DOI: 10.5748/16CONTECSI/SEC-6166

IMPLEMENTATION OF A SOLUTION WITH IDENTIFICATION BY FINGERPRINT AND SHAMIR'S IDENTITY-BASED SIGNATURE IN ELECTRONIC DOCUMENTS

Eduardo Takeo Ueda - IPT - Instituto de Pesquisas Tecnológicas - edutakeo@usp.br
Antonio CARLOS DIAS Lino - Instituto Pesquisas Tecnológicas - adiaslino@uol.com.br

Abstract. The integrity of the information, the process traceability and the authenticity of the human resources involved in the validation of the Completion Works (TCC) and Supervised Internship are essential requirements for the students to have access to the high school diploma integrated with the technician. This work proposes the development of an applied research making possible the creation of a prototype, which allows the digital signature of PDF files using the identity-based signature scheme proposed by Adi Shamir (1984), with fingerprint recognition, collaborating for the increase of process productivity, authenticity and irretratability of the employees and the integrity of the information that constitute the motivation of this article.

Key-words: Identity-Based Signature, Public Key Infrastructure, Biometrics, Identity Based Encryption.

Implementação de uma Solução com Identificação por Impressão Digital e Assinatura Baseada em Identidade de Shamir em Documentos Eletrônicos.

Resumo. A integridade das informações, a rastreabilidade do processo e a autenticidade dos recursos humanos envolvidos na validação dos Trabalhos de Conclusão de Curso (TCC) e Estágio Supervisionado são quesitos imprescindíveis para que discentes possam ter acesso ao diploma de conclusão do ensino médio integrado ao técnico. Este trabalho propõe o desenvolvimento de uma pesquisa aplicada tornando possível a criação de um protótipo, o qual permite a assinatura digital de arquivos PDF utilizando o esquema de assinatura baseada em identidade proposto por Adi Shamir (1984), com reconhecimento por impressão digital, colaborando para o aumento da produtividade do processo, autenticidade e irretratabilidade dos funcionários e a integridade das informações as quais constituem a motivação deste artigo.

Palavras-chave: Assinatura baseada em identidade, Infraestrutura de Chave Pública, Biometria, Criptografia baseada em identidade.

1. Introdução

A criptografia permite a troca de mensagens entre duas partes, de forma que uma ação mal intencionada provocada por alguém que não esteja inserida no contexto desta troca não tenha condições de acessar o conteúdo das mensagens. Dê acordo com Choudhury (2002, p. 29) “Confiança é a base de toda a comunicação, seja ela física ou eletrônica”. Na comunicação física, a construção da relação de confiança é algo relativamente fácil tendo em vista que é possível identificar a entidade ou pessoa através das interações face-a-face ou por meio de outras formas de identificação, como assinaturas, selos de tabelião, ou mesmo papel timbrado. Como a utilização da Internet aumenta exponencialmente, as aplicações em geral representam hoje uma importante forma de interação na grande rede, sendo que estas aplicações são dependentes de um fluxo bidirecional de trocas de dados entre o servidor e o cliente. A segurança torna-se um requisito indispensável nas aplicações em que se faz necessário o tráfego de informações confidenciais mantendo a integridade, confidencialidade e autenticidade. Assim este artigo tem o propósito de apresentar uma pesquisa aplicada, que visa produzir um sistema utilizando impressão digital para assinatura baseada em identidade, permitindo a identificação de usuários, assinatura digital e o armazenamento seguro de informações.

Este artigo está organizado como descrito a seguir: A Seção 2 apresenta a metodologia utilizada no desenvolvimento deste artigo. A Seção 3 apresenta conceitos sobre criptografia simétrica e assimétrica, a criptografia de chaves públicas, assinatura digital, hash e biometria. Na Seção 4 são apresentados os principais trabalhos relacionados que tratam de assinatura digital e biometria. Na Seção 5 são apresentadas as principais atividades relacionadas ao desenvolvimento da proposta elencando o modelo conceitual, arquitetura da aplicação e fluxograma dos processos envolvidos. Na Seção 6 são apresentados os aspectos de desenvolvimento da aplicação como: Biblioteca GMP responsável pela geração de números primos grande, o esquema de assinatura baseada em identidade, quadros comparativos dos processos de geração de chaves, assinatura e verificação de assinaturas de arquivos PDF através do algoritmo proposto por Adi Shamir (1984) e o processo de registro e verificação de impressão digital. Na Seção 7 é apresentada análise de resultados com a definição das métricas utilizadas no processo de validação da aplicação e os resultados obtidos após a interação de usuários e finalmente, na Seção 8 é apresentada a conclusão com as contribuições do sistema.

2. Metodologia

A metodologia consiste de quatro fases principais, conforme Figura 1, a seguir.

Figura 1 - Metodologia da Pesquisa



Pesquisa Bibliográfica.	Análise dos aspectos conceituais sobre o tema.	**Parte 1** Pesquisa Aplicada. -Aspectos de desempenho. -Aspectos de Segurança. **Parte 2** Pesquisa Teórica. -Aspectos de desempenho. -Aspectos de segurança.	**Parte 1** Arquitetura da proposta. **Parte 2** Implementação da proposta. **Parte 3** Análise dos resultados.

Fonte: Elaborado pelos Autores

O método de trabalho para desenvolvimento da pesquisa deste artigo foi estruturado em quatro fases, sendo a fase 1, a pesquisa bibliográfica; a fase 2, a análise dos aspectos conceituais; a fase 3, a análise de trabalhos relacionados e a fase 4, a arquitetura da proposta, implementação e análise dos resultados.

3. Referencial Teórico

3.1 Infraestrutura de chaves públicas

A Infraestrutura de Chaves Públicas (ICP) é um conjunto de hardware, software, pessoas e processos que permite a gestão dos certificados digitais. Para Buchmann et al. (2013), o propósito da ICP é fornecer provas de autenticidade de chaves públicas e controlar acessos indevidos durante seu ciclo de vida. A ICP se propõe a resolver problemas subjacentes de segurança, entre o mundo físico e o mundo eletrônico, permitindo que se possa confiar nas transações realizadas. Em Misaghi (2008), uma ICP possui recursos que contribuem para alcançar confidencialidade, irretratabilidade e autenticidade com uma estrutura confiável, entretanto, conforme a demanda pelos serviços oferecidos pela ICP aumenta, torna-se mais complexo manter esta estrutura. Esse crescimento contribui para o surgimento de problemas como revogação de certificados, custos de emissão de certificados, custo computacional durante a fase de validação dos certificados e armazenamento, apresentando-se como um desafio a ser superado.

3.2 Criptografia simétrica

A criptografia simétrica possibilita transformar uma mensagem de texto legível em texto cifrado utilizando uma chave secreta. Esta chave secreta é de conhecimento das partes envolvidas na comunicação (remetente e destinatário), as quais utilizarão para ciframento e deciframento da mensagem. Segundo Karamanian et al. (2011), a vantagem de utilizar a criptografia simétrica está relacionada a sua simplicidade, colaborando para seu bom desempenho, entretanto, uma grande desvantagem refere-se ao compartilhamento da chave secreta que deve ser de conhecimento de ambas as partes.

3.3 Criptografia assimétrica

Na criptografia de chave assimétrica presente em uma Infraestrutura de Chave Pública (ICP), duas pessoas que não se conhecem e precisam se comunicar de forma privada na Internet, podem fazê-lo resguardando os requisitos básicos de segurança (autenticidade, integridade e confidencialidade). Vamos considerar como exemplo o usuário Bob que necessite enviar uma mensagem confidencial para a usuária Alice. Poderíamos tentar usar criptografia de chave simétrica para permitir a comunicação confidencial entre Bob e Alice, porém, quando Bob publica uma chave simétrica em um diretório *on-line*, qualquer pessoa que tenha acesso a esse diretório, terá acesso a essa chave e poderá decifrar todas as mensagens criptografadas, independentemente de Alice, que seria o destinatário da mensagem.

3.4 Funções hash

Conforme descrito por Carlos et al. (2010), uma função resumo, conhecida como função hash, é uma função matemática que permite transformar um conjunto de dados qualquer como entrada para uma função (H), em uma pequena sequência de dados de tamanho fixo (resumo criptográfico). Essa sequência permite identificar um arquivo ou informação unicamente, como por exemplo, se uma determinada mensagem que originou um resumo criptográfico for submetida a alguma alteração durante a fase de comunição entre duas partes, será possível identificar uma ação maliciosa na mensagem transmitida quando esta for submetida novamente a função (H), gerando um resumo diferente do original. Outra característica importante referente às funções resumo, é que não deve ser possível obter a informação original a partir de um hash, ou seja, tais funções devem ser unidirecionais.

Como a sequência do hash é limitada (128, 256, 512 bits etc), podem existir colisões (sequências iguais para entradas diferentes) e quanto maior a dificuldade de colisões serem descobertas, mais eficiente é o algoritmo.

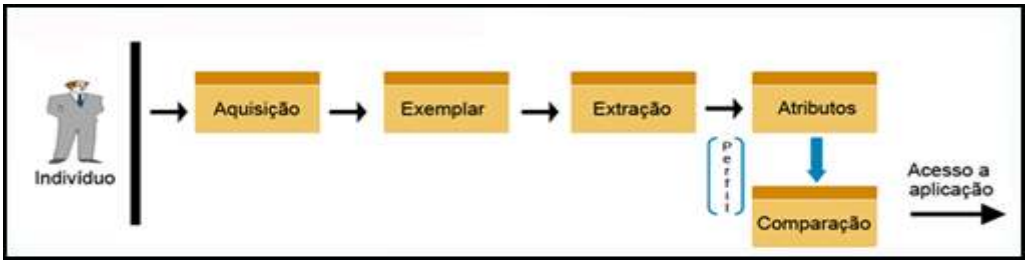
3.5 Assinatura digital

Em um esquema de assinatura digital, utiliza-se uma chave secreta (chave privada) para assinar digitalmente um documento e a verificação desta assinatura será feita utilizando uma chave pública. As assinaturas digitais são utilizadas para provar a autenticidade e integridade dos dados. Além disso, a assinatura digital oferece autenticação e pode conferir irretratabilidade e, devido a essas inúmeras aplicações, as assinaturas digitais são extremamente importantes nas comunicações eletrônicas. Para Carlos et al. (2010), a utilização da assinatura digital gera uma prova de quem é o autor, ou emissor, da mensagem, além de prover integridade e irretratabilidade. O processo de assinatura consiste em gerar o resumo criptográfico da mensagem e criptografar com a chave privada do assinante. Para a verificação de uma assinatura digital, é necessário verificar a assinatura usando a chave pública do assinante e comparar o resultado dessa operação com o resumo do documento original.

3.6 Biometria

A tecnologia da informação e comunicação (TIC) evolui a passos largos e a forma como as pessoas se comunicam e realizam transações eletrônicas estão cada vez mais presentes no dia-a-dia. O interesse pela tecnologia biométrica aumenta a cada dia e vem contribuindo para o crescimento de aplicações baseadas em biometria. A tecnologia biométrica apresenta características que eleva o nível de segurança na validação da identidade de usuários, fornecendo recursos para a realização de operações eletrônicas, agregando confiabilidade e eficiência. A Figura 2 apresenta o modelo de um sistema biométrico.

Figura 2 – Modelo conceitual do sistema biométrico.



Fonte: Elaborado pelos autores, adaptado de (Pinheiro, 2008, p.44).

O modelo conceitual apresenta as fases de “Aquisição e Exemplar”, que trata da obtenção das características biométricas, “Extração e Atributos”, que trata da produção da imagem denominado “Template” e “Comparação” responsável pela verificação do grau de similaridade entre as características extraídas.

4 Trabalhos Relacionados

Durante a fase de pesquisa bibliográfica buscou-se na literatura trabalhos publicados sobre a temática deste artigo, permitindo analisar os aspectos abordados e a identificação de oportunidades. A atividade de análise possibilitou ainda, além de compreender melhor os conceitos e práticas abordados pelos autores, evitar a duplicação de pesquisas sob o mesmo enfoque. Os principais trabalhos foram classificados em duas categorias, a saber: Pesquisa teórica e Pesquisa aplicada.

4.1 Pesquisa Teórica

Goya (2011) apresentou a evolução dos sistemas de criptografia, tratando inicialmente da proposta de Diffie e Hellman (1976), com o surgimento da criptografia de chave pública denominada assimétrica utilizando um par de chaves (pública e privada), e que a legitimação da chave pública apresentava-se como um problema. Como premissa, foi afirmado que a chave pública é certificada estando vinculada a seu dono e a solução encontrada foi o surgimento de um modelo chamado Infraestrutura de Chave Pública (ICP), cuja responsabilidade seria o gerenciamento de certificados associados à chave pública. Foi ressaltado que este modelo apresenta problemas como, a complexidade de implantação e manutenção, custo na emissão, distribuição, armazenamento e revogação de certificados e os custos associados no processo de recuperação e validação de certificados. Baseado nos problemas encontrados em uma ICP Goya(2011) propõe a utilização de modelos alternativos, mais especificamente o modelo proposto por Al-Riyami e Paterson (2003) conhecido como criptografia de chave pública sem certificado ou *certificateless* associado ao desenvolvimento de protocolos, em que a autenticidade fosse um requisito aplicado a este modelo.

Colombo et al. (2013) apresentaram conceitos sobre biometria e sua relevância ao elevar o nível de segurança e velocidade em determinadas atividades utilizando as características físicas de cada indivíduo. Conforme Colombo et al. (2013), a característica do indivíduo é capturada por um sensor no formato analógico e convertida em uma imagem digital, a qual posteriormente será comparada com um modelo biométrico armazenado utilizando um algoritmo responsável por validar a

identidade do indivíduo. Em sua conclusão, Colombo et al. (2013), afirma que a biometria é capaz de identificar as pessoas permitindo o acesso a informação e locais específicos. Formas tradicionais de identificação através de senhas, cartões magnéticos, entre outras, são comumente utilizadas, porém, o ser humano possui características únicas que são perfeitas para sua identificação. A biometria vem ganhando mercado no mundo digital, onde todos estão conectados em rede, oferecendo maior controle e confiança no acesso a informação.

Moraes (2011) destaca que as técnicas biométricas contribuem com benefícios para a segurança de um sistema a partir da identificação de um indivíduo, baseando-se em suas características físicas e comportamentais. Segundo Moraes (2011), não existe um sistema biométrico exato e que na impressão digital, vários são os fatores que contribuem para isto como: iluminação ambiental, condição física da pele, entre outras. Em sua proposta, Moraes (2011) avalia a exatidão que um sistema biométrico poderá apresentar e para isto utilizou quatro leitores digitais, sendo que dois destes dispositivos apresentam evolução no processo de captura: um aplica a leitura por multiespectro de luz e o outro, utiliza uma fina película de silicone sobre sua lente. A avaliação das variações do sistema biométrico foi delineada em um experimento fracionado, baseado na abordagem de matrizes ortogonais presentes no método Taguchi.

4.2 Pesquisa Aplicada

Em Misaghi (2008), é tratado o modelo de criptografia que utiliza os dados pessoais na geração de chaves e cifras, denominadas criptografia baseada em identidade, dispensando o uso de certificados. Foram demonstrados vários modelos de ciframento, assinatura e acordo de chaves, descritos os pré-requisitos de um ambiente de criptografia baseado em identidade que permita realizar operações de ciframento, assinatura e acordo de chaves com o menor custo computacional. Foi ressaltado o momento da pesquisa (2008) e a evolução dos criptosistemas baseados em identidade, os critérios necessários para este ambiente criptográfico e as possibilidades de aplicação nas operações de ciframento, assinatura e acordo de chaves.

Em Chen et al. (2009), foi proposto o projeto e implementação do modelo ID-Based Encryption (IBE) para autenticação em Object-Based Storage System (OBSS). O OBSS é um modelo de armazenamento de dados distribuído de alto desempenho, apresenta facilidade de expansão, proporciona acesso a milhares de usuários e como forma de garantir a segurança no acesso a informações, estes usuários devem estar autenticados validando sua identidade. Conforme explica Chen et al. (2009), o alto

custo e a complexidade de gerenciamento encontrados no modelo convencional de autenticação utilizando certificados digitais, inviabiliza sua utilização em muitos casos e aponta como uma alternativa a ser considerada o modelo IBE, abordando suas principais características propondo o projeto da solução e implementação.

Silveira (2013) estuda a criptografia baseada em identidade com o objetivo de criar um sistema utilizando mecanismo de autenticação através de um cartão de identificação eletrônica, permitindo o uso das características de identidade presentes no cartão, ciframento e deciframento de arquivos. O autor justifica o projeto embasado no aumento pela procura de soluções que possam garantir a privacidade e confidencialidade de dados. O sistema deverá permitir o ciframento de arquivos com múltiplas identidades (chave pública), sendo que o ciframento será efetuado sem a necessidade de compartilhamento prévio de chaves, utilizando a identidade do usuário como chave pública. Uma terceira entidade será responsável por gerar a chave privada, na qual deverá estar depositada a confiança na segurança do sistema.

Para Silva et al. (2011), a biometria foi utilizada visando eliminar os custos atuais atrelados ao uso de cartões de acesso, aumentar o nível de segurança no acesso a dependências da UNIFOA (Centro Universitário Volta Redonda) e agilizar o processo de entrada e saída do edifício. Segundo Silva et al. (2011), foi desenvolvido um produto utilizando os princípios da orientação a objeto com o auxilio da UML, Linguagem de Modelagem Unificada, do inglês *Unified Modeling Language*, linguagem de programação Java e banco de dados Oracle. O modelo atual de acesso ao centro universitário faz uso de cartões de identificação que apresentam problemas relacionados a seus portadores como: perda, esquecimento e quebra gerando filas e transtornos no acesso ao edifício e suas dependências. O novo sistema fez uso da identificação biométrica eliminando os custos atuais relacionados à emissão e manutenção dos atuais cartões de identificação, elevou o nível de segurança no processo de identificação e agilizou o acesso as dependências da instituição.

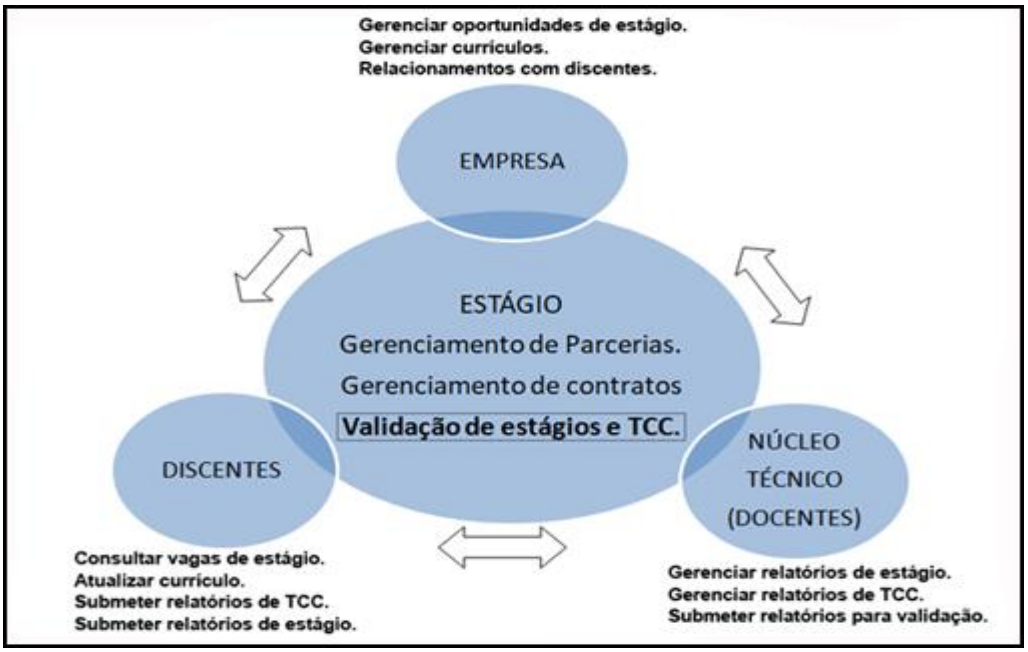
Para Ferreira (2015), no desenvolvimento de um sistema com o objetivo de melhorar a segurança no reconhecimento de pessoas, como por exemplo, processos seletivos para ingresso na instituição e o registro de alunos, foi adotada a biometria por meio da impressão digital. Conforme explica Ferreira (2015), o sistema permitiu o registro da impressão digital e a captura de fotos dos candidatos do curso de medicina no vestibular de 2014, os dados registrados foram verificados no momento da matrícula, aumentando o nível de segurança e credibilidade. Em relação a frequência de alunos, Ferreira (2015) explica que foram efetuados testes com o objetivo de verificar a viabilidade de utilizar a tecnologia biométrica em processos críticos da instituição que

necessitem de autenticação, garantindo a segurança e acesso e informações confiáveis para tomada de decisão.

5 Arquitetura da proposta

Nesta seção são apresentadas as principais atividades de desenvolvimento, ferramentas utilizadas e infraestrutura necessária para operacionalização. A Figura 3 apresenta a arquitetura conceitual do sistema de estágio, contemplando as funcionalidades e áreas envolvidas.

Figura 3 – Arquitetura conceitual do sistema de estágio

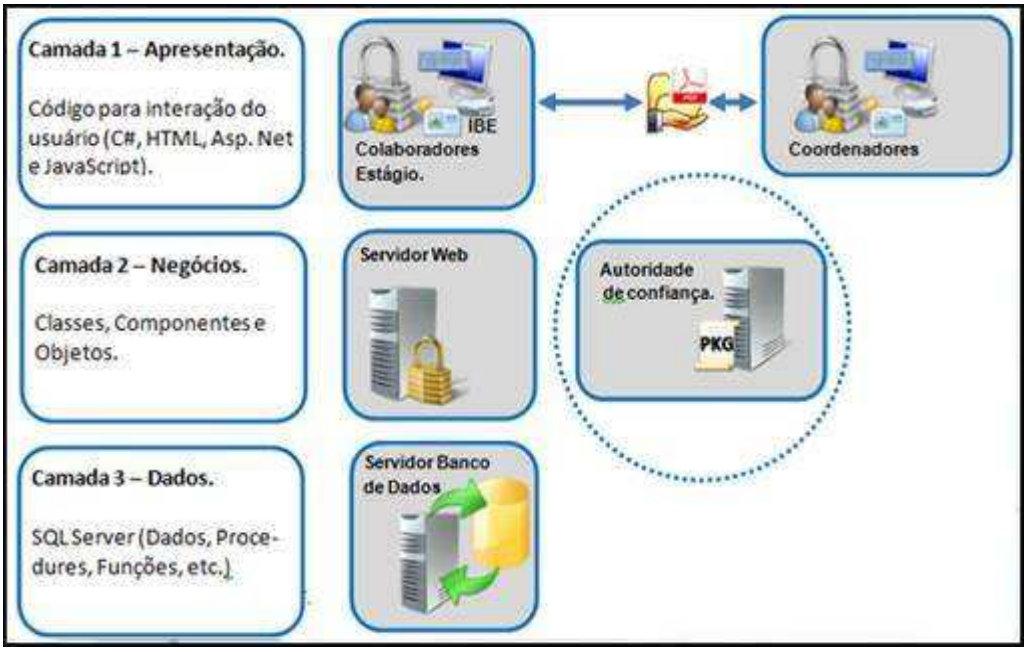


Fonte: Elaborado pelos Autores

5.1 Arquitetura de Software

A arquitetura da proposta possui 3 (três) componentes básicos, conforme Figura 4, além disso, possui um módulo de segurança denominado Private Key Generator (PKG) responsável por gerenciar a emissão de chaves utilizadas no processo de assinatura, verificação de assinatura e posterior armazenamento em dispositivo seguro, as quais serão geradas após a autenticação dos coordenadores de estágio utilizando suas credenciais biométricas.

Figura 4 – Arquitetura do ambiente do sistema de estágio



Fonte: Elaborado pelos Autores

CAMADA 1 – APRESENTAÇÃO

A camada de apresentação é responsável pela interação entre o usuário e as funcionalidades previstas no sistema como, por exemplo, requisições de consultas, etc. A interface foi implementada utilizando a tecnologia .Net (C#) e SQL Server.

CAMADA 2 – NEGÓCIOS

A camada de negócios contempla as classes, componentes e objetos responsáveis pela validação e execução das funcionalidades obedecendo às regras definidas. Nesta camada, não existe uma interface para o usuário, ou seja, toda informação foi tratada por esta camada e será transparente para o usuário, finalizando o processo na camada de dados. As classes que envolvem o processo de assinatura, verificação de assinatura e posterior armazenamento em dispositivo seguro foram implementadas nesta camada, e foram executadas através da das ações dos usuários utilizando as ferramentas disponibilizadas na camada 1.

CAMADA 3 – DADOS

A camada de dados é definida como repositório das informações tratadas pelas classes, componentes e objetos presentes na camada de negócios. Esta camada recebe as solicitações da camada de negócios através de seus métodos que executam essas requisições em uma base de dados.

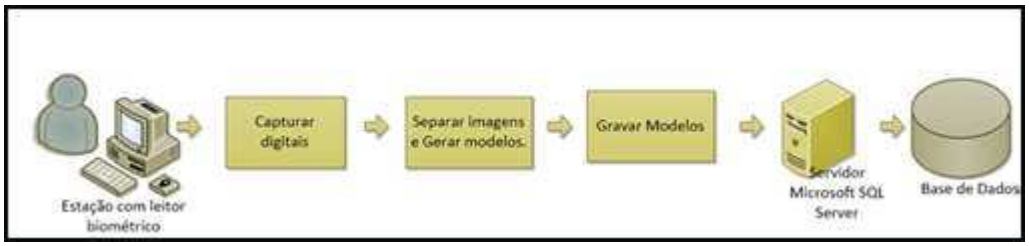
AUTORIDADE DE CONFIANÇA – PKG

A autoridade de confiança PKG é responsável pela geração das chaves necessárias ao processo de assinatura e verificação, distribuindo-as aos coordenadores de estágio, através de um canal seguro a partir da interação destes com o respectivo módulo. O acesso à autoridade de confiança, PKG, será autorizada através do processo de autenticação do usuário mediante a confirmação de sua identidade através da tecnologia biométrica, utilizando a impressão digital do usuário previamente armazenada na base de dados.

5.2 Fluxograma do processo

Para o processo de validação do protótipo foram escolhidos arquivos de TCC (Trabalho de Conclusão de Cursos) e estágio supervisionado dos mais diversos cursos técnicos oferecidos pela fundação, considerando os processos já validados em ambiente de produção (real). A proposta foi concebida com base nas características, funcionalidades e requisitos funcionais. As Figuras 5, 6 e 7 apresentam o funcionamento do processo de validação de trabalhos de conclusão de curso e estágio supervisionado, apresentando as etapas de registro de digital, assinatura e verificação de assinatura e posterior armazenamento em dispositivo seguro, respectivamente.

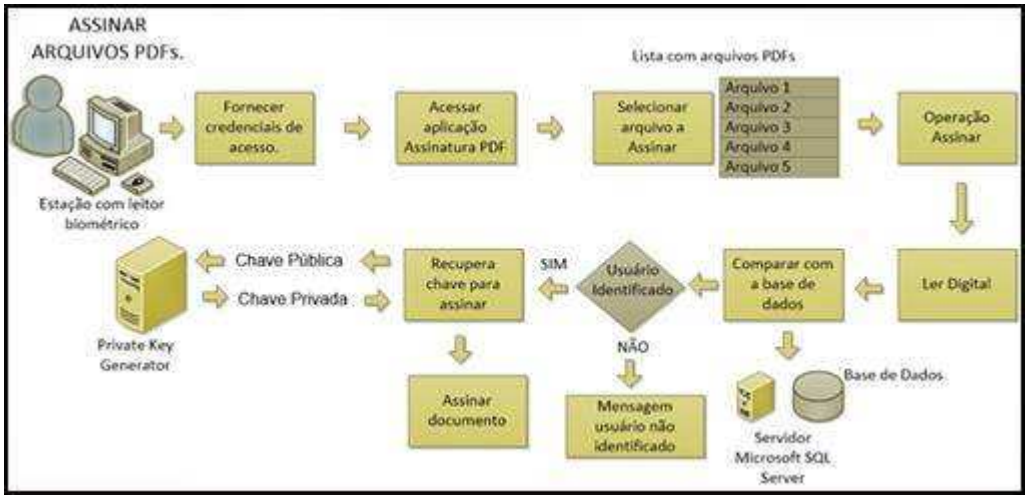
Figura 5 – Etapa de registro da digital



Fonte: Elaborado pelos autores.

A Figura 5 apresenta o processo de registro das impressões digitais de cada Coordenador de estágio, as quais serão utilizadas no processo de identificação permitindo o acesso ao processo de assinatura e verificação de assinatura de arquivos PDF.

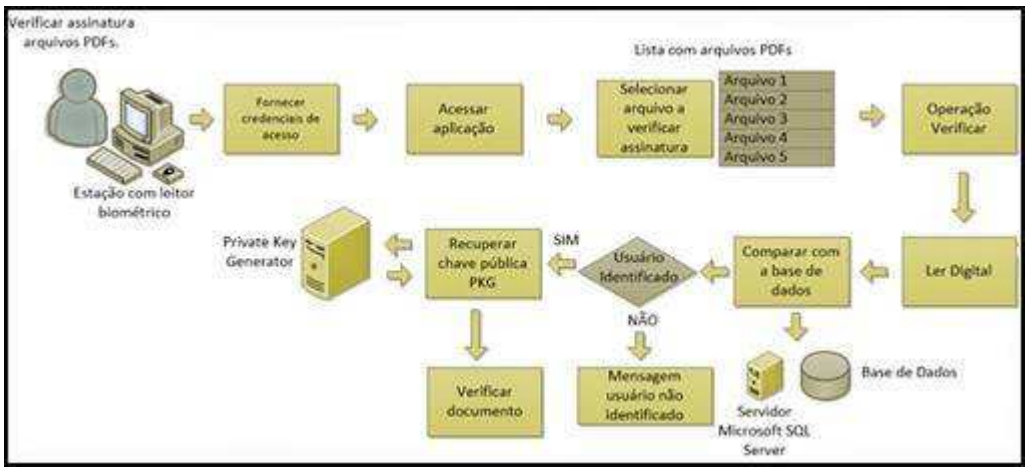
Figura 6 – Processo de assinatura do documento



Fonte: Elaborado pelos autores.

A Figura 6 apresenta o processo de assinatura de arquivos PDF. Os arquivos a serem assinados são disponibilizados na rede de computadores em pasta compartilhada, e estes estarão disponíveis aos Coordenadores de estágio. Ressaltamos que o processo de assinatura de arquivos PDF é individual, ou seja, um arquivo por vez.

Figura 7 – Processo de verificação de assinatura do documento



Fonte: Elaborado pelos autores.

A Figura 7 apresenta o processo de verificação de assinatura de arquivos PDF. Como no processo de assinatura, os arquivos assinados são disponibilizados na rede de computadores em pasta compartilhada, estando estes disponíveis aos Coordenadores de estágio. Ressaltamos que o processo de verificação de assinatura de arquivos PDF é individual, ou seja, um arquivo por vez.

6 Implementação

A seguir, são apresentadas as técnicas e recursos utilizados na implementação do sistema cujo objetivo é realizar a assinatura de arquivos PDF utilizando o esquema de assinatura baseado em identidade proposto por Adi Shamir (1984). Adicionalmente é apresentada uma visão geral sobre a biblioteca GMP utilizada neste artigo, responsável pela geração e operação com números primos grandes necessários no processo de criação das chaves (pública e privada) utilizada no processo de assinatura e verificação.

6.1 GMP Native Interface for .NET Library

A GMP Native Interface for .NET Library (BARON R.) é uma biblioteca para aritmética de precisão arbitrária aplicada a números inteiros, números racionais e números de ponto flutuante. O objetivo é fornecer a aritmética para todos os aplicativos que precisam de maior precisão do que a suportada diretamente pelos tipos C básicos. Muitos aplicativos usam apenas algumas centenas de bits de precisão, mas alguns aplicativos podem precisar de milhares ou até milhões de bits. A GMP é projetada para fornecer um bom desempenho para ambos, escolhendo algoritmos com base nos tamanhos de operandos e mantendo cuidadosamente a sobrecarga. A velocidade da GMP é alcançada usando algoritmos sofisticados, incluindo código assembly cuidadosamente otimizado para os loops internos mais comuns para muitas CPUs diferentes e ênfase geral na velocidade.

Os principais alvos de aplicação do GMP são: criptografia, segurança na Internet, sistemas algébricos e álgebra computacional. Ao adotarmos esta biblioteca, consideramos principalmente o uso de algoritmos eficientes pelas funções relacionadas à criptografia e teoria de números (para tornar os resultados próximos aos desejados em uma situação real).

6.2 Esquema de assinatura baseado em identidade de Shamir

Adi Shamir (1984) introduziu um tipo de esquema de criptografia que permite um par de usuários se comunicarem de forma segura e verificar suas identidades sem a troca de uma chave privada e pública. O esquema assume a existência de um PKG (Private Key Generate), entidade confiável, responsável pela geração das chaves baseado em sua identidade que lhe permitirá acesso a rede, estando estas chaves armazenadas em um *smartcard*, que também habilitará o usuário assinar e encriptar mensagens, assim como, verificar e decriptar as mensagens recebidas.

O esquema está baseado nos sistemas de chaves públicas, porém, o usuário pode escolher seu nome, email, fone como sua chave pública, contrariando o método tradicional, pois, a geração de um par de chaves é executada de forma aleatória e publicada em um serviço de diretórios. Conforme Adi Shamir (1984), o esquema é recomendado para grupos fechados de usuários salientando que a corporação deve garantir a integridade e confiabilidade do PKG. A chave secreta é computada a partir do PKG, armazenada em *smartcard* para ser utilizada na autenticação de acesso a rede. A seguir são apresentadas as etapas do esquema proposto por Adi Shamir (1984).

Assinatura

Para assinar uma mensagem m, o usuário deverá escolher um número r aleatório e calcular,

$t = r^e \ (mod\ n)$

$s = g * r^{f(t,m)} \ (\mathbf{mod\ n})$ onde,

n = produto de 2 (dois) números primos grandes
s, t = assinatura
g = chave secreta do usuário
f = uma função de hash
r = número aleatório
e = número primo grande relativo a $\varphi(n)$
m = mensagem.

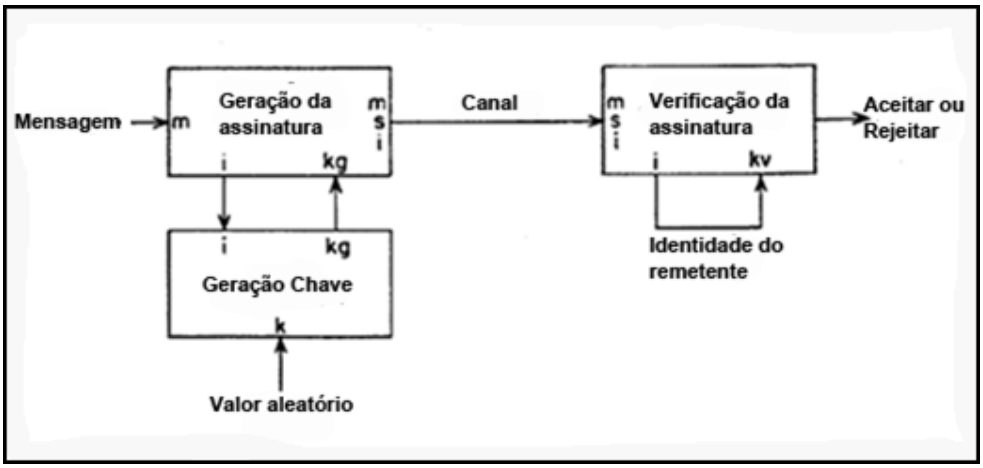
Verificação

Para verificar uma mensagem assinada, o usuário deverá submeter à mensagem assinada e Chave Pública e calcular,

s^e **(mod n) = i*** $t^{f(t,m)}$ **(mod n)** onde**,**
m = mensagem
s, t = assinatura
i = identidade
n = produto de 2 (dois) números primos grandes
e = número primo grande relativo a $\varphi(n)$
f = uma função de hash.

Os parâmetros “n”, “e” e “f” são escolhidos pelo PKG e todos os usuários terão o mesmo valor de “n” e “e”, e o mesmo algoritmo. Conforme explica Adi Shamir (1984), somente o valor de i é diferente entre os usuários e a chave secreta que corresponde a i é um número único g onde, g = i (mod n). A Figura 8 apresenta o esquema simplificado de Adi Shamir (1984) com os processos de geração de chaves, assinatura e verificação da assinatura.

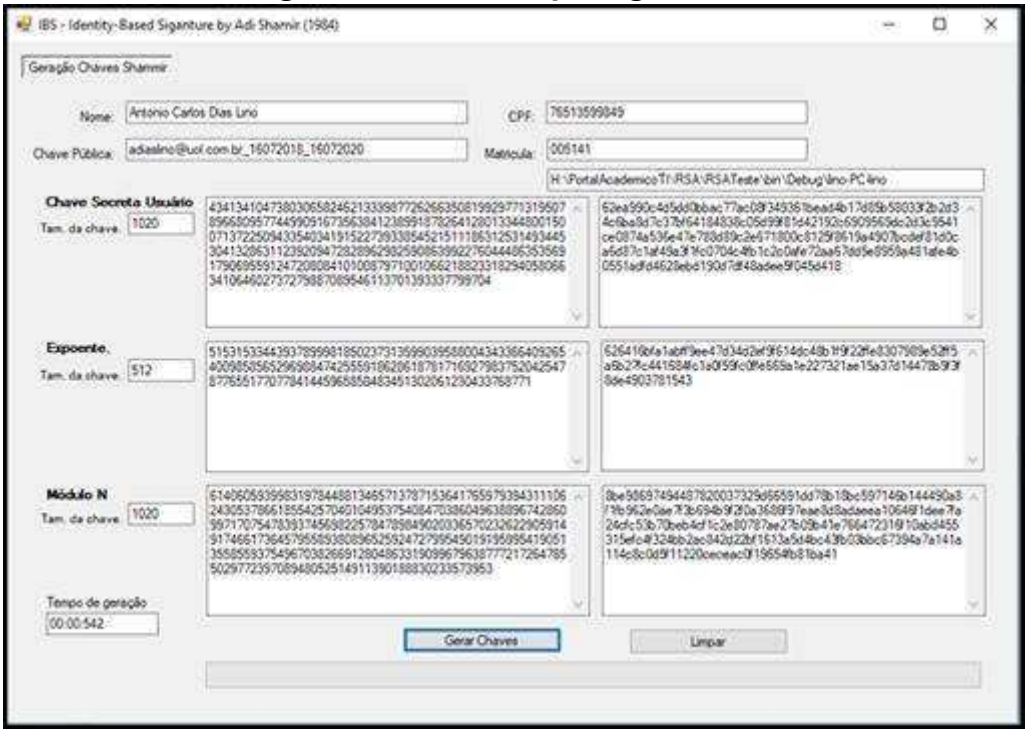
Figura 8 – Esquema de assinatura baseado em identidade de Adi Shamir



Fonte: Elaborado pelos autores. Adaptado de Identity-based Cryptosystems and Signature Schemes – Adi Shamir (1984).

A seguir, a Figura 9 apresenta a interface desenvolvida em C# (C-Sharp) responsável pela geração das chaves, seguindo o algoritmo proposto por Adi Shamir (1984).

Figura 9 – Interface para geração chaves



Fonte: Elaborado pelos autores

No processo de geração de chaves conforme interface exibida através da Figura 9, o usuário deverá informar Nome, CPF e Matricula para efeito de cadastro. Um endereço eletrônico concatenado com datas de inicio e fim é a base para a geração das chaves, e estas datas definem a validade da chave gerada. A Tabela 1 apresenta a média aritmética e o desvio padrão para cada módulo analisado em milissegundos correspondentes à geração chaves do esquema assinatura baseado em identidade de Adi Shamir divididos em 100 e 500 chaves geradas.

Tabela 1 – Comparativo do processo de geração de chaves

Esquema de assinatura baseada em identidade ADI SHAMIR						
Quantidade de chaves geradas: 100						
Tam. Bits	1º	2º	3º	SOMA	MÉDIA	DPAD
	ms	ms	ms	ms	ms	ms
512	8732	9318	9543	27593	9197,667	341,8482
1024	38957	38921	41500	119378	39792,67	1207,356
2048	257946	287893	283567	829406	276468,7	13216,04
Quantidade de chaves geradas: 500						
Tam. Bits	1º	2º	3º	SOMA	MÉDIA	DPAD
	ms	ms	ms	ms	ms	ms
512	48142	47796	45707	141645	47215	1075,632
1024	193790	189937	193245	576972	192324	1702,465
2048	1392760	1343293	1346265	4082318	1360773	22650,98

Fonte: Elaborado pelos autores.

Para efeito de análise do processo de assinatura e verificação, foram utilizados arquivos PDF de tamanhos variáveis apurando os tempos individuais conforme demonstra a Tabela 2.

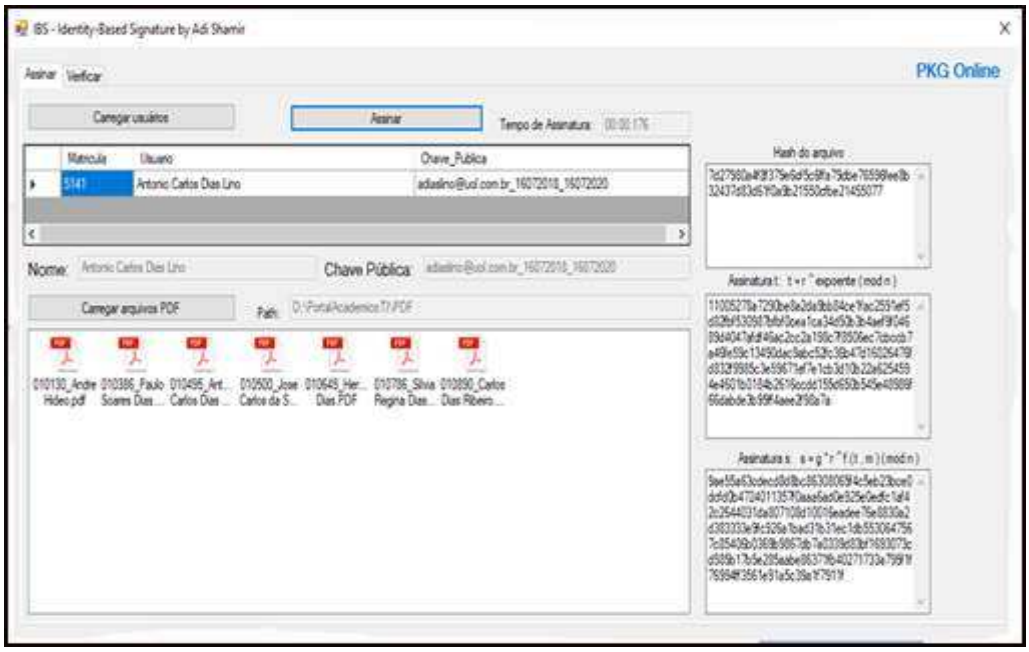
Tabela 2 – Comparativo de tempo assinatura e verificação de PDFs

Esquema de assinatura baseada em identidade de Adi Shamir		
Chave de 1024 bits		
ARQUIVO PDF	ASSINATURA	VERIFICAÇÃO
TAM. KB.	Milissegundos	Milissegundos
172	63	16
372	69	26
830	70	36
1724	127	66
3953	284	186

Fonte: Elaborado pelos autores.

Abaixo, a Figura 10 apresenta a interface desenvolvida em C# (C-Sharp) responsável pela assinatura de arquivos PDFs seguindo algoritmo proposto por Adi Shamir (1984).

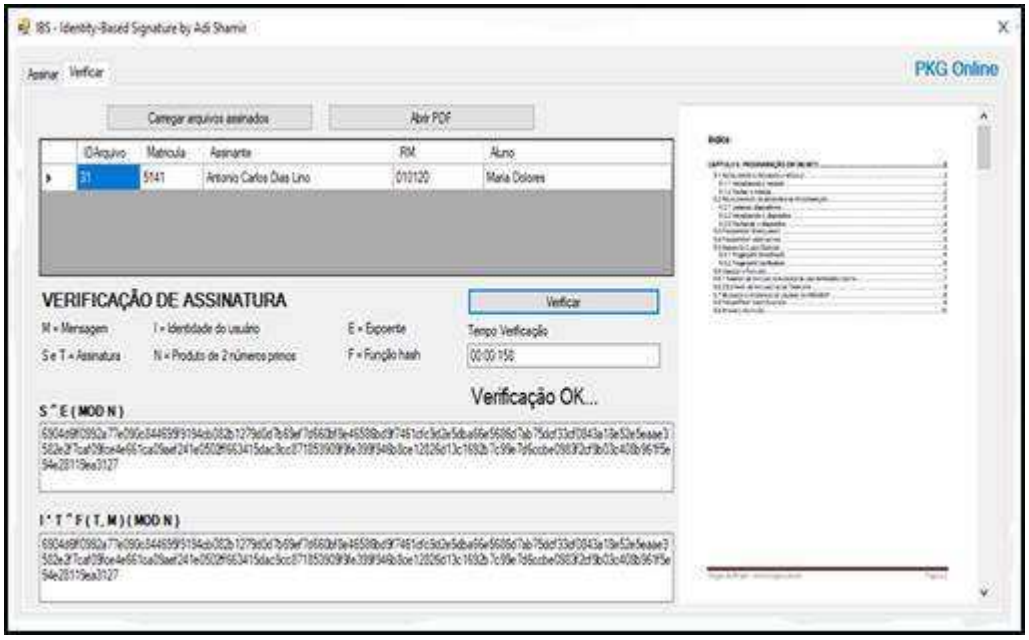
Figura 10 – Interface para assinatura de arquivos PDF



Fonte: Elaborado pelos autores

No processo de assinatura de documentos conforme interface exibida através da Figura 10, o usuário deverá selecionar um documento e em seguida clicar no botão assinar. As informações sobre a assinatura do documento selecionado será exibida na lateral direita da interface e concomitantemente armazenada em base de dados para posterior consulta ou validação de assinatura. Abaixo, a Figura 11 apresenta a interface desenvolvida em C# (C-Sharp) responsável pela verificação de assinatura de arquivos PDFs seguindo algoritmo proposto por Adi Shamir (1984).

Figura 11 – Interface para verificação de assinaturas de arquivos PDF



Fonte: Elaborado pelos autores

No processo de verificação, conforme interface exibida pela Figura 10, o usuário deve seguir a sequência:

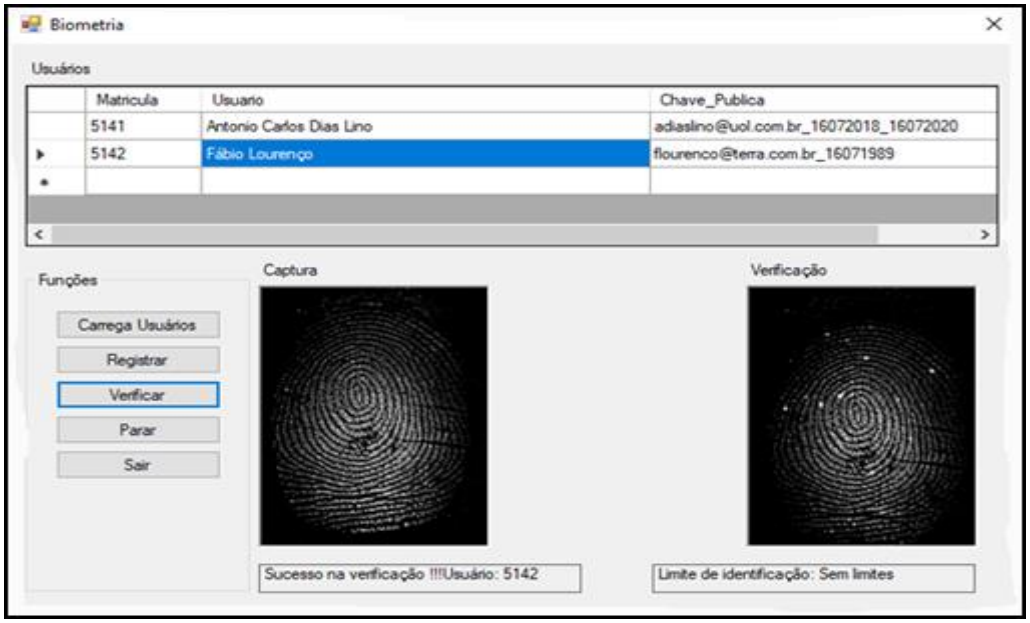
1 - Efetuar a carga dos arquivos previamente assinados;

2 - Selecionar o arquivo e em seguida clicar em “Abrir PDF”. Este procedimento abre o documento selecionando conforme exibido na lateral direita da interface.

3 – Em seguida, o usuário deve clicar no botão “Verificar”. A assinatura do documento será verificada retornando o resultado do processo.

A seguir, a Figura 12 apresenta a interface desenvolvida em C# (C-Sharp) responsável pelo processo de registro e verificação da impressão digital dos Coordenadores de estágio, as quais serão utilizadas quando da assinatura e verificação da assinatura de arquivos PDF.

Figura 12 – Interface para registro e verificação de impressão digital



Fonte: Elaborado pelos autores.

O processo de cadastro de impressão digital, conforme interface exibida pela Figura 12, segue o procedimento:

1 – Ao acessar a interface exibida através da Figura 12, os usuários previamente cadastrados durante o processo de geração de chaves serão exibidos;

2 – O responsável pela coleta das amostras deve selecionar um usuário, clicar no botão “Registrar” e em seguida solicitar ao usuário que posicione seu dedo “indicador” no leitor. O processo de captura será iniciado, finalizando com a gravação das amostras em base de dados.

3 – É possível validar uma amostra previamente cadastrada. O funcionário responsável pela verificação deve selecionar um usuário previamente cadastrado e com amostra já coletada, e em seguida, clicar no botão “Verificar”. Será solicitado ao usuário que posicione seu dedo indicador no leitor e em seguida, o sistema fará o acesso à base de dados visando validar a amostra coletada.

7 Análise dos Resultados

A seguir, é apresentado o processo de homologação junto aos usuários considerando as características do ambiente, instalação e configuração dos módulos da aplicação, plano de testes e apuração de resultados mediante métricas pré-definidas.

7.1 Planos de teste

"Teste de software é o processo de executar o software de uma maneira controlada com o objetivo de avaliar se o mesmo se comporta conforme o especificado" (BLANCO, 2012). Baseado em procedimentos especificados em Blanco (2012) foi adotado a documentação conforme apresentado na Tabela 3.

Tabela 3 - Plano de teste do sistema

Plano de teste	
Nome do projeto	Sistema de estágio
Pessoas envolvidas	Coordenadores de curso e funcionários do departamento de estágio.
Funcionalidades	Assinatura, verificação da assinatura, autenticação biométrica, armazenamento de dados biométricos e arquivos assinados digitalmente.
Hardware / Software	Servidores e Desktop (Windows Server e Win 10 Pro).
Local de teste	Ambiente de homologação instalado e configurado obedecendo as características do ambiente real de produção.
Observações	O relatório de incidentes será enviado ao departamento responsável pelo desenvolvimento. Serão criados casos de testes, relatórios de incidentes e relatório final de teste.

Fonte: Elaborado pelos autores, adaptado de Blanco (2012).

O plano de teste é utilizado na tarefa de planejamento para a execução do teste, no qual serão identificadas as funcionalidades a serem testadas, pessoal envolvido e local. Blanco (2012) afirma que esse documento é de responsabilidade da equipe de teste. A seguir, a Tabela 4 apresenta os casos de testes que foram validados no protótipo.

Tabela 4 – Casos de teste

Item	Função	Entrada	Descrição
1	Autenticação	Impressão Digital	Coordenador de estágio efetua autenticação no PKG através de sua identidade biométrica.
2	Assinatura	Arquivos PDFs	Coordenador de estágio efetua a assinatura de arquivo incorporando a assinatura ao PDF.
3	Verificação	Arquivos PDFs assinado	Coordenador de estágio ao receber um arquivo assinado, efetua a verificação da assinatura validando o arquivo PDF.

Fonte: Elaborado pelos autores, adaptado de BLANCO (2012).

Os casos de teste acima especificados foram aplicados utilizando arquivos PDF de tamanhos diversos, usuários credenciados e não credenciados a utilizar o sistema, totalizando 5 usuários participantes no processo de homologação.

A Tabela 5 apresenta os resultados das métricas aplicadas considerando os casos de testes mencionados na Tabela 4.

Tabela 5 – Resultado do processo de homologação

Métricas	Função	Resultado
Funcionalidade	Adequação	Após submeter o protótipo a validação por parte dos usuários, foi registrada sugestões de melhoria no *front-end* visando melhorar a interatividade usuário/aplicação colaborando no ganho de produtividade e eliminação de processos repetitivos.
	Segurança	O protótipo de mostrou seguro nas ações de assinatura, verificação e registro de informações confidenciais na base de dados. Ressalta-se a necessidade de melhoria quanto ao uso da biometria no que tange a qualidade das amostras capturadas as quais se mostraram

		inconsistentes durante a fase de autenticação.
Eficiência	Comportamento de tempo	A função de autenticação do usuário merece um aprimoramento quanto ao cadastro de digitais dos usuários, pois durante a fase de autenticação para assinatura e verificação, esta funcionalidade apresentou baixo desempenho e erros de *run-time*, não sendo possível em alguns casos autenticar usuários. As funções de assinatura e verificação se mostraram dentro de padrões aceitáveis, já que o desempenho não é um fator crítico considerado na aplicação.
	Utilização de recursos	Dê acordo com o ambiente operacional proposto, o aplicativo se mostrou aderente a plataforma utilizando os recursos de hardware e software dentro dos padrões aceitáveis na busca da eficiência, velocidade e segurança no processo de validação dos trabalhos submetidos. Identificou-se a necessidade de melhor avaliar as bibliotecas utilizadas na comunicação entre o aplicativo e o hardware utilizado na identificação do usuário (biometria) que chegou em alguns instantes travar o funcionamento do aplicativo sendo necessário sua reinicialização.

Fonte: Elaborado pelos autores, adaptado de Martins (2011).

A partir dos resultados obtidos mediante a aplicação das métricas especificadas na Tabela 5, pode-se chegar ao nível de aderência da proposta e identificar deficiências a serem tratadas.

8 Conclusão

O sistema desenvolvido para assinar digitalmente documentos eletrônicos cumpriu seu propósito, fornecendo condições para os Coordenadores de Estágio aprovarem, por meio da assinatura digital, os arquivos provenientes dos processos de TCC e Estágio Supervisionado, agregando facilidade, aumento de produtividade e segurança. A utilização da impressão digital no processo de assinatura digital elevou o nível de segurança, tratando a condição de irretratabilidade, propriedade esta não garantida pela ID-Based Encryption (IBE). Os resultados obtidos sugerem que a aplicação deve ser submetida às melhorias tornando-a mais aderente aos processos. O esquema de assinatura baseado em identidade desenvolvido por Adi Shamir (1984) apresentou bons tempos no processo de assinatura e verificação de arquivos PDFs quando aplicado em ambiente corporativo restrito a um grupo de pessoas, desde que não seja necessário submeter estes arquivos a validações externas.

Para trabalhos futuros fica como sugestão: a) Gerar assinaturas de arquivos PDF a partir do modelo de assinatura baseada em identidade de Adi Shamir (1984) tornando possível anexar estas assinaturas aos arquivos; b) A partir do modelo de assinatura baseada em identidade de Adi Shamir (1984), implementar a autenticação de usuários utilizando Smart Card e Tokens, pois o processo de identificação de usuários neste artigo limitou-se a utilizar a biometria por meio da impressão digital.

Referências

BARON R. GNU Native Interface for .NET. Consulta geral a

Homepage. Disponível em: <https://www.nuget.org/packages/Math.Gmp.Native.NET/>.

BLANCO, M. Z. Documentação de teste baseado na norma IEEE 829 – Estudo de caso: “Sistema de apoio a tomada de decisão”. Departamento de Computação, Universidade Federal de São Carlos (UFSCar), São Carlos, SP, Jul, 2012, p. 91-97.

BUCHMANN J. A.; KARATSIOLIS E.; WIESMAIER A. Introduction to Public key Infrastructures, Springer, 2013, 194p.

CARLOS, M. C.; SUTIL, J. M.; MOECKE, C. T.; KOHLER, J. G. Introdução a infraestrutura de chaves públicas e aplicações. Escola Superior de Redes (RNP), 2010, 219p.

CHEN, J. et al. IBE Applied to Identity Authentication for Object-Based Storage System. School of Computer Science and Technology, Huazhong University of Science and Technology. In: Fifth International Joint Conference on INC, IMS and IDC, Proceedings… 2009, p.1681-1684.

CHOUDHURY, S.; BHATNAGAR, K.; HAQUE, W. Public key infrastructure implementation and design. John Wiley & Sons, Inc. New York, USA, 2002. 316p.

COLOMBO, F. J.; NETO, B. B.; BARROS, L. J. R. Um estudo sobre biometria. Interface Tecnológica, p. 37-44, 2013.

FERREIRA, A. L. S.; MOTA, J. R.; Aplicação de reconhecimento biométrico por meio de impressão digital no Centro Universitário de Patos de Minas. Revista Perquirere, p. 127-141, 2015.

GOYA, D. H. Criptografia de chave pública sem certificado. 152p. Tese (Doutorado) – Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo, 2011.

KARAMANIAN, A.; TENNETI, S.; DESSART, F. PKI Uncovered – Certificate-Based Solutions for Next-Generation Network. Cisco Press, 2011. 253p.

MARTINS J. V. P. Geração de um modelo de métricas para controle de qualidade no processo de desenvolvimento de software. Rio Grande do Sul, 2011. 92f. Trabalho de conclusão de curso.(Sistemas de Informação), Universidade Feevale, Novo Hamburgo, Rio Grande do Sul, 2011.

MENEZES, A.; OORSCHOT P. van; VANSTONE S. Handbook of Applied Cryptography, CRC Press, p. 458, 1997.

MISAGHI, M. Um ambiente criptográfico baseado em identidade. 2008. 146f. Tese (Doutorado) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2008.

MORAES, F. V. Avaliação da influência de variações de arquitetura em um sistema biométrico de impressão digital baseado no método Taguchi e norma ISSO 19795. 137p. Dissertação (Mestrado) - Instituto Pesquisas Tecnológicas do Estado de São Paulo – IPT, Engenharia da Computação, São Paulo, 2011.

PINHEIRO, J. M.; Biometria nos Sistemas Computacionais Você é a Senha. Editora Ciência Moderna, 2008, 193p.

SHAMIR, A.; Identity-Based Cryptosystems and Signature Schemes. G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPT0 '84, LNCS 196, pp. 47-53, 1985

SILVA, M. S. da.; FILHO, V. S. Biometria através da impressão digital. Cadernos UNIFOA, Volta Redonda, p. 19-28, 2011.

SILVEIRA, J. P. C. Aplicações de criptografia baseada em identidade com cartões de identificação eletrônica. 2013. 80f. Dissertação (Mestrado) – Universidade da Beira Interior, Engenharia Informática, Covilhã, Portugal, 2013.