UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ELEMENTOS DE SUSTENTAÇÃO DA EFETIVIDADE DO USO DA CERTIFICAÇÃO DIGITAL EM APLICAÇÕES DE INTERNET BANKING – ESTUDO DE CASO EM UMA INSTITUIÇÃO PÚBLICA BANCÁRIA

RÚBIA SCRÓCARO

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR

DISSERTAÇÃO DE MESTRADO ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGEE.DM - 538/2013
BRASÍLIA/DF: SETEMBRO – 2013

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ELEMENTOS DE SUSTENTAÇÃO DA EFETIVIDADE DO USO DA CERTIFICAÇÃO DIGITAL EM APLICAÇÕES DE INTERNET BANKING - ESTUDO DE CASO EM UMA INSTITUIÇÃO PÚBLICA BANCÁRIA

RÚBIA SCRÓCARO

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE:

APROVADA POR:

_____

Prof. Rafael Timóteo de Sousa Júnior, Dr. (ENE-UnB)
(Orientador)

_____

Prof. Laerte Peotta, Dr. (ENE-UnB)
(Examinador Interno)

_____

Robson de Oliveira Albuquerque, Dr. (ABIN)
(Examinador Externo)

_____

Edna Dias Macedo, Dr. (ENE-UnB)
(Suplente)

BRASÍLIA/DF, 15 DE JULHO DE 2013

FICHA CATALOGRÁFICA

Scrócaro, Rúbia
Elementos de sustentação da efetividade do uso da certificação digital em aplicações de Internet Banking – Estudo de caso em uma Instituição Pública Bancária. [Distrito Federal] 2013.
ENE/FT/UnB, Engenharia Elétrica
Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1.Framework de Certificado Digital 2.Certificado Digital
3.Internet Banking 4.Assinador Digital
I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Scrócaro, Rúbia (2013). Elementos de sustentação da efetividade do uso da certificação digital em aplicações de Internet Banking – Estudo de caso em uma Instituição Pública Bancária. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGEE.DM - 538/2013, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF,

CESSÃO DE DIREITOS

AUTOR: Rúbia Scrócaro

TÍTULO: Elementos de sustentação da efetividade do uso da certificação digital em aplicações de Internet Banking – Estudo de caso em uma Instituição Pública Bancária.

GRAU: Mestre ANO: 2013

_____

Rúbia Scrócaro
SCRN 716 Bloco H, Entrada 16, Apt. 301, Asa Norte
70.770.680 Brasília – DF – Brasil.

AGRADECIMENTOS

Agradeço a Deus por a mais esta conquista, por Ele ter promovido tantas mudanças na minha vida, me fazendo perceber a importância de cada passo percorrido, com amor e amadurecimento.

Imensamente meu agradecimento ao orientador Professor Rafael Timóteo Sousa Júnior, que me acolheu, teve paciência e soube compreender amigamente a dedicação aos estudos e carreira profissional.

DEDICATÓRIA

A minha mãe e ao meu irmão, que mesmo longe, sempre perto estão.

Aos meus chefes que reconhecem a importância do estudo.

Aos meus amigos que compartilharam ideias, principalmente a Josi, Laerte, Robson, Edna e a Jaqueline e Eduardo que transferiram toda concentração e o esforço necessário.

RESUMO

ELEMENTOS DE SUSTENTAÇÃO DA EFETIVIDADE DO USO DA CERTIFICAÇÃO DIGITAL EM APLICAÇÕES DE INTERNET BANKING –ESTUDO DE CASO EM UMA INSTITUIÇÃO PÚBLICA BANCÁRIA

Autor: Rúbia Scrócaro
Orientador: Professor Dr. Rafael Timóteo de Sousa Junior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 15 de Julho de 2013.

Esta dissertação apresenta uma análise dos elementos de sustentação da efetividade do uso do certificado digital em aplicações de Internet Banking, com estudo de caso de uma Instituição Pública Bancária, com nome fictício de Banco Capital.

O Banco Capital, para implementar o projeto certificado digital no Internet Banking, adotou uma solução de framework de certificado digital que assina e verifica a assinatura digital em documento eletrônico, requisição carimbo de tempo de uma autoridade certificadora, válida o certificado digital e sua correspondente cadeia de certificação e gerencia as listas de certificados revogados.

O presente trabalho foi desenvolvido com embasamento em pesquisas do setor bancário e revisões de literatura relacionadas ao tema, com a finalidade de analisar se a solução de framework de certificado digital trata os elementos suficientes que garantem a sustentação da efetividade do projeto na Instituição.

O projeto certificado digital no Internet Banking está em fase de testes, o piloto está disponível para os acessos de empregados do banco, com previsão de expansão para todos os clientes.

Durante a realização do estudo, a solução de framework de certificado digital apresentou características não satisfatórias em relação às considerações apontadas pelos autores. Uma proposta com recomendações é sugerida em forma de plano de ação.

ABSTRACT

ELEMENTS TO SUPPORT THE EFFECTIVENESS OF THE USE OF CERTIFICATION IN DIGITAL APPLICATIONS OF INTERNET BANKING-CASE STUDY IN A PUBLIC INSTITUTION BANK

Author: Rúbia Scrócaro
Supervisor: Professor Dr. Rafael Timóteo de Sousa Junior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 15 july 2013

This paper presents an analysis of the elements supporting the effectiveness of using the digital certificate in Internet Banking applications, with case study of a Public Bank, with real name of Bank Capital.

The Capital Bank, to implement the project digital certificate in Internet Banking, adopted a solution framework digital certificate that signs and verifies the digital signature on an electronic document, requests the time stamp of a certification authority, validates the digital certificate and its corresponding certificate chain and manages the certificate revocation lists.

This work was developed with grounding in research in banking and literature reviews related to the topic, in order to examine whether the solution framework of the digital certificate is sufficient to ensure the support of the effectiveness of the project in the institution.

The project digital certificate in Internet Banking is in the testing phase, the pilot is available for access to bank employees, with expected expansion to all customers. During the study, the solution framework of digital certificate presented unsatisfactory characteristics in relation to the considerations mentioned by authors. A proposal with recommendations is suggested in the form of an action plan.

SUMÁRIO

1- INTRODUÇÃO 1
1.1 - JUSTIFICATIVA 2
1.2 - DEFINIÇÃO DO PROBLEMA 3
1.3 - OBJETIVOS 4
1.3.1 - Objetivos Específicos 4
1.4 –METODOLOGIA DE PESQUISA 5
1.5 - ESTRUTURA DO TRABALHO 5

2 – REVISÃO DE LITERATURA 7
2.1 – INVESTIMENTOS EM TECNOLOGIA DA INFORMAÇÃO 7
2.2 – SEGURANÇA BANCÁRIA NO INTERNET BANKING 9
2.3 – SEGURANÇA DA INFORMAÇÃO 11
2.4 – TECNICAS DE SEGURANÇA DA INFORMAÇÃO APLICADAS EM INTERNET BANKING 12
2.4.1 – Criptografia *12*
2.4.1.1- Criptografia Simétrica 13
2.4.1.2 -Criptografia Assimétrica 14
2.4.1.3 -Função de Resumo Hash 15
2.4.2 – Certificado Digital *15*
2.4.2.1 -Infra-Estrutura de Chaves Públicas 18
2.4.3 – Assinatura Digital *19*
2.5 – ICP BRASIL - ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS 21
2.6 - QUESTÕES DO EMPREGO DE CERTIFICADOS DIGITAIS NO INTERNET BANKING 22
2.6.1 – Aderência ao Internet Banking *23*
2.6.2 - Prática de Segurança no Internet Banking *23*
2.6.3 - Aceitação de uso da Certificação e Imagem *24*
2.6.4 - Frameworks para Gestão *25*
2.6.5 - Auditoria *26*
2.6.6- Arquivamento *27*
2.6.7- Confiabilidade *29*
2.6.8 - Integridade *30*
2.6.9 - Autenticidade *31*
2.6.10 -Disponibilidade *34*

3 - ESTUDO DE CASO EM UMA INSTITUIÇÃO PÚBLICA BANCÁRIA 36
3.1 – CENÁRIO DA INSTITUIÇÃO 36
3.1.1 – Declaração de Políticas Internas *37*
3.1.1.1- Política da Criptografia 37
3.1.1.2- Política do Certificado Digital 38
3.1.1.3- Política da Assinatura Digital 39
3.1.1.4- Política do Carimbo do Tempo 40
3.1.2 - Internet Banking *41*
3.1.3 - Projeto Certificado Digital na Internet Banking *42*
3.2 – SOLUÇÃO DE FRAMEWORK DE CERTIFICADO DIGITAL 42
3.2.1- Componente Assinador *45*
3.2.2 - Componente Verificador *45*
3.2.3- Componente Validador *45*
3.2.4 - Componente Carimbador *45*
3.2.5 - Componente Gerenciador de LCR *46*
3.2.6 - Autoridade de Carimbo do Tempo (ACT) *46*
3.3 - REQUISITOS FUNCIONAIS DA SOLUÇÃO 47
3.4 - FUNCIONAMENTO DA SOLUÇÃO 47
3.4.1- Assinatura Digital Básica *49*
3.4.2- Assinatura Digital com Carimbo de Tempo ..... *..50*
3.4.3 - Verificação de Assinatura Digital sem carimbo do Tempo *51*
3.4.4 - Verificação de Assinatura Digital com carimbo do Tempo *52*
4 – PROSPECÇÃO DA INSTITUIÇÃO E DOS CLIENTES DA SOLUÇÃO DE INTERNET BANKING COM CERTIFICADO DIGITAL **54**
4.1 – OBSERVAÇÕES DA INSTITUIÇÃO PÚBLICA BANCÁRIA 54
4.1.1 - Visão da Tecnologia da Informação *54*
4.1.2 - Visão do Negócio *55*
4.1.3 -Visão dos Clientes *58*
4.2 – ANÁLISE DOS ELEMENTOS DE SUSTENTAÇÃO 58
4.2.1- Riscos *59*
4.3 – PROPOSTA DE RECOMENDAÇÕES 68
4.3.1- Plano de Ação *68*

5- CONCLUSÃO 73
5.1 – PUBLICAÇÃO RELACIONADA A ESTE TRABALHO 75

REFERÊNCIAS BIBLIOGRÁFICAS 76

LISTA DE TABELAS

Tabela 2.1: Bancos eClientes (Febraban, 2012).....8
Tabela 2.2: Cadeia de Autoridades Certificadoras (ITI, 2012).....21
Tabela 2.3: Ciclo de vida dos Certificados Digitais(ITI, 2012).....22
Tabela 2.4: Auditorias, Fiscalizações e Homologações(ITI, 2012).....27
Tabela 4.1: Resumo dos fatores apontados pela Instituição.....56
Tabela 4.2: RiscoAderência ao Internet Banking.....60
Tabela 4.3: Risco Prática de segurança no Internet Banking.....60
Tabela 4.4: Risco Aceitação de uso da Certificação e Imagem.....61
Tabela 4.5: Risco Frameworks para Gestão 62
Tabela 4.6: Risco Auditoria.....63
Tabela 4.7: Risco Arquivamento.....64
Tabela 4.8: Risco Confiabilidade, Integridade, Autenticidade, Disponibilidade.....65
Tabela 4.9: Plano de ação.....69

LISTA DE FIGURAS

Figura 2.1: Despesas e Investimentos em Tecnologia por Bancos no Brasil (Febraban, 2012).7
Figura 2.2: Participação das Transações Bancárias(Febraban, 2012).....10
Figura 2.3: Criptografia Simétrica (adaptado de Stallings, 1999).....13
Figura 2.4: Criptografia Assimétrica(Schneier,1996).....15
Figura 2.5: Modelo de Malha de Confiança (Jie e Hong, 2010).....16
Figura 2.6: Modelo Hierárquico(Jie e Hong, 2010).....17
Figura 2.7: Infra-Estrutura de Chaves Públicas (ICP) (Nakamura e Geus, 2002).....18
Figura 2.8: Assinatura Digital(Jie e Hong, 2010).....20
Figura 3.1–Web Servicesdo Framework de Certificação Digital (Bry, 2012).....44
Figura 3.2 - Topologia do Framework de Certificação Digital (Requisições e Especificações, 2009).....44
Figura 3.3: Portal de Certificação Digital(Intranet da Instituição).....48
Figura 3.4: Fluxo das operações da Solução de Framework(Requisições e Especificações, 2009).....49
Figura 3.5: Fluxo Assinatura Digital básica(Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010).....50
Figura 3.6: Fluxo Assinatura digital com carimbo de tempo(Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010).....51
Figura 3.7: Fluxo Verificação de assinatura digital sem carimbo de tempo(Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010).....52
Figura 3.8: Fluxo Verificação de assinatura digital com carimbo de tempo(Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010).....53

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

AC	*Autoridade Certificadora*
AC-Raiz	*Autoridade Certificadora Raiz*
ACT	*Autoridade de Carimbo do Tempo*
AD-A	*Assinatura Digital com Informações para Arquivamento*
AD-B	*Assinatura Digital Básica*
AD-C	*Assinatura Digital com Informações Completas*
AD-R	*Assinatura Digital com Referências para Validação*
AD-T	*Assinatura Digital com Carimbo de Tempo*
AR	*Autoridade de Registro*
ATM	*Automated Teller Machines*
HTTP	*Hypertext Transfer Protocol*
ICP	*Infraestrutura de Chaves Públicas*
ICP-Brasil	*Infraestrutura de Chaves Públicas Brasileira*
ITI	*Instituto Nacional de Tecnologia da Informação*
ITU	*Telecommunication Standardization Sector*
LCR	*Lista de Revogação de Certificados*
OCSP	*On-line Certificate Stastus Protocol*
PKI	*Infraestrutura de Chaves Públicas*
SPB	*Sistema de Pagamentos Brasileiro*
SOA	*Service Oriented Architeture*
TI	*Tecnologia da Informação*
TSQ	*Timestamp*

1- INTRODUÇÃO

As Instituições Bancárias tem se caracterizado por mudanças aceleradas no ambiente de tecnologia, tornando-se um fator importante no futuro do desenvolvimento dos serviços financeiros. Neste cenário, o serviço remoto oferecido pelo Internet Banking vem se apresentando como alternativa de baixo custo e de maior flexibilidade na promoção da inclusão financeira, tornando a principal estratégia de negócio (Chatzipoulidis e Mavridis, 2010).

Segundo a Febraban (2012) o Internet Banking é considerado o canal mais utilizado para realização de transações financeiras no Brasil, em consequência, a segurança se torna a palavra-chave para a total integração desse serviço.

Com o crescimento do Internet Banking, Instituições de grande porte tem adotado o Certificado Digital, representando um crescimento de 74% (TIC Empresas, 2010).

Para a Febraban (2012), o certificado digital atribui um nível maior de segurança nos serviços e transações eletrônicas, permitindo a identificação inequívoca das partes envolvidas, bem como a integridade e a confidencialidade dos documentos e dados da transação, conferindo ainda, a mesma validade jurídica que a assinatura de próprio punho, conforme (Medida Provisória 2.200, 2011).

Buscando sustentar a efetividade do uso do certificado digital no Internet Banking, uma Instituição Pública Bancária com nome fictício de Banco Capital, adotou uma solução de framework de certificado digital. A aplicação da solução na Instituição faz com que todos os processos e sistemas que utilizam o certificado digital passem pelo framework, que é capaz de assinar, verificar, carimbar, validar e gerencias as listas de certificados revogados.

Dentre os atributos oferecidos pelo certificado digital, demais elementos de sustentabilidade são apontados como necessários para garantir a efetividade de todo processo, sendo eles, a aderência ao Internet Banking, a aceitação da certificação, a imagem da Instituição, a prática de segurança no Internet Banking, frameworks para gestão, auditória, arquivamento, autenticidade e disponibilidade das informações.

Garantir a efetividade para Arretche (2006) é a capacidade de promover resultados pretendidos, a satisfação, o sucesso na prática do que é feito. A avaliação de efetividade é o exame da relação entre a implementação de uma solução e seus impactos e resultados, torna-se mais clara a necessidade de demonstrar que os resultados encontrados estão alinhados ao objetivo do negócio.

A análise dos elementos de sustentação da efetividade da solução de framework de certificado digital na aplicação do projeto certificado digital no Internet Banking da Instituição Pública Bancária foi realizada de acordo com a prospecção da Instituição na visão da tecnologia, negócio e clientes, considerando os apontamentos feitos na revisão de literatura. A análise resultou em um mapeamento de possíveis riscos, ameaças e vulnerabilidades que podem causar impactos à Instituição Bancária analisada por este estudo.

Para mitigar esses riscos, foi sugerida uma proposta de recomendações em forma de plano de ação para cada elemento de sustentação da efetividade do uso do certificado digital.

1.1 – JUSTIFICATIVA

O Certificado Digital tem sido utilizado em serviços e produtos dos canais de atendimento aos clientes, inclusive com parcerias no Governo Federal e Empresas Privadas. Canal é entendido pelos bancos como o ponto de acesso dos clientes, sendo as agências, terminais eletrônicos, telefônico, Internet Banking e outros meios.

As movimentações transacionais nestes canais fazem com que proteção aos dados e informações se torne a preocupação constante das Instituições Bancárias, haja vista que os vazamentos de dados sigilosos podem comprometer a estratégia de negócio e põe em risco a credibilidade e imagem do banco, podendo causar sérios prejuízos (Plano de Projeto, 2010).

Os recordes de transações realizadas no Internet Banking têm demonstrado uma aceitação e confiança dos clientes nas Instituições Bancárias, fazendo com que os bancos apliquem as práticas de segurança em todos os sistemas (Febraban, 2012).

No estudo de caso do Banco Capital, a tecnologia da informação é completamente atuante no atendimento específico ao negócio, otimizando os processos e fluxos, inovando e mantendo a disponibilização de toda rede de atendimento no consumo de serviços prestados, maior comprometimento, responsabilização com os resultados, maior colaboração, coordenação entre a tecnologia e o negócio e a capacidade de absorver crescimento de produção sem inviabilizar o modelo gestão.

Dessa forma, aplicar maior segurança e qualidade no Internet Banking tem sido premissa para o negócio do Banco Capital, que em parceria com a tecnologia, implementa o projeto de certificado digital no Internet Banking.

Este estudo foi realizado em ambiente bancário devido ao grande número de transações e valores que estão sendo movimentados através do Internet Banking, e ainda, para demonstrar se a solução de framework de certificado digital garante os elementos de sustentação da efetividade do uso do certificado digital para os usuários e clientes.

1.2 - DEFINIÇÃO DO PROBLEMA

Um sistema financeiro saudável, ético e eficiente é condição essencial para que os clientes possam confiar nos serviços oferecidos pelos bancos. Investir em novas tecnologias e observar os comportamentos dos clientes traz um mundo de oportunidades e de negócios para as Instituições (Febraban, 2012).

O Internet Banking do Banco Capital apresentou um crescimento de mais de 38% no último ano em quantidade de clientes cadastrados, alcançando 9,7 milhões de clientes em maio de 2013, que realizaram 100,9 milhões de transações com volume financeiro de aproximadamente R$ 23,8 bilhões.

Com esses números, garantir evolução e manter a estabilidade dos sistemas torna-se um importante desafio para a tecnologia da informação, e ainda, é um fator determinante para a competição baseada em ganhos de escala e alavancagem de negócios, que exigem mais agilidade e flexibilidade (Plano de Projeto, 2010).

O uso de certificado digital no Internet Banking exige soluções e elementos que garantem a segurança e confiabilidade, aumentando a agilidade em responder as necessidades de negócio e garantindo a disponibilidade e continuidade dos serviços oferecidos aos clientes.

Atualmente, para atender os objetivos e iniciativas da tecnologia em relação ao negócio no Internet Banking, o Banco Capital não possui um ambiente centralizado para aplicação e gestão do uso do certificado digital de maneira adequada. Para isso, foi desenvolvido o projeto de certificado digital no Internet Banking.

Para a implementação do projeto de certificado digital no Internet Banking, o Banco Capital adotou uma solução de framework de certificado digital, que traz a problemática desse estudo. A solução adotada atende os elementos de sustentação que garante a efetividade do uso do certificado digital no Internet Banking?

1.3 - OBJETIVOS

O objetivo deste trabalho é avaliara efetividade da solução de framework de certificado digital através dos elementos que dão sustentação a utilização de certificado digital no Internet Banking da Instituição Pública Bancária.

1.3.1 - Objetivos Específicos

No contexto desta pesquisa, os seguintes objetivos específicos são:

- Pesquisar as tendências tecnológicas das Instituições bancárias financeiras;
- Realizar revisão de literatura;
- Apresentar estudo de caso de uma Instituição Pública Bancária, como nome fictício de Banco Capital, na implementação do projeto certificado digital no Internet Banking;
- Analisar os elementos de sustentação oferecidos pela solução de framework de certificado digital;
- Avaliar a efetividade da solução de framework de certificado digital na aplicação do projeto certificado digital no Internet Banking;

- Propor um plano de ação sugerindo recomendações para mitigar os riscos mapeados quanto a efetividade da solução de framework de certificado digital na Instituição Pública Bancária.

1.4- METODOLOGIA DE PESQUISA

Segundo Vergara (2007) existem diversas tipologias de pesquisa que podem ser utilizadas para a realização de um trabalho científico, nesta foi adotada a proposta da autora na qual qualifica o tipo de pesquisa em relação a dois critérios:

- Quanto aos fins: descritiva, que constata de que forma a Instituição aplica o uso do certificado digital no Internet Banking e como o projeto atua nas visões da tecnologia, negócio e clientes.
- Quanto aos meios: a pesquisa bibliográfica, documental e de estudo de caso.

A pesquisa descritiva foi realizada de forma documental, baseada em documentos do gerenciamento de projeto, manuais normativos, políticas internas, requisições, especificações e considerações do gerente do projeto.

A bibliográfica foi realizada de forma ampla em consulta de materiais publicados em livros, revistas especializadas, sites especializados, intranet, jornais e simpósios. Essa abordagem permite criar um arcabouço teórico de ideias na visão de vários autores relacionados com o tema da pesquisa.

Vergara (2007) destaca que todo método tem possibilidades e limitações, Este estudo não permite generalização, pois se trata de um estudo de caso investigado naárea de tecnologia da informação de uma Instituição financeira pública.

1.5 - ESTRUTURA DO TRABALHO

Esta dissertação está organizada em cinco capítulos, incluindo este introdutório, conforme explanado a seguir:

O Capítulo 2 traz uma abordagem conceitual dos Investimentos em Tecnologia da Informação, a Segurança Bancária no Internet Banking, a Segurança da Informação, as Técnicas de Segurança da Informação aplicadas em Internet Banking (Criptografia, Certificado Digital e Assinatura Digital), a Infraestrutura de Chaves Públicas Brasileira e as Questões de Emprego de Certificados Digitais no Internet Banking, juntamente com os artigos correlatos.

O Capítulo 3 apresenta um estudo de caso de uma Instituição Pública Bancária, com nome fictício de Banco Capital, com a contextualização do cenário da Instituição, Declaração das Políticas Internas, Internet Banking, Projeto Certificado Digital na Internet Banking, a Solução de Framework de Certificado Digital, Requisitos Funcionais e o Funcionamento da Solução.

O Capítulo 4 traz uma prospecção da Instituição e dos clientes da solução de Internet Banking com certificado digital, a metodologia aplicada, as observações da Instituição Pública Bancária na visão da tecnologia da informação, negócio e clientes. Apresenta a análise dos elementos de sustentação, mapeamentos dos riscos e a proposta de recomendações através de um plano de ações.

O Capítulo 5 apresenta uma síntese dos aspectos abordados, proporcionando respaldo necessário para conclusão da análise e estudo futuro.

2 – REVISÃO DE LITERATURA

Neste capítulo é realizada uma abordagem conceitual dos investimentos em tecnologia da informação, a segurança bancária no Internet Banking, a segurança da informação, as técnicas de segurança da informação aplicadas no Internet Banking e as questões de utilização de certificados digitais no Internet Banking.

2.1 – INVESTIMENTOS EM TECNOLOGIA DA INFORMAÇÃO

As tecnologias têm aguçado e expandido os horizontes da gestão, ofertando produtos e serviços em todo o mundo. Os sistemas de informação têm criado uma nova infraestrutura para a economia mundial, fornecendo aos usuários a opção de uma vantagem competitiva com as novas tecnologias. A tecnologia da informação tornou-se o coração do setor bancário, remodelando as dimensões e direções (Ahmed et al., 2010). Os bancos veem na TI uma importante alavanca para suas estratégias de crescimento e que estão se preparando para maiores desafios tecnológicos futuros.

Em pesquisa realizada pela Febraban (2012), as despesas e investimentos em tecnologia dos bancos cresceram de forma importante nos últimos anos: cerca de 27% entre 2007 e 2011, um alcance de R$ 18 bilhões, conforme apresentado na Figura 2.1:

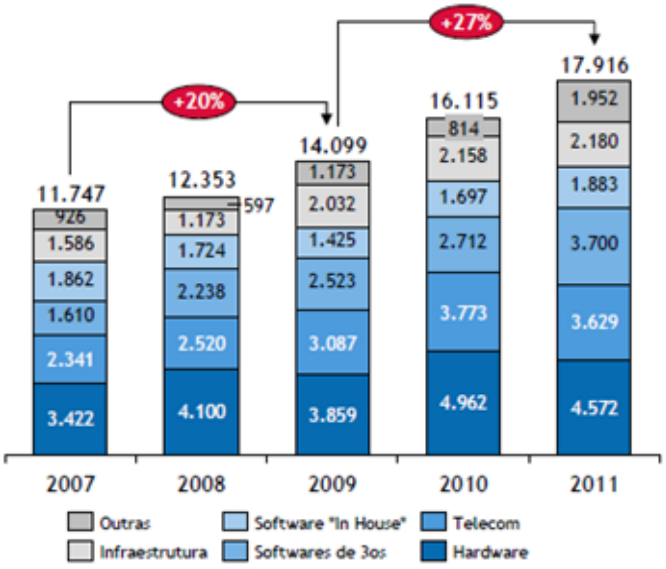

Figura 2.1: Despesas e Investimentos em Tecnologia por Bancos no Brasil.

Fonte: Febraban, 2012.

Conforme relatório de inclusão financeira (RIF, 2010) os bancos são os principais agentes no processo de intermediação financeira, fazendo da tecnologia um apoio fundamental para a evolução desse setor.

Os bancos têm apostado como estratégia competitiva o Banco Eletrônico. Esta estratégia se confirma com a pesquisa Adendo Estatístico (2011), apontando que a Internet passou a ser o canal de atendimento bancário mais usado pelos brasileiros. Logo, a Febraban (2012) destacou que o Brasil é um participante relevante do setor de tecnologia para Bancos, atuando como participante importante desta indústria global, com investimentos intensivos e projeções de um aumento de 42% até 2015.

O Banco eletrônico é visto como um conjunto de produtos e serviços suportados por modernas ferramentas tecnológicas, o qual cresce a cada dia pela implementação de produtos (Nami, 2009).

Os Bancos eletrônicos (e-Banking) permitem criar novos produtos financeiros, oferecendo oportunidades aos bancos, como desafios e inovação de aplicativos de TI (Nami, 2009).

O e-Banking começou com o uso de caixas eletrônicos ATM (Automated Teller Machines) e as transações por telefone. Com o e-Banking na Internet, diversos canais foram criados: o Internet Banking (serviços bancários on-line), o serviços bancários por telefone e móvel (Nami, 2009). Na visão dos Bancos e Clientes, os serviços prestados através do canal eletrônico têm suas vantagens, conforme apresentado na Tabela 2.1.

Tabela 2.1: Bancos e Clientes.

Fonte: Nami, 2009.

Recursos do e-Banking para Clientes	**Recursos do e-Banking para Bancos**
Economia de tempo	Mais eficiente
Redução de custos	Redução de custos
Rápido e sem fronteiras	
Vários serviços disponíveis	

Ahmed et al. (2010) apontam que para a adoção da tecnologia nos serviços bancários, desafios tem sido enfrentados, como, o alto custo de instalação e manutenção de infraestrutura, mão de obra qualificada, crescente demanda para atender às expectativa do cliente na qualidade do serviço, confiabilidade e segurança nos sistemas de informações.

2.2 – SEGURANÇA BANCÁRIA NO INTERNET BANKING

Polasik e Wisniewski (2009) definem o termo Internet Banking como uma gama de serviços bancários que podem ser acessados remotamente com o uso de um navegador de Internet, oferecendo motivadores, como, aumento do número de clientes, intensificação do volume de negócios, migração de serviços da rede física para a virtual, redução do custo operacional e processual, incremento da marca e um diferencial no mercado.

O Internet Banking é descrito pelas próprias Instituições Bancárias da seguinte maneira:

- Internet Banking do Banco, você contrata empréstimos, adquire títulos de capitalização, realiza investimentos e cadastra contas em débito automático. Além disso, pode consultar extratos e saldos da conta corrente, efetuar e agendar pagamentos e transferências, entre muitas outras operações, com toda a comodidade e segurança (Santander, 2012).
- O canal certo para quem quer segurança e comodidade. Acessando o Internet Banking pelo computador, você consulta saldo, extrato, paga suas contas e faz transferências. O Internet Banking CAIXA é o seu banco aberto 24 horas por dia, todos os dias, onde você estiver em qualquer lugar do mundo (CAIXA, 2012).
- No Banco do Brasil você encontra um ambiente para acesso à conta, completo em operações e informações sobre produtos e serviços, além de leiaute e menu de acesso personalizados de acordo com o seu perfil de relacionamento: a qualquer momento você escolhe quais as informações da sua conta vão aparecer na sua Página Personalizada (Banco do Brasil, 2012).

O Internet Banking tem se destacado como o canal mais importante e inovador dos serviços bancários dos últimos anos (Diniz et al. 2009). A Febraban (2012) aponta que o Internet Banking firmou-se como o canal preferido para transações bancárias, conforme

apresenta a Figura 2.2. A quantidade de operações realizadas por intermédio desse canal de atendimento apresentou um crescimento de 20%, um total de 46% de contas correntes com Internet Banking ativas, patamar próximo ao de países desenvolvidos.

Figura 2.2: Participação das Transações Bancárias.
Fonte: Febraban, 2012.

As Instituições Bancárias com o intuito de resguardar a própria imagem, não divulgam os valores de perdas financeiras ocasionadas por fraudes eletrônicas. Porém, segundo a Febraban (2012), as perdas dos bancos brasileiros decorrentes de fraudes eletrônicas somaram R$ 1,4 bilhão em 2012. O montante é 6,7% menor que o verificado em 2011, quando os prejuízos causados por golpes em canais eletrônicos de atendimento ao cliente somaram R$ 1,5 bilhão, ressaltando que o volume, embora expressivo, representa menos que 0,007% das transações. Do total de despesa e investimentos em tecnologia em 2012, 10% foram destinados à prevenção de fraudes eletrônicas.

Sanayei e Noroozi (2009) colocam que a segurança é importante no ambiente do Internet Banking. Todas as transações necessitam de um elemento de confiança. A confiança só ocorre quando os clientes têm garantia de disponibilidade dos bancos e capacidade para cumprir suas obrigações. Neste caso, a confiança pode ser visto como o resultado de promessas e garantias para produtos de alta qualidade e serviços. Além da segurança, os autores defendem outra dificuldade enfrentada no Internet Banking, a falta de identidade e conhecimento dos participantes.

Sanayei e Noroozi (2009) apresentam um estudo que aborda o impacto da segurança e confiança entre os utilizadores de internet Banking e a influência que tem na decisão de adotar esse serviço. Questões como os receios de privacidade e riscos de segurança

juntamente com a facilidade e as vantagens relativas do uso de Internet Banking podem ser destacada para atrair novos clientes. Os autores destacam que os Bancos apliquem a Internet Banking de maneira rápida, fácil de usar e principalmente seguro para realizar transações financeiras. Apontam que os Bancos da Malásia não adotaram totalmente o Internet Banking devido à falta de adequação do quadro jurídico e as preocupações de segurança.

Zhang(2009) propôs um sistema projetado para compartilhamento de informações de fraude pela internet, afirmando que a segurança é um dos fatores importantes considerados pelos clientes quando utilizam o Internet Banking. Quando uma fraude é identificada, os dados, o perfil de transação e as impressões digitais são movidos para um repositório centralizado do sistema que dissemina para todos os membros da rede, oferecendo proteção proativa contra novos incidentes.

Zhang(2009) aponta o certificado digital como uma técnica eficaz de prevenção de fraudes no Internet Banking.

2.3 – SEGURANÇA DA INFORMAÇÃO

Solms (1999) aponta que a informação é um recurso importante nas Instituições, demonstrando a necessidade de estar atento aos princípios do ciclo de vida da informação. O valor da informação muitas vezes não é facilmente mensurável dada à quantidade crescente de dados que as Instituições possuem, por conta disso, torna-se essencial identificar todos os elementos que compõem a comunicação de dados (Wadlow, 2000).

Devido ao crescimento da seriedade das informações como ativo de valor, as Instituições têm adotado diversas práticas para promover a política de segurança da informação. A segurança da informação é um tema importante para qualquer empresa (Wadlow, 2000) e deve garantir que as informações sejam verificadas, completas, úteis e eficazes (Laudon, 2003).

Os princípios básicos da segurança da informação são apontados por (Tanenbaum, 2003) como:

- Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
- Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
- Autenticidade - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
- Irretratabilidade ou não repúdio - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

Manter esses princípios é importante para que sistemas possam operar de forma confiável. Para que isso ocorra, técnicas e mecanismos de segurança da informação são aplicados no Internet Banking.

2.4 – TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO APLICADAS EM INTERNET BANKING

São apresentadas as definições das técnicas de segurança da informação aplicadas em produtos e serviços bancários através do Internet Banking.

2.4.1 – Criptografia

A palavra Criptografia vem das palavras gregas que significam escrita secreta (Tanenbaum, 2003).

É uma técnica utilizada para cifrar uma informação, tornando-a incompreensível, exceto para os destinatários e o transmissor, que sabem como decifrá-las (Kurose, 2003) e se faz necessária em operações bancárias nos serviços on-line, sendo algo bastante comum no dia a dia (Pfleeger, 1997).

Leavitt (2011) apresenta a criptografia como, Cripto=enigma e grafia=escrever, a arte de escrever por enigmas, como um processo matemático usado para embaralhar os dados de uma mensagem que deve ser secreta.

Menezes et al (2001) define criptografia como sendo o estudo de técnicas matemáticas relacionadas a aspectos de segurança da informação como confidencialidade, integridade de dados, autenticação e autenticação de origem de dados. Não e a única forma de oferecer segurança da informação, mas sim uma dentro de um conjunto de técnicas.

Existem dois tipos fundamentalmente diferentes de criptografia, a simétrica e a assimétrica (Fitzgerald, 2005).

2.4.1.1- Criptografia Simétrica

A criptografia simétrica ou criptografia de chave única utiliza uma única chave para encriptar e decriptar os dados, conforme apresenta a Figura 2.3.

A chave é compartilhada entre os envolvidos na comunicação, o que torna esse sistema suscetível a falhas de segurança. Acaso a chave caía em mãos erradas, as mensagens podem ser lidas e forjadas pelo novo participante da conversa.

Não é possível garantir a identidade da pessoa que enviou a mensagem porque a chave pode estar em poder de mais pessoas, caracterizando que todos podem ter potenciais para ser remetentes (Jie e Hong, 2010).

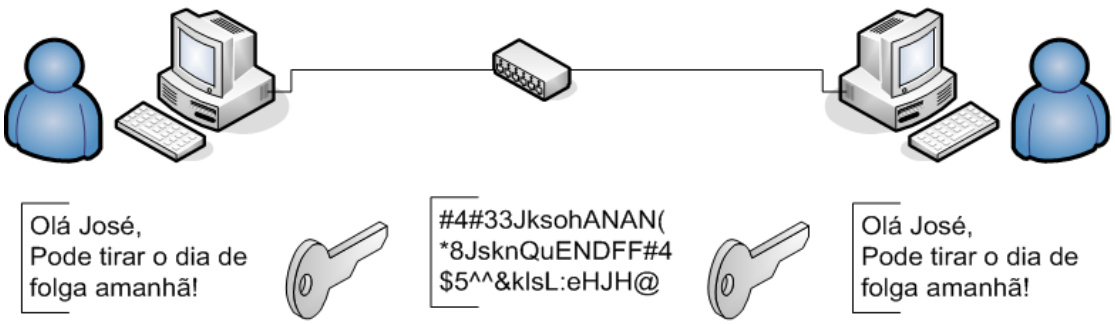

Figura 2.3: Criptografia Simétrica.
Fonte: adaptado de Stallings, 1999.

Como principal vantagem da criptografia simétrica é a rapidez na criptografia e decifração das informações e um menor número de portas lógicas necessárias para implementação em hardware (Sarma et al, 2003). Como desvantagem é o gerenciamento de chaves, pois a chave secreta deve ser transmitida ou comunicada para o receptor, tornando-a mais vulnerável a roubo.

2.4.1.2 -Criptografia Assimétrica

A criptografia assimétrica para Stallings (1999), conhecida ainda como Criptografia de Chave Pública, veio para resolver o problema de a chave ter que ser compartilhada e ao mesmo tempo evitar que os não merecedores consigam lê-las.

Utiliza duas diferentes chaves, uma pública e outra privada, de modo que é computacionalmente complexo e normalmente impraticável a dedução da chave privada por meio da chave pública (Schneier, 1996). Qualquer pessoa pode cifrar a mensagem com a chave pública, mas jamais pode decifrá-la com a mesma chave, sendo necessário à chave privada para decifrá-la, que, teoricamente, só a pessoa autorizada, dona da chave pública informada e utilizada para cifrar a mensagem tem.

As duas chaves (pública e privada) detêm uma relação matemática entre elas. A geração das chaves (problema direto) é rápida e eficiente, já o problema reverso (a partir da chave pública definir a chave privada), é oneroso e proibitivo. Segundo Schneier (1996) a técnica de criptografia de chave pública pode ser observado na Figura 2.4. Alice deseja enviar uma mensagem de forma segura para Bob; Alice e Bob concordam com um sistema de criptografia de chave pública em comum; Bob fornece para a Alice sua chave pública, podendo enviá-la ou disponibilizá-la em qualquer meio de comunicação, não sendo necessário um meio seguro; Alice cifra a mensagem que ela deseja enviar com a chave pública do Bob e a envia para Bob; Bob ao receber a mensagem, a decifra utilizando sua chave privada e obtém a mensagem original enviada por Alice.

.

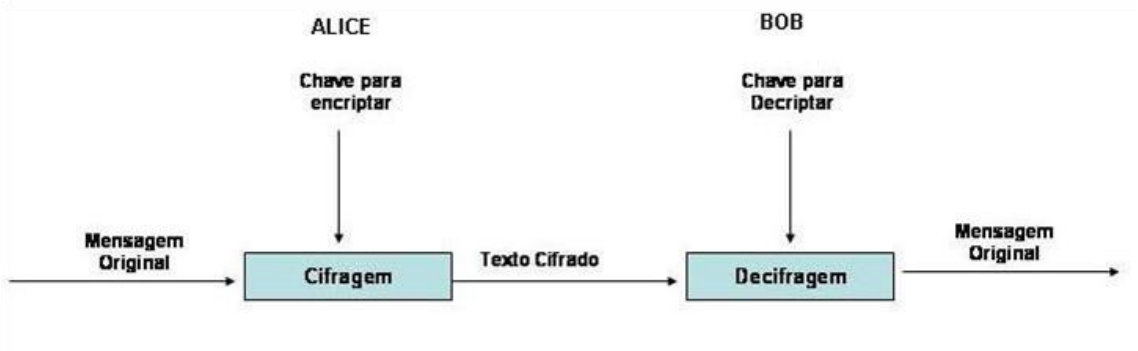

Figura 2.4: Criptografia Assimétrica.
Fonte: Schneier, 1996.

Os autores Hu e Ma (2010) descrevem a Criptografia Hibrida aplicada no governo da China, que integra quatro tipos de tecnologia: a tecnologia de criptografia, síntese digital, autenticação digital e assinatura digital.

O autor aponta que a criptografia Hibrida não pode garantir a verdade e integridade dos dados, por isso é necessário combinar outros mecanismos de integridade com base na criptografia, ou seja, a utilização da função de Hash.

2.4.1.3 - Função de Resumo Hash

É uma função matemática aplicada em algoritmos que utilizam mensagens de texto para criação de um código chamado *message digest* (resumo de mensagem) (Stallings, 1999). As funções hash são utilizadas nos mecanismos de assinatura digital, quando em um arquivo, significa a execução de um algoritmo de cálculo sobre o arquivo para geração de um número com resultado, toda alteração pode produzir mudança do resultado calculado, possibilitando saber se o arquivo foi alterado. O método pode ser aplicado para saber se um arquivo foi modificado para fraude (Fitzgerald, 2005).

2.4.2 – Certificado Digital

Para Humphreys (1998) o certificado digital é uma técnica de criptografia de informações em geral, que permite que se identifique corretamente qualquer pessoa física ou entidade jurídica, isso permite que se tenha certeza de que uma pessoa ou entidade é realmente quem diz ser.

A certificação digital baseia-se na criptografia de chave pública que garante o sigilo, a integridade, a autenticação e o não repúdio. Tecnicamente, um certificado digital é um conjunto de dados, um arquivo, assinado digitalmente pela autoridade certificadora, que têm a função de criar, manter e controlar todos os certificados por elas emitidos, incluindo a invalidação de certificados comprometidos ou expirados (Leavitt, 2011).

Os certificados digitais são compostos pelas seguintes informações, entre outros: Nome, endereço e empresa do solicitante, chave pública do solicitante, validade do certificado, nome e endereço da Autoridade Certificadora (AC) e política de utilização (limites de transação).

Os autores Jie e Hong (2010)descrevem que para fazer a certificação é necessário um modelo de infraestrutura que valide o certificado com demais entidades. Os modelos apontados são:

a) Modelo de Malha de Confiança, demonstrado na figura 2.5, é baseado na criação de uma rede em que as entidades pertencentes devem confiar umas nas outras. Cada vez que um usuário obtém a chave pública de outro usuário, ele pode verificar a assinatura digital da chave obtida por meio das demais entidades, garantindo certeza de que a chave é a verdadeira. Nesse modelo, a confiança é controlada pelo próprio usuário. Além disso, a confiança não é transitiva, ou seja, se uma entidade A confia em B e B confia em C, isso não significa necessariamente que A confia em C.

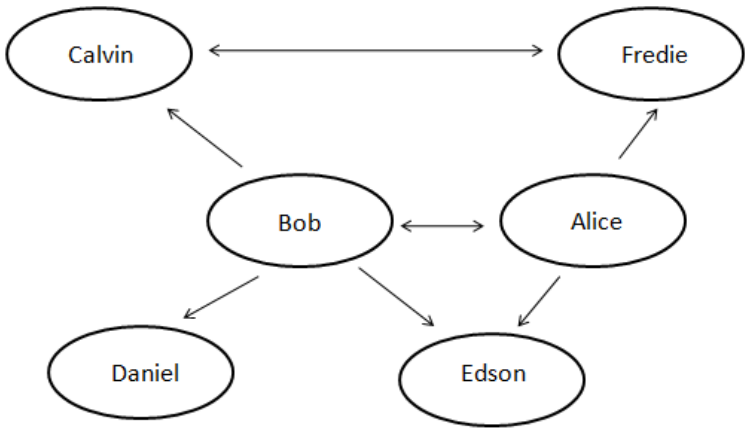

Figura 2.5: Modelo de Malha de Confiança.
Fonte: Jie e Hong, 2010.

b) Modelo Hierárquico, demonstrado na figura 2.6, é baseado na montagem de uma hierarquia de Autoridades Certificadoras (AC). As Autoridades certificam os usuários e a autoridade certificadora raiz (AC-Raiz) certificam todas as AC's, se são de sua jurisdição. Nesse modelo, os certificados digitais precisam da assinatura digital de uma AC para ser válido. Caso alguma entidade duvide de sua validade, basta consultar na AC para verificar se o certificado não foi revogado. Caso haja dúvida da validade do certificado da AC, basta conferir na AC-Raiz, que em regra é assinada por si mesmo e é mantida por uma entidade governamental. Esse é o modelo utilizado para a montagem de infraestrutura de chaves públicas.

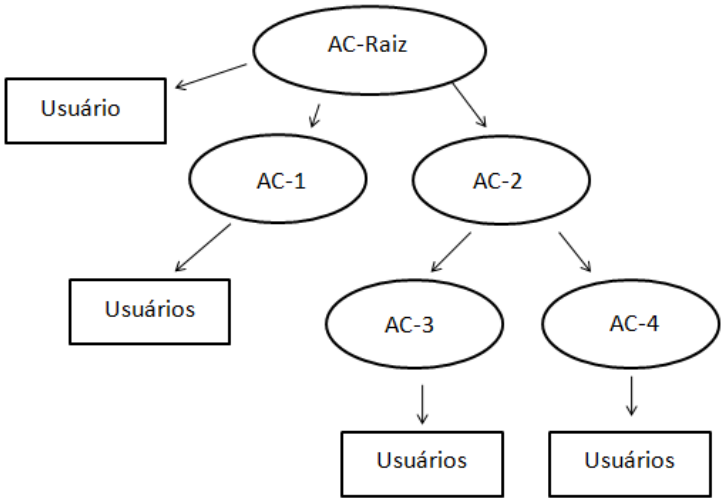

Figura 2.6: Modelo Hierárquico.
Fonte: Jie e Hong, 2010.

c) Modelo de Autoridade Central é a autoridade certificadora é única e absoluta. O Padrão X.509 é o padrão da ITU-T criação de uma infraestrutura de chaves públicas (ICP). O X.509 atualmente, está na versão 3 e padroniza os formatos das chaves públicas e atributos para os certificados, listas de revogação de certificados (LCR) e algoritmos para procura do caminho de validação.

O Certificado X.509 v.3 é composto pela seguinte estrutura: Certificado (informações), Versão, Número de Série, Algoritmo de Assinatura, Certificador, Validade, Entidade, Informações da chave pública da Entidade; Algoritmo de chave pública usado; Chave pública da entidade, Identificador único do certificador (opcional), Identificador único da

entidade (opcional), Extensões (opcional), Algoritmo de assinatura do certificado e Assinatura do certificado.

2.4.2.1 -Infraestrutura de Chaves Públicas

A Infraestrutura de Chaves Públicas (ICP) demonstrado na Figura 2.7, é um ambiente formado por vários níveis, sendo eles a Autoridades Certificadoras, Usuários, Autoridades Certificadoras Raiz e Autoridade Raiz. É um conjunto de regras, técnicas, práticas e procedimentos que existe para gerar garantias aos seus usuários, em suma, uma cadeia de confiança.

ICP é definido por Nakamura e Geus (2002) como uma infraestrutura de segurança na qual os serviços são implementados e utilizados, por meio de conceitos e técnicas criptografia de chave pública.

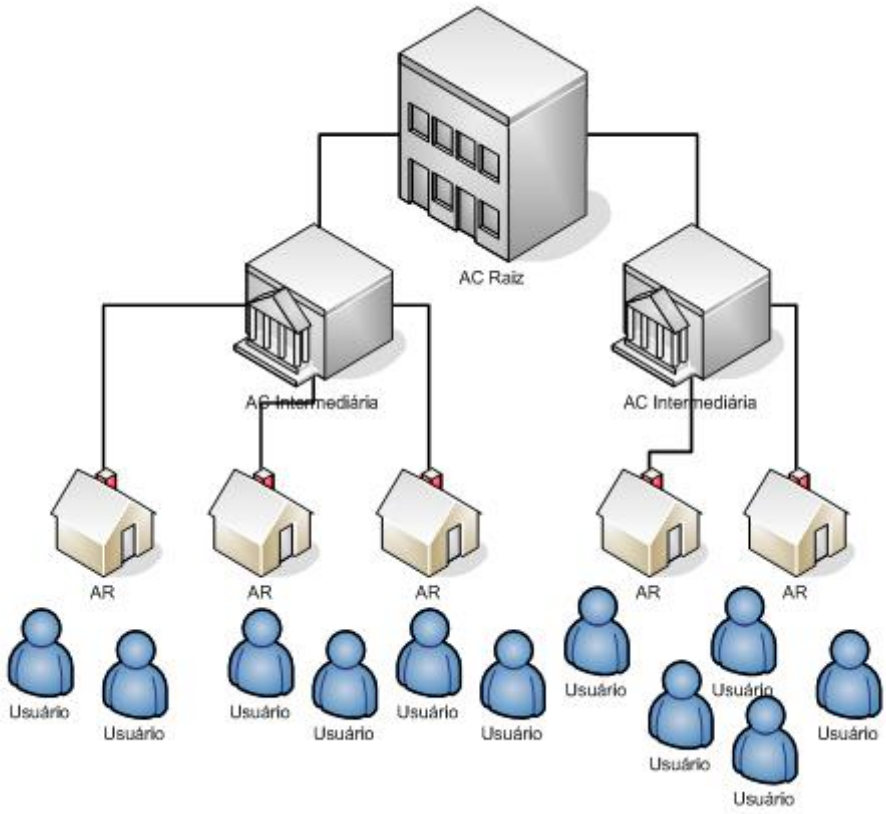

Figura 2.7: Infraestrutura de Chaves Públicas (ICP).

Fonte: Nakamura e Geus, 2002.

Nakamura e Geus (2002) apontam que as funções especificadas em uma ICP são: registro, inicialização, certificação, recuperação de par de chaves, atualização de chaves, geração de chaves, certificação cruzada, revogação e distribuição e publicação dos certificados e da notificação de revogação.

2.4.3 – Assinatura Digital

Assinatura digital é entendida por Fitzgerald (2005) como um código utilizado para verificar a integridade de uma informação ou mensagem, podendo ser utilizada para verificar se o remetente de uma mensagem é o mesmo quem diz ser, o que é feito através da criptografia assimétrica.

No processo de assinatura digital, com qual se deseja a autenticidade, o remetente usa sua chave privada para assinar a mensagem. Por outro lado, o destinatário usa a chave pública do remetente para confirmar que ela foi enviada realmente por aquela pessoa.

Conforme Figura 2.8, a assinatura digital funciona da seguinte maneira: O remetente (João) escreve um e-mail para José e o assina, usando sua chave privada. A mensagem não é criptografada, é apenas assinada, ou seja, o remetente usa sua chave privada para gerar um valor numérico associado ao e-mail. Esse valor é único para cada chave. Quando a mensagem chegar ao destino, José usará a chave pública de João para confirmar, matematicamente, que se trata da assinatura feita pela chave de João. Quando confirmada, José pode ter certeza de que a mensagem de e-mail realmente veio de João, pois é difícil que outra pessoa possua sua chave privada, a menos que a chave tenha sido extraviada.

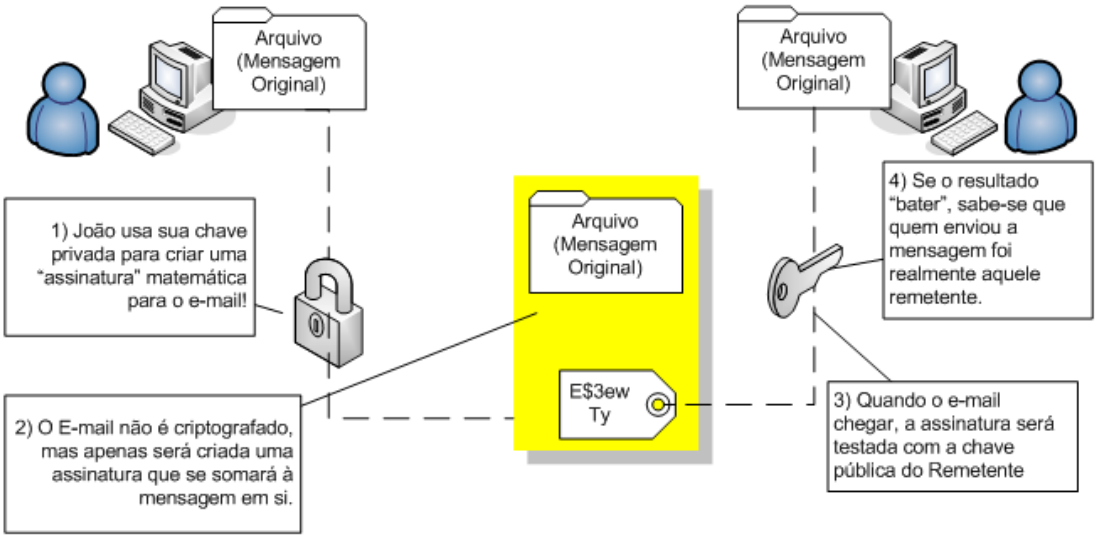

Figura 2.8: Assinatura Digital.

Fonte: Jie e Hong, 2010.

As etapas do ciclo de vida da assinatura digital são:

- Criação: processo de criação de um resumo criptográfico.
- Verificação inicial: processo de verificação quanto à validade de uma ou mais assinaturas digitais.
- Armazenamento: processo que trata da guarda da assinatura digital.
- Revalidação: processo que estende a validade do documento assinado.

Com a assinatura digital pode-se garantir (Stewart, 2008):

- Autenticidade: O fato de a assinatura ter sido realizada pela chave privada do remetente e confirmada por sua chave pública, garante que foi realmente aquele usuário que a enviou.
- Integridade: Como a assinatura digital usa a função Hash, é possível garantir que a mensagem não foi alterada no meio do caminho.
- Não-Repúdio: O usuário não poderá dizer que não foi ele quem escreveu aquela mensagem.

2.5– ICP BRASIL-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS

O Brasil conta com um sistema nacional de certificação digital regulamentada pela Medida Provisória 2.200(2001) e Decreto nº 3.872(2001), que dispõem e instituem a infraestrutura de chaves públicas brasileira - ICP-Brasil e transforma em autarquia federal, vinculada à Casa Civil da Presidência da República.

O comitê gestor da ICP-Brasil é composto por membros do governo e da sociedade civil e tem como principal atribuição coordenar a implantação e o funcionamento do ICP-Brasil, que definiu uma nova plataforma hierárquica da certificação digital, conhecida como cadeia versão 2 (ITI, 2012).

O ICP-Brasil é composto por uma cadeia de autoridades certificadoras, conforme apresenta a Tabela 2.2.

Tabela 2.2: Cadeia de Autoridades Certificadoras.

Fonte: ITI, 2012.

Autoridade Certificadora Raiz(AC-Raiz)	Compete emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. Emite a Lista de Certificados Revogados (LCR), fiscaliza e audita as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil.
Autoridade Certificadora(AC)	É uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado.
Autoridade de Registro (AR)	É a entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes.

Os tipos mais emitidos de certificados digitais são: A1, validade de um ano, armazenado no computador e A3, validade de até cinco, armazenado em cartão ou token criptográfico. Além desses, o tipo T3 e S3 tem validade de até cinco anos. Conforme declaração do ITI (2012), o certificado A3 passou a ter até cinco anos de validade, enquanto o A4, para apoiar o Passaporte Eletrônico Brasileiro, passou a valer por até 6 anos. As etapas do ciclo de vida dos certificados digitais são demonstradas na Tabela 2.3.

Tabela 2.3: Ciclo de vida dos Certificados Digitais.

Fonte: ITI, 2012.

Solicitação	Processo no qual é acessado o sistema AC e preenchido formulário especifico de solicitação do certificado digital.
Validação	Processo no qual o solicitante do certificado comparece a uma instalação técnica de AR e apresenta seus documentos de identidade.
Emissão	Processo no qual o solicitante, utilizando uma senha especial, recebida pela AR, comanda a emissão do seu certificado.
Revogação	Processo no qual um certificado já emitido é revogado pelo próprio titular ou AR.

O ICP-Brasil é responsável ainda pela homologação de Carimbo do Tempo conforme o Manual de Condutas Técnicas (2009). O carimbo de tempo (ou timestamp) é um documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado. O carimbo de tempo destina-se a associar a um determinado hash de um documento assinado eletronicamente ou não, uma determinada hora e data de existência. Ressalta-se que o carimbo de tempo oferece a informação de data e hora de registro deste documento quando este chegou à entidade emissora, e não a data de criação deste documento.

2.6 –QUESTÕES DO EMPREGO DE CERTIFICADOS DIGITAIS NO INTERNET BANKING

Neste estudo foram identificados elementos que dão sustentação a efetividade do uso do certificado digital no Internet Banking, sendo apontada pelos autores a aderência e as

práticas de segurança no Internet Banking, aceitação da certificação e a imagem, frameworks para gestão, auditoria, arquivamento, confiabilidade, integridade, autenticidade e disponibilidade.

2.6.1 –Aderência ao Internet Banking

O atendimento em agências bancárias é historicamente um dos principais canais, especialmente para movimentação financeira, porém tem perdido participação no total de transações. A facilidade de uso dos meios digitais, associadas ao perfil dos usuários faz com que a sociedade tenha cada vez mais um comportamento virtualizado (Febraban, 2013).

O volume de transações em Internet Banking aumentou 23,7% ao ano, indicando uma maior inclusão digital da população. O usuário de Internet Banking realiza em média 3,2x o volume de transações que os clientes em geral — esse número tem crescido 4,1% ano a ano, deixando claro que os Bancos devem investir na maximização do uso do Internet Banking, prover uma experiência do consumidor cada vez mais amigável neste canal e ofertar produtos e serviços que melhor se encaixam neste meio (Febraban, 2013).

2.6.2 - Prática de segurança no Internet Banking

A utilização do Internet Banking propicia aos bancos diversas oportunidades, mas em contrapartida, exige mais tecnologia em relação à segurança (Humphreys, 1998). A proteção das informações e dos dados é de vital importância para a sobrevivência dos setores bancários, pois uma falha de segurança pode gerar perda de mercado, negócio, imagem e consequentemente, perda financeira.

Albertini e Moura (2002) defendem que os aspectos de segurança, como, a proteção das informações, privacidade, autenticação e confiabilidade são pré-requisitos críticos para a funcionalidade do Internet Banking.

Os bancos, de acordo com institucionalização do Bacen (2001), devem garantir o sigilo e a segurança dos meios eletrônicos tornados disponíveis, bem como o adequado monitoramento das informações relativas à movimentação das contas.

Os autores de Peotta et al. (2011) demonstram uma análise dos dispositivos de segurança implementados pelos dez maiores bancos no Brasil e concluiu que várias camadas e métodos de segurança são simultaneamente adotadas pelas instituições bancárias, mas que vulnerabilidades de segurança nos sistemas bancários são detectados.

Vulnerabilidades são deficiências de diversas origens, as quais muitas vezes, não são identificadas a tempo ou mesmo quando isso ocorre, não são devidamente tratadas de modo a evitar um ataque (Nakamura, 2002).

Peotta et al. (2011) comprovou que a utilização do certificado digital não é segura, sendo possível exportar certificados do tipo A1 e utilizá-los remotamente, e os certificados do tipo A3 podem ser utilizados por mais de um usuário ao mesmo tempo.

Destacou ainda, que os modelos atuais de segurança estão focados em identificar os autores das fraudes, em vez executarem um procedimento preventivo a elas, não havendo assim um modelo de segurança eficiente por parte dos bancos que oferecem total segurança aos sistemas bancários. Os ataques se tornam eficiente no atual modelo de segurança ineficiente, demonstrando o Internet Banking como vulnerável, através da na obtenção de informação de autenticação e identificação. Este fato indica que os sistemas bancários devem fornecer mecanismos de segurança capazes de reduzir o vazamento de informações e problemas de segurança que afetam o sistema e que leva à fraude.

2.6.3 - Aceitação de uso da Certificação e Imagem

Zhao (2010) registra um estudo de vários modelos teóricos que analisam os efeitos sobre a aceitação de tecnologia. Percebeu-se que as administrações das Instituições bancárias devem aumentar a satisfação dos usuários através dos sistemas que oferecem qualidade e segurança das informações e serviços.

Chatzipoulidis e Mavridis (2010) acreditam que todos os fatores que moldam o ambiente do Internet Banking são dependentes e correlacionados uns com os outros, que se uma violação de segurança ocorrer devido à uma perda de integridade durante uma transação do Internet Banking, o impacto influência todos os outros parâmetros de aceitação do usuário em relação aos serviços bancários eletrônicos. Conclui que, embora a confiança dos consumidores no seu Banco seja forte, a sua confiança na tecnologia é fraca.

2.6.4 - Frameworks para Gestão

Os autores Almeida e Baranauskas (2008) definem que os frameworks constituem uma representação estruturada dos conceitos propostos em modelos,oferecendo suporte para que designers possam instanciá-los conforme as características específicas de um sistema colaborativo, ou seja, são um passo intermediário entre um modelo conceitual e as funções, relacionamentos e objetos que serão construídos.

Os autores Chen e Argles (2010) vem considerar a importância dos frameworks analisarem os requisitos e metodologia quando utilizam a certificação, principalmente sua gestão.

A gestão compreende o uso de técnicas de administração com a finalidade de assegurar que a variável tecnológica seja utilizada no máximo de sua pontencialidade como apoio aos objetivos da organização (Vasconcellos et al., 1994).

Chen e Argles 2010) apontam quatro áreas em relação aos sistemas, sendo, o produto final bem sucedido, o controle de segurança com sucesso do sistema, o desempenho estrutural que pode afetar a capacidade de adaptação de outros sistemas e o impacto social, como confiança e cultura. O autor defende que os frameworks devem tratar questões relacionadas a países e culturas diferentes, lei de proteção de dados e questões legais, impactando nos efeitos sobre o design do sistema. Os sistemas ainda devem ser seguro para enfrentar ameaças, vulnerabilidade e equilíbrio.

A utilização de chaves criptográficas e certificados digitais fazem com que seja imprescindível a definição de políticas, processos, procedimentos e ferramentas tecnológicas, como os sistemas automatizados de gerenciamento, para o controle completo do ciclo de vida dos certificados. A falta de um gerenciamento apropriado expõe as Instituições a um risco não quantificado dentro das organizações, incluindo acesso não autorizado e falhas em auditorias de segurança (Gartner, 2011).

A gestão dos certificados ajuda a identificar questões de segurança, conformidade e operacionais dentro de um ambiente, além de prover indicações que as organizações devem seguir no sentido de eliminar riscos (Gartner, 2011).

2.6.5 - Auditoria

Auditoria é definida por Boynton (2002) como um processo sistemático de obtenção e avaliação de evidências sobre afirmações a respeito de ações e eventos econômicos, para aquilatação do grau de correspondência entre as afirmações e critérios estabelecidos, e de comunicação dos resultados a usuários interessados.

Os procedimentos de auditoria possibilitam afirmar se as informações partem de fontes confiáveis e se os procedimentos para obtê-las estão sendo seguidos corretamente, possibilitando aos seus usuários analisar com maior confiança as informações oferecidas pelas entidades, sustentando melhor as decisões que precisam ser tomadas. Atestam ainda se as informações estão adequadas aos princípios de contabilidade geralmente aceitos, se todos os demais procedimentos das atividades operacionais desempenhadas estão no nível de qualidade, eficiência e eficácia (Boynton, 2002).

O risco de informações distorcidas, geradas por sistemas com controles ou processos deficientes, induz a decisões danosas às Instituições bancárias, a concentração de dados e a manutenção de cadastros e contabilizações diversas tornam as organizações vulneráveis à segurança desses dados, a erros e até a fraude (Trevisan, 1996)

A atividade de auditoria em sistemas de informática consiste na união entre os conhecimentos dos procedimentos de auditoria, sistemas de informações e processamento eletrônico de dados e seu objetivo é o de garantir que os processos estão sendo eficientes, estão produzindo resultados eficazes, estão sendo garantidos os níveis de segurança das informações e atendem às necessidades dos usuários e da alta administração em relação à rapidez, qualidade e custo das informações (Boynton, 2002).

Para os autores Pereira e Santos (2010) frameworks adotado como sistemas de informações devem passar pela auditoria de segurança, realizadas para avaliar a eficácia da capacidade de uma instituição protegendo seus ativos valorizados ou críticos. Para manter a integridade das informações, confidencialidade e disponibilidade as instituições desenvolvem estratégias de gestão de segurança, em resposta aos requisitos de segurança de informações estarem em constante evolução. Realizar auditorias regulares de segurança em sistemas e frameworks é uma forma de avaliar o desempenho e verificar se as práticas de segurança existentes estão atendendo ou se necessitam ser revisadas.

No âmbito do governo, a infraestrutura de chaves pública brasileira é responsável por realizar as auditorias, fiscalizações e homologações das certificações, conforme apresentado na Tabela 2.4.

Tabela 2.4: Auditorias, Fiscalizações e Homologações.
Fonte: ITI, 2012.

Auditorias	São realizadas de forma independente e reguladas pela Resolução n.º 72, que dita às normas de credenciamento das empresas.
Fiscalização	Tem como objetivo verificar o cumprimento das resoluções, normas, procedimentos e atividades dos Prestadores de Serviço de Certificação (PSC), Autoridades Certificadoras (AC) e Autoridades de Registro (AR). A fiscalização e o respectivo andamento do processo são normatizados pela Resolução n° 45 – DOC-ICP 09.
Homologação	O processo de homologação de sistemas e equipamentos de certificação digital e toda condução do processo é de responsabilidade da ICP-Brasil. Segundo a Resolução, as mídias que armazenam os certificados digitais e respectivas leitoras, além dos sistemas e equipamentos necessários à realização da certificação digital, devem obedecer a padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por eles utilizados. Para homologação de Softwares de Assinatura Digital é utilizado o Manual de Condutas Técnicas 4 e para Software de Autenticação, o Manual de Condutas Técnicas 5, ambos com Requisitos, Materiais e Documentos Técnicos que tem o objetivo de propiciara interoperabilidade e operação segura por meio da avaliação técnica de aderência aos requisitos técnicos.

2.6.6- Arquivamento

Rousseau e Couture (1994) definem o arquivo como um conjunto de informações, que necessitam de uma estratégia constante de proteção aos seus mecanismos de armazenamento e visualização, uma vez que esses estão sujeitos a se tornarem indisponíveis devido à rápida obsolescência.

Os arquivos existem para armazenar informações e permitir que estas sejam recuperadas mais tarde. São gerenciados por sistemas que oferecem diferentes tipos de armazenamento e recuperação das informações, baseados na estrutura, acessos, como são utilizados, protegidos e implementados (Tanebaum, 2003).

Teixeira (2002) destaca que tão ou mais importante que a identidade vinculada ao passado é a identidade que se projeta para o futuro e afirma a importância do uso de tecnologias apropriadas em documentos de formato digital, pois a preservação depende principalmente da solução tecnológica adotada e dos custos que ela envolve.

O ICP-Brasil fica instituído 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 (Medida Provisória 2.200, 2011).

De acordo com a Lei nº 12.682 (2012), que se refere ao arquivamento de documentos em meios eletromagnéticos, o ICP-Brasil é citado como:

- Art. 3º O processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP – Brasil.

  Parágrafo único: Os meios de armazenamento dos documentos digitais deverão protegê-los de acesso, uso, alteração, reprodução e destruição não autorizada.

- Art. 4 º As empresas privadas ou os órgãos da administração Pública direta ou indireta que utilizarem procedimentos de armazenamento de documentos em meio eletrônico, óptico ou equivalente deverão adotar sistema de indexação que possibilite a sua precisa localização, permitindo a posterior conferencia da regularidade das etapas do processo adotado.

Assim o ICP-Brasil descreve a política geral de arquivamento de registros no DOC-ICP 05 (2012), a qual estabelece os períodos de retenção para cada registro arquivado, sendo:

- As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;

- As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. As prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado;
- As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por no mínimo 6 (seis) anos.

Os autores de Peotta et al. (2009) apresentam um estudo sobre as regulamentações adotadas pelo ICP-Brasil, identificando que as normas que contemplam os aspectos relevantes para conferir os documentos assinados digitalmente e as características técnicas não são suficientes e efetivas ao longo prazo. Comparando os padrões internacionais e legislação de outros países, apresentam que uma das lacunas que necessitam ser sanada é referente ao armazenamento de documentos assinados digitalmente, não identificando orientações do ICP-Brasil que tratassem dessas orientações.

2.6.7- Confiabilidade

É definido por Laudon (2003) como a probabilidade de um sistema cumprir sem falhas uma missão com uma duração determinada. A perda da confiabilidade é quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

Leavitt (2011) aponta que vários ataques foram realizados contra organizações que emitem certificados digitais, criando dúvidas sobre o uso do sistema. O autor afirma que ações estão sendo tomadas para diminuir os certificados fraudulentos, mas ressalta a necessidade das empresas corrigirem o processo e problemas que virem identificar.

Os autores Sanayei e Noroozi (2009) trazem uma preocupação quanto as Autoridades Certificadoras com certificados fraudulentos. As autoridades certificadoras (AC) são atuantes em diversos países, fornecem autenticação de rede de serviços, são responsáveis pela emissão e gestão das transações de todas as entidades envolvidas com certificados

digitais. As certificadoras são consideradas confiáveis, devido ao processo de auditoria, entretanto, algumas ACs autorizam intermediárias para emitir os certificados, que podem roubar certificados digitais e utilizar de modo forma fraudulenta, gerando assim, dúvidas sobre a segurança e integridade do certificado digital. Verificou-se um registro de 100 Autoridades Certificadoras na China, mas apenas 22 delas têm a aprovação do Ministério da Tecnologia da Informação e Telecomunicações para atuar, registrando assim a existência de Autoridades Certificadoras ilegais no país.

Leavitt (2011) mostra que por quase 20 anos os certificados digitais têm sido um aspecto chave na segurança na Internet, mas que vários ataques contra organizações que emitem os certificados foram registrados. Dentre os ataques às Autoridades Certificadoras, a Comodo e DigiNotar foram bem sucedidos e StartCom(RedHat) não foi sucedido. Evidências indicaram que os ataques vieram de um endereço IP iraniano, todos feitos por um hacker conhecido como IchSol e Comodohacker.

2.6.8 - Integridade

O termo integridade de dados refere-se ao formato como os dados são armazenados, ou seja, duas entradas inconsistentes podem gerar arquivos com falha na integridade (Tanenbaum, 2003). A integridade está ameaçada quando, propositada ou acidentalmente, houver inconsistência nos repositórios de dados ou quando os seus conteúdos estiverem, por algum motivo, corrompidos.

Ma, Abie, Skramstad e Nygârd (2011) apontam uma preocupação com o mau uso dos mecanismos e segurança para proteger o arquivamento dos documentos digitais, que no recebimento de um registro digital, o primeiro questionamento é sobre sua confiabilidade. Os mecanismos de segurança, como a criptografia, são desenvolvidos para proteger os registros digitais, oferecendo a garantia de serem confiáveis a curto prazo e não eficaz a longo tempo.

A utilização da criptografia ao longo da vida digital introduz dois problemas, a perda da chave privada e a de compromisso dos algoritmos criptografados, além da preservação de documentos criptografados não serem geralmente aceitos pela comunidade internacional de arquivamento, porque a codificação não é geralmente preservada uma vez que não há

parte integrante dos registros de arquivamento. Um registro é considerado perdido quando sua chave de decifração é ausente.

O autor apresenta um quadro que tem o objetivo de avaliar a confiabilidade dos registros digitais ao longo do tempo através de combinação de valores probatórios. O método é capaz de avaliar as incertezas, insuficiências de provas, o tempo, os conflitos, aspectos de dependências e ponderações. O quadro fornece informações e uma porcentagem ao utilizador, a decisão de confiar ou não no registro é do usuário, o quadro apenas oferece subsídios para a decisão.

2.6.9 - Autenticidade

Autenticação é técnica através da qual um processo confirma que seu parceiro na comunicação é quem deve ser e não um impostor (Tanenbaum, 2003).

Um estudo feito pelos autores Lekkas e Gritzalis (2007) sobre a validação da autenticidade em registros eletrônicos na área de saúde, mostra que a vida dos pacientes é bem mais longa que o prazo de validade das chaves e dos certificados digitais utilizados como atributos de autenticidade e comprovação da integridade e origem dos dados.

A preservação da legibilidade, verificabilidade e da validade da assinatura digital são crucial para o valor futuro dos dados as saúde. A longevidade desses dados depende apenas da preservação da sua legibilidade, já a assinatura digital utilizada depende de múltiplos fatores, apontados pelo autor, como:

- As chaves usadas para criação de assinatura e verificação deve ter limitado tempo de vida, a fim de evitar a longa exposição a ameaças de segurança.
- Os algoritmos utilizados para criação de assinaturas pode ser quebrado ou chaves de assinatura pode ser comprometida antes da conclusão de sua vida útil.
- As informações necessárias para a verificação de uma assinatura digital, como cadeias de certificados digitais e de estado de revogação de certificado, pode não estar disponível em um momento futuro.
- A terceira parte confiável que liga os dados de verificação de assinaturas para uma identidade específica, podendo não ser confiável no futuro, ou porque ele deixou de operação, ou porque ele não preenche os requisitos necessários mais.

Para assinatura digital para os registros de saúde eletrônicos, o artigo propõe um processo de verificação de assinatura baseado em relacionamentos de confiança, eliminando qualquer dependência de relações de confiança obsoletos que são invalidados futuramente, como formatos de dados diferentes, armazenamento limitado e outros. A proposta concentra-se na preservação da confiança na informação necessária para verificar a identidade de um signatário de uma forma incessante, através de uma transição contínua de confiança sucessivas para novas entidades, dados e tecnologias, gerando um esquema de reconhecimento notarial cumulativa.

O paradigma de carimbo do tempo e notarização tem sido usados para prolongar a vida de uma assinatura digital, indicando que a assinatura foi criada ou que foi transferida a confiança para uma nova entidade, o Notário. No entanto, o carimbo e os notários consistem em assinaturas digitais, perdendo sua validade ao longo do tempo.

O esquema de reconhecimento notarial cumulativo faz com que a última verificação bem sucedida do notário indica que a assinatura é válida, respeitando os direitos, regulamentos e critérios sobre os serviços, dependendo sempre de atuais entidades confiáveis para verificar a assinatura digital. Sua vantagem é que preserva as características fortes de segurança de uma assinatura digital, eliminando a necessidade de confiar no provedor do certificado. Além disso, não requer um sistema seguro de arquivamento, pois tem a capacidade da tecnologia atualizada.

Os autores Ansper, Buldas, Roos e Wilemson (2001) apontam as técnicas convencionais de validação dos certificados digitais como não sendo práticas de validação para longo prazo. Questões de dispositivos de segurança, regras de responsabilidade, atualização, distribuição eficiente e armazenamento das informações das chaves públicas são citadas como problemas fundamentas a serem tratados para uso das certificações a longo prazo. As perguntas mais específicas tratadas nesse estudo são as medidas eficientes para obtenção e preservação das provas de validade, a complexidade computacional de obtenção de provas e a confiança do serviço.

Soluções existentes e suas falhas são apontadas pelo autor, como a solução off-line de PKI, onde o verificador verifica se a chave pública do certificado não está vencida e se não está na lista dos revogados, a qual somente a autoridade certificadora é confiável. A

desvantagem desse modelo é a não revogação imediata do certificado, dependendo sempre da publicação da próxima lista de atualização e ainda com o crescimento do número dos certificados, a função linear do número dos certificados emitidos pelas AC pode ser tornar impraticáveis.

Os métodos online fazem com que as informações de validação estejam sempre atualizadas. O protocolo OCSP (On-line Certificate Stastus Protocol) é um típico exemplo de protocolo de validação on-line, juntamente com o carimbo do tempo. As mensagens de revogação podem ser enviadas diretamente ao confirmador. A deficiência apontada nesse método são as grandes demandas de assinaturas digitais, que podem se tornando demoradas, exigindo equipamentos de hardwares para melhor gerir os processamentos.

Assim, os autores propõem melhorar a eficiência e a confiabilidade das novas técnicas de validação utiliza um novo serviço notarial, que confirma a validade do certificado no momento em que a assinatura digital foi criada, nesse momento, o notário fornece um link direto entre o certificado e a assinatura. O notário utiliza a árvores de autenticação merkle para comprimir as respostas às perguntas que os clientes apresentaram durante cada minuto (ou alguma outra unidade) de tempo. A árvore de merkle é um exemplo de um conjunto de dados apropriados em estrutura. Após cada minuto, o tabelião assina a raiz da árvore. Este truque já é usado no carimbo do tempo e nas certificações, reduz significativamente o número de criações de assinatura. O arvore de merkle também é utilizado entre os notários, que assina o hash raiz dessa arvore.

O método também reduz o papel de terceiros de confiança a longo prazo de validação, melhorando a confiabilidade desses serviços. Nesse método não é necessário a marcação de tempo de serviço, pois a forma de link entre o carimbo de tempo e as assinaturas são provas que a assinatura foi criada verdadeiramente naquele dia, que comprova a validade da assinatura totalmente independente de qualquer serviço de validação on-line, sendo eficiente, escalável e não exigindo adicionais partes confiáveis.

Os autores Hu, Giri, Chengyu e Li (2009) destacam que verificar a data de validade e autenticidade de um certificado digital por si só nunca é suficiente, pois é possível que um certificado tenha sido revogado antes da data de sua expiração, com as seguintes razões: comprometimento da chave, compromisso da autoridade certificadora (CA),

mudança de filiação, substituição ou cessação de operação. O autor ressalta que gerenciar as revogações de certificados de forma eficiente faz com que a infraestrutura de chave pública (PKI) seja uma plataforma mais útil, pois é através dela que é obtida a verificação do certificado digital.

Os autores estudaram vários mecanismos de revogação do certificado, incluindo o significado de revogação, o modelo de revogação, custo de comunicação da revogação, vantagens e desvantagens de sistemas de revogação de certificado e gerenciamento de riscos na revogação de certificado. Destacou que há uma clara necessidade de compreender a natureza das decisões enfrentadas por uma autoridade de certificação na gestão das operações de certificados revogados e a liberação de listas desses certificados.

Como forma de oferecer um estudo com orientações concretas de gestão e liberação de LCR feito pelas autoridades certificadoras(AC), o autor baixou arquivos de LCR da autoridade certificadora VeriSign, para entender a propriedades dos pedidos de revogação de certificado. O objetivo dessa análise foi desenvolver uma estratégia de minimização de custos que podem ser usados por uma autoridade certificadora e escolher quantas vezes ela deve liberar o LCRs, minimizando os custos operacionais.

Várias conclusões foi percebida, como ao contrário do senso comum, a probabilidade de revogação pedidos tende a diminuir ao longo do tempo. As pessoas tendem a pensar que esta probabilidade será estar aumentando ao longo do tempo, porque quanto mais um certificado se acostuma expor, o mais provável pode ficar comprometido e que o intervalo de lançamento ideal para publicação das LCR, depende da escolha das ACs, deve equilibrar o custo operacional e o risco de se atrasar a liberação de LCR.

2.6.10 –Disponibilidade

Definida por Tanenbaum (2003) como medida do grau em que um item estará em estado operável e confiável no início da missão, quando a missão for exigida aleatoriamente no tempo. A perda de disponibilidade acontece quando a informação deixa de estar acessível por quem necessita dela, causada por falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

A disponibilidade da informação é uma característica muitas vezes esquecida, mas cada vez mais essencial. As ameaças à disponibilidade dos dados ou às funcionalidades do sistema ocorrem quando é impossível ao sistema completar, no momento que lhe é pedido, tarefas que normalmente lhe são exigidas (Wadlow, 2000).

Os autores Fujishiro, Sato, Kumagai, Kaji e Okada (2010) apresentam um estudo sobre como pode ser melhorada a velocidade da verificação da validade dos certificados digitais no futuro. Defende que com o aumento das Infraestrutura de dados criptográficos, as oportunidades de aplicações e utilizações dos certificados farão que a velocidade de operação dos PKI ficam inferior as exigidas pelos usuários de aplicativos.

O autor apresenta os dois modelos que fazem abordagem à validação de certificados, o modelo âncoras de confianças, que é utilizado por navegadores web para validar certificados em servidores e o modelo certificação cruzada, que utiliza a validação cruzada, trocando certificados entre as Autoridades Certificadoras, exigindo mais processo, carregando assim muita cadeia de certificados, cada vez que recebidos. Assim, os autores sugerem a aplicação de um modelo de servidor de validação de certificados, que durante seu processamento, pode acelerar o atendimento de outras solicitações requeridas repetidamente, baseado na função de validação das cadeias de certificação com o armazenamento em cachê.

Nestes apontamentos buscou-se identificar os elementos essenciais, as atribuições e empregabilidade capazes de sustentar a efetividade do uso do certificado digital em aplicações de Internet Banking. Pretende-se analisar o estudo de caso de uma Instituição Pública Bancária que adotou uma Solução de Frameworks de Certificado Digital para acessos ao Internet Banking com certificado digital e avaliar se a Instituição adota os elementos citados pelos autores, que possam garantir a real sustentação deste mecanismo de segurança no negócio e aos clientes.

3 –ESTUDO DE CASO EM UMA INSTITUIÇÃO PÚBLICA BANCÁRIA

Este capítulo apresenta o cenário da Instituição Bancaria analisada e estudada neste trabalho, com nome fictício de Banco Capital. É descrito as políticas internas, o Internet Banking, o projeto certificado digital no Internet Banking e a solução framework de certificado digital, com os requisitos e funcionamento.

3.1 – CENÁRIO DA INSTITUIÇÃO

A Instituição estudada dispõe de uma governança corporativa que atua num desempenho empresarial responsável, aliado à sustentabilidade e à transparência, e integrando as dimensões social, econômica e ambiental, com o modelo de gestão que auxilia a concretizar sua visão de futuro, sendo baseado em sete princípios:

- Sinergia público/comercial: desempenho financeiro em prol de desenvolvimento econômico e social;
- Foco cliente: criação de valor para o cliente como orientador;
- Responsabilização: empregados comprometidos com o resultado de suas atividades;
- Simplicidade: redução da burocracia, minimizando etapas, interfaces e níveis de aprovação;
- Integração: maior colaboração e coordenação entre unidades;
- Eficiência: maior atenção à produtividade e controle de custos;
- Escalabilidade: capacidade de absorver crescimento.

A área de tecnologia da informação é composta pela vice-presidência, uma diretoria, três superintendências nacionais (Governança/Segurança, Operacional e Negócio), onze gerências nacionais, três centralizadoras nacionais e dezesseis unidades de representação e suporte técnico.

Dispõe de uma rede de telecomunicação para disponibilizar produtos e serviços com agilidade, desempenho e segurança, com o objetivo de demandar a construção,

manutenção e disponibilização de soluções de Tecnologia da Informação e Comunicação (TIC) para sustentar as atividades de negócio e funcionais.

Diversos serviços são oferecidos, como, relacionamento com os clientes internos, inovação em TI, segurança da informação com a elaboração e implementação de políticas, operacional para manter o ambiente tecnológico em pleno funcionamento, a governança que define instrumentos que serão adotados e implementados e o desenvolvimento de sistemas.

Dentre os macroprocessos que a área de tecnologia atua, a gerência de infraestrutura de chaves pública é responsável pelos serviços de certificação digital, a gerência de certificação digital que é responsável pelas estratégias de certificação, funcionamento das entidades e instalações técnicas no processo de certificação e representa a instituição junto ao ITI e entidades representativas nos assuntos pertinentes a atuação.

Para atuação na estratégia e gestão de canais, como o Internet Banking, a gerência de meios digitais é responsável por prospecta oportunidades de negócios a serem realizados no Internet Banking e definir, em conjunto com os gestores de produtos e de tecnologia, o formato e os serviços a serem disponibilizados, visando a sua operacionalização e comercialização, define sobre o lançamento, reposicionamento ou retirada de produtos e serviços do Internet Banking, em conjunto com as áreas gestoras de produtos e serviços e acompanha os resultados e a evolução dos negócios efetuados no canal.

3.1.1 –Declaração de Políticas Internas

Para Tanenbaum (2003) políticas de segurança são criadas para definir quais ações as entidades têm permissão de executar e quais são proibidas. Declarações a respeito dos das práticas que fundamentam o uso da criptografia, certificado digital, assinatura digital e carimbo do tempo são normatizadas pelo Banco Capital (Manual Normativo, 2012).

3.1.1.1- Política da Criptografia

A Instituição define por meio de diretrizes orientações de uso da criptografia que visa aumentar o nível de segurança e confiança na infraestrutura de comunicação, informações e sistema.

Os métodos criptográficos devem ser utilizados de acordo com padrões consagrados nacional e internacionalmente e em conformidade com as leis brasileiras, sujeita as normas estabelecidas pela ICP-Brasil. A escolha do método criptográfico sempre devem convergir para aquele que, comprovadamente, garanta maior nível de proteção e dificuldade de quebra, disponíveis pela Instituição

Os procedimentos definidos para as cerimônias de manipulação, implementação e manutenção de chaves criptográficas utilizadas em algoritmos simétricos da Instituição estão descritos no Manual de Cerimônia de Chaves Criptográficas Simétricas, que são implementados em processos criptográficos de sistemas corporativos em produção, definindo padrões e procedimentos adotados para manutenção destas chaves.

3.1.1.2- Política do Certificado Digital

A política de certificado digital descreve os requisitos, procedimentos e nível de segurança adotado para a emissão, revogação e gerenciamento do ciclo de vida de um Certificado Digital.

O objetivo do uso do certificado digital na Instituição é confirmar a identidade do usuário na Internet e Intranet, correio eletrônico, transação on-line, redes privadas virtuais, transação eletrônica, informação eletrônica, cifrar chaves de sessão e assinatura de documento eletrônico, dando-lhe validade jurídica e garantindo a segurança de suas informações.

A gestão do negócio certificado digital é gerenciada por uma unidade específica da Instituição, com a responsabilidade de gerir o conteúdo do sítio institucional da Certificação Digital, estabelecer critérios para credenciamento e descredenciamento de entidades, conforme preconizado nas normas da ICP-Brasil, identificar e promover o credenciamento e o descredenciamento de instalações técnicas junto à ICP-Brasil, avaliar e controlar o resultado do uso de certificados digitais, bem como o seu retorno financeiro, definir os perfis de usuário e criar os templates de certificado digital referentes aos sistemas de certificação digital.

Os tipos de certificados aceitos são certificados digitais do tipo A1 – pessoa física e aplicação ou equipamento, certificados digitais do tipo A3 – pessoa física, certificados digitais do tipo A1 – pessoa jurídica, certificados digitais do tipo A3 – pessoa jurídica, certificados digitais do tipo A1 – aplicação ou equipamento da justiça, certificados digitais do tipo A3 – pessoa física – servidor da justiça.

As auditorias internas têm por objetivo avaliar se os processos, procedimentos, atividades e controles estão em conformidade com as respectivas políticas de certificado, declaração de práticas de certificação, política de segurança e demais normas e procedimentos estabelecidos pelo comitê gestor da ICP-Brasil. É auditado o pré-operacional, previamente ao credenciamento junto à ICP-Brasil e o operacional, para fins de manutenção do credenciamento.

3.1.1.3- Política da Assinatura Digital

O objetivo desta política é subscrever e verificar documentos eletrônicos em consonância à regulamentação da ICP-Brasil, por meio do serviço de Assinatura Digital da Instituição, de forma a garantir a autenticidade e a integridade da informação.

Para assinar digitalmente um documento eletrônico, é necessário possuir certificado digital padrão ICP-Brasil e constar, na norma que institui o uso do referido documento, autorização para que ele seja assinado digitalmente.

A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, da mesma forma que a assinatura de próprio punho comprova a autoria ou a concordância com um documento escrito em papel.

O conteúdo de documentos eletrônicos assinados digitalmente tem validade jurídica, desde que os certificados utilizados estejam válidos no momento de sua assinatura e a assinatura digital gerada esteja no padrão da ICP-Brasil.

Para verificar a assinatura em documentos eletrônicos assinados digitalmente é necessário constar na norma que trata do documento, autorização para que ele seja recebido em

forma eletrônica e que sua assinatura digital, na Instituição, possa ser validada com o uso do serviço de assinatura digital.

A geração de assinatura digital em documentos eletrônicos é disponibilizada no ICP-Brasil no padrão Advanced Electronic Signature (CAdES) e é reconhecida quando gerada durante o prazo de validade do certificado digital em que está baseada.

A verificação é a ação realizada para determinar com precisão que a assinatura digital foi criada durante o período operacional de um certificado digital válido, mediante o uso de uma chave privada correspondente à chave pública contida no certificado, conforme o padrão definido pela ICP-Brasil, e se o conteúdo do documento associado não sofreu alteração após a criação da Assinatura Digital.

Sua verificação tem como objetivo constatar a integridade do documento assinado digitalmente e validar o certificado utilizado e a sua cadeia de vinculação, confirmando a autoria da assinatura. O término do processo de verificação de assinatura digital mostra como resultado o estado de cada assinatura avaliada em termos de válido, inválido e indeterminado, identificando também os signatários.

3.1.1.4-Política do Carimbo do Tempo

Política de carimbo do tempo descreve os requisitos, procedimentos e nível de segurança adotados para a emissão do carimbo do tempo, credenciada na ICP-Brasil, com o objetivo de evidenciar a existência de informações digitais em um determinado momento do passado.

O carimbo de tempo da Instituição é solicitado no processo de assinatura digital, por pessoas físicas e jurídicas, considerando válido quando tiver sido assinado corretamente, usando certificado ICP-Brasil específico para equipamentos de carimbo do tempo e quando a chave privada usada para assinar o carimbo do tempo não tenha sido comprometida até o momento da verificação.

A certificação de tempo da Instituição é parte integrante da ICP-Brasil na execução dos seus serviços de carimbo do tempo e tem a obrigação de assegurar que seus relógios estejam sincronizados, com autenticação na rede de carimbo do tempo da ICP-Brasil,

notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades, monitorar e controlar a operação dos serviços fornecidos e tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações.

A gerência de certificação digital é responsável por gerir o carimbo do tempo, gerir o conteúdo do sítio institucional da certificação digital no que se refere ao carimbo do tempo e avaliar e controlar o resultado do uso do carimbo do tempo.

3.1.2- Internet Banking

A Internet Banking disponibiliza autoatendimento aos clientes, permitindo acesso à conta bancária para consultas e transações financeiras através da rede Internet. Na visão da Instituição, este canal intensifica o volume de negócios com menores custos, aumenta o número de clientes e reduz o fluxo nas agências (Manual Normativo, 2012).

A vantagem é redução dos custos operacionais, em função da redução do fluxo de pessoas nos pontos de venda, mais tempo disponível nos pontos de venda para atendimento ao cliente na comercialização de produtos e serviços, clientes mais satisfeitos, tendo as mesmas facilidades oferecidas pelos concorrentes e fidelização do cliente, em função do atendimento mais personalizado, cômodo e eficiente (Manual Normativo, 2012).

Em números apresentados pela Instituição em junho/2012, mais de 8 milhões de clientes possuíam conta ativa com acesso à Internet Banking, representando aproximadamente 17 bilhões em valores movimentados.

Para oferecer melhor serviço aos clientes, dar garantias de segurança contra as fraudes eletrônicas e fomentar o uso de certificação digital em negócios e produtos da Instituição, adotou-se o Certificado Digital na Internet Banking (Plano do Projeto, 2010).

3.1.3- Projeto Certificado Digital no Internet Banking

O Projeto certificado digital no canal Internet Banking está sendo implementado em duas fases, a primeira para acesso/log ao sistema e a segunda para assinatura de efetivação e confirmação de transações.

A efetividade e confirmação de transações está na fase de planejamento, entretanto, após sua implementação as contestações ou questionamentos de clientes quanto a fraudes serão descartados, pois no entendimento da Instituição, a responsabilidade será única e exclusiva do cliente os cuidados e uso do certificado digital, podendo a contestação ser caracterizada como auto fraude. Auto fraude é uma ocorrência de transferência de recursos com anuência do cliente, sendo o único responsável por ter feito a transação (Manual Normativo, 2012).

A implantação do acesso/log está em fase de piloto, apenas para os empregados internos, com certificados tipo A3 emitidos pela ICP-Brasil. Foram registrados em 2012 cerca de 25 mil adesões e acessos com Certificado Digital no Internet Banking. Nenhum registro de instabilidade, indício de fraude, vulnerabilidade ou contestação financeira foram apontados.

Os registros desses acessos e adesão estão arquivados em computadores das equipes envolvidas no projeto, que capturam e compactam as informações por períodos.

Adaptar o Internet Banking para o uso de certificados digitais só foi possível com a especificação e contratação de uma Solução de Framework de Certificado Digital.

3.2 – SOLUÇÃO DE FRAMEWORK DE CERTIFICADO DIGITAL

A Febraban (2012) aponta que o setor bancário se tornou pioneira na utilização do certificado digital, com a compensação digital por imagem no Sistema de Pagamentos Brasileiro (SBP) sendo realizada através de um framework validador de assinaturas digitais, oferecendo maior agilidade nas liquidações e transferências de recursos.

O ICP-Brasil não determina a forma que cada Instituição Bancária deve utilizar, aplicar e gerir os Certificados Digitais em sistemas e produtos internos, apenas define os padrões.

Entretanto, o ICP-Brasil realizou um acordo de cooperação técnica firmado com o Colégio Notarial do Brasil para desenvolvimento de um framework Assinador Digital de Referência específico para os Tabeliães de Notas Brasileiros. O projeto foi criado para solidificar e dar credibilidade ao uso dos documentos eletrônicos, uma vez que notários e registradores detêm a expertise no ciclo de vida do documento em papel.

A solução de framework de certificado digital adotada pela Instituição é oferecida pela empresa de mercado com o benefício de agilizar o desenvolvimento e a operação dos aplicativos através da chamada a serviços criptográficos (webservices), que eliminam a necessidade de programar e manter rotinas complexas de assinatura digital e carimbo do tempo. Concentra funcionalidades como logs para auditoria e rastreabilidade, permitindo ao cliente focar seu esforço de desenvolvimento em suas aplicações. Facilita a manutenção das aplicações, que não precisam ser modificadas para manter a aderência aos padrões de segurança e sua atualização é centralizada, ficando disponível automaticamente para todas as aplicações (Bry, 2012).

Com uma arquitetura SOA (Service Oriented Architeture), a Solução é composta por um conjunto de Web Services, conforme apresenta a Figura 3.1, que oferecem:

- Assinatura digital: gera assinaturas em documentos e transações digitais. Suporta assinaturas com diferentes níveis de garantia de segurança e longevidade, conforme definido pelo padrão brasileiro de assinatura digital.
- Verificação de assinaturas: valida padrões internacionais e nacionais. Oferece como resposta um relatório completo da assinatura, com dados dos assinantes, validade da assinatura, bem como detalhes acerca dos certificados digitais e carimbos do tempo utilizados.
- Validação de certificados digitais: gerencia o repositório de certificados confiáveis. Monitora a validade dos certificados digitais, notificando o titular quando estiver prestes a expirar.
- Carimbo do Tempo: emprega carimbos de tempo para marcar o momento exato de cada assinatura coletada, bem como garantir a validade jurídica do documento por longo prazo.

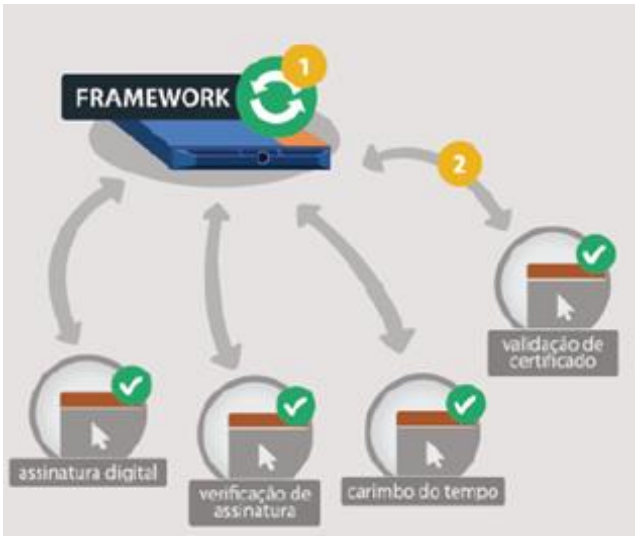

Figura 3.1–Web Servicesdo Framework de Certificação Digital.

Fonte: Bry, 2012.

A solução de framework de certificação adotada pela Instituição está publicada em edital público e é detalhada pelo documento de Requisições e Especificações (2009), que contempla os componentes que geram a assinatura digital, verificam a validade de assinatura digital em documento eletrônico, requisitam o carimbo de tempo de uma autoridade certificadora de tempo externa, validam o certificado digital e sua correspondente cadeia de certificação e gerenciam as listas de certificados revogados. A topologia é representada na Figura 3.2:

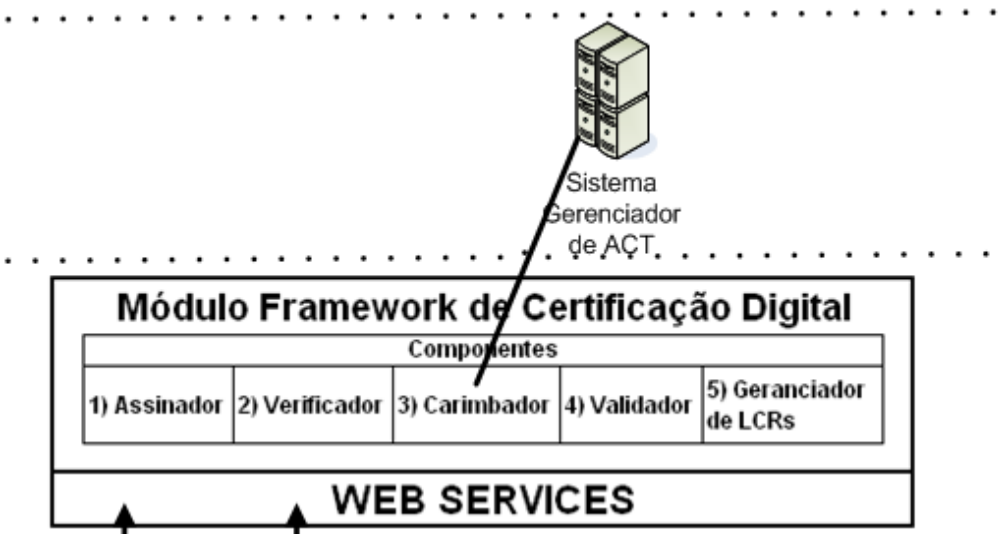

Figura 3.2–Topologia do Framework de Certificação Digital.

Fonte: Requisições e Especificações, 2009.

3.2.1- Componente Assinador

O componente assinador gera assinaturas simples, co-assinaturas e contra-assinaturas nos padrõesCAdES (attached e detached) e XAdES (detached, enveloping e enveloped), nos formatos de: Assinatura digital básica (AD-B), Assinatura digital com carimbo de tempo (AD-T), Assinatura digital com referências para validação (AD-R), Assinatura digital com informações completas (AD-C) em Assinatura digital com informações para arquivamento (AD-A), de acordo com as definições do documento DOC-ICP-15.01 da ICP-Brasil.

3.2.2 - Componente Verificador

O componente verificador possui funcionalidade de visualização do conteúdo do documento verificado.

Permite a visualização das assinaturas digitais e os atributos do certificado de cada signatário do documento e valida o certificado digital no ato da conferência da assinatura e permiti que, para cada assinatura digital, seja visualizada a situação da verificação ou a descrição do erro caso a assinatura digital seja inválida.

3.2.3- Componente Validador

O componente validador é capaz de validar qualquer tipo de certificado digital e sua correspondente cadeia de certificação padrão ICP-Brasil. A validação da cadeia de certificação bem como a consulta da lista de certificados revogados (LCR) é feita de forma parametrizável, de modo que seja possível direcionar o validador para uma base de dados específica por meio de HTTP e OCSP (Online Certificate Status Protocol).

3.2.4 - Componente Carimbador

Realiza a requisição do Carimbo do Tempo junto à Autoridade de Carimbo do Tempo – ACT, bem como insere o carimbo do tempo nas assinaturas digitais, quando necessário, de acordo com as definições do documento DOC-ICP-11 da ICP-Brasil.

3.2.5 - Componente Gerenciador de LCR

O componente gerenciador de LCR capturar na Internet as Listas de Certificados Revogados de todas as Autoridades Certificadoras (AC) necessárias à validação dos certificados apresentados, armazenando-as numa base de dados específica. Essa base de dados fica disponível para uso pelos demais componentes do Framework, permitindo a consulta acerca do status de revogação dos certificados digitais nela mantidos.

A base de dados criada é acessível por meio de HTTP e OCSP (Online Certificate Status Protocol). Identifica e lida com todos os tipos de certificados digitais ICP-Brasil, manipula lista de certificados revogados que implementam a versão 2, ou versão atual, do padrão ITU-T X.509.

Verifica a validade de cada LCR armazenada na base dados específica, de modo a capturar automaticamente uma nova versão na Autoridade Certificadora - AC emissora, mantendo essa base sempre atualizada e autentica cada LCR obtida junto às AC, conferindo se realmente a LCR foi emitida pela Autoridade Certificadora indicada.

Em termos de gerência das listas mantidas na base de dados, o componente gerenciador de LCR:

- Permiti a inclusão e exclusão de Autoridades Certificadoras das quais as LCR devem ser capturadas;
- Prove um mecanismo de alerta por e-mail ou site de monitoramento web que dê ciência ao administrador do sistema sobre problemas com alguma AC cadastrada ou problemas de atualização/validade de cada LCR tratada, informando, ao final de cada processo de atualização da base, problemas de não-conformidade encontrados.

3.2.6- Autoridade de Carimbo do Tempo (ACT)

A Autoridade de Carimbo do Tempo (ACT) fornece o carimbo do tempo TSQ(Timestamp), que possibilita acrescentar a hora legal brasileira no padrão ICP-Brasil, em arquivos eletrônicos de forma autêntica e auditável, fornecendo a prova temporal.

O Carimbo do Tempo é um documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital, que diz respeito ao instante em que o mesmo foi submetido ao carimbo e não à data de sua criação.

3.3 - REQUISITOS FUNCIONAIS DA SOLUÇÃO

Os componentes estão em conformidade com as demais resoluções e documentos disponibilizados e aprovados pelo ITI, em relação às rotinas e procedimentos específicos quanto à criptografia, certificação digital, assinatura digital, verificação das assinaturas e do carimbo de tempo, para todos os requisitos e funcionalidades.

O Framework e seus componentes suportam todos os algoritmos criptográficos e tamanhos de chaves aprovados pela Resolução nº 65 (2009) quando cabíveis.

Todos os componentes permitem a geração, visualização e armazenamento de registro eletrônico, log dos procedimentos executados, bem como das informações pertinentes à usuário e rede, para fins de auditoria.

O Framework suporta uma carga inicial de no mínimo 500 requisições de assinaturas por segundo, podendo ser escalável para atender necessidades futuras da Instituição.

3.4 - FUNCIONAMENTO DA SOLUÇÃO

A interface da Solução de Framework de Certificado Digital está disponível no Portal de Certificação Digital na intranet da Instituição. O portal tem o objetivo de reunir todas as informações sobre certificação digital em um só ambiente, conforme Figura 3.3.

Figura 3.3: Portal de Certificação Digital

Fonte: Intranet da Instituição.

As funcionalidades são disponibilizadas em componentes modulares distintos para permitir assinar, co-assinar, contra assinar, validar as assinaturas digitais e requisitar e anexar ou incorporar carimbo do tempo, representados na Figura 3.4, com o fluxo das operações da Solução de Framework.

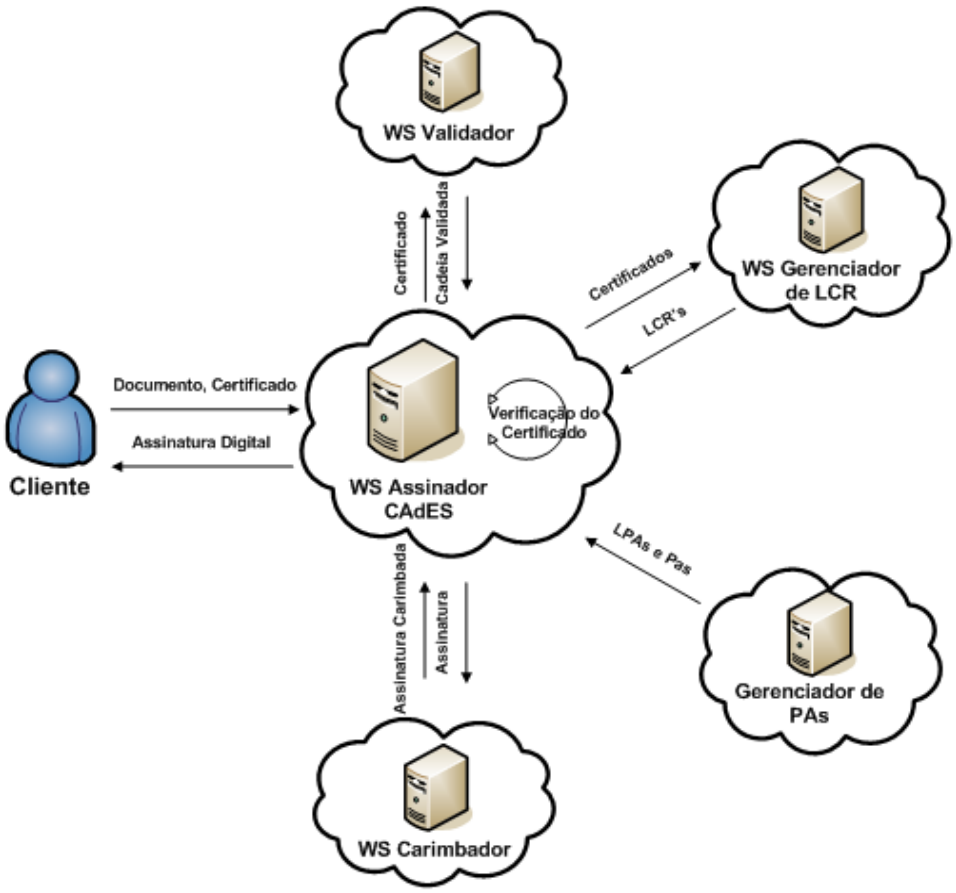

Figura 3.4: Fluxo das operações da Solução de Framework.

Fonte: Requisições e Especificações, 2009.

3.4.1-Assinatura Digital Básica

O processo de assinatura digital básica é apresentado na Figura 3.5. O sistema Internet Banking verifica no módulo verificador se não tem componente em cachê, se tem, o módulo verifica se é a mesma versão, caso seja, retorna a confirmação para o sistema Internet Banking. Caso não tenha o componente em cachê, encaminha ao sistema Internet Banking o componente solicitado e mais o componente validador. O sistema Internet Banking consulta no módulo validador, na base de dados de cadeia de certificados digitais, se o componente é correspondente e consulta no módulo gerenciador de Lista de Certificados Revogados (LCR), na base de dados de LCR se o certificado não está revogado, estando válido, o módulo assinador gera a assinatura digital e encaminha ao sistema Internet Banking. O módulo gerenciador de LCR não permite gerar assinatura digital se o certificado digital do usuário for inválido.

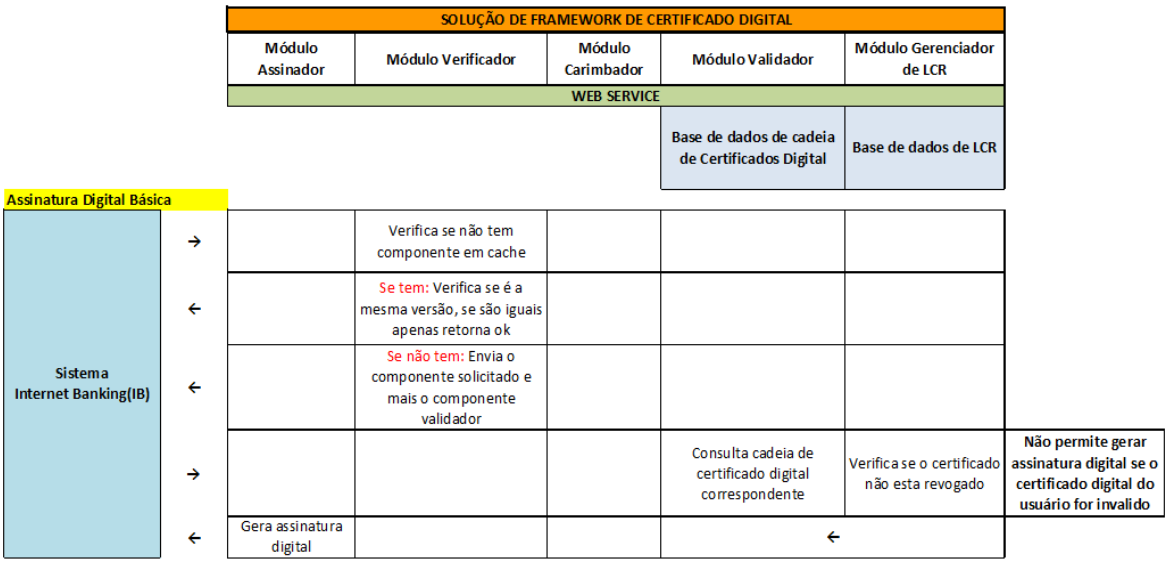

Figura 3.5: Fluxo Assinatura Digital básica

Fonte: Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010.

3.4.2-Assinatura Digital com Carimbo de Tempo

O processo de assinatura digital com carimbo de tempo é apresentado na Figura 3.6. O sistema Internet Banking verifica no módulo verificador se não tem componente em cachê, se tem, o módulo verifica se é a mesma versão, caso seja, retorna a confirmação para o sistema Internet Banking. Caso não tenha o componente em cachê, encaminha ao sistema Internet Banking o componente solicitado e mais o componente validador. O sistema Internet Banking consulta no módulo validador, na base de dados de cadeia de certificados digitais, se o componente é correspondente e consulta no módulo gerenciador de Lista de Certificados Revogados (LCR), na base de dados de LCR se o certificado não está revogado, estando válido, o módulo carimbador gera o hash e envia a ACT – autoridade certificadora de tempo com o requerimento TimeStampReq (TSQ), que registra e encaminha o requerimento ao módulo assinador, que gera a assinatura digital com o carimbo de tempo e encaminha ao sistema Internet Banking. O módulo gerenciador de LCR não permite gerar assinatura digital se o certificado digital do usuário for inválido.

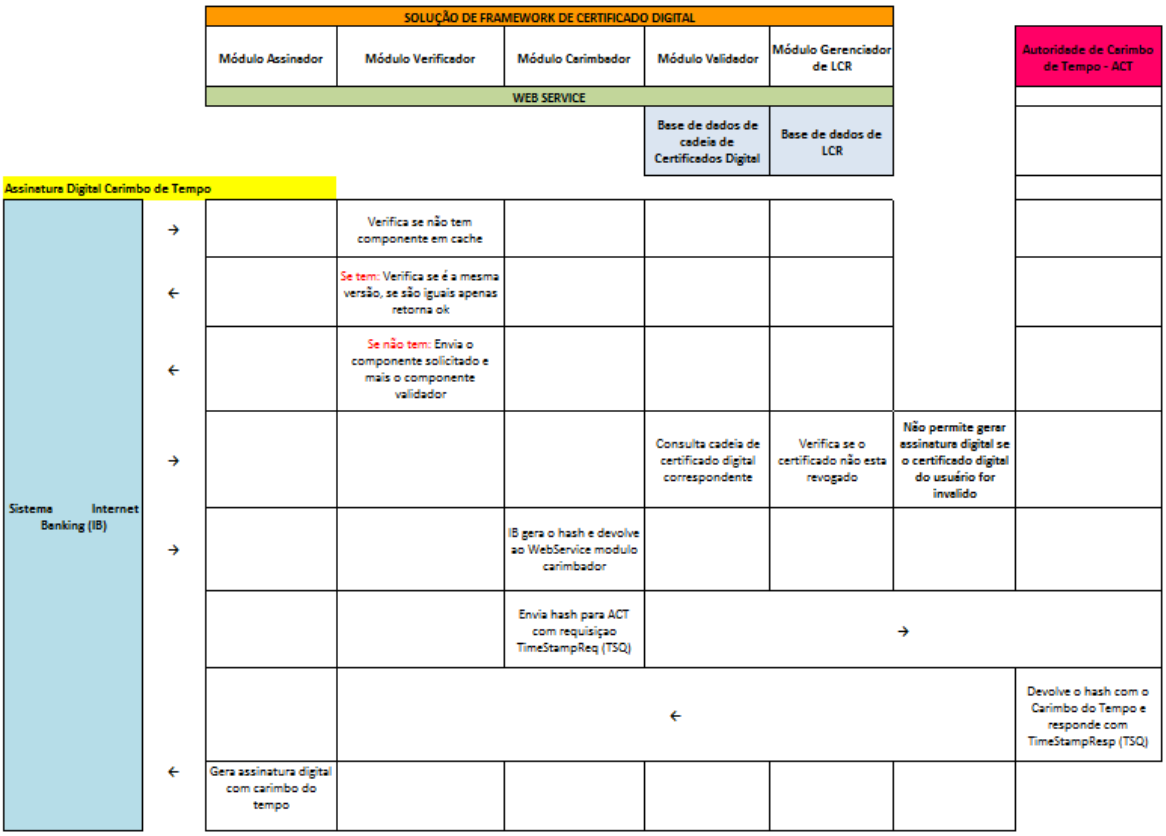

Figura 3.6: Fluxo Assinatura digital com carimbo de tempo.

Fonte: Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010.

3.4.3 - Verificação de Assinatura Digital sem carimbo do Tempo

O processo de verificação de assinatura digital sem carimbo do tempo é apresentado na Figura 3.7. O sistema Internet Banking verifica no módulo verificador se não tem componente em cachê, se tem, o módulo verifica se é a mesma versão, caso seja, retorna a confirmação para o sistema Internet Banking. Caso não tenha o componente em cachê, encaminha ao sistema Internet Banking o componente validador e o componente verificador. O sistema Internet Banking consulta no módulo validador, na base de dados de cadeia de certificados digitais, se o componente é correspondente e consulta no módulo gerenciador de Lista de Certificados Revogados (LCR), na base de dados de LCR se o certificado não está revogado, estando válido, encaminha ao modulo verificador que verifica a assinatura digital e retorna a validação para o sistema Internet Banking.

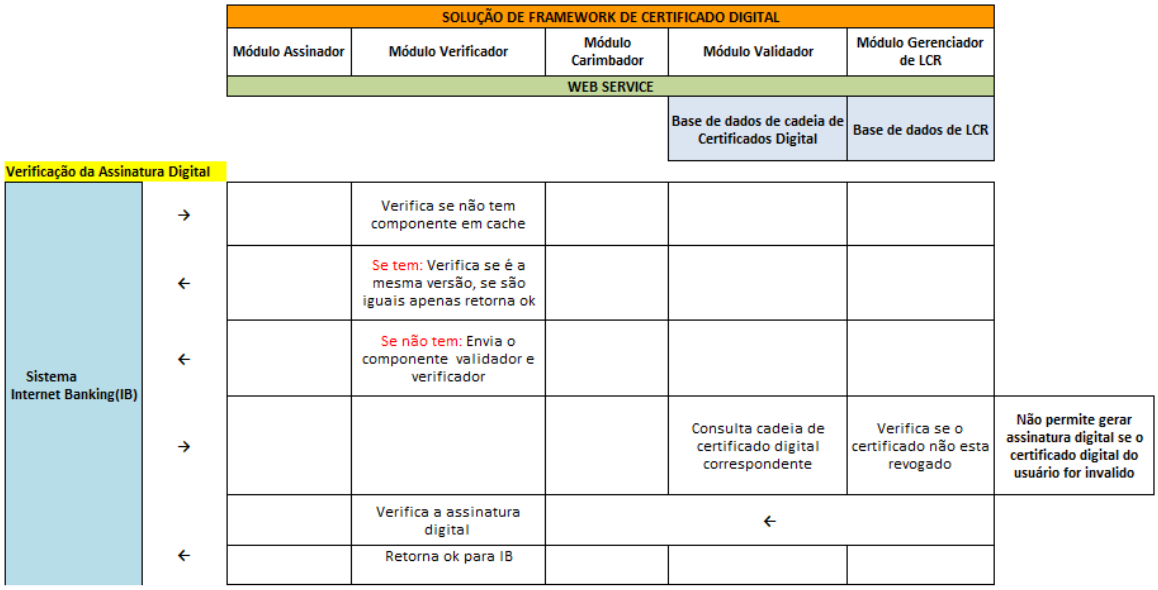

Figura 3.7: Fluxo Verificação de assinatura digital sem carimbo de tempo.

Fonte: Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010.

3.4.4 - Verificação de Assinatura Digital com carimbo do Tempo

O processo de verificação de assinatura digital com carimbo do tempo é apresentado na Figura 3.8. O sistema Internet Banking verifica no módulo verificador se não tem componente em cachê, se tem, o módulo verifica se é a mesma versão, caso seja, retorna a confirmação para o sistema Internet Banking. Caso não tenha o componente em cachê, encaminha ao sistema Internet Banking o componente validador e o componente verificador. O sistema Internet Banking consulta no módulo validador, na base de dados de cadeia de certificados digitais, se o componente é correspondente e consulta no módulo gerenciador de Lista de Certificados Revogados (LCR), na base de dados de LCR se o certificado não está revogado, estando válido, encaminha o componente para o módulo verificador para verificar e envia o hash para o módulo carimbador, que encaminha o hash para a ACT – autoridade certificadora de tempo com o requerimento TimeStampReq (TSQ), a ACT verifica se o carimbo do tempo confere e retorna ao sistema Internet Banking.

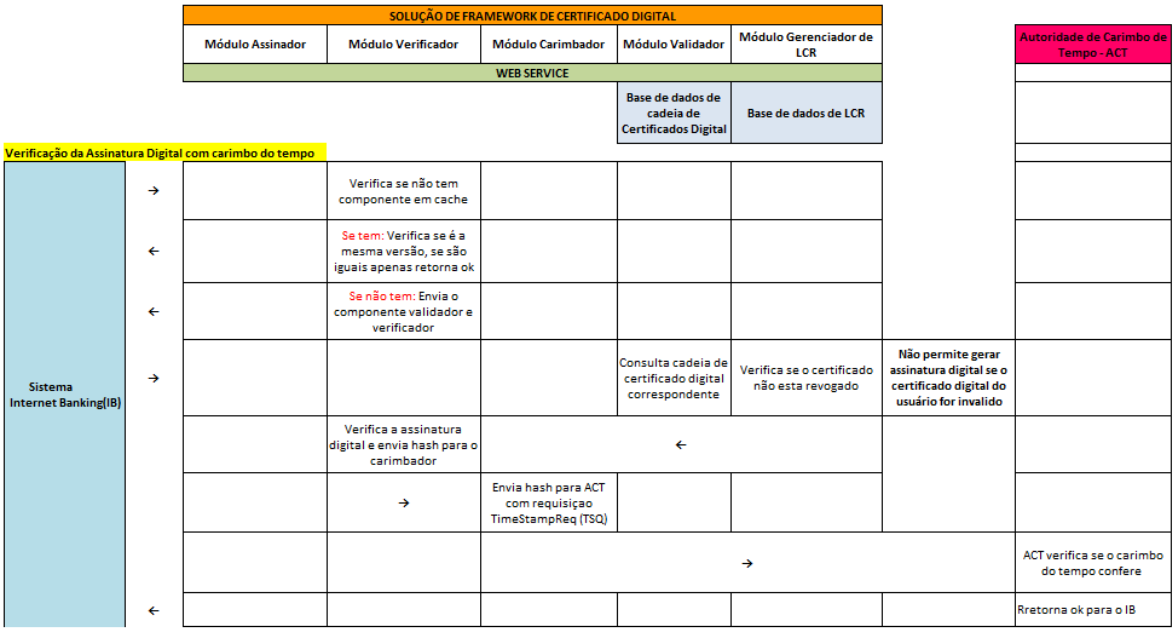

Figura 3.8: Fluxo Verificação de assinatura digital com carimbo de tempo.
Fonte: Adaptado de Requisições e Especificações, 2009 e Plano de Projeto, 2010.

Diante da implementação do projeto certificado digital no Internet Banking, utilizando a solução de framework de certificado digital aqui descrita, conhecer e identificar as vulnerabilidades da solução é uma tarefa que envolve análise e constante estudo dos processos inerentes às atividades corporativas da Instituição, pois são impactantes na visão da tecnologia, negócio e principalmente dos clientes.

Assim, se pretende pontuar se os elementos de sustentação ao uso do certificado digital no Internet Banking, apontados pelos autores, estão sendo tratados de forma a garantir sua efetividade em todo processo.

4 –PROSPECÇÃO DA INSTITUIÇÃO E DOS CLIENTES DA SOLUÇÃO DE INTERNET BANKING COM CERTIFICADO DIGITAL

Neste capítulo é descrito o projeto certificado digital no Internet Banking utilizando a solução de framework de certificado digital do Banco Capital, sob o ponto de vista da tecnologia, negócio e clientes. As vantagens, benefícios e objetivos que se pretende alcançar com esta técnica de segurança são avaliados com os apontamentos da revisão de literatura e uma proposta de recomendações é sugerida.

4.1 - OBSERVAÇÕES DA INSTITUIÇÃO PUBLICA BANCÁRIA

Na percepção do Banco Capital, a aplicação do projeto certificado digital na Internet Banking é descrita na visão da tecnologia da informação, negócio e cliente.

4.1.1 – Visão da Tecnologia da Informação

A aquisição da solução de framework veio atender as iniciativas estratégicas de TI, definidas no plano executivo da Instituição, buscando revisar o modelo do processo de desenvolvimento e implantar a integração de serviços de TI.

O projeto Internet Banking com certificado digital é coordenado pela gerência de segurança e continuidade de negócios em TI, que tem o objetivo de estabelecer e gerir as diretrizes, padrões e modelos de segurança para ativos, processos e serviços de TI, visando garantir a segurança tecnológica e viabilização do negócio. A gerência é vinculada a superintendência de suporte de TI, responsável por operacionalizar e manter disponíveis as soluções tecnológicas que suportam os produtos e serviços da Instituição.

A disponibilização da solução para implementação de serviços e produtos, como no Internet Banking, garante a maior agilidade nas transações e automação do processo de certificado digital, tornando o único local para replicar atualizações, de acordo com os padrões vigentes da ICP-Brasil, centralizando os sistemas que possam utilizar a solução. A Solução de Framework de Certificado Digital implementa a prática de melhoria de processo, apresenta uma nova tecnologia no ambiente e transfere o conhecimento

tecnológico para as equipes internas, permitindo o domínio da tecnologia de certificação digital na Instituição (Plano de Projeto, 2010).

A solução está hospedada em ambiente de Brasília, estrutura preparada para garantir o melhor tempo de processamento e disponibilidade, nos padrões definidos pelo Manual Normativo (2011), que tem o objetivo de estabelecer as diretrizes de desenvolvimento seguro, guiando e promovendo a aplicação das melhores práticas de segurança no ciclo de desenvolvimento de sistemas, além de destacar a adoção de mecanismos e processos para a garantia da confidencialidade, integridade, disponibilidade e autenticidade das informações armazenadas nos sistemas de informação da Instituição.

A solução adquirida pela BRy Tecnologia S.A., empresa brasileira especializada no desenvolvimento de soluções de segurança para documentos eletrônicos, com modelo e metodologia próprios, cabendo assim, a Instituição definir que todos os sistemas e produtos que são dependentes de assinatura digital, devem utilizar a solução de framework de certificação digital como a infraestrutura.

Na visão da Instituição, esta ação melhora a imagem de TI junto aos clientes e mantém a tecnologia conhecida e dominada.

4.1.2 – Visão do Negócio

Com a ampliação dos negócios e transações realizadas no canal Internet Banking, maturidade do mercado frente e o aumento das fraudes eletrônicas, a Instituição requer soluções de segurança imediatas, tornando a implantação da certificação digital no Internet Banking propícia (Plano do Projeto, 2010).

A adoção do certificado digital está alinhada aos objetivos definidos no planejamento estratégico da Instituição, com as perspectivas de ter um processo eficiente, com inteligência competitiva e processo voltado para inovação.

O Internet Banking com certificado digital oferece maior alçada para realização de transações, substituição de senha internet para aplicação, resgate de fundos, solicitação e desbloqueio de talão de cheques e limites diferentes para transações a partir de login com

certificado, ou seja, oferece transações com valores diferenciados aos clientes, que utilizam o certificado digital (Plano do Projeto, 2010).

O aumento da segurança no uso do canal Internet Banking e ampliação da movimentação financeira por meio de transações mais seguras têm gerado maior competitividade no mercado e projeção positiva da Instituição na mídia externa, passando a atender vários outros serviços, como, validação de alvará eletrônico, validação de documentos eletrônicos previstos em cláusulas contratuais acordadas com fornecedores e autorização de débito emitida pelas agências regionais da Receita Federal, dentre outros (Plano do Projeto, 2010).

Dessa forma, pode-se visualizar na Tabela 4.1 um resumo dos fatores apontados pela Instituição com a aquisição da solução de framework de certificado digital e a implantação do projeto certificado digital no Internet Banking.

Tabela 4.1: Resumo dos fatores apontados pela Instituição

Proposta Implantada	**Vantagens Pontuadas**
- Aquisição da solução de framework de certificado Digital	Iniciativas estratégicas de TI
- Disponibilização da solução de framework de certificado digital	Garante maior agilidade nas transações e automação do processo de Certificado Digital, centraliza e torna o único local para replicar atualizações
- Conhecimento da solução de framework de certificado digital	Apresenta uma nova tecnologia no ambiente, transfere o conhecimento tecnológico para as equipes internas, permitindo o domínio da tecnologia de Certificação Digital na Instituição
- Ambiente da solução de framework de certificado digital	Estrutura preparada para garantir o melhor tempo de processamento e disponibilidade, de acordo com as diretrizes de práticas de segurança no ciclo de desenvolvimento de sistemas, destacando os mecanismos e processos para a garantia da confidencialidade, integridade, disponibilidade e

Proposta Implantada	Vantagens Pontuadas
	autenticidade das informações armazenadas nos sistemas de informação da Instituição.
- TI com a solução de framework de certificado digital	Melhora a imagem de TI junto aos clientes e mantém a tecnologia conhecida e dominada.
- Certificação digital no Internet Banking	Solução de segurança imediata contra o aumento das fraudes eletrônicas. Oferece maior alçada para realização de transações, substituição de senha internet para aplicação, resgate de fundos, solicitação e desbloqueio de talão de cheques e limites diferentes para transações a partir de login com certificado.
- Adoção do certificado digital na Instituição	Está alinhado aos objetivos do Planejamento Estratégico, com as perspectivas de ter um processo eficiente, com inteligência competitiva e processo voltado para inovação.
- Imagem da Instituição com o certificado digital no Internet Banking	Gera maior competitividade no mercado e projeção positiva da Instituição na mídia externa.

A utilização da solução de framework para certificado digital no Internet Banking busca alcançar os seguintes objetivos (Plano do Projeto, 2010):

- Criação de novos negócios por meio do canal Internet Banking, devido ao reconhecimento da validade jurídica dos contratos firmados por certificado digital;
- Racionalização do tempo dos recursos humanos lotados nas agências, incentivando a migração de clientes para o canal Internet Banking;
- Aumento no volume financeiro transacionado com redução nos custos de transação;
- Fidelização de clientes com a isenção de tarifas dos certificados;
- Reforço da imagem da Instituição como moderna;

- Aumento da clientela de Pessoa Jurídica por meio dos escritórios de contabilidade.

4.1.3-Visão dos Clientes

Milan e Trez (2005) afirmaram que a definição mais importante de qualidade percebida nos serviços é a definida pelo cliente, já que muitas vezes o que os gestores entendem como qualidade difere totalmente da opinião dos usuários.

Carvalho (2009) caracteriza que conseguir se aproximar da percepção dos clientes é fundamental para a definição de ações, melhoria de desempenho, sobrevivência e lucratividade das instituições.

A Instituição mensura a satisfação dos clientes do Internet Banking através da disponibilidade do serviço, sendo, mensurado em indicadores a quantidade de operação x tempo de resposta da aplicação x fila de espera de abertura de chamados dos usuários.

A monitoração do canal é realizada através da gerência de operações tecnológicas que tem como atividade os recursos tecnológicos, processos e rotinas do ambiente centralizado e de alta disponibilidade e o processamento, disponibilização e armazenamento das soluções de TI no ambiente centralizado e de alta disponibilidade.

É mantida uma sala de contingência para o gerenciamento de incidentes, que busca restaurar a operação normal do serviço o mais rápido possível, minimizando os prejuízos à operação do negócio, garantindo o melhor nível de serviço, disponibilidade e produtividade do negócio.

4.2 - ANÁLISE DOS ELEMENTOS DE SUSTENTAÇÃO

Para analisar os elementos de sustentação da efetividade da solução de framework de certificado digital fazem-se necessário citar as considerações abordadas pelos autores na revisão de literatura, comparando com as descrições e práticas exercidas pelo Banco Capital no projeto de certificado digital no Internet Banking.

4.2.1 – Riscos

Quanto aos riscos, pode-se dizer que são as possibilidades das ameaças explorem as vulnerabilidades, ocasionando danos ou perdas de dados, proporcionando prejuízos aos negócios da empresa e que acabam por afetar os princípios de confiabilidade, integridade e disponibilidade. A visão do risco como parte do negócio obriga a uma preocupação quanto aos principais eventos que possam colocar perigo o resultado, as pessoas, as informações, o ambiente e os demais entes relacionados (Beal, 2008).

Beal (2008) aponta que a gestão de risco é o conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos aos seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Cobit (2007) define que a gestão dos riscos requer a conscientização da alta direção executiva da empresa, um claro entendimento do risco que a empresa está disposta a correr, compreender os requisitos normativos envolvidos, transparência quanto aos riscos significativos para a empresa e a inserção das responsabilidades na administração de riscos dentro da organização.

Todo evento que representa um risco deve ser identificado, analisado e estimado, o que, uma vez realizado, deve buscar minimizar os seus e comunicar o risco residual, que é o risco que se sabe estar ainda correndo (Cobit, 2007).

Os elementos de sustentação da efetividade do projeto de certificado digital no Internet Banking do Banco Capital foram mapeados em forma de riscos, considerando os apontamentos dos autores e a posição do Banco Capital. Os riscos do projeto de certificado digital são apontados na Tabela 4.2: Risco Aderência ao Internet Banking, Tabela 4.3: Risco Prática de segurança no Internet Banking, Tabela 4.4: Risco Aceitação de uso da Certificação e Imagem, Tabela 4.5: Risco Frameworks para Gestão, Tabela 4.6: Risco Auditoria, Tabela 4.7: Risco Arquivamento e Tabela 4.8: Risco Confiabilidade, Integridade, Autenticidade e Disponibilidade.

Tabela 4.2: Risco Aderência ao Internet Banking

Elementos	Apontamentos dos autores
Aderência ao Internet Banking	O Internet Banking tem se destacado como canal o mais importante inovação de serviços bancários dos últimos anos (Diniz et al., 2009). Febraban (2012) aponta que o Internet Banking firmou-se como o canal preferido para transações bancárias. O usuário de Internet Banking realiza em média 3,2x o volume de transações que os clientes em geral (Febraban, 2013). Os Bancos devem investir na maximização do uso do Internet Banking, prover uma experiência do consumidor cada vez mais amigável neste canal e ofertar produtos e serviços que melhor se encaixam neste meio (Febraban, 2013).
Posição do Banco Capital	
A Instituição definiu diretrizes no planejamento estratégico com o objetivo de alavancar o uso do certificado digital em sistemas e produtos, como forma de oferecer maior segurança no canal.	

Tabela 4.3: Risco Prática de segurança no Internet Banking

Elementos	Apontamentos dos autores
Prática de segurança no Internet Banking	Bacen (2001), devem garantir o sigilo e a segurança dos meios eletrônicos tornados disponíveis, bem como o adequado monitoramento das informações relativas à movimentação das contas. Peotta et al. (2011) demonstram uma análise dos dispositivos de segurança implementados pelos dez maiores bancos no Brasil e concluiu que várias camadas e métodos de segurança são simultaneamente adotadas pelas instituições bancárias, mas que vulnerabilidades de segurança nos sistemas bancários são detectados. Indica que os sistemas bancários devem fornecer

	mecanismos de segurança capazes de reduzir o vazamento de informações e problemas de segurança que afetam o sistema e que leva à fraude. Zhang (2009) aponta o certificado digital como uma técnica eficaz de prevenção de fraudes no Internet Banking.
Posição do Banco Capital	
Para implementar o certificado digital no Internet Banking, a Instituição adquiriu a solução de framework de certificado digital. Apesar da solução estar instalada em ambiente seguro, com permissões de acesso aos gestores de tecnologia e do canal Internet Banking, percebeu-se que a solução não atende requisitos das práticas de segurança internos, definidos pela própria Instituição no Manual Normativo (2011).	

Tabela 4.4: Risco Aceitação de uso da Certificação e Imagem

Elementos	**Apontamentos dos autores**
Aceitação de uso da Certificação e Imagem	Zhao (2010) percebeu que as Instituições bancárias devem aumentar a satisfação dos usuários através dos sistemas que oferecem qualidade e segurança das informações e serviços. Chatzipoulidis e Mavridis (2010) acreditam que se uma violação de segurança ocorrer devido à uma perda de integridade durante uma transação do Internet Banking, o impacto influência todos os outros parâmetros de aceitação do usuário em relação aos serviços bancários eletrônicos. Carvalho (2009) caracteriza que conseguir se aproximar da percepção dos clientes é fundamental para a definição de ações, melhoria de desempenho, sobrevivência e lucratividade das instituições.
Posição do Banco Capital	

A tecnologia com a solução de framework de certificado digital melhora a imagem de TI junto aos clientes e mantém a tecnologia conhecida e dominada. Gera maior competitividade no mercado e projeção positiva na mídia externa. O gestor de cada canal é responsável pela gestão do seu negócio, sistemas e produtos, cabendo apenas a TI a implementação das tecnologias para atender os gestores. A Instituição mensura a satisfação dos clientes do Internet Banking através da disponibilidade do serviço, sendo apontada em indicadores a quantidade de operação x tempo de resposta da aplicação x fila de espera de abertura de chamados dos usuários.

Tabela 4.5: Risco Frameworks para Gestão

Elementos	**Apontamentos dos autores**
Frameworks para Gestão	Chen e Argles (2010) vêm considerar a importância dos frameworks analisarem os requisitos e metodologia quando utilizam a certificação, principalmente sua gestão. A falta de um gerenciamento apropriado expõe as Instituições a um risco não quantificado dentro das organizações, incluindo acesso não autorizado e falhas em auditorias de segurança. A gestão dos certificados ajuda a identificar questões de segurança, conformidade e operacionais dentro de um ambiente, além de prover indicações que as organizações devem seguir no sentido de eliminar riscos (Gartner, 2011).
Posição do Banco Capital	
A disponibilização da solução de framework de certificado digital garante maior agilidade nas transações e automação do processo de certificado digital, centraliza e torna o único local para replicar atualizações. Conhecimento da solução de framework de certificado digital apresenta uma nova tecnologia no ambiente, transfere o conhecimento tecnológico para as equipes internas, permitindo o domínio da tecnologia de certificação digital na Instituição.	

A certificação digital no Internet Banking tem a solução de segurança imediata contra o aumento das fraudes eletrônicas. Oferece maior alçada para realização de transações, substituição de senha internet para aplicação, resgate de fundos, solicitação e desbloqueio de talão de cheques e limites diferentes para transações a partir de login com certificado. A Instituição, na visão da tecnologia, coloca que a solução não foi preparada para fazer o gerenciamento e nem realizar a gestão dos certificados digitais internamente utilizados. Além disso, a solução não possui preparo para tratamento específico de incidentes que possam vir a acontecer no uso do certificado digital. A metodologia da solução de framework de certificado digital foi desenvolvida pela empresa BRySigner® - Assinador de documentos eletrônicos no padrão ICP-Brasil, diante de especificação realizada pela Instituição. Entretanto, não foram identificadas informações de referências dos conceitos adotados pela empresa para atender a Instituição e nem referências em outras soluções bancárias.

Tabela 4.6: Risco Auditoria

Elementos	**Apontamentos dos autores**
Auditoria	Boynton (2002) descreve os procedimentos de auditoria possibilitam afirmar se as informações partem de fontes confiáveis e se os procedimentos para obtê-las estão sendo seguidos corretamente, possibilitando aos seus usuários analisar com maior confiança as informações oferecidas pelas entidades, sustentando melhor as decisões que precisam ser tomadas. Pereira e Santos (2010) frameworks adotado como sistemas de informações devem passar pela auditoria de segurança, realizadas para avaliar a eficácia da capacidade de uma instituição protegendo seus ativos valorizados ou críticos.

	ITI (2012) infraestrutura de chaves pública brasileira é responsável por realizar as auditorias, fiscalizações e homologações das certificações.
Posição do Banco Capital	
A Instituição realiza este procedimento baseado no Manual Normativo (2011) de segurança para o desenvolvimento e manutenção de sistemas, sendo emitido um relatório de aprovação a cada versão atualizada do framework. A solução de framework não tem um manual normativo específico que define os sistemas e os produtos que utilizarão a solução, as áreas envolvidas, as versões homologadas, o fluxo de funcionamento, comunicação e padronizações internas. Não há, ainda, um normativo que relacione a solução de framework com a área jurídica da Instituição, para o tratamento do reconhecimento da validade jurídica do certificado digital no canal Internet Banking, inclusive para orientar as futuras contestações quanto ao ônus da prova nos processos de fraude.	

Tabela 4.7: Risco Arquivamento

Elementos	**Apontamentos dos autores**
Arquivamento	Os arquivos existem para armazenar informações e permitir que estas sejam recuperadas mais tarde. São gerenciados por sistemas que oferecem diferentes tipos de armazenamento e recuperação das informações, baseados na estrutura, acessos, como são utilizados, protegidos e implementados (Tanebaum, 2003). Teixeira (2002) destaca que tão ou mais importante que a identidade vinculada ao passado é a identidade que se projeta para o futuro. O ICP-Brasil fica instituído 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 (Medida Provisória 2.200, 2011).

	Lei nº 12.682 (2012) que se refere ao arquivamento de documentos em meios eletromagnéticos. ICP-Brasil descreve a política geral de arquivamento de registros no DOC-ICP 05 (2012). Peotta et al. (2009) apresentam um estudo sobre as regulamentações adotadas pelo ICP-Brasil, identificando que as normas que contemplam os aspectos relevantes para conferir os documentos assinados digitalmente e as características técnicas não são suficientes e efetivas ao longo prazo.
Posição do Banco Capital	
Não foi identificado no Plano de Projeto (2011) qualquer tratamento quanto ao arquivamento das informações registradas pela solução de framework de certificado digital. Os registros são arquivados em computadores da própria equipe de TI envolvidos no projeto, que a cada período capturam e compactam esses registros.	

Tabela 4.8: Risco Confiabilidade, Integridade, Autenticidade e Disponibilidade

Elementos	**Apontamentos dos autores**
Confiabilidade	Leavitt (2011) aponta que vários ataques foram realizados contra organizações que emitem certificados digitais, criando dúvidas sobre o uso do sistema. Os autores Sanayei e Noroozi (2009) trazem uma preocupação quanto as Autoridades Certificadoras com certificados fraudulentos. As certificadoras são consideradas confiáveis, devido ao processo de auditoria, entretanto, algumas ACs autorizam intermediárias para emitir os certificados, que podem roubar certificados digitais e utiliza rde modo forma fraudulenta, gerando assim, dúvidas sobre a segurança e integridade do certificado digital.
Elementos	**Apontamentos dos autores**
Integridade	Ma, Abie, Skramstad e Nygârd (2011) apontam uma preocupação com o mau uso dos mecanismos e segurança para proteger o

	arquivamento dos documentos digitais, que oferecem garantia de serem confiáveis a curto prazo e não eficaz a longo tempo. A utilização da criptografia ao longo da vida digital introduz dois problemas, a perda da chave privada e a de compromisso dos algoritmos criptografados, além da preservação de documentos criptografados não serem geralmente aceitos pela comunidade internacional de arquivamento, porque a codificação não é geralmente preservada uma vez que não há parte integrante dos registros de arquivamento.
Elementos	**Apontamentos dos autores**
Autenticidade	A preservação da legibilidade, verificabilidade e da validade da assinatura digital são crucial para o valor futuro. A longevidade desses dados depende apenas da preservação da sua legibilidade, já a assinatura digital utilizada depende de múltiplos fatores (Lekkas e Gritzalis, 2007). Ansper, Buldas, Roos e Wilemson (2001) apontam as técnicas convencionais de validação dos certificados digitais como não sendo práticas de validação para longo prazo. Questões de dispositivos de segurança, regras de responsabilidade, atualização, distribuição eficiente e armazenamento das informações das chaves públicas são citadas como problemas fundamentas a serem tratados para uso das certificações a longo prazo. Ansper, Buldas, Roos e Wilemson (2001) citam que a deficiência apontada nos método de grandes demandas de assinaturas digitais podem se tornando demoradas, exigindo equipamentos de hardwares para melhor gerir os processamentos, assim propõem melhorar a eficiência ea confiabilidade das novas técnicas de validação. Hu, Giri, Chengyu e Li (2009) destacam que verificar a data de validade e autenticidade de um certificado digital por si só nunca é suficiente, pois é possível que um certificado tenha sido revogado antes da data de sua expiração, com as seguintes razões:

	comprometimento da chave, compromisso da autoridade certificadora (CA), mudança de filiação, substituição ou cessação de operação.
Elementos	**Apontamentos dos autores**
Disponibilidade	Fujishiro, Sato, Kumagai, Kaji e Okada (2010) apresentam um estudo sobre como pode ser melhorada a velocidade da verificação da validade dos certificados digitais no futuro. Defende que com o aumento das Infraestrutura de dados criptográficos, as oportunidades de aplicações e utilizações dos certificados farão que a velocidade de operação dos PKI ficam inferior as exigidas pelos usuários de aplicativos.

Posição do Banco Capital

O ambiente da solução de framework de certificado digital é a estrutura preparada para garantir o melhor tempo de processamento e disponibilidade, de acordo com as diretrizes de práticas de segurança no ciclo de desenvolvimento de sistemas, destacando os mecanismos e processos para a garantia da confidencialidade, integridade, disponibilidade e autenticidade das informações armazenadas nos sistemas de informação da Instituição.

Não foram identificados documentos relacionados à solução de framework de certificado digital e nem do projeto de certificado digital no Internet Banking que tratasse da garantia verificabilidade das informações e dados ao longo do tempo na Instituição.

Na visão da TI, sua responsabilidade é apenas de entregar e disponibilizar a solução de framework de certificado digital funcionando, em ambiente seguro e estável, cabendo ao gestor do negócio do Internet Banking aplicar a verificabilidade e, o negócio, por sua vez, entende que a TI é a área domina a visão futura da tecnologia.

Nenhum documento relata parcerias internas e externas, inclusive outras Instituições bancárias que pudessem tratar essas citações, sobretudo por se tratar do canal que realiza altos números de transações no Brasil.

A Instituição, na visão do gestor do projeto de certificado digital no Internet Banking visa apenas à entrega do acesso à Internet Banking com certificados digitais aos empregados e expansão as clientes, atendendo o Plano de Projeto (2010).

Na Instituição, não foi identificado documentos que envolvem o ICP-Brasil nas regras e aplicações da solução de framework de certificado digital, ficando ausente quanto aos questionamentos ligados a verificabilidade e funcionamento da solução.

A Instituição não possui orientações do ICP-Brasil quanto às dúvidas, homologação, validação e gestão dos processos e dados manipulados na solução de framework de certificado digital a longo tempo.

Não há informações de parcerias realizadas entre os bancos e o ICP-Brasil para o desenvolvimento de um único framework bancário. Ainda, não foram localizados documentos que envolva a FEBRABAN neste processo, por estar atuando na compensação de cheques, SPB- Sistema de Pagamentos Brasileiro.

Com a análise aqui realizada dos elementos de sustentação da efetividade do uso do certificado digital em aplicações de Internet Banking, percebe-se que o Banco Capital não atende as principais considerações apontadas pelos autores. Assim, uma proposta de recomendações é sugerida em forma de plano de ação.

4.3 – PROPOSTA DE RECOMENDAÇÕES

Diante da análise dos elementos de sustentação da efetividade do uso da certificação digital em aplicações de Internet Banking, sugere-se adaptações nas políticas, diretrizes e processos que envolvem certificado digital do Banco Capital.

4.3.1 – Plano de Ação

Um plano de ação consiste em analisar as ocorrências de ameaças baseando-se nos mecanismos instalados e também em ações concretas que visem reduzir os riscos existentes em um processo de melhoria contínua (Carvalho, 2005).

As recomendações sugeridas neste plano de ação, Tabela 4.9, ao projeto certificado digital no Internet Banking, tem o objetivo de mitigar os riscos mapeados para os elementos de sustentação da efetividade do uso da certificação digital no Banco Capital.

Tabela 4.9: Plano de Ação

Elementos	Recomendações
Prática de segurança no Internet Banking	Rever o enquadramento da solução de framework de certificado digital no manual normativo interno de segurança para o desenvolvimento e manutenção de sistemas, alinhando com a resolução de proteção e dados definida pelo BACEN. Incluir as recomendações nas políticas de uso interno do Banco.
Aceitação de uso da Certificação e Imagem	Aplicar pesquisas de satisfação de uso do certificado digital no canal Internet Banking, inicialmente para o público do piloto, os empregados internos. Mensurar o índice de satisfação e utilização e logo após, realizar uma medição entre os clientes.
Frameworks para Gestão	Criar componente gestão na solução de framework de certificado digital, afim de que a área de negócio e de TI possam gerenciar as demandas e os sistemas que são utilizados e tratados pela Solução, oferecendo subsídio para tomada de decisões internas e externas. Gerenciar o uso da solução relacionado ao número de transações e negócios realizados pela Instituição. Oferecer ao jurídico e as áreas envolvidas relatórios para avaliações e acompanhamentos do uso do certificado digital. Registrar e controlar os processos e fluxos de documentos digitaisde cada sistemas. Notificar e permitir que as partes envolvidas acompanhem o processo e a assinatura digital dos documentos eletrônicos. Registrar todas as movimentações referentes aos documentos eletrônicos de modo a permitir o rastreamento e auditoria,

	fornecendo todas as evidências necessárias para garantir o não-repúdio de transações eletrônicas, prevenindo e detectando alterações ou manipulações fraudulentas nos documentos. Permitir que todas as inclusões, alterações e exclusões sejam realizadas de forma on-line, mantendo históricos das manutenções e possibilitar a transferência para backups e o expurgo dos dados de acordo com a periodicidade definida pela Instituição. Apresentar ao ICP-Brasil proposta direta de acompanhamento e consultoria para aplicação e gestão de soluções de frameworks relacionados ao setor bancário. Envolver o ICP-Brasil nos futuro da Certificação Digital voltados ao canal do Internet Banking e aos diversos sistemas que utilizarão a Solução de Certificados Digitais. Adotar um padrão único de Framework Bancário.
Auditoria	Criar manual normativo da tecnológica especificando asolução de framework de certificado digital, detalhando as áreas envolvidas, os responsáveis, fluxo de demanda e atendimentos e armazenamento dos dados. Incluir a solução de framework de certificado digital nos demais manuais normativos relacionados, principalmente no Internet Banking. Incluir as regras de tratamento e utilizações da solução nos manuais normativos do jurídico, relacionando o tratamento da auditoria para fiscalização da solução e para futuras contestações de fraude.
Arquivamento	Tratar o arquivamento para os registros e logs realizados na solução de framework de certificado digital adequadamente, de acordo com a Lei 12.682, definições do ICP-Brasil e

	principalmente ao manual normativo interno. Mantendo os documentos armazenados pelo período de tempo determinado pela Lei aplicável a cada tipo ou operação. Definir regras e responsáveis, entre gestores de negócio, TI e jurídico para acesso aos arquivos tratados pela solução, implementando um fluxo de autorizações para tratamento de demandas de solicitação dos arquivos. Prover o armazenamento dos dados da solução, com a guarda dos documentos eletrônicos participantes dos fluxos em banco de dados corporativo, compatível nos padrões e ambiente definidos, podendo ser acessados somente pelas partes envolvidas ou previamente autorizadas pelo criador do documento, garantindo integridade, disponibilidade e confidencialidade da documentação.
Confiabilidade **Integridade** **Autenticidade** **Disponibilidade**	Criar grupo de estudo com parcerias entre ICP-Brasil, Febraban e outras Instituições bancárias, áreas jurídicas, acadêmicas e mercado para tratar a verificabilidade do uso do Certificado Digital ao longo do tempo. Mapear internamente com área da TI e negócio os impactos futuros do uso do certificado digital para os clientes do Internet Banking. Alinhar com as áreas internas os papéis e responsabilidade para o uso e tratamento das informações geradas pela solução de framework de certificado digital no Internet Banking.

Com as recomendações sugeridas no plano de ação, pode-se mitigar os riscos do projeto. As melhorias alcançadas com essas ações promovem a melhor gestão do negócio e da tecnologia no portfólio dos produtos e serviços oferecido pela Instituição. Garante o controle e gerenciamento de acessos e movimentações de transações realizadas pelos clientes no Internet Banking, com mais autonomia e domínio do processo.

Após a aplicação do plano de ação sugerido com este estudo, uma política de gestão dos elementos de efetividade do uso da certificação na Instituição deverá ser criada, de forma a estruturar e atualizar as práticas que fundamentam o uso da criptografia, certificado digital, assinatura digital e carimbo do tempo já existentes no Banco Capital.

5- CONCLUSÃO

Este trabalho apresenta a importância e necessidade das organizações bancárias investirem em tecnologia, em seus equipamentos, infraestrutura, software e inovação para alavancar os serviços do setor bancário.

A tecnologia adotada é responsável pela disponibilidade dos canais de atendimento bancário, oferecendo novos aplicativos e segurança na realização de toda transação. O uso do Internet Banking fez com que os clientes ganhassem mais autonomia nas movimentações bancárias das contas, tronando um canal mais eficiente, rápido e sem custos.

Os representativos números de transações bancárias realizadas nesse canal fizeram com que as Instituições Bancárias adotassem técnicas de segurança eficaz contra fraude, pois a proteção das informações e dados dos clientes gera mais confiança, ganho de mercado, negócios e destaque da imagem.

A técnica de certificação digital no Internet Banking foi adotada pela Instituição apresentada neste trabalho, como forma de oferecer maior segurança, integridade, autenticidade e não repúdio. O projeto de certificação digital no Internet Banking na Instituição vem sendo implementado por etapas, inicialmente no acesso/log ao canal.

Para a execução do projeto, a Instituição adquiriu a solução de framework de certificado digital, com o intuito de centralizar todos os processos que envolvem certificação nos produtos e sistemas interno.

A infraestrutura implementada gera todo ciclo de vida do certificado digital, atendendo as necessidades especificadas para empresa de desenvolvimento, porém, a proposta desse trabalho foi analisar os elementos de sustentação da efetividade do uso do certificado digital em aplicações de Internet Banking, através da solução de framework adotada pelo Banco Capital.

A análise foi realizada com o apoio em pesquisa e revisões de literatura relacionadas ao tema. Foi apresentado o estudo de caso da Instituição, detalhando o projeto, arquitetura, funcionamento e as visões da tecnologia, negócio e clientes.

Percebeu-se que a solução de framework não trata os elementos de sustentação da efetividade do uso do certificado digital no Internet Banking. Sua prospecção não foi definida com os aspectos indicados pelos autores. Sendo que sua aplicação no projeto de certificado digital no Internet Banking pode gerar diversos questionamentos.

Notou-se que questões como prática de segurança no Internet Banking, aceitação de uso da certificação e imagem, framework para gestão, auditoria, o arquivamento, a confiabilidade, integridade, autenticidade e disponibilidade não são completamente apontados pelos gestores do Internet Banking, nem pela tecnologia e jurídico do Banco, necessárias para aporte de decisões quando contestações de fraude forem efetuados por este canal.

Conclui-se que o objetivo desse estudo foi alcançado, demonstrando que os elementos de sustentação da efetividade do uso do certificado digital no Internet Banking do Banco Capital, através da solução de framework de certificado digital, não atende os elementos de sustentação da efetividade do projeto certificado digital no Internet Banking, que só poderá ser efetivo quando a técnica de segurança com certificado digital puder oferecer real segurança no tratamento das informações.

Neste caso, recomenda-se que para a solução de framework de certificado digital e o processo que envolve o uso do certificado digital no Internet Banking da Instituição, apliquem as ações relacionadas no plano de ação.

Como trabalho futuro sugere-se encaminhar este estudo para os gestores do Banco Capital para que possam reestruturar o projeto em uma nova etapa, com referência e embasamento teórico, temas e autores relacionados, buscando verificar como os elementos de sustentação deverão implementados. Além disso, desenvolver um novo sistema bancário que possa centralizar e padronizar todas as técnicas de segurança aplicadas no Internet Banking, atendendo os mesmos elementos de sustentação da efetividade.

As recomendações aqui sugeridas podem evitar impactos na Instituição, inclusive a perca da imagem e credibilidade diante dos milhares de clientes que utilizam o Internet Banking.

5.1 – PUBLICAÇÃO RELACIONADA A ESTE TRABALHO

1) SCRÓCARO, Rubia; Rafael Timóteo de Sousa Júnior; Laerte Peotta; Robson de Oliveira Albuquerque e Edna Dias Canedo. **Análise da Efetividade da Solução de Framework de Certificado Digital utilizada pelo Internet banking de uma Instituição Pública Bancária.** X SEGET – Simpósio em Excelência em Gestão em Tecnologia para Competitividade, 2013, 23 24 e 25 Outubro, Resende – Rio de Janeiro. (trabalho aceito).

REFERÊNCIAS BIBLIOGRÁFICAS

Adendo Estatístico (2011), Diagnóstico do Sistema de Pagamentos de Varejo do Brasil, Banco Central do Brasil. Disponível em <http://www.bcb.gov.br/htms /spb/Diagnostico-Adendo-2011.pdf>

Ahmed A., Rezaul M. K, Rahman A. M (2010), "E-Banking and Its Impact on Banks, Performance and Consumers Behaviour", icds, pp.238-242, Fourth International Conference on Digital Society, AntilhasHolandesas.

Albertini A. e Moura L. (2002), "Administração de Informação: funções e fatores críticos de sucesso", 4ª ed. São Paulo: Editora Atlas.

Almeida A. L., BaranauskasC.M (2008), Universidade Estadual de Campinas - UNICAMP, Anais do Simpósio Brasileiro de Fatores VIII Humanos em Sistemas Computacionais, Sociedade Brasileira de Computação Porto Alegre.

Ansper A., Buldas A., Roos M. e Wilemson M. (2001)," Efficient long-term validation of digital signatures", 4th International Workshop on Practice and Theory in Public Key Cryptography, pp. 402-415, Korea.

Arretche, Marta(2006), Tendências no estudo sobre avaliação. In: RICO, E.M. Avaliação de Políticas Sociais. Uma questão em debate. São Paulo, Cortez.

Bacen - Banco Central do Brasil (2001), Resolução n° 2.817 - Dispõe sobre a abertura e a movimentação de contas de depósitos exclusivamente por meio eletrônico, bem como acerca da utilização desse instrumento de comunicação. Disponível em <www.bcb.gov.br>

Banco do Brasil (2012). Disponível em <www.bancodobrasil.com.br>

Beal, Adriana. (2008) Segurança da Informação: Princípios e Melhores Práticaspara a Proteção dos Ativos da Informação nas Organizações. São Paulo: Editora Atlas.

Bry Tecnologia. (2012). Disponível em: <http://www.bry.com.br/wp-content/uploads/ 2012/11 /folder_bry_framework_site.pdf>

Boynton, William C.; Johnson, Raymond N.; Kell, Walter G (2002). Auditoria. São Paulo: Atlas.

CAIXA- Caixa Econômica Federal (2012). Disponível em <www.caixa.gov.br>

Carvalho, Luciano Gonçalves. (2005) Segurança de redes. RJ: Ciência Moderna Ltda.

Carvalho, M. C.(2009) Avaliação da qualidade percebida nas instituições de ensino técnico: um estudo no município de Lavras, Minas Gerais. 2009. 108 p. Dissertação (Mestrado em Administração) – Universidade Federal de Lavras.

Chatzipoulidis A. e Mavridis I. (2010), "A Study on User Behavior and Acceptance of Electronic Banking Services," pci, pp.180-183, 14th Panhellenic Conference on Informatics, Grécia.

Chen W. L. e Argles D. (2010), "Towards a Framework of a Secure E-Qualification Certificate System," iccms, vol. 1, pp.493-500, Second International Conference on Computer Modeling and Simulation.

Decreto nº 3.872 (2001), Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CGICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

Diniz, E., Poro, R.M. and Tomi, A. (2009), "Internet Banking in Brazil: evaluation of functionality, reliability and usability", The Electronic Journal of Information Systems Evaluation, Vol. 8 No. 1, 41-50.

DOC-ICP-05 (2012) - Requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil, versão 3.6. Disponível em < http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-05_-_Versao_3.6.pdf>

Febraban - O Setor Bancário Setor Bancário em Números, Tendências Tecnológicas e Agenda Atual (2012), Disponível em <http://www.febraban.org.br /7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Ciab12-Anuario%20Febraban%2006.07.pdf>

Febraban - O Setor Bancário Setor Bancário em Números, Tendências Tecnológicas e Agenda Atual (2013), Disponível em <http://www.febraban.org.br>

Fitzgerald, Jerry; Dennis, Alan. (2005) Comunicação de Dados Empresariais e Redes. RJ: LTC.

Fujishiro T., Sato A., Kumagai Y., Kaji T., Okada K. (2010), "Development of Hi-Speed X.509 Certification Path Validation System," Advanced Information Networking and Applications Workshops", International Conference on, pp. 269-274, IEEE 24th International Conference on Advanced Information Networking and Applications Workshops.

Gartner, Inc. (2011) X.509 Certificate Management: Avoiding Downtime and Brand Damage www.gartner.com/id1840016.

Hu N., Giri K., Chengyu M. T., Li Y. (2009), “Certificate revocation release policies", Journal of Computer Security, Pages: 127-157, Volume 17 Issue 2.

Hu X. e Ma L. (2010), "A Study on the Hybrid Encryption Technology in the Security Transmission of Electronic Documents," isme, vol. 1, pp.60-63, International Conference of Information Science and Management Engineering, China.

Humphreys K. (1998), " Banking on the Web: Security First Network Bank and the development of virtual financial institutions", p. 75-104, Banking and Finance on the Internet, Canada.

ITI - Instituto Nacional de Tecnologia da Informação (2012), Disponível em <http://www.iti.gov.br>

ITIL, Office of Government Commerce Aligning CobiT 4.1 (2008), ITILV3 and ISO/IEC 27002 for Business Benefit. Illinois, USA: IT GovernanceInstitute.

Jie Z. e Hong X. (2010), "E-Commerce Security Policy Analysis," icece, pp.2764-2766, International Conference on Electrical and Control Engineering, China.

Kurose. J.F.K.W. (2003) Redes de computadores e a Internet. São Paulo. AddilsonWeslwy.

Leavitt N. (2011), "Internet Security under Attack: The Undermining of Digital Certificates," Computer, vol. 44, no. 12, pp. 17-20, doi:10.1109/MC.2011.367.

Lei nº 12.682 (2012), Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Disponível em <http://www.planalto. gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12682.htm>

Lekkas D. e Gritzalis (2007), "Long-term verifiability of the electronic healthcare records' authenticity", International Journal of Medical Informatics, Volume 76, Issues 5-6, Virtual Biomedical Universities and E-Learning and Secure eHealth: Managing Risk to Patient Data - Elearning and Secure eHealth Double S.I., p. 442-448.

Ma J., Abie H., Skramstad T., Nygârd M. (2011), "A Framework for the Assessment of the Trustworthiness of Digital Records over Time," IEEE TrustCom/IEEE ICESS/FCST, International Joint Conference of, pp. 738-744, IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications.

Manual de Condutas Técnicas (2009) - Procedimentos de Ensaios para Homologação de Equipamentos de Carimbo do Tempo no âmbito da ICPBrasil, versão 1.0, Manual de Condutas Vol II (MCT 10 Vol. II). Disponível em

<http://www.iti.gov.br/images/consulta-publica/encerradas/LEA_MCT-0_VolII_v1.0.pdf>

Manual Normativo Interno (2011), TE197 - Segurança para o desenvolvimento e manutenção de sistemas. Vigência 10/12/2011.

Manual Normativo Interno (2012), C089 - Internet Banking, Vigência 29/06/2012.

Medida Provisória n°2.200 - Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências, (2001). Disponível em <http://www.planalto.gov.br/ ccivil_03 /mpv/Antigas_2001/2200-2.htm>

Menezes A.J., van Oorschot P.C., Vanstone S.A., (2001) "Handbook of applied cryptography", CRCPress, http://www.cacr.math.uwaterloo.ca/hac/,816pp.

Milan, G.S, Trez, G. (2005). Pesquisa de satisfação: um modelo para planos de saúde. ERA Light, v.4, n.2, jul-dez.

Nakamura, E. T. e Geus P. L. (2002), Segurança de Redes em Ambiente Cooperativos. São Paulo, Editora Berkeley.

Nami R. M. (2009), "E-Banking: Issues and Challenges,",pp.263-266, 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing.

Peotta L. M., Bertol V. e Souza T. R. J (2009), Um Modelo para as Normas sobre Certificação Digital no Brasil, FourthInternationalConferenceof Forense Computer Science.

Peotta L. M., Bertol V. e Souza T. R. J, David B., Deus F., Holtz M. (2011), "A Formal Classification of Internet Banking Attacks and Vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT).

Pereira M. S. T. e Santos H. (2010), "A Security Framework for Audit and Manage Information System Security," Web Intelligence and Intelligent Agent Technology, IEEE/WIC/ACM International Conference on, vol. 3, pp. 29-32, IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology.

Plano do Projeto (2010), Internet Banking com Certificado Digital utilizando a Solução de Framework de Certificado Digital.

Polasik M. e Wisniewski P. T. (2009), "Empirical analysis of internet banking adoption in Poland", vol. 27 Iss: 1, pp.32 - 52, International Journal of Bank Marketing.

Pfleeger, Charles P.(1997) Security in Computing. 2. Ed. New Jersey. USA: Prentice Hall.

Requisições e Especificações (2009), Solução de Framework de Certificado Digital, publicada em Edital Público.

Resolução nº 65 (2009), Aprova versão 2.0 do documento padrões e algoritmos criptográficos da ICP-Brasil e plano de migração relacionado. Publicado no Diário Oficial da União e Disponível em <http://www.iti.gov.br/images/icp-brasil/legislacao /Resolucoes/resolucao65.pdf>

RIF - Relatório de Inclusão Financeira, Banco Central do Brasil (2010). Disponível em: <http://www.bcb.gov.br/Nor/relincfin/relatorio_inclusao_financeira.pdf>

Rousseau, Jean-Yves, Couture, Carol.(1994).Os fundamentos da disciplina arquivística. Lisboa: Publicações Dom Quixote.

Sanayei A., Noroozi A. (2009), "Security of Internet Banking Services and its Linkage with Users Trust: A Case Study of Parsian Bank of Iran and CIMB Bank of Malaysia," icime, and pp.3-7, International Conference on Information Management and Engineering, Malásia.

Santander Banco (2012). Disponível em <www.santander.com.br>

Sarma S.E., Weis, S.A., Engels, D.W., (2003) "Radio Frequency Identification: Security Risks and Challenges", Cryptobytes, RSALaboratories, Volume 6, No 1, página 2

Schneier, Bruce (1996). Applied Cryptography: Protocols, Algorithms and Source. Code in C. 2. ed.New York: John Wiley & Sons.

Stallings, Wiliam. (2003) Cryptography and Network Security: Principles and Practice, Third Edition. Prentice-Hall.

Sols,R. von(1999). Information security management: why standards are important.Information Management & Computer Security, vol. 7, n.1, p.50-57.

Stewart, J. Michael, Tittel, E.,Chapple, M. (2008), Certified Information Systems Security Professional Study Guide. New Jersey, USA: John Wiley & Sons Publication

Tanenbaum, Andrew S. (2003), Redes de Computadores. 4 ed. Rio de Janeiro – Elsiever,Traduzido por Vandenberg D. de Souza.

Teixeira, Dilza Aurora Matos. (2002), Ações de conservação epreservação da memória no contexto digital. Transformação, SãoPaulo, v.4, n. 2, p. 179-181, jul./dez.Disponível em<http://revistas.puccampinas.edu.br/transinfo/viewarticle. php?id=8>

TIC Empresas - Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil (2010). Disponível em <http://www.cetic.br/empresas/2010/index.htm>

Trevisan, A.(1996) Auditoria suas áreas de ação. São Paulo: Atlas.

Vasconcellos, Eduardo, Evan. Werther, Willian(1994). Estratégia Tecnológica no Brasil, Japão e EUA: um estudo comparado. In: Anais do XIII Simpósio de Gestão da Inovação Tecnológica. São Paulo.

Vergara, Sylvia Constant. (2006). Métodos de Pesquisa em Administração. 2. ed. São Paulo: Atlas.

Zhang Q. (2009), "Study on Fraud Risk Prevention of Online Banks," vol. 2, pp.181-184, International Conference on Networks Security, Wireless Communications and Trusted Computing, China.

Zhao L. (2010), "Study on Online Banking Adoption and Its Predictors," mmit, vol. 1, pp.155-158, Second International Conference on MultiMedia and Information Technology, Kaifeng, China.

Wadlow, Thomas. (2000). Segurança de Redes – Projeto e Gerenciamento de Redes Seguras. SP: Campus.