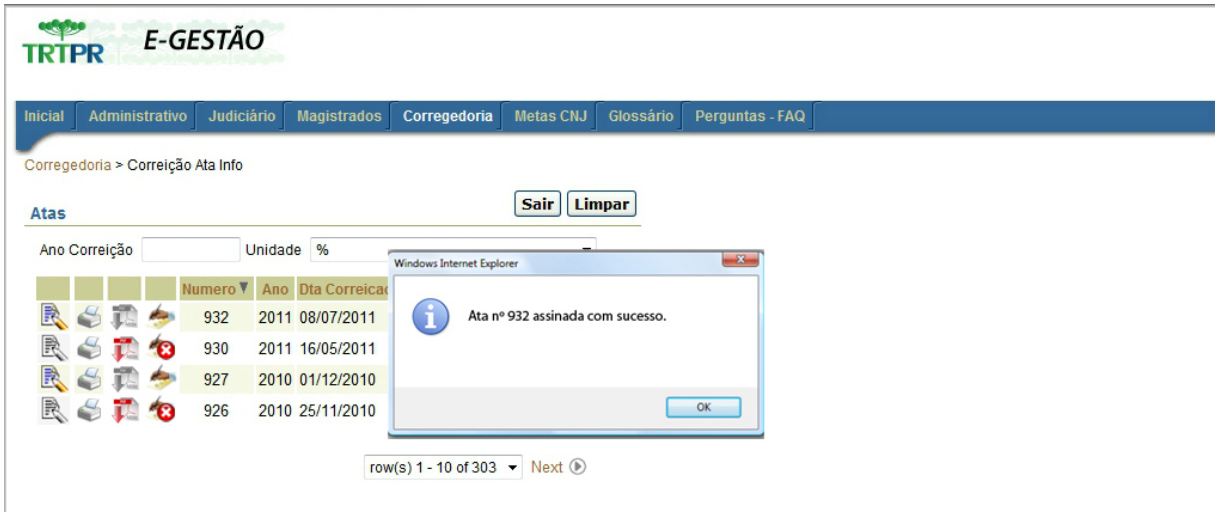


Figura 17: Tela de Atas de Correição - Assinatura realizada com sucesso.

Fonte: (TRT9, 2012d).

6. Fim do Fluxo Principal.

A.1.5.2 FLUXO ALTERNATIVO

A.1.5.2.1 ERRO AO ASSINAR DOCUMENTO

- Se o passo 3 do fluxo principal retornar erro:
  - Sistema: Exibe a mensagem de que ocorreu erro na assinatura do documento (Figura 18).
  - Sistema: Retorna ao passo 1 do fluxo principal.

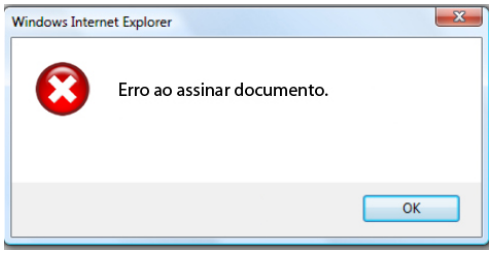


Figura 18: Erro ao assinar documento.
Fonte: (TRT9, 2012d).

A.1.6 PÓS-CONDIÇÕES

- A Ata estará assinada e não será mais permitida sua alteração (edição).
- Após a assinatura não serão mais exibidos os botões “Assinar” e “Editar” e serão exibidos os botões “Cancelar” e “Exibir PDF” (Figura 19).

Figura 19: Tela de Atas de Correição - Configuração após assinatura.
Fonte: (TRT9, 2012d).

A.2 UCS_02_LOCALIZAR_DOCUMENTO_ASSINADO

Este caso de uso é utilizado na localização de documentos assinados.

A.2.1 ATOR

Qualquer usuário.

A.2.2 FLUXO DE EVENTOS

A.2.2.1 FLUXO PRINCIPAL

1. Ator: Este caso de uso é iniciado quando o Ator acionar a página de localização de documentos assinados, que será disponibilizada no site do TRT9 (Figura 20).

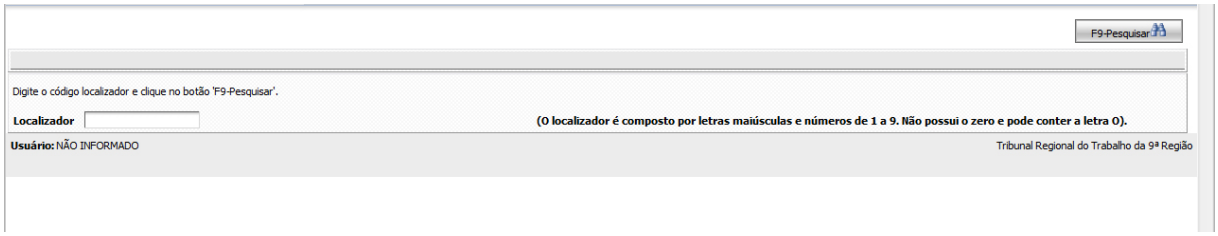


Figura 20: Tela do Localizador.
Fonte: (TRT9, 2012e).

2. Ator: Insere o número de controle constate na tarja de assinatura do documento a ser verificado e clica no botão “Localizar”.
3. Sistema: Recupera o documento na base de dados e exibe em formato PDF.
4. Fim do Fluxo Principal.

A.2.2.2 FLUXO ALTERNATIVO

A.2.2.2.1 DOCUMENTO NÃO ENCONTRADO

- Se no passo 2 do fluxo principal não localizar o código informado:
  - Sistema: Exibe mensagem “Documento não encontrado”.

A.3 UCS_03_CANCELAR_ASSINATURA

Este caso de uso é utilizado na assinatura de documentos.

A.3.1 ATOR

Usuário logado.

A.3.2 REQUISITOS FUNCIONAIS

- Todos os casos de cancelamento de assinatura devem ser registrados em Log.

A.3.3 REQUISITOS NÃO FUNCIONAIS

- Cancelar de qualquer lugar (não necessariamente de dentro da rede do TRT9).

A.3.4 PRÉ-CONDIÇÕES

- A Ata de Correição deve estar assinada.

A.3.5 PÓS-CONDIÇÕES

- A assinatura da Ata foi removida e será permitida sua alteração (torna-se editável novamente).
- Após a remoção da assinatura serão exibidos os botões “Assinar” e “Editar” e não serão exibidos os botões “Cancelar” e “Exibir PDF” (Figura 21).

Figura 21: Tela de Atas de Correição - Configuração após remoção da assinatura.
Fonte: (TRT9, 2012f).

A.3.6 FLUXO DE EVENTOS

A.3.6.1 FLUXO PRINCIPAL

1. Ator: Este caso de uso é iniciado quando o Ator acionar, através da Tela de Ata de Correição, o botão “Cancelar” (Figura 22).
2. Sistema: Exibe a mensagem: “Deseja cancelar a assinatura da Ata?” (Figura 23).
3. Ator: Clica no botão “OK”.
4. Sistema: Remove o PDF assinado da base e outros dados referentes à assinatura.
5. Sistema: Exibe a mensagem “Assinatura removida com sucesso” (Figura 24).

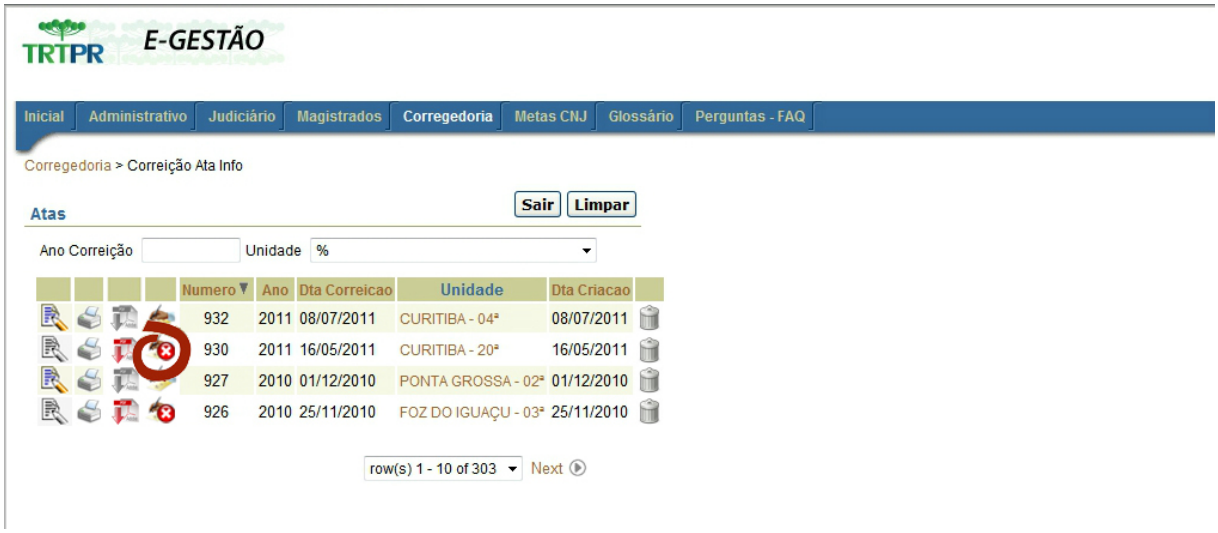


Figura 22: Tela de Atas de Correição - Detalhe para o botão "Cancelar".

Fonte: (TRT9, 2012f).

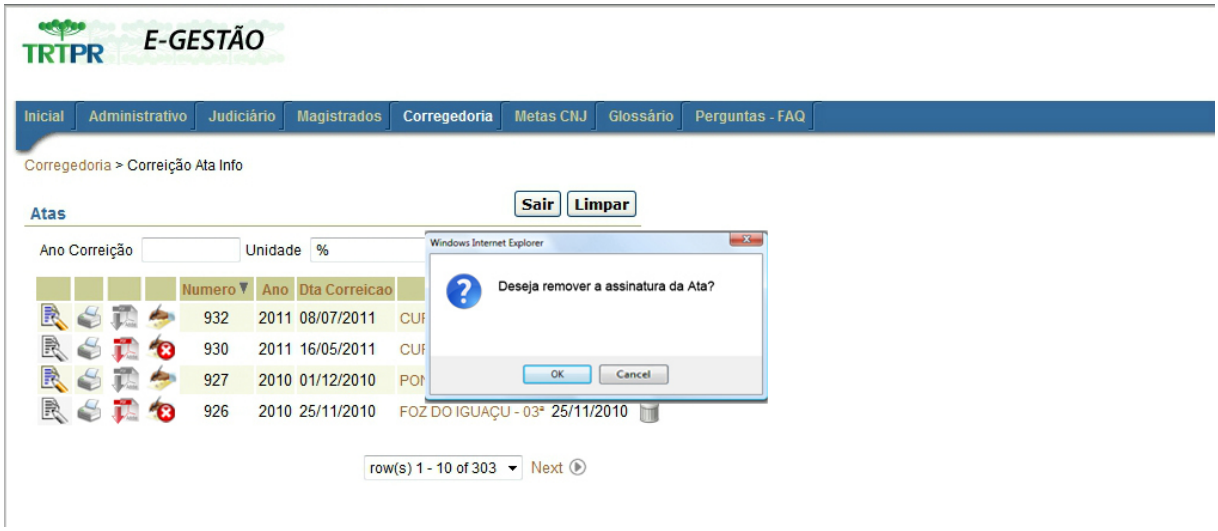


Figura 23: Tela de Atas de Correição - Confirmação de cancelamento.

Fonte: (TRT9, 2012f).

6. Fim do Fluxo Principal.

A.3.6.2 FLUXO ALTERNATIVO

A.3.6.2.1 ERRO AO REMOVER ASSINATURA

- Se o passo 3 do fluxo principal retornar erro:
  - Sistema: Exibe a mensagem de que ocorreu erro ao remover assinatura.

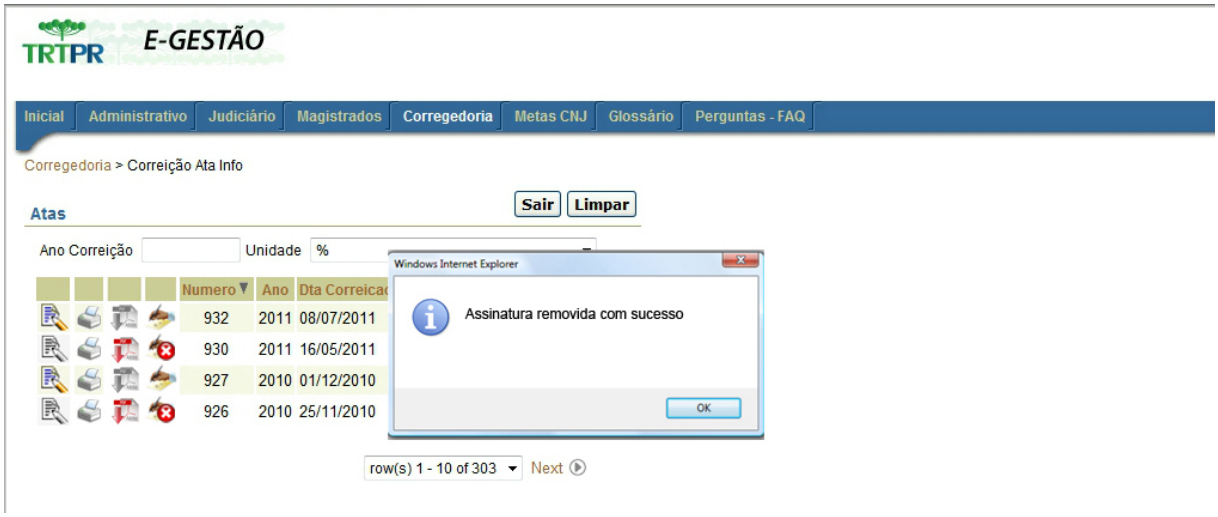


Figura 24: Tela de Atas de Correição - Mensagem de sucesso na remoção.
Fonte: (TRT9, 2012f).

– Sistema: Retorna ao passo 1 do fluxo principal.

A.3.6.2.2 CANCELAR REMOÇÃO DA ASSINATURA

- Se no passo 2 do fluxo principal o Ator clicar em “Cancelar”:
  – Sistema: Retorna ao passo 1 do fluxo principal.

A.4 UCS_04_EXIBIR_PDF

Este caso de uso é utilizado na assinatura de documentos.

A.4.1 PRÉ-CONDIÇÕES

- A Ata de Correição deve estar assinada.

A.4.2 ATOR

Usuário Logado.

A.4.3 FLUXO DE EVENTOS

A.4.3.1 FLUXO PRINCIPAL

1. Ator Este caso de uso é iniciado quando o Ator acionar, através da Tela de Ata de Correição, o botão “Exibir PDF” (Figura 25).

Figura 25: Tela de Atas de Correição.

Fonte: (TRT9, 2012g).

2. Sistema: Exibe o PDF gerado na assinatura com a tarja referente à ata selecionada.

3. Fim do Fluxo Principal.

A.4.3.2 FLUXO ALTERNATIVO

A.4.3.2.1 ERRO AO EXIBIR PDF

- Se o passo 2 do fluxo principal retornar erro:
  - Sistema: Exibe a mensagem “Erro ao exibir PDF”
  - Sistema: Retorna ao passo 1 do fluxo principal.

REFERÊNCIAS

CANADA, M. of Justice of. **Personal Information Protection and Eletronic Documents Act**. 04 2000. Disponível em: <http://laws-lois.justice.gc.ca/eng/acts/p-8.6>. Acesso em: 8 de setembro de 2014.

COMMERCE, U. of. **Digital Signature Standard (DSS)**. 07 2013. Disponível em: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>. Acesso em: 20 de setembro de 2014.

FOWLER, M. **LocalDTO**. 2004. Disponível em: <http://martinfowler.com/bliki/LocalDTO.html>. Acesso em: 06 de outubro de 2014.

FUNDATION, A. **Enterprise Single Sign-On**. 2014. Disponível em: <http://jasig.github.io/cas/4.0.0/index.html>. Acesso em: 3 de novembro de 2014.

GOVERNMENT, U. **GPE Act, Sec. 1710 definitions**. 09 1999. Disponível em: <http://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm>. Acesso em: 9 de setembro de 2014.

GOVERNMENT, U. **ESIGN Act. Sec. 106 definitions**. 06 2000. Disponível em: <http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/html/PLAW-106publ229.htm>. Acesso em: 9 de setembro de 2014.

GOVERNMENT, U. **Code of Federal Regulations (annual edition) Title 21—Food and Drugs**. 04 2011. Disponível em: <http://www.gpo.gov/fdsys/granule/CFR-2011-title21-vol1/CFR-2011-title21-vol1-sec11-3>. Acesso em: 9 de setembro de 2014.

HARRIS, S. **CISSP All-in-One Exam Guide**. Third edition. [S.l.]: McGraw-Hill, 2005. (All-in-One).

IETF, T. I. E. T. F. **Internet Security Glossary**. Maio 2000. Disponível em: <https://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 2 de novembro de 2014.

IETF, T. I. E. T. F. **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**. 05 2008. Disponível em: <http://tools.ietf.org/html/rfc5280>. Acesso em: 1 de novembro de 2014.

ITEXT, P. P. S. **About**. 2014. Disponível em: <http://itextpdf.com/about>. Acesso em: 13 de outubro de 2014.

ITI, I. N. de Tecnologia da I. **VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL - DOC-ICP-15**. 2.1. ed. [S.l.], Julho 2012.

ITI, I. N. de Tecnologia da I. **ICP-Brasil - O que é**. 2014. Disponível em: <http://www.iti.gov.br/icp-brasil>. Acesso em: 31 de outubro de 2014.

ITI, I. N. de Tecnologia da I. **Repositório**. 11 2014. Disponível em: <http://www.iti.gov.br/noticias/144-icp-brasil/repositorio/113-repositorio>. Acesso em: 1 de novembro de 2014.

ITI, I. N. de Tecnologia da I. **Sobre Carimbo de Tempo**. 2014. Disponível em: <http://www.iti.gov.br/perguntas-frequentes/>. Acesso em: 23 de setembro de 2014.

ITU, I. T. U. **Recommendation X.509 (10/12)**. 2012. Disponível em: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>. Acesso em: 28 de outubro de 2014.

JUSTIçA, C. N. de. **Certificação digital: você já tem a sua?** 2014. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/sistemas/processo-judicial-eletronico-pje/certificacao-digital>. Acesso em: 27 de setembro de 2014.

JUSTIçA, C. N. de. **Processo Judicial Eletrônico (PJe)**. 2014. Disponível em: <http://www.cnj.jus.br/programas-de-a-a-z/sistemas/processo-judicial-eletronico-pje>. Acesso em: 27 de setembro de 2014.

LABORATORIES, R. **PKCS 12 v1.0: Personal Information Exchange Syntax**. 1999. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf>. Acesso em: 1 de novembro de 2014.

NIST, N. I. of S. a. T. **Introduction to Public Key Technology and the Federal PKI Infrastructure**. 02 2001. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>. Acesso em: 9 de setembro de 2014.

ORACLE. **How do I control when an untrusted applet or application runs in my web browser?** 2014. Disponível em: <https://www.java.com/en/download/help/jcp_security.xml>. Acesso em: 6 de novembro de 2014.

ORACLE. **Why are Java applications blocked by your security settings with the latest Java?** 2014. Disponível em: <https://www.java.com/en/download/help/java_blocked.xml>. Acesso em: 6 de novembro de 2014.

REPúBLICA, S. para Assuntos Jurídicos Casa Civil Presidência da. **Medida Provisória Nº2200-2, 24 de agosto de 2001.** 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 31 de outubro de 2014.

SAFENET, I. **eToken PRO**. 2014. Disponível em: <http://www.safenet-inc.com/multi-factor-authentication/authenticators/pki-usb-authentication/etoken-pro/>. Acesso em: 1 de novembro de 2014.

STALLINGS, W. **Cryptography and Network Security - Principles and Practice**. Fifth edition. [S.l.]: Prentice Hall, 2010.

TRABALHO, C. S. da Justiça do. **Sobre o PJe-JT - Histórico**. 2014. Disponível em: <http://www.csjt.jus.br/historico>. Acesso em: 27 de setembro de 2014.

TRT9, S. de Desenvolvimento de Soluções em TI do. **Projeto Assinatura Eletrônica de Atas de Correição - Plano Integrado de Projeto**. 2012.

TRT9, S. de Desenvolvimento de Soluções em TI do. **Status Report 02 - Atas de Correição**. 2012.

TRT9, S. de Desenvolvimento de Soluções em TI do. **Status Report 05 - Atas de Correição**. 2012.

TRT9, S. de Desenvolvimento de Soluções em TI do. **UCS_01_Assinar_Documento**. 2012.

TRT9, S. de Desenvolvimento de Soluções em TI do. **UCS_02_Localizar_Documento_Assinado**. 2012.

TRT9, S. de Desenvolvimento de Soluções em TI do. **UCS_03_Cancelar_Assinatura**. 2012.

TRT9, S. de Desenvolvimento de Soluções em TI do. **UCS_04_Exibir_PDF**. 2012.

WIKIPEDIA. **Cross-Site Scripting**. 2014. Disponível em: <http://en.wikipedia.org/wiki/Cross-site_scripting>. Acesso em: 6 de novembro de 2014.

WIKIPEDIA. **Cryptographic Hash Function**. 2014. Disponível em: <http://en.wikipedia.org/wiki/Cryptographic_hash_function>. Acesso em: 20 de setembro de 2014.

WIKIPEDIA. **Digital Signature**. 2014. Disponível em: <http://en.wikipedia.org/wiki/Digital_signature>. Acesso em: 23 de setembro de 2014.

WIKIPEDIA. **PDF/A**. 2014. Disponível em: <http://en.wikipedia.org/?title=PDF/A>. Acesso em: 8 de novembro de 2014.

WIKIPEDIA. **PKCS 12**. 2014. Disponível em: <http://en.wikipedia.org/wiki/PKCS_12>. Acesso em: 1 de novembro de 2014.

WIKIPEDIA. **X.509**. 2014. Disponível em: <http://en.wikipedia.org/wiki/X.509>. Acesso em: 31 de outubro de 2014.