

REGIVALDO GOMES COSTA

**SISTEMA SEGURO DE VOTAÇÃO
ELETRÔNICA MULTI-CÉDULAS**

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática Aplicada.

CURITIBA - PR

2008

REGIVALDO GOMES COSTA

**SISTEMA SEGURO DE VOTAÇÃO
ELETRÔNICA MULTI-CÉDULAS**

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática Aplicada.

Áreas de Concentração: Sistemas Distribuídos
Orientador: Prof. Dr. Altair Olivo Santin

CURITIBA - PR

2008

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central

C837s
2008 Costa, Regivaldo Gomes
Sistema seguro de votação eletrônica multi-cédulas / Regivaldo Gomes
Costa ; orientador, Altair Olivo Santin. -- 2008.
xiv, 111 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná,
Curitiba, 2008
Bibliografia: f. 82-86

1. Sistema eleitoral. 2. Votação – Eleições. 3. Votação – Processamento de
Dados. 4. Voto eletrônico. 5. Sistemas de segurança. 6. Arquitetura de redes
de computadores. I. Santin, Altair Olivo. II. Pontifícia Universidade Católica do
Paraná. Programa de Pós-Graduação em Informática. III. Título.

CDD 20. ed. – 324.6



Pontifícia Universidade Católica do Paraná
Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Informática

**ATA DE DEFESA DE DISSERTAÇÃO DE MESTRADO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA**

DEFESA DE DISSERTAÇÃO Nº 11/2008

Aos 25 dias do mês de agosto de 2008 realizou-se a sessão pública de Defesa da Dissertação de Mestrado “**Sistema Seguro de Votação Eletrônica Multi-Cédulas**”, apresentada pelo aluno **Regivaldo Gomes Costa** como requisito parcial para a obtenção do título de **Mestre em Informática**, perante uma Banca Examinadora composta pelos seguintes membros:

Prof. Dr. Altair Olivo Santin
PUCPR (orientador)


(assinatura)

Aprov
(aprov/reprov.)

Prof. Dr. Carlos Alberto Maziero
PUCPR



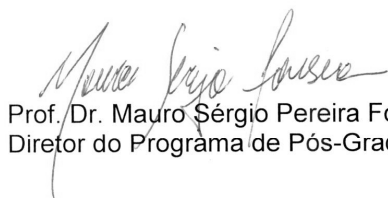
aprov

Prof. Dr. Ricardo Dahab
UNICAMP



aprov

Conforme as normas regimentais do PPGLa e da PUCPR, o trabalho apresentado foi considerado Aprovado (aprovado/reprovado), segundo avaliação da maioria dos membros desta Banca Examinadora. Este resultado está condicionado ao cumprimento integral das solicitações da Banca Examinadora registradas no Livro de Defesas do programa.


Prof. Dr. Mauro Sérgio Pereira Fonseca
Diretor do Programa de Pós-Graduação em Informática



Dedico a minha esposa e filhos.

Agradecimentos

Pelo apoio incondicional, pela compreensão e pelas dificuldades enfrentadas diante da minha ausência e momentos de desatenção, agradeço com carinho a minha esposa Helna e meus filhos Stephanie e Phelipe.

Agradeço à Câmara dos Deputados, através do Diretor da Coordenação do Sistema Eletrônico de Votação, Sr. Leírton Saraiva de Castro e do ex-diretor do Centro de Informática, Sr. Luiz Antonio Souza da Eira, que, prontamente, autorizaram-me para o novo desafio.

Agradeço ao colega de trabalho, Geraldo Castro, que, para minha ausência, propôs-se a absorver minhas atividades, permitindo, assim, minha saída para o pleito.

Agradeço ao meu orientador, o professor Altair Olivo Santin, que, na fase de minha aprovação para ingresso ao mestrado, acatou minha proposta. Que, durante o mestrado, foi uma pessoa que me direcionou de forma certa junto aos objetivos deste trabalho, para o qual seu apoio, a geração de idéias, a dedicação e a persistência foram fundamentais.

Agradeço ao professor Carlos Maziero e ao colega de mestrado Cleber Olivo, que colaboraram nos trabalhos de publicação, principalmente quanto à revisão/tradução dos textos no idioma inglês, cujos resultados foram positivos.

Agradeço aos colegas do mestrado Arlindo Marcon, Maicon Stihler e Marcelo Vithoft pelos debates quanto aos trabalhos de publicação, pelo que desenvolvemos em conjunto junto às diversas disciplinas, pela amizade e companheirismo que mantivemos durante o curso.

Agradeço à empresa Gemalto do Brasil, através do Sr. Robson Alves, que nos forneceu gratuitamente os cartões *Java Card* e documentação necessária ao desenvolvimento do protótipo.

Resumo

Em uso desde a Grécia antiga e atualmente massificado na maioria dos países do mundo, o sistema de votação tradicional baseado em cédulas de papel possui diversos problemas associados à segurança, tais como dificuldades para evitar coerção do eleitor, venda do voto e substituição fraudulenta do eleitor. Além de problemas de usabilidade que acarretam erros de preenchimento da cédula e um processo de apuração lento, que pode durar dias. Ao lado disso, o sistema tradicional não fornece a contraprova do voto, que permite ao eleitor conferir se o seu voto foi corretamente contabilizado na apuração. Inicialmente acreditou-se que a informatização do sistema de votação resolveria todos os problemas do sistema tradicional. Porém, com a sua implantação em alguns países o sistema de votação eletrônica não mostrou-se capaz de fornecer garantias irrefutáveis que não tivesse sido alvo de alterações fraudulentas durante o seu desenvolvimento ou operação. A má reputação do sistema eletrônico está principalmente associada à falta de transparência dos processos que, em sua maioria, não proporcionam a materialização do voto, conferido pelo eleitor para fins de contagem manual, e nem geram evidências (contraprova) da correta contabilização do voto do eleitor. O objetivo deste trabalho é propor uma arquitetura de votação eletrônica que integra, de forma segura, o anonimato e autenticidade do votante, a confidencialidade e integridade do voto/sistema. O sistema aumenta a usabilidade do esquema de votação baseado em "Três Cédulas" de papel, implementando-o computacionalmente. O esquema oferece maior credibilidade ao sistema de votação através da materialização e contraprova do voto, resistência à coerção e ao comércio do voto. Utilizando esquemas de criptografia assimétrica e segurança computacional clássica, associado a um sistema de auditoria eficiente, a proposta garante segurança e transparência nos processos envolvidos. A arquitetura de construção modular distribui a responsabilidade entre suas entidades, agregando-lhe robustez e viabilizando eleições em grande escala. O protótipo do sistema desenvolvido usando Serviços web e *Election Markup Language* mostra a viabilidade da proposta.

Palavras-chave: Segurança em votação eletrônica, Contraprova do voto, Materialização do voto, Sistema baseado em três-cédulas.

Abstract

Being used since the old Greece, and currently seeing massive adoption in the majority of the countries in the world, the traditional ballots of paper-based voting systems has many problems related to security, such as difficulty to avoid coercion of voters, vote trade and voters impersonation. Besides usability problems that cause errors when filling the ballot and a slow tallying process, which can take several days. Also, the traditional system does not provide a vote receipt which would allow the voters to know if their vote has been taken into account correctly on the tallying process. Initially, it was believed that computerization of voting systems would solve all the problems of the traditional system. However, the deployment of electronic voting systems in some countries was not able to provide irrefutable guarantees that the system was not compromised during its development or operation. The bad reputation of electronic systems is mostly associated to the lack of transparency of processes, which, in its majority, do not propose the materialization of vote, given to the voter on purpose of manual recounting and to generate evidence (receipt) of correct accounting of the voters' vote. The aim of this work is to propose architecture for electronic voting that integrates, in a secure way, the anonymity and authenticity of the voter, and the confidentiality and integrity of the vote. The system increases the usability of the Three-Ballot paper-based voting system, implementing it computationally. This scheme offers greater credibility to the voting system through the vote materialization and receipt, resistance to coercion and vote trading. Using schemes for asymmetric cryptography and classic computational security associated to an efficient auditing system, the proposal guarantees security and transparency to the election processes. The modularized construction of the architecture distributes the responsibility among its entities, strengthening and enabling its use for large scale elections. The prototype system developed using Web Services and Election Markup Language shows the proposal's viability.

Keywords: Electronic voting security, Vote receipt, Vote materialization, Tree-Ballot-Based System.

Lista de Figuras

Figura 2.1: As diversas tecnologias de equipamentos utilizadas em SEVs.....	16
Figura 3.1: Cédulas preenchidas segundo o esquema proposto por [RIVEST, 2007].....	26
Figura 3.2: Parte da cédula, com faces alinhadas e com texto legível [CHAUM, 2004].	29
Figura 3.3: Face da cédula usada como recibo e com texto ilegível [CHAUM, 2004].	29
Figura 3.4: Face destruída pelo mesário diante do eleitor [CHAUM, 2004].....	29
Figura 3.5: Camadas com os <i>pixels</i> que formam a imagem [CHAUM, 2004].	30
Figura 3.6: Recomposição da imagem a partir das duas camadas [CHAUM, 2004].	31
Figura 3.7: Processo de reconstrução da última polegada da cédula [CHAUM, 2004].	31
Figura 3.8: Diagrama de seqüência das fases de registro e votação [ROSSLER, 2005].	34
Figura 3.9: XML assinado e cifrado, antes e após a votação [ROSSLER, 2005].....	35
Figura 3.10: Mensagens da fase de registro [KOFER, 2003].....	37
Figura 3.11: Mensagens da fase de votação [KOFER, 2003]	38
Figura 4.1: Diagrama da arquitetura proposta [COSTA, 2008].....	46
Figura 4.2: Diagrama de interação entre os módulos da Fase de Registro e Habilitação.	47
Figura 4.3: Diagrama interativo entre os módulos da Fase de Votação.	51
Figura 4.4: Diagrama interativo entre os módulos da Fase de Apuração.	55
Figura 5.1: Troca de mensagens na Fase de Registro/Habilitação.	58
Figura 5.2: Troca de mensagens na Fase de Votação.	61
Figura 5.3: Troca de mensagens na Fase de Apuração.	65
Figura 5.4: Interface com o eleitor/administrador (cliente/servidor).....	67
Figura 5.5: Processo de registro e recuperação de informações WSDL.....	68
Figura A.1: Representação simples de uma rede de mistura.	89
Figura A.2: Representação simples de canais anônimos.	90
Figura B.1: EML - Processo de nomeação de candidatos [OASIS, 2007]	93
Figura B.2: EML - Processo de nomeação de Opções de Referendo [OASIS, 2007].	94
Figura B.3: EML - Processos relacionados ao registro do eleitor [OASIS, 2007].	95
Figura B.4: EML - Processo de Votação [OASIS, 2007]	98
Figura B.5: EML – Processo de contagem e de divulgação de resultados [OASIS, 2007].	99
Figura B.6: EML – Processos envolvidos na auditoria [OASIS, 2007].	100
Figura B.7: EML – Arquitetura de segurança [OASIS, 2007].....	101
Figura C.1: Relações entre as entidades dos <i>Serviços Web</i> [CHAPPEL, 2002].....	104
Figura C.2: Arquitetura do WS-Security	107
Figura C.3: Protocolo Request/Response do STS.....	109

Lista de Tabelas

Tabela 2.1: Alguns aspectos comparativos entre os sistemas de votação	14
Tabela 2.2: Matriz de acesso conforme [LAMPSON, 1971]	18
Tabela 5.1: Descrição das mensagens protocolares na Fase de Registro	59
Tabela 5.2: Descrição das mensagens protocolares na Fase de Votação	62
Tabela 5.3: Descritivo das mensagens protocolares na Fase de Apuração.....	66
Tabela 5.4: Recursos utilizados nos testes	77
Tabela 5.5: Desempenho na fase de Habilitação/Votação	77

Lista de Abreviaturas

Abreviatura	Significado
ACL	<i>Access Control List</i>
AE	<i>Autoridade Eleitoral</i>
AR	<i>Agente de Registro</i>
BBS	<i>Bulletin Board System (Boletim de Resultados)</i>
BSD	<i>Berkeley Software Distribuiton</i>
CV	<i>Console de Votação</i>
DDOS	<i>Distributed Denial-of-Service</i>
DOS	<i>Denial-of-Service</i>
DRE	<i>Direct Recording Electronic</i>
DSA	<i>Digital Signature Algorithm</i>
GNU	<i>GNU is Not Unix</i>
GPL	<i>General Public Licence</i>
GRPS	<i>General Radio Packet Service</i>
GV	<i>Gerente de Votação</i>
HAVA	<i>Help American Vote Act</i>
HSM	<i>Hardware Security Module</i>
HTML	<i>HiperText Markup Language</i>
HTTPS	<i>Hypertext Transfer Protocol over Secure Socket Layer</i>
ICP	<i>Infra-Estrutura de Chaves Públicas</i>
ID	<i>Identification</i>
IDS	<i>Intrusion Detection System</i>
NIST	<i>National Institute of Standards and Technology</i>
OASIS	<i>Organization for the Advancement of Structured Information Standards</i>
PC	<i>Personal Computer</i>

PCOS	<i>Precinct Count Optical Scan</i>
PDA	<i>Personal Digital Assistant</i>
PHP	<i>Hipertext Preprocessor</i>
RSA	<i>Sigla associada a um sistema de criptografia que leva o nome do autores (Rivest, Shamir e Adleman)</i>
SAML	<i>Security Assertion Markup Language</i>
SEV	<i>Sistema Eletrônico de Votação</i>
SMS	<i>Short Message Service</i>
SOAP	<i>Simple Object Access Protocol</i>
SQL	<i>Simple Query Language</i>
SSL	<i>Secure Sockets Layer</i>
STS	<i>Security Token Service</i>
TLS	<i>Transport Layer Security</i>
TRE	<i>Tribunal Regional Eleitoral</i>
TSE	<i>Tribunal Superior Eleitoral</i>
UDDI	<i>Universal Description Discovery and Integration</i>
UE	<i>Urna Eletrônica</i>
URL	<i>Uniform Resource Locate</i>
Vo	<i>Votante</i>
VVPT	<i>Voter Verified Paper Trail</i>
W3C	<i>World Wide Web Consortium</i>
WAP	<i>Wireless Application Protocol</i>
WS	<i>Web Services</i>
WSDL	<i>Web Services Description Language</i>
XKMS	<i>XML Key Management Specification</i>
XML	<i>eXtensible Markup Language</i>

Sumário

Capítulo 1	1
Introdução.....	1
1.1. Motivação.....	2
1.2. Objetivos	3
1.3. Organização do trabalho	5
Capítulo 2	6
Sistemas de Votação Eletrônica e Aspectos de Segurança.....	6
2.1. Sistemas de Votação.....	6
2.1.1. Sistema de votação tradicional.....	8
2.1.2. Sistema Eletrônico de Votação (SEV)	10
2.1.3. SEVs com infra-estrutura de redes de telecomunicações.....	13
2.1.4. Comparativo entre os sistemas de votação	14
2.1.5. Equipamentos utilizados em SEVs	15
2.3. Segurança Computacional Clássica.....	17
2.4. Segurança Aplicada a SEVs	18
2.4.1. Equipamentos de votação	19
2.4.2. Software.....	19
2.4.3. Infra-estrutura de telecomunicações	21
2.4.4. Aspectos gerais de segurança.....	22
2.5. Falhas e ideologias aplicadas a Sistemas de Votação	23
2.6. Conclusão.....	24
Capítulo 3	25
Trabalhos Relacionados.....	25
3.1. Trabalhos Científicos.....	25
3.1.1. Sistema baseado em cédulas físicas, com contraprova e sem uso de criptografia	25
3.1.2. Sistema baseado em cédulas físicas, com contraprova e com uso de criptografia	28
3.1.3. Sistema baseado em HSM e documentos XML.....	33
3.1.4. Sistema baseado em assinaturas às cegas	36
3.2. Relatórios técnicos.....	39
3.2.1. Relatório Caltech/MIT	39
3.2.2. Relatório CESG	39
3.2.3. Relatório Brennan	40
3.3. Conclusão.....	41
Capítulo 4	42
Um Sistema Seguro de Votação Eletrônica Multi-Cédula.....	42
4.1. Motivação.....	42
4.2. Objetivos	43
4.3. Arquitetura Proposta.....	44
4.3.1. Visão Geral da Arquitetura proposta	45
4.3.2. Fase de Registro e Habilitação.....	46
4.3.3. Fase de Votação.....	50
4.3.4. Fase de Apuração.....	54
4.3.5. Infra-estrutura de Chaves Públicas	56
4.4. Conclusão.....	56

Capítulo 5.....	57
Protocolo, Protótipo e Aspectos de Implementação.....	57
5.1. Protocolo Proposto.....	57
5.1.1. Fase de Registro e Habilitação	58
5.1.2. Fase de Votação.....	60
5.1.3. Fase de Apuração	65
5.2. Infra-estrutura de Serviços	67
5.2.1. Interfaces homem-máquina	67
5.2.2. Comunicação e registro entre entidades/módulos	67
5.2.3. Mecanismos de autenticação e autorização	69
5.3. O Protótipo e Aspectos de Implementação	70
5.3.1. Ferramentas, Frameworks e APIs.....	70
5.3.2. Uso da EML	72
5.4. Descrição dos Módulos Implementados.....	73
5.4.1. Módulos da Fase de Registro e Habilitação	73
5.4.2. Módulos da Fase de Votação.....	74
5.4.3. Módulos da Fase de Apuração.....	75
5.5. Resultados obtidos	76
5.6. Conclusão	78
Conclusão.....	79
Referências Bibliográficas	81
Apêndice A	86
Esquemas Criptográficos	86
A.1. Assinaturas às Cegas	87
A.2. Criptografia Homomórfica	88
A.3. Redes de Mistura (Mixnets)	88
A.4. Canais Anônimos	89
A.5. Prova de Conhecimento Zero.....	90
Apêndice B	91
Normas e padrões.....	91
B.1. IEEE P-1622 (Voting Systems Electronic Data Interchange)	91
B.2. Election Markup Language (EML)	92
B.2.1. Processos envolvidos na PRÉ-ELEICÃO	92
B.2.2. Processos envolvidos na ELEICÃO	96
B.2.3. Processos envolvidos na PÓS-ELEICÃO	100
Apêndice C	103
Introdução a Serviços Web	103
C.1. Entidades	104
C.1.1. O protocolo SOAP	104
C.1.2. A linguagem WSDL	105
C.1.3. Serviço UDDI	105
C.2. Linguagem XML e Mecanismos de Segurança	106
C.2.1. XML Signature	106
C.2.2. XML Encryption.....	107
C.3. O WS-Security.....	107
C.4. O WS-Policy	108
C.5. O WS-Trust	108
C.6. O XML Key Management Specification	109
C.7. O WS-AtomicTransaction.....	110

Capítulo 1

Introdução

O processo de eleição a cargos políticos, no qual os candidatos se elegem segundo a regra da maioria, é um dos mais antigos meios de votação em toda a história mundial. Todo o processo ocorre por um conjunto de mecanismos que se denomina **Sistema de Votação**, sempre apoiado em regras e leis de cada país [O'CONNOR, 2002].

Atualmente, os Sistemas de Votação se dividem em duas classes: o tradicional, ou manual, e o eletrônico. O tradicional, e mais antigo sistema, consiste em um processo sem automatização: o eleitor profere o seu voto em cédulas de papel e, numa fase posterior, é feito o escrutínio (apuração), ou seja, a contagem e tabulação das cédulas uma a uma.

O sistema de votação tradicional, apesar de consolidado e em uso na maioria dos países do mundo, apresenta diversos problemas, tais como: o tempo de apuração, que pode levar dias; erros de preenchimento da cédula; ausência de uma evidência do voto proferido (contraprova); o armazenamento e guarda das urnas que contêm os votos traz margem a fraudes em decorrência da baixa segurança envolvida no processo, principalmente no transporte; e, por fim, o voto-de-cabresto, que figura o uso irregular de alguma forma de poder sobre o eleitor, a coerção e o comércio do voto.

Com o avanço tecnológico e com o uso da computação, surgiram os Sistemas Eletrônicos de Votação (SEVs), cujo objetivo principal é suprir as deficiências do sistema tradicional e reduzir o tempo entre o término da votação e o seu resultado, eliminar erros de preenchimento de cédulas e melhorar o fator usabilidade, possibilitando que idosos e pessoas com baixo grau de discernimento possam proferir seu voto com maior facilidade.

Já em operação em alguns países, inclusive no Brasil, os SEVs têm como premissa atender os requisitos, propriedades, regras e leis estabelecidas para o sistema eleitoral e que

visam estar em consonância com os preceitos democráticos de cada país. No entanto, os SEVs possuem algumas deficiências no atendimento de alguns requisitos e propriedades impostos pelo sistema eleitoral, o que pode resultar no funcionamento incorreto do sistema, seja por falhas ou por procedimentos fraudulentos. O relatório [NORDEN, 2006] aponta 120 pontos de falhas que podem contribuir no uso incorreto desses sistemas. Nele se destaca o uso de programas de computador com código malicioso ou corrompido, equipamentos de votação operacionalmente inadequados ou descalibrados, indisponibilidade do sistema, desativação de recurso de ajuda ao eleitor e ataques a sistema de comunicação sem fio.

No Brasil, as eleições oficiais geridas pelo TSE (Tribunal Superior Eleitoral) ocorrem através de um SEV. Promovido pelo parlamento brasileiro, o Seminário do Voto Eletrônico [JAKOBSKIND, 2002] ocorrido no ano de 2002 relaciona diversas probabilidades de falhas e ausência de transparência do sistema brasileiro. Pode citar-se a ausência de padrões (sistema de criptografia proprietário/fechado, por exemplo); o processo de identificação do eleitor, votação e apuração provido por um único equipamento, a “urna eletrônica”; um sistema de auditoria deficiente e o acesso a essas informações por órgãos de auditoria externa dificultado pelo TSE, colocando, assim, em dúvida a lisura dos processos.

A má reputação dos SEVs, decorrentes de suas falhas, tem despertado interesse em especialistas e cientistas das áreas governamental, privada e acadêmica, em todo o mundo, com um objetivo comum: resolver os problemas inerentes aos SEVs de forma a tornar os mesmos sistemas seguros e robustos e com as premissas na qual foram concebidos.

Diante do exposto, este trabalho traz contribuições para a melhoria dos SEVs, apresentando proposta de um modelo de SEV que agrega os requisitos e propriedades que atendem os preceitos democráticos da maioria dos sistemas eleitorais do mundo.

1.1. Motivação

Os países que optaram por substituir os sistemas tradicionais de votação por sistemas eletrônicos têm enfrentado problemas por ferirem algumas regras que visam à correteza do processo. Podemos destacar o Brasil, cujo SEV não contempla a contraprova do voto que permita a conferência pelo eleitor após a apuração e a materialização do voto. Isso para que seja possível, em situações de divergência, efetuar a recontagem, como no sistema tradicional, visto que, atualmente, os resultados são totalizados eletronicamente e muitas dúvidas pairam quanto à correteza desse processo.

Ao término das eleições, o eleitor deseja ter uma prova de que seu voto foi contado corretamente. No entanto, essa prova não pode apresentar indícios que permitam ao eleitor provar a terceiros a qualidade (atribuição) do voto, de forma a evitar a comercialização do voto ou a coação do eleitor. Assim, é necessário que os SEVs produzam uma contraprova de seu voto para o eleitor, sem ferir os princípios do direito democrático. Já existem alguns trabalhos nessa área, mas muitos deles se valem de tecnologias complexas e, na maioria dos casos, inviáveis de serem implementadas em sistemas reais.

Como o sistema pode falhar, seja por ações involuntárias ou voluntárias, e a correção dos resultados numa eleição pode vir a ser comprometida, deve haver dispositivos que possibilitem auditar o sistema de forma a identificar qualquer tipo de erro. No entanto, o desafio consiste em auditar o processo sem infringir as propriedades do anonimato do eleitor (não relacionar o voto ao votante), da confidencialidade do voto (não permitir que se saiba o total de votos que um determinado candidato já obteve até o momento) e ainda garantir que os rastros das operações não sejam adulterados, de forma a mascarar o próprio processo de auditoria.

A autenticidade do eleitor é outro fator falho no sistema brasileiro, pois não há garantias de que o eleitor que está votando é de fato a pessoa que diz ser. Não há identificação biométrica inspecionável do eleitor em seu documento de identificação eleitoral (título de eleitor). Não tendo uma relação direta com sistemas computacionais, a possibilidade de se ter eleitores votando com registro de pessoas falecidas ou falsamente criadas é real. Assim, sistemas computacionais que garantam a identificação biométrica do eleitor são recursos indispensáveis para eliminar esse tipo de fraude.

São esses, entre outros problemas de menor relevância, que serão referenciados ao longo deste trabalho que motivam essa contribuição.

1.2. Objetivos

Este trabalho tem como objetivo trazer contribuições para que a sociedade disponha de Sistemas Eletrônicos de Votação (SEVs) seguros, robustos, de fácil uso, que atendam em plenitude as regras e leis que demandam um processo eleitoral e que, principalmente, estejam em consonância com a democracia.

Assim, motivado pelas limitações dos SEVs atualmente disponíveis, este trabalho traz um modelo de **Sistema Seguro de Votação Eletrônica** baseado em estudos de renomados

cientistas da comunidade acadêmica, aliados à adoção da mais moderna tecnologia para promover o desenvolvimento de um protótipo passível de ser aplicado no mundo real e que atenda às seguintes propriedades, adicionais às propriedades clássicas de segurança:

- a) **Materialização do voto:** possibilitar a materialização do voto através de um sistema computacional é uma necessidade básica, visto que não se pode garantir que ações inadvertidas ou maliciosas possam violar o sistema, e o resultado final de uma eleição ser alvo de qualquer tipo de adulteração. A impressão física do voto permite ao eleitor conferir sua qualidade antes do mesmo ser adicionado a uma urna física tradicional, garantindo que, em casos de divergências do resultado eletrônico, se possa efetuar a recontagem;
- b) **Contraprova do voto:** produzir a contraprova, em decorrência de a mesma ser uma forma do eleitor fiscalizar a contabilização do seu voto garante que procedimentos de fraudes que infringem a integridade do sistema quanto à qualidade do voto sejam coibidos. Assim, após o voto, é entregue um recibo ao eleitor, que será divulgado em uma publicação eletrônica após o término das eleições. Desse modo, o eleitor poderá conferir se o recibo divulgado é igual ao que ele possui. Geralmente produzido a partir de técnicas criptográficas, o recibo traz indícios do voto proferido, mas somente o eleitor possui condições de identificar. Se o recibo divulgado não for idêntico ao do eleitor ou até mesmo não constar na listagem de votos contados, há um indício de fraude. A contraprova é um recurso adotado nos atuais sistemas de votação implantados nos países que adotaram a votação eletrônica, dada a dificuldade técnica da produção da mesma; o mecanismo de contraprova não deve gerar informações que possibilitem ao eleitor utilizar-se do mesmo para comercializar seu voto ou ser coagido;
- c) **Auditabilidade:** um sistema de votação deve deixar rastros de suas operações visando à aferição funcional e falhas do mesmo. No entanto, o desafio é garantir que esses rastros não venham ferir as propriedades do anonimato do eleitor, a confidencialidade e integridade do voto;
- d) **Co-responsabilidade administrativa:** em um sistema de votação, a responsabilidade administrativa de ações sobre os processos do sistema deve ser compartilhada por mais de um administrador, visando à co-responsabilidade. Assim, evita-se que poderes administrativos, por parte da autoridade eleitoral, tenham possibilidades de agir irregularmente sobre o sistema.

1.3. Organização do trabalho

Este trabalho foi dividido em cinco capítulos, organizados da seguinte forma:

Neste primeiro Capítulo, a introdução do trabalho.

O Capítulo 2 apresenta os fundamentos dos sistemas de votação, uma introdução da segurança computacional clássica e aplicada aos Sistemas Eletrônicos de Votação e alguns aspectos ideológicos co-relacionados.

O Capítulo 3 aborda os trabalhos relacionados que trazem contribuições quanto aos estudos de ataques a deficiências dos sistemas eletrônicos e apresenta contramedidas que visam minimizar os problemas de segurança.

O Capítulo 4 apresenta a proposta, que compreende um modelo de um **Sistema Seguro de Votação Eletrônica Multi-Cédula**, baseado na garantia dos requisitos e propriedades que asseguram a corretude de funcionamento desse sistema, e que dá transparência e lisura ao processo de votação.

No Capítulo 5 são apresentados aspectos de implementação do protótipo, com base na arquitetura apresentada no Capítulo 4.

Visando embasar algumas teorias e informações apresentadas nos capítulos supracitados, este trabalho contempla três apêndices conforme descrito a seguir:

O Apêndice A traz uma abordagem dos principais esquemas criptográficos utilizados para prover os requisitos associado aos SEVs.

O Apêndice B esboça normas e especificações que propõem padronizar aspectos computacionais do *software*, *hardware* e comunicação em SEVs.

Por fim, o Apêndice C explana a infra-estrutura e conceitos-base de *Serviços Web* aplicados à proposta deste trabalho.

Capítulo 2

Sistemas de Votação Eletrônica e Aspectos de Segurança

Este capítulo tem como objetivo dar um embasamento teórico no que diz respeito aos SEVs. A maior demanda relativa à melhoria dos SEVs tem se concentrado na área da segurança computacional, pois os mesmos devem atender às regras e leis eleitorais e também estar protegidos contra possíveis ataques, mau funcionamento, falhas por erro de *software* ou operação, vulnerabilidades, entre outros.

2.1. Sistemas de Votação

Para facilitar o entendimento do trabalho, seguem abaixo algumas definições de termos comuns a serem utilizados neste texto. Os termos utilizados se relacionam a ambos os sistemas, o tradicional e o eletrônico. Em alguns casos, são aplicados a somente um deles e a distinção é feita na própria definição, quando aplicável. Outras definições serão apresentadas posteriormente, quando contextualizado pelo tema em discussão.

- **Autoridade Eleitoral:** é a entidade responsável pelo registro de eleitores e pela implantação, administração e fiscalização de todo o processo eleitoral do país. No Brasil, esse papel é feito pelo Tribunal Superior Eleitoral (TSE) e demais entidades regionais (TRE e Cartórios Eleitorais);
- **Apuração:** mais conhecida como escrutínio, é a contagem efetiva dos votos após o término das eleições. No sistema tradicional, o escrutínio ocorre através das cédulas de papel que foram depositadas nas urnas de lona. No sistema eletrônico, a apuração ocorre através de *software*, que conta as cédulas virtuais gravadas em

meio persistente, proveniente da urna eletrônica. Essa apuração ocorre na própria seção eleitoral, cujo documento gerado se chama Boletim de Urna [BRUNAZO, 2006];

- **Boletim de Urna:** Denominado pelas autoridades eleitorais brasileiras no uso da urna eletrônica, é um documento obtido ao término da apuração. É proveniente de um arquivo eletrônico gravado em meio persistente da urna eletrônica de cada seção eleitoral e contém a relação de votos por candidato. Os dados desse boletim são encaminhados para o TSE ou cartório eleitoral para que seja utilizado na totalização. Como o boletim de urna é retirado ainda na seção eleitoral, fiscais de partido obtêm uma cópia para fins de auditoria, se necessário;
- **Cargo eleitoral:** é o cargo na qual um candidato se torna elegível dentro de um pleito eleitoral, ou seja, para presidente, senador, deputado, vereador etc.;
- **Cartório Eleitoral:** é a sede física da autoridade eleitoral, referente a uma zona eleitoral. Após o término do pleito, é para o cartório eleitoral que são encaminhados os boletins de urna, para totalização.
- **Candidato:** é todo indivíduo nominado para concorrer a um cargo, o objeto da eleição em um pleito eleitoral;
- **Cédula eleitoral:** no sistema tradicional, a cédula se apresenta na forma de papel e contém a relação de candidatos e área para que o eleitor marque o seu voto ou espaço para escrever o nome ou número do candidato. No sistema eletrônico, a cédula é simbolizada por uma imagem desenhada na tela de um dispositivo com interface de interação homem-máquina (console de votação) e normalmente contém as mesmas informações da cédula tradicional, podendo adicionalmente possuir a foto do candidato, entre outras facilidades;
- **Contraprova:** dispositivo que possibilita ao votante obter uma prova material do seu voto ao término da fase de votação. Uma listagem das contraprovas registradas no sistema eletrônico é publicada no término do pleito (pela Internet, por exemplo), possibilitando ao eleitor o confronto da publicação com sua prova material. Se ambas forem iguais (a do eleitor e a divulgada), o eleitor passa a ter indícios de que seu voto foi computado corretamente no processo de apuração. Normalmente, essa prova é uma parte da cédula preenchida pelo eleitor, a qual não possibilita ao mesmo provar a qualidade de seu voto a terceiros;

- **Eleitor ou votante:** é todo indivíduo legitimado a exercer o voto em um pleito eleitoral;
- **Pleito eleitoral:** período da fase de votação, estabelecido pela autoridade eleitoral por uma data e horário de início e fim;
- **Processo eleitoral:** todo o mecanismo de gerenciamento administrativo e operacional de eleitores e pleitos eleitorais de um país, cujas regras são determinadas pelas leis criadas para esse propósito;
- **Qualidade do voto:** indica o voto atribuído a um candidato por um eleitor em um pleito eleitoral;
- **Seção eleitoral:** local onde se encontra instalada uma única urna para o eleitor votar;
- **Totalização:** é a soma das apurações constantes em todos os boletins de urna, que fornecerá o número de votos obtidos por um candidato durante um pleito eleitoral;
- **Materialização do voto:** é a impressão do voto virtual (qualidade do voto) do eleitor em papel, por exemplo, visando procedimentos de auditoria futuros. O voto é depositado automaticamente na urna depois de conferido pelo eleitor;
- **Zona eleitoral:** é um nome subjetivo dado a um grupo de seções eleitorais e normalmente está associada a uma região geográfica.
- **Sistemas de votação:** podem ser tradicional, manual ou semi-automatizado, ou eletrônico.

2.1.1. Sistema de votação tradicional

O Sistema tradicional ou manual se caracteriza pelo uso de cédulas de papel cujos mecanismos de votação e totalizações transcorrem através da manipulação da cédula, isto é, a marcação e apuração dos votos. Precede ao processo de marcação da cédula a habilitação do eleitor, e ao procedimento de contagem o depósito da cédula em uma urna. Ao término do pleito e efetuada a totalização dos votos por candidato, é eleito o que obtiver maior número de votos, conforme a regra da pluralidade, por exemplo. Porém, há outros sistemas de escolha do eleitor, como a representação proporcional ou a majoritária [AMADO, 1999][FERREIRA, 2001].

A seguir, são relacionados os mecanismos operacionais de votação associados a esse sistema:

- a) **Identificação e habilitação para votar:** o eleitor se dirige à sua seção eleitoral, identifica-se à autoridade eleitoral (mesário) e, após verificação, estando habilitado, o mesário o autoriza a se dirigir à urna para proferir seu voto;
- b) **Marcação do voto na cédula** (processo de votação. A distinção entre os dois métodos se dá pela forma como o voto é marcado na cédula):
- **Manual** (pode-se escolher o candidato basicamente por dois métodos):
 - o **Marca:** preenche-se a cédula através de uma marcação à caneta, através de um símbolo, normalmente representado pela letra 'X' em um círculo ou quadrado, que se encontra à frente ou ao lado do nome do candidato;
 - o **Nome ou número:** preenche-se manualmente na cédula o nome ou número associado ao candidato.
 - **Semi-automática** (neste caso, a escolha do candidato também pode ser feita basicamente por dois métodos):
 - o **Cartão perfurado:** neste caso, o processo é similar ao voto por marca, porém, ao invés de marcar com uma caneta a escolha do eleitor, é feita uma perfuração por uma máquina destinada a esse fim;
 - o **Hachura:** preenche-se (hachurando completamente) à caneta um círculo ou quadrado que se encontra à frente ou ao lado do nome do candidato.
- c) **Apuração** (a distinção entre os dois sistemas de apuração se dá de acordo com a maneira como ocorre o escrutínio dos votos):
- **Manual:** ao término do pleito eleitoral, abrem-se as urnas e a autoridade eleitoral começa o processo de apuração, cédula por cédula, no qual é computado cada voto ao respectivo candidato lido da marcação do eleitor na cédula. Este processo normalmente é utilizado para os mecanismos cujas cédulas são preenchidas com marca, nome ou número do candidato;
 - **Semi-automático:** utilizado para contagem das cédulas cujas marcações foram feitas através do mecanismo de hachura ou cartão perfurado. O cartão passa por um leitor óptico que registra o voto marcado na cédula respectivamente para cada candidato identificado na leitura.

Os sistemas tradicionais sempre foram criticados pelo longo prazo decorrido entre o término da eleição e a sua apuração e também quanto a questões de fraude, entre as quais as mais conhecidas são o voto-de-cabresto (coação do eleitor), identificação da cédula (venda do

voto) e os erros de natureza humana, como os de preenchimento errôneo das cédulas de votação, cuja consequência direta é a anulação do voto.

2.1.2. Sistema Eletrônico de Votação (SEV)

Com o objetivo de eliminar alguns problemas inerentes ao sistema tradicional, principalmente quanto ao atraso na apuração final em uma eleição e os erros de preenchimento das cédulas, surgiram implementações de SEVs, sendo o Brasil o primeiro país do mundo a ter suas eleições para presidente, senadores e deputados processadas por um sistema 100% eletrônico, no ano de 2000 [BRUNAZO, 2006].

Associados à tecnologia computacional, podemos dizer que SEVs são sistemas nos quais o voto é obtido através de equipamentos com interface homem-máquina (console de votação), comandados pelo votante. O processamento do voto ocorre por meio de recursos computacionais (*hardware* e *software*) com armazenamento em memória persistente local (em algumas arquiteturas), para posterior envio a um sistema central ou mesmo com envio em tempo real através de uma rede de telecomunicações. No sistema central, gerido pela autoridade eleitoral, ocorrerá a totalização dos votos após o término do pleito eleitoral.

No entanto, muito se tem questionado a segurança desses sistemas, principalmente quanto a garantir as propriedades básicas determinadas para um sistema de votação tradicional, tais como a confiabilidade, robustez e auditabilidade. Além dos requisitos do sistema tradicional, em um SEV, outros requisitos ou propriedades inerentes à tecnologia se fazem presentes.

Esses requisitos se apóiam em algumas regras do processo eleitoral que procuram garantir a correteza, democracia e lisura do processo de votação, conforme leis instituídas em cada país, pelas quais a autoridade eleitoral e outras entidades da sociedade civil (em alguns casos) são responsáveis por garantir sua efetivação. Esses requisitos também determinam as “regras de negócio” numa implementação prática de um sistema de votação.

Ressalta-se que, em alguns países, a lei do processo eleitoral atribui a entidades da sociedade civil a responsabilidade na fiscalização dos pleitos eleitorais. No Brasil, o TSE, além de ser o executor, também é o fiscalizador de suas próprias ações [BRUNAZO, 2006]. No contexto de segurança em SEVs, é uma ironia aos princípios da transparência, da lisura e da democracia, o Brasil ter o órgão executor como fiscalizador de suas próprias ações, amparado no princípio meramente legal (não computacional) da fé pública.

Apesar de não ter nenhum papel fiscalizador direto, em muitos países ditos democráticos, a presença de observadores internacionais junto aos pleitos eleitorais são fatores que contribuem no sentido de avaliar se foram respeitados os princípios democráticos.

Seguem abaixo os requisitos necessários ao cumprimento de um pleito eleitoral baseado em um SEV (contemplando também o sistema tradicional) que esteja em concordância com as leis e regras da maioria dos sistemas eleitorais do mundo quanto à confiabilidade, robustez, lisura, transparência e democracia, os quais são objetos de estudos [COOL, 2001][MERCURI, 2001] em todo o mundo:

a) **Registro e autenticidade do eleitor:**

- Todos os eleitores, para exercer o seu direito de voto, devem estar devidamente registrados e habilitados, junto à autoridade eleitoral, a votar para determinado pleito;
- Devem existir mecanismos que afirmam a autenticidade do eleitor no dia de votação, visando evitar fraudes de personificação (votante que se apresenta falsamente como outro).

b) **Anonimato do eleitor:** o voto deve ser anônimo e não deve haver mecanismos que possibilitem associar o voto ao votante durante o processo, seja na votação, apuração, totalização ou em qualquer processo de auditoria/recontagem de votos. Esse requisito visa inibir procedimentos de *coação do eleitor* por terceiros e a *comercialização de voto* por iniciativa do mesmo, sendo estes procedimentos caracterizados como crime eleitoral;

c) **Unicidade:** em consonância com as leis de cada país, o eleitor somente poderá votar uma única vez em um mesmo pleito eleitoral, devendo o total de votos refletir proporcionalmente o total de votantes;

d) **Confidencialidade:** a partir do término da votação e armazenamento do voto, seja depositando-o numa urna tradicional ou numa urna eletrônica, a confidencialidade do mesmo deve ser mantida até o momento da apuração. Assim, não pode haver meios de se obter, durante o pleito, a quantidade de votos recebidos por um determinado candidato. Ou seja, não devem ser permitidas apurações parciais. Desse modo, a apuração só pode ocorrer após o término do pleito eleitoral;

e) **Integridade:** todo voto proferido por um votante não pode ser alvo de alteração ou eliminação durante o processo de votação ou apuração/totalização. A apuração/totalização deve garantir o princípio da unicidade;

- f) **Não-coação:** nenhum votante deve ser vítima de nenhum tipo de repressão que o obrigue a votar contra a sua vontade.
- g) **Não-comercialização do voto:** nenhum votante, depois de votar, deve usufruir de condições ou prova material que ateste a terceiros a qualidade de seu voto;
- h) **Materialização do voto:** o SEV deve prover meios de materialização da qualidade do voto, ou seja, a impressão do voto do eleitor e seu depósito em uma urna convencional;
- i) **Contraprova do voto:** num SEV, a totalização é feita computacionalmente e não através do procedimento de escrutínio da autoridade eleitoral sob fiscalização da sociedade, tal como é feito no sistema convencional. A contraprova deve ser fornecida pelo SEV para permitir que o votante tenha um indício de que seu voto foi computado corretamente, mas sem propiciar a coação, venda do voto, ou revelação da identidade do eleitor;
- j) **Auditabilidade:** um sistema de votação deve proporcionar auditabilidade, fornecendo, em todas as fases do processo, informações necessárias à obtenção de quaisquer indícios que possam representar fraude, funcionamento inadequado de *software* e *hardware* ou erro de operação humana. No entanto, as informações geradas não podem, em hipótese alguma, guardar dados que comprometam os requisitos de anonimato do eleitor, de confidencialidade e integridade do voto;
- k) **Usabilidade:** em um SEV, a usabilidade [BYRNE, 2007] do sistema deve contribuir para que o eleitor profira seu voto de forma amigável, ágil e sem erros. Assim, as interfaces devem ser projetadas de forma a garantir que o eleitor vote no menor espaço de tempo e com auto-suficiência. Além disto, possibilitar sua utilização por eleitores com baixo nível de escolaridade e com qualquer tipo de limitação física, visual ou auditiva. Para os eleitores com alguma deficiência, o normal é a existência de teclados com código em Braille e instruções através de áudio, entre outros mecanismos de acessibilidade;
- l) **Disponibilidade:** um SEV deve agregar a robustez necessária para garantir a disponibilidade do serviço, com as garantias dos demais requisitos, em todo o transcorrer do pleito eleitoral.

Outro requisito, nomeado como **Zerésima** [BRUNAZO, 2006] pelas autoridades eleitorais brasileiras, instrui que antes do início do pleito eleitoral, deve ser constatada a ausência de quaisquer votos para quaisquer candidatos, depositados na urna.

2.1.3. SEVs com infra-estrutura de redes de telecomunicações

Os requisitos e propriedades de um SEV abordados na seção 2.2.2 verificam-se quando o eleitor se dirige fisicamente a uma seção eleitoral e profere o seu voto sob “vigilância” e fiscalização das autoridades eleitorais na própria seção eleitoral. Porém, há implementações de SEVs em que o votante, de seu domicílio, vota remotamente pela Internet [MOHEN, 2001] ou em locais públicos, através de quiosques similares aos utilizados em auto-atendimento bancário, por exemplo, e, portanto, longe da fiscalização das autoridades eleitorais. Na Europa, o uso de telefones celulares, TV Digital e outros dispositivos já são objetos de estudos [CROW, 2002] para o uso em SEVs. Para todos os casos, é difícil garantir a não-coação e comercialização do voto.

Nessas arquiteturas de SEV, o voto do eleitor, na maioria das implementações, não fica armazenado no local físico onde o eleitor votou e sim, trafega através de redes de telecomunicações até ser armazenado de fato numa urna eletrônica. O eleitor apenas interage com uma interface comunicando-se com um sistema central, seja através de *software* dedicado ou através de navegadores de acesso a *World Wide Web*.

São vários os complicadores dessa arquitetura, desde problemas quanto a garantir parte dos requisitos apresentados no item anterior, como a necessidade de implementação de controle de acesso e *capabilities* [LAMPSON, 1971][LANDWEHR, 2001]. Além disso, é necessário poder garantir a disponibilidade do SEV durante o pleito eleitoral. Ataques do tipo *Denial Of Service* (DOS) [MOORE, 2001] podem ser o maior problema no que tange à disponibilidade do sistema e, caso ocorra, comprometerá o pleito eleitoral.

A complexidade para manter os requisitos de confidencialidade e integridade toma outra dimensão, mas o grande desafio dessa arquitetura, também objeto de estudos entre técnicos, especialistas e cientistas em todo o mundo, é garantir os requisitos do anonimato, não-coação, não-comercialização e materialização do voto.

Na realidade, os requisitos que se referem ao controle de acesso e *capabilities* enquadram-se nos requisitos de registro e autenticidade vistos anteriormente, mas através de técnicas de segurança computacional destinadas a prover segurança em sistemas de controle de acesso remoto. Também, técnicas de assinatura digital e de criptografia podem subsidiar as propriedades de confidencialidade e integridade.

Um dos grandes desafios nessa arquitetura de SEV é que os requisitos de não-coação e comercialização do voto ficam associados ao caráter do eleitor, pois não há como evitar que o

mesmo utilize o fato de não estar sendo vigiado para utilizar o seu voto como “moeda de troca”, tal como o comércio de voto, que pode ser chamado de voto-de-cabresto pós-moderno [BRUNAZO, 2006].

2.1.4. Comparativo entre os sistemas de votação

Minimizar o tempo de apuração e eliminação de erros no preenchimento de cédulas são os dois requisitos de maior impacto para justificar à sociedade civil o uso de SEVs. Por outro lado, a insegurança na legitimidade dos resultados, associada à falta de transparência dos produtos de *software* e *hardware* que compõem um SEV são desvantagens incontestáveis dos mesmos.

Por outro lado, num sistema de votação tradicional, a necessidade de esquemas complexos de proteção física das urnas, a demora na apuração dos votos, a usabilidade limitada e os erros de preenchimento de cédulas são aspectos que representam desvantagens desse sistema. Tendo como base o sistema eleitoral brasileiro e outras regras de contexto mundial, a Tabela 2.1 apresenta um resumo comparativo entre os sistemas, avaliando pontos de maior relevância quanto às desvantagens e vantagens de ambos.

Tabela 2.1: Alguns aspectos comparativos entre os sistemas de votação

Quesito	Sistema convencional	Sistema eletrônico
Tempo de apuração	Variável conforme o país. Pode demorar até 30 dias.	Até 24 horas
Erros de preenchimento	Marcação inválida ou rasuras que anulam o voto.	Inexistente, o sistema não permite preenchimento incorreto.
Recontagem	Sim	Eletrônica e/ou por cédulas quando há materialização do voto.
Falhas de Segurança	Comércio do voto e coação do eleitor; problemas de rasura do voto.	Falhas de <i>software</i> e seu uso pela Internet não evita o comércio de votos.
Interface com o usuário	Consiste numa cédula rústica e nem sempre traz um leiaute amigável.	Interface flexível, podendo ter figuras, fotos, vídeo e áudio.

Quesito	Sistema convencional	Sistema eletrônico
Materialização do voto	Sim	Dependente da implementação.
Contraprova do voto	Não	Dependente da implementação.

2.1.5. Equipamentos utilizados em SEVs

Para que um SEV atenda aos requisitos da redução do tempo da apuração da votação e eliminação de erros de preenchimento das cédulas, algumas tecnologias de *hardware* associadas ao *software*, foram desenvolvidas para esse fim. Para uma melhor visualização, a figura 2.1 esboça o modelo de votação tradicional e de três tecnologias de uso dedicado em SEVs. Essas tecnologias normalmente são utilizadas em um pleito tradicional, em que o eleitor se dirige à seção eleitoral e, na presença das autoridades eleitorais, profere seu voto. Seguem, abaixo, características de cada tecnologia:

- Tecnologia **DRE** (“Direct Recording Electronic”) [NORDEN, 2006] [FISCHER, 2003] ou de **gravação eletrônica direta**: é um equipamento composto por *hardware* e *software* (basicamente um microcomputador dedicado), no qual o eleitor registra seu voto, utilizando uma cédula virtual na tela, sendo a interação homem-máquina efetuada através de toque direto na tela (*touch screen*) ou através de teclas especiais. O voto é cifrado e gravado em meio persistente e, ao término do pleito eleitoral, o voto armazenado é encaminhado a um centro de processamento para ser totalizado conjuntamente com dados de votação de outros DREs. Para o processo de contagem, é utilizada uma chave para decifrar o voto e nenhuma associação entre voto e votante deve ser efetuada. A tecnologia de equipamentos baseada em DRE é a mesma utilizada pelo TSE nas eleições brasileiras, com pequenas diferenças.
- Tecnologia **DRE w/ VVPT** (“DRE with Voter Verified Paper Trail”) [NORDEN, 2006] [FISCHER, 2003] ou DRE com **voto impresso conferido pelo eleitor**: possibilita que o voto seja impresso e, antes de ser armazenado em uma urna tradicional, o eleitor confere a qualidade do voto. O voto impresso somente é utilizado em caso de discordância na apuração e, portanto, utilizado para recontagem. A materialização do voto através do VVPT em SEVs agrega uma

confiabilidade maior ao sistema, visto que qualquer sinal de burla na apuração eletrônica possibilitará a recontagem convencional, cédula a cédula, com a vantagem de que não haverá cédula inválida decorrente de preenchimento irregular, fato comum no sistema convencional. No Brasil, o voto impresso conferido pelo eleitor já foi utilizado, mas abandonado em 2003 por força de lei.

- Tecnologia **PCOS** (“Precinct Count Optical Scan”) [NORDEN, 2006] [FISCHER, 2003] ou **sistema de contagem por leitura óptica**, no qual o eleitor utiliza uma cédula similar aos cartões de loteria, para marcação a caneta ou perfuração no campo correspondente ao candidato desejado e, ao término, a cédula é submetida ao equipamento óptico para leitura e registro do voto. Tal como o DRE w/ VVPT, a qualidade do voto (cédula) vai para uma urna tradicional, possibilitando futuras auditorias quando da contestação dos resultados.

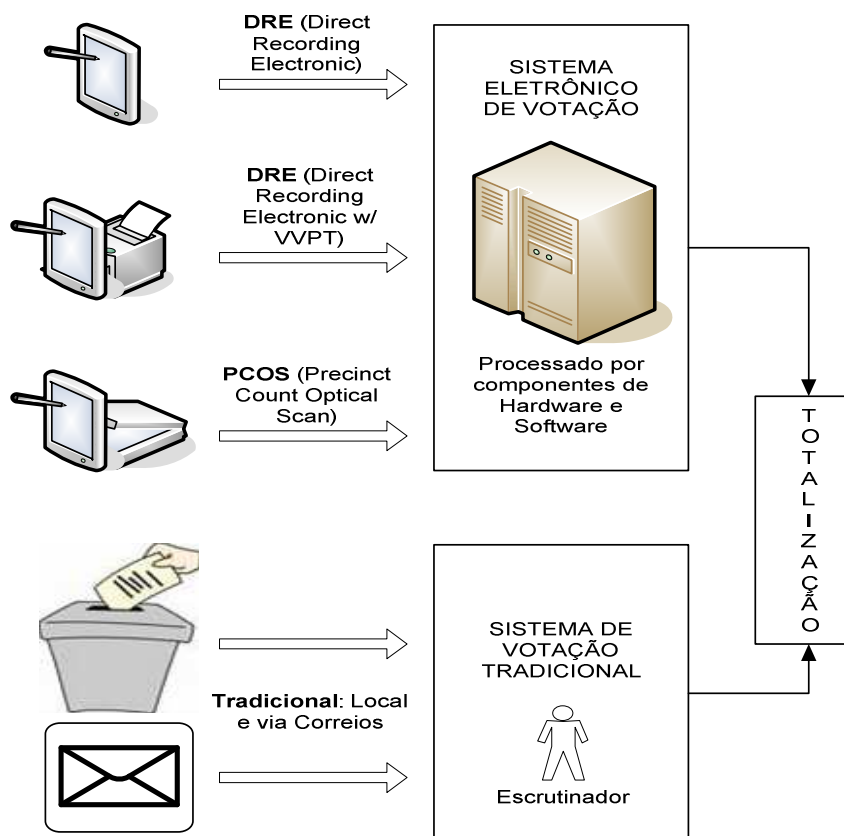


Figura 2.1: As diversas tecnologias de equipamentos utilizadas em SEVs

2.3. Segurança Computacional Clássica

Em [SANTIN, 2004], o autor define que segurança em sistemas computacionais não é exclusivamente um meio para permear fins, mas é, antes de tudo, uma disciplina que, através de seus conceitos, metodologias e técnicas, tenta manter as propriedades de um sistema, evitando ações danosas de entidades não autorizadas sobre as informações e os recursos do mesmo.

Quando passa a operar, seja por ser novo ou por ter sofrido modificações, o mesmo pode estar sob ameaça, que compreende procedimentos de exploração de falhas até então desconhecidas. A ação resultante da exploração de falhas é o ataque. Quando se tem uma falha conhecida, podemos dizer que o sistema está vulnerável.

Pode-se afirmar que os sistemas computacionais estão sempre sujeitos a ameaças e, portanto, passíveis de ataques dos mais variados tipos, os quais decorrem da presença de vulnerabilidades (falhas de programação, configuração, projeto, atualização etc.).

Conforme [LANDWEHR, 2001], para manter as propriedades de segurança de um sistema, deve-se garantir ao mesmo:

- **Confidencialidade:** a informação somente poderá ser revelada ao sujeito que detém a autorização sobre a mesma;
- **Integridade:** a informação não pode ser passível de alteração por sujeitos não autorizados, seja de forma maliciosa ou acidental;
- **Autenticidade:** provê garantia da legitimidade de uma identidade;
- **Disponibilidade:** a informação deve estar disponível, a qualquer momento, a sujeitos que são usuários legítimos da mesma;
- **Não-repúdio (irretratabilidade):** uma comunicação legítima entre duas entidades não pode ser negada por nenhum dos sujeitos que dela participaram.

Associado aos pilares da segurança computacional tem-se o controle de acesso [LAMPSON, 1971], que, em função das regras (políticas de segurança), autoriza o acesso do sujeito a determinado recurso com base no sistema autenticação.

A autorização consiste em atribuir direitos de acesso a recursos aos sujeitos e depois regular o acesso desses sujeitos aos recursos, com base nas políticas de controle de acesso. A autenticação é o processo de identificação do sujeito que a partir da apresentação de uma

contraprova, possibilita que o mesmo possa ser identificado de forma legítima. Como exemplo, um dos processos de autenticação mais conhecido é o esquema usuário/senha.

As políticas de autorização, de forma geral, são baseadas em regras ou ACLs (*Access Control List*) definidas a partir de uma matriz de acesso (D), onde, na intersecção D_{ij} , temos os atributos de autorização/acesso, que, no esquema de permissões, pode ser: leitura, escrita, execução. Assim, para ' i ', temos os sujeitos e em ' j ', os objetos ou recursos do sistema.

Tabela 2.2: Matriz de acesso conforme [LAMPSON, 1971]

	Recurso 1	Recurso 2
Sujeito A	Direitos (D_{ij})	Direitos (D_{ij})
Sujeito B	Direitos (D_{ij})	Direitos (D_{ij})

Na matriz de acesso (Tabela 2.2), tem-se a lista de controle de acesso (ACL), onde o sujeito se relaciona com os objetos e os direitos sobre o mesmo. Outra relação é a de lista de competências (*capabilities*) com o objeto e os direitos que o sujeito possui sobre o mesmo.

2.4. Segurança Aplicada a SEVs

O projeto e a implementação de um SEV devem ser concebidos de forma que a segurança computacional nele provida atenda os requisitos e propriedades apresentadas na Seção 2.2, de forma a agregar confiabilidade, robustez, transparência e estar sincronizado com os preceitos democráticos associados ao uso desses sistemas.

No entanto, a reputação dos SEVs tem sido abalada junto à sociedade em decorrência das possíveis ameaças de vulnerabilidades a que esses sistemas estão suscetível, motivada pela tecnologia utilizada.

Alguns estudos [CROW, 2002], [FISCHER, 2003], [NORDEN, 2006] avaliaram as vulnerabilidades e ameaças baseadas nas três tecnologias de votação mais utilizadas em todo o mundo, isto é, o DRE, o DRE w/ VVPT (*DRE with Voter Verified Paper Trail*), o PCOS (*Precinct Count Optical Scan*), *software* e infra-estrutura de comunicação associada. Como todas as tecnologias utilizam produtos de *software*, parte-se da premissa de que todas as três tecnologias são vulneráveis a ataques e falhas. No entanto, sendo conhecidos os possíveis ataques e falhas desses sistemas, podem-se tomar contramedidas que elevem o nível de proteção e confiabilidade dos mesmos.

2.4.1. Equipamentos de votação

Os equipamentos DREs sem dispositivos que materializam o voto do eleitor no momento da votação e utilizados atualmente no Brasil não possuem recursos que permitam procedimentos de recontagem através da cédula em papel, permitindo, assim, que o produto de *software* possa maliciosamente, ou por falha, alterar o resultado final do pleito eleitoral.

Como regra geral, qualquer SEV que não produza a materialização do voto pode sofrer ataques quanto aos requisitos de integridade, um dos itens mais relevantes em um sistema de votação, pois reflete na exatidão dos resultados, conseqüentemente, ferindo os desejos dos eleitores e, se malicioso, a democracia.

Já os equipamentos DREs ou PCOS que possibilitam a materialização do voto, apesar de mais confiáveis por possibilitarem a recontagem, por si só são questionáveis. Para que esse procedimento fosse válido, faz-se necessário iniciar a recontagem dos votos em papel após o término do pleito e com o mesmo rigor de fiscalização do sistema tradicional. Os anseios por sistemas mais rápidos na apuração, mesmo com a contagem manual, são atendidos, pois o resultado eletrônico será imediato e a contagem das cédulas apenas servirá como uma contraprova do resultado já apurado. Talvez esse procedimento seja visto como um retrocesso, mas é necessário até que os cientistas apresentem um novo paradigma na programação do *software* e que se tenha um sistema de auditoria, de fato, amplo e confiável.

2.4.2. Software

Os ataques sobre produtos de *software* nem sempre são fáceis de descobrir, mesmo sobre processo de auditoria. Em eleições políticas, por força de lei, é facultada a algumas entidades a auditoria do sistema, principalmente do *software*. Esse processo ocorre meses antes do início do pleito eleitoral, permitindo que o *software* seja alterado posteriormente a essa auditoria. Ainda deve-se considerar que o tempo hábil que os auditores dispõem é mínimo, quando se trata de programas com códigos extensos.

Proporcionar o tempo necessário a essa auditoria de forma a ser executada uma avaliação segura e com consistência é um primeiro passo. O segundo seria gerar resumos (*hash function*) [RIVEST, 1993] de todos os arquivos de programa e de configurações envolvidos para que, no dia do pleito eleitoral, quando for impressa a **Zerésima** [BRUNAZO, 2006], também sejam gerados e impressos os resumos dos programas em tempo real e que os auditores/fiscais façam a checagem dessas informações.

Passando para os aspectos de faltas em *software*, passíveis de ocorrer, as premissas são básicas, ou seja, o uso de metodologias aplicadas à engenharia de *software* que compreendam testes exaustivos e adversos é indispensável e necessário.

Adicionalmente, alguns organismos de padronização e testes de *software* publicaram os documentos [RODRIGUEZ, 2002], [ISSO/IEC, 1999], [WANG, 2003], tendo como público-alvo projetistas e desenvolvedores de *software*. Esses documentos contemplam um conjunto de diretrizes para a escrita de programas com elevado nível de qualidade e segurança sob vários aspectos e que são instrumentos úteis frente às ameaças em produtos de *software*. Parte-se do princípio que um *software*, quando escrito e testado dentro “das melhores práticas” e utilizando padrões reconhecidos e consolidados, apresenta a possibilidade de faltas por programação inadequada próxima de zero.

O uso de *trojan horses* ou outros programas corruptos é o meio mais fácil de alterar o resultado de uma eleição. Apesar de não se ter registro desse tipo de ataque, o mesmo figura como uma ameaça primária e a sua identificação nem sempre poderá ser detectada por processo de inspeção prévia, mas o uso de criptografia e *software* de segurança contribui na proteção desse tipo de ataque.

Em [NORDEN, 2006] há um posicionamento quanto às diversas dificuldades para que um ataque por *software* possa ser implantado, visto que:

- O atacante teria que ter algum meio de inserir esse *software* na máquina e para isso teria que estar em conluio com funcionários, fabricante, entre outros envolvidos no processo;
- O atacante teria que conhecer bem a estrutura do *software*, base de dados e da própria cédula e padrões físicos do sistema, para produzir um programa corrupto adequado;
- O atacante também teria que saber exatamente os padrões da cédula e dos candidatos para, de fato, inferir no resultado de forma desejada;
- A implantação do *software* corrupto pelo atacante deveria ser feita de forma que, no procedimento inspeção e/ou auditoria anterior ou posterior à eleição, não fosse detectado.

Em suma, o *software* corrupto pode ser inserido no sistema em qualquer ponto do processo e normalmente é dependente do sistema operacional ou está presente no próprio *software* básico do sistema de votação, ficando para os procedimentos de inspeção e auditoria a verificação desse tipo de ameaça.

2.4.3. Infra-estrutura de telecomunicações

O uso de SEVs sobre infra-estrutura de redes de telecomunicações aumenta significativamente os riscos de ameaças a esses sistemas, principalmente se a infra-estrutura for a meta-rede Internet. Numa rede como a Internet, independente do uso de *firewall* ou sistemas de detecção de intrusão (IDS), existe toda uma “comunidade” de *hackers* espalhados pelo mundo, disponíveis e prontos para explorar vulnerabilidades e, portanto, gerar ataques sobre o sistema. Numa rede privativa, o nível de insegurança é menor, visto que os ataques se limitam à concessionária locatária do serviço e às autoridades eleitorais que administram a infra-estrutura do sistema. Seguem abaixo algumas vulnerabilidades e/ou ataques mais comuns, passíveis de ocorrerem sobre SEVs, utilizando infra-estrutura de telecomunicações:

- a) **Negação de serviço:** conhecido como DOS (*Denial-Of-Service*) [MOORE, 2001], é a principal ameaça a um SEV utilizando a Internet, visto que qualquer ataque desta natureza poderá negar acesso ao sistema, ferindo o requisito de disponibilidade. Normalmente, esse tipo de ataque consiste em se enviar um número muito grande de pacotes de abertura de conexão para o servidor, sem que a origem dê continuidade com o estabelecimento da mesma, fazendo com que os recursos do servidor, ora limitados, esgotem-se. Ainda mais danoso é o DDOS (*Distributed Denial-Of-Service*), que é um ataque de negação de serviço distribuído. Esse, além de efetuar o já exposto, facilmente fará com que o canal de comunicação também se esgote. Em redes privadas, dificilmente esse tipo de ataque será possível, visto a facilidade de se identificar a origem, sendo esse um fator de inibição. Nesse tipo de ataque, normalmente o endereço de origem é forjado, dificultando o rastreamento;
- b) **Ameaças de integridade:** como todo o tráfego dos dados entre o Console de Votação e o centro de gerência do SEV ocorre pela rede de telecomunicações, é imprescindível o uso de criptografia fim-a-fim na camada de transporte [OSI/IEC, 1997], tanto para sistemas baseados na Internet como em redes privadas. O uso de protocolos seguros, tais como SSL/TLS, é alternativa consagrada para esse tipo de comunicação, pois garante que os dados não serão alvos de inspeção e adulteração entre origem e destino. Ainda, cifrar e assinar digitalmente os documentos na camada de aplicação [OSI/IEC, 1997] eleva o nível de segurança frente a essa vulnerabilidade;

- c) **Redes sem fio:** Apesar de agregarem praticidade e economia em alguns casos, o uso de redes sem fio em equipamentos para SEVs (computadores, urnas etc.), no atual contexto, mostra-se uma ameaça quando se trata do requisito disponibilidade. As exposições de [BARNES, 2002] e [VLADIMIROV, 2004] mostram que, em decorrência de o sinal no qual trafega o dado ser por rádio frequência, diferente dos baseados em fios – nos quais o acesso físico é necessário, no sem fio basta estar, em qualquer momento, no raio de recepção do sinal que se podem efetuar ataques que comprometam o canal de comunicação. Ataques à segurança da integridade por interceptação ou escuta através de *sniffers*, SSID e MAC *Spoffing* são uma séria ameaça, mas podem ser resolvidos com algumas técnicas atualmente existentes. Diferente dos ataques na camada física (rádio frequência), cujas técnicas de resolução são insuficientes para garantir a disponibilidade do sistema.

2.4.4. Aspectos gerais de segurança

Vulnerabilidades e ameaças em sistemas de votação são fatos antigos e as contramedidas devem ser pró-ativas, isto é, prover testes periódicos para avaliar os riscos e vulnerabilidades. Isso fica evidente quando se implementa uma nova versão de *software*, onde novas vulnerabilidades podem estar surgindo e testes metódicos e apurados devem ser uma constante.

No relatório Brennan [NORDEN, 2006], entre os diversos pontos estudados, identificou-se que: os SEVs são vulneráveis; foram apontadas 120 possíveis vulnerabilidades com margem a fraudes: a adulteração dos resultados através de *software* de forma maliciosa é um ponto forte; e procedimentos de fiscalização e auditoria devem ser criteriosos.

Desenvolver políticas de testes de votação paralelos e com nível de amostragem significativo, associados à escolha aleatória de urnas e/ou equipamentos envolvidos, além de definir regras para resolução quanto a evidências de fraudes ou erro de apuração, são contramedidas necessárias na prevenção e resolução de fraudes.

Por fim, não direcionada ao ponto de vista computacional, existe a questão da confiabilidade do registro do eleitor, que inclui o uso do registro de pessoas já falecidas, refletindo-se, portanto, no resultado final, o que é uma ameaça à democracia. Alguns países [CYBERTRUST, 2005][LIETOLD, 2005] já adotam a identificação por cartões inteligentes, denominados eID e/ou *Citizen Card*, e o uso de dispositivos biométricos que contêm dados do

eleitor, incluindo foto e assinatura digital, possibilitando uma identificação mais confiável. Esses são utilizados em todas as transações entre cidadão e governo. No caso da biometria, é uma garantia de que a pessoa seja, de fato, quem se diz ser.

2.5. Falhas e ideologias aplicadas a Sistemas de Votação

Informatizar um sistema de eleição tradicional levanta algumas controvérsias. Em [GOTTERBARN, 2006] são apresentados questionamentos quanto às falhas de cunho profissional, ou seja, administradores que se deixam levar pela tecnologia e influenciam decisões que levam o uso de mecanismos tecnológicos na resolução de problemas, que nem sempre vêm a ser a melhor opção.

Alguns aspectos culturais e ideológicos são fatores que levam tais profissionais ao erro, por acreditarem que informatizar ou automatizar um processo manual resultará em ganho de tempo e segurança.

No entanto, isso não se aplica em todas as áreas de conhecimento ou produção e deve ser analisado com cuidado. A decisão quanto às mudanças não poderá partir unicamente de um profissional que se posiciona favorável, mas de um estudo conjunto envolvendo os diversos participantes do processo de votação.

Em processos de votação de larga escala e de grande impacto na sociedade, tais como as eleições presidenciais e parlamentares, apenas automatizar o processo pode não levar aos resultados desejados. É necessário considerar a usabilidade, a padronização e a segurança.

A usabilidade de um SEV [BYRNE, 2007] é um requisito a ser considerando para o sucesso do sistema, visto que idosos e pessoas com baixo nível de escolaridade tendem a ter um nível de dificuldade mais acentuado no uso do sistema. Assim, um SEV que não agrega facilidade no preenchimento da cédula eletrônica pode gerar grandes rejeições e atrasos nos procedimentos, decorrentes da dificuldade no uso do sistema, inviabilizando-o.

Por outro lado, jovens ou pessoas com melhor nível de escolaridade, ou até mesmo que já se influenciam pela tecnologia do mundo moderno, tornam-se facilitadores do processo, pois se pudessem votar através de seus telefones celulares, PDAs e Internet, seriam bastante motivados por estas opções.

Segurança, em conjunto com usabilidade, é aspecto de suma importância em SEV, e o conjunto fornece confiabilidade e aplicabilidade aos processos. Os SEVs são produtos de *software* que contabilizam e guardam o voto em sigilo. A exatidão da quantidade de votantes

e da qualidade de voto é um requisito indispensável num pleito eleitoral, pois, ao seu término, o número de votantes deve coincidir com o número de votos contados, e a qualidade do voto ser fidedigna ao desejo do votante.

Diante do apresentado, percebe-se que falhas de condução dos profissionais envolvidos no processo podem desencadear problemas operacionais e de confiabilidade ao processo de automatização relacionados às áreas de logística, *hardware* ou *software*.

Nos Estados Unidos, um congresso promovido pelo grupo denominado *Help American Vote Act*-HAVA sugeriu que o sistema de votação americano devesse ser automatizado, e que os cartões perfurados utilizados naquele momento nos processos eleitorais de grande escala fossem substituídos por outros que utilizassem meios tecnológicos mais avançados. Porém, essa posição partiu de estudos científicos que envolvem experimentos para fundamentar a proposta.

Desta forma, o sucesso de um novo projeto pode não estar aliado ao uso da tecnologia, mas sim a um estudo minucioso e com experimentos que reflitam o contexto real no qual será utilizado e ideologias não devem ser colocadas à frente da ciência.

2.6. Conclusão

Este capítulo abordou uma introdução à segurança computacional e analisou dois sistemas de votação em uso no mundo: o sistema tradicional, que já sobrevive há séculos, e o sistema eletrônico, que atualmente tem despertado interesse de pesquisadores em toda a comunidade acadêmica, pelo seu evidente uso em sistemas eleitorais, associado a algumas falhas inerentes à tecnologia, quanto a garantir algumas propriedades básicas para esses sistemas.

Dando-se maior ênfase ao sistema eletrônico, foram apresentados alguns conceitos básicos, os requisitos e propriedades necessários para garantir a reputação, transparência, lisura de um pleito eleitoral, um comparativo entre os sistemas e um parecer associado a erros de ideologia na concepção desses sistemas. O objetivo não foi abordar de forma minuciosa todos os aspectos dos sistemas, visto que outros capítulos detalharão alguns itens aqui apresentados, com maior riqueza de pormenores.

Capítulo 3

Trabalhos Relacionados

Com o surgimento dos SEVs como alternativa aos sistemas tradicionais, diversos problemas de segurança foram identificados, o que lançou suspeitas sobre a mera informatização dos sistemas de votação.

Nos Estados Unidos e Europa, entidades governamentais e da sociedade civil têm se mobilizado em workshops e outros eventos, pesquisando soluções que visam determinar a melhor solução quanto ao uso de um sistema de votação para o seu país, no sentido de eliminar as vulnerabilidades e ameaças aos SEVs.

3.1. Trabalhos Científicos

3.1.1. Sistema baseado em cédulas físicas, com contraprova e sem uso de criptografia

Em [RIVEST, 2007] é apresentado um modelo de sistema de votação tradicional (baseado em papel) que fornece ao eleitor uma contraprova de seu voto.

A proposta apresenta um sistema de votação baseado em papel com o uso de três cédulas idênticas, onde os candidatos estão dispostos em linhas organizados por cargo (ex: presidente, senador, deputado etc.). À frente da identificação de cada candidato, há um círculo para marcação do voto, permitindo que essa marcação possa ser lida por um sistema de leitura óptica. A única diferença entre as cédulas é um ID numérico disposto no rodapé da mesma, que é único em cada processo eleitoral.

Para indicar o candidato a ser votado, o eleitor deve hachurar/marcar o círculo à frente da identificação do candidato em duas das três cédulas. Todos os candidatos (não votados) receberão uma marcação aleatória única em uma das três cédulas. Esse procedimento deve ser repetido para os diversos cargos presentes na cédula. A figura 3.1 ilustra uma cédula marcada

conforme o critério apresentado, onde o **Candidato A** foi o candidato votado pelo eleitor para o **Cargo I**.

Preenchidas as cédulas, o eleitor deve entregá-las ao mesário ou à Autoridade Eleitoral competente no recinto de votação, o qual submeterá as cédulas para validação por um equipamento do tipo *Mark Sense*, onde indicativos sonoros diferenciados indicarão se a cédula está ou não adequadamente preenchida.

CÉDULA 1	CÉDULA 2	CÉDULA 3
<u>Cargo I</u>	<u>Cargo I</u>	<u>Cargo I</u>
Candidato A ●	Candidato A ●	Candidato A ○
Candidato B ●	Candidato B ○	Candidato B ○
Candidato C ○	Candidato C ○	Candidato C ●
ID1	ID2	ID3

Figura 3.1: Cédulas preenchidas segundo o esquema proposto por [RIVEST, 2007].

O conjunto de cédulas devidamente preenchidas habilita o eleitor a receber uma CÓPIA de qualquer uma das cédulas como recibo do processo. Então, o equipamento que valida as cédulas fixa uma tarja vermelha no rodapé da cédula cobrindo a área onde se encontra o ID da cédula de forma a indicar que a mesma já foi utilizada. O processo de depósito das cédulas na urna é feito após a separação das cédulas, agora individualmente armazenadas na mesma. A máquina de validação não mantém nenhum registro dessa validação. Apenas informa o preenchimento correto, podendo também gerar uma autenticação nas cédulas e imprimir o recibo.

Para que o voto seja considerado, na apuração, a fórmula é subtrair o número de votantes da quantidade de marcas que o candidato obteve:

$$\text{Total de votos do candidato} = (\text{Total de marcas do candidato}) - (\text{Total de Votantes})$$

Como exemplo, considere dois votantes. Se, hipoteticamente, ambos votaram conforme o exemplo da figura 3.1, de acordo com a fórmula acima, teremos o seguinte resultado para o **Cargo I**: **Candidato A**: Total de Votos = 4 – 2 = 2 votos; **Candidato B**: Total de Votos = 2 – 2 = 0 votos e **Candidato C**: Total de Votos = 2 – 2 = 0 votos.

Após o término do pleito, o eleitor poderá conferir via *World Wide Web* se o seu voto foi computado no processo de apuração, comparando a cédula que levou consigo como contraprova com uma cópia da mesma publicada no boletim de votos apurados na *web*.

Assim, bastar verificar se a qualidade do voto e o ID conferem, para que o votante tenha indícios que o seu voto foi contado durante a apuração.

Pode-se aferir que o modelo agrega alguns pontos positivos no atendimento aos requisitos de um sistema de votação, tais como:

- O **anonimato** é garantido tal como no sistema tradicional, pois não há associação entre o processo do voto e a habilitação do eleitor ao voto como ocorre no sistema brasileiro (há uma conexão do sistema de habilitação e voto o qual é comandado pelo mesário). Ainda, como a cédula é depositada em uma urna física, o processo de desvinculação das três cédulas ocorre naturalmente. A tarja vermelha que esconde o ID é apenas mais um dispositivo para garantir o anonimato;
- Apesar do uso da contraprova, o eleitor não terá como provar a terceiros qual foi o seu voto, independente da cédula de **contraprova** que o mesmo detém. Isso porque, para provar efetivamente a qualidade do seu voto, o eleitor teria que ter a posse de, no mínimo, duas cédulas para identificar o candidato no qual votou, garantindo, assim, a **não-comercialização do voto** e as propriedades da **confidencialidade** e **não-coação**;
- Como existe a materialização do voto, o processo de recontagem é possível em caso de suspeitas de fraudes;

Esse modelo de votação apresenta algumas limitações nos seguintes aspectos:

- Por se tratar de um esquema manual de marcação de três cédulas diferentes, entende-se que a **usabilidade** do sistema pode estar comprometida. O processo de votação pode se tornar confuso para alguns eleitores (principalmente os mais idosos, com menor grau de instrução etc.), podendo gerar inúmeras recusas no processo de validação por preenchimento incorreto, provocando atrasos no pleito;
- A **integridade** dos votos precisa ser garantida com esquemas especiais de proteção das urnas.
- A **substituição ou adulteração** de cédulas, de modo malicioso, é uma forma de fraude possível de comprometer a votação, apesar de ser um procedimento mais difícil. Esse procedimento também implica a necessidade de acesso ao banco de dados do boletim de contraprova e de ID válida para aquela seção/eleição.

- Como os IDs estão impressos na cédula antes do eleitor votar, um mesário mal intencionado poderia anotar os IDs e distribuir de modo tendencioso as cédulas.
- A geração da **cópia da cédula** que servirá como contraprova pode não ser trivial.
- O processo de identificação do eleitor não é abordado, podendo ocorrer a substituição (personificação) do eleitor como em qualquer outro processo de votação tradicional.

Conclui-se que esse sistema, de fato, agrega condições de auditoria por parte do votante e demais órgãos fiscalizadores, pois a lista de votantes é divulgada conjuntamente com a contraprova. Isso possibilita ao eleitor verificar a contabilização do seu voto. Por outro lado, há várias desvantagens relacionadas ao sistema tradicional que são herdadas neste sistema, como mencionado acima.

A proposta do autor pode ser operacionalizada, mas está sujeita a não trazer absoluta agilidade para o processo de votação manual, principalmente se consideramos que, no sistema brasileiro, o grande número de deputados faria com que a cédula ficasse extensa.

3.1.2. Sistema baseado em cédulas físicas, com contraprova e com uso de criptografia

Em 2004 [CHAUM, 2004] propôs um modelo de SEV que propicia ao eleitor um recibo como contraprova do seu voto. Diferente do sistema apresentado na seção 3.2.1, esse modelo é totalmente direcionado a SEVs e codifica a cédula através de esquemas baseados em criptografia visual [NAOR, 1994].

O modelo proposto considera os seguintes aspectos:

- A área da cédula onde o eleitor marca a sua qualidade de voto é composta por duas faces, a frontal e a de fundo, sendo ambas de material plástico transparente;
- A qualidade do voto é impressa em ambas as faces da cédula, utilizando a técnica - de criptografia visual. Quando as faces forem sobrepostas (alinhadas), pode-se identificar o voto do eleitor em texto claro. A figura 3.2 ilustra a área da cédula que contém a qualidade do voto do eleitor, onde ambas as faces se encontram alinhadas, sendo possível visualizar normalmente o texto *Separate layers before leaving booth*;
- Cada uma das faces, visualizada separadamente, não identifica a qualidade do voto do eleitor em função do processo criptográfico utilizado. As figuras 3.3 e 3.4 apresentam a face frontal e de fundo separadas uma da outra, onde se pode

observar que o texto fica completamente ilegível, não sendo possível identificar a qualidade do voto;

- A contraprova compreende uma cópia de uma das faces que o eleitor escolherá aleatoriamente;



Figura 3.2: Parte da cédula, com faces alinhadas e com texto legível [CHAUM, 2004].



Figura 3.3: Face da cédula usada como recibo e com texto ilegível [CHAUM, 2004].

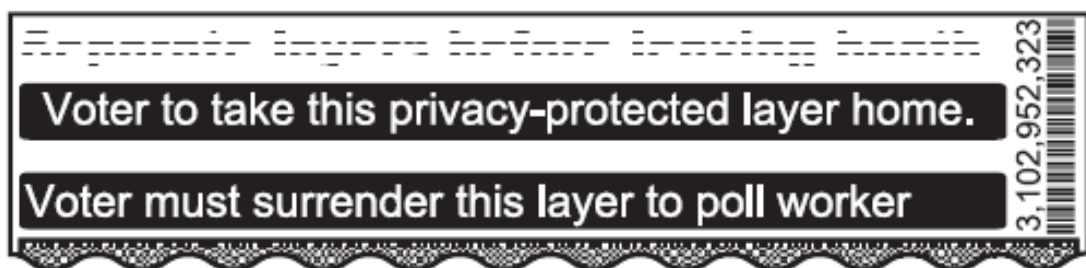


Figura 3.4: Face destruída pelo mesário diante do eleitor [CHAUM, 2004]

A figura 3.5 apresenta, de forma mais clara e macroscópica, o mecanismo da codificação visual. Pode-se considerar um pixel composto por quatro sub-pixeis, sendo que em cada pixel, temos a impressão de dois pixeis pretos e de dois brancos, sendo um inverso ao outro. Quando, em cada camada, a posição dos sub-pixeis é igual dentro do pixel, o resultado é um pixel parcialmente preenchido (transparente) ao serem alinhadas as camadas. Quando

temos, em cada camada, os quatros sub-pixeis inversos em relação às camadas, o resultado será um pixel totalmente preenchido (opaco) quando do alinhamento das camadas.

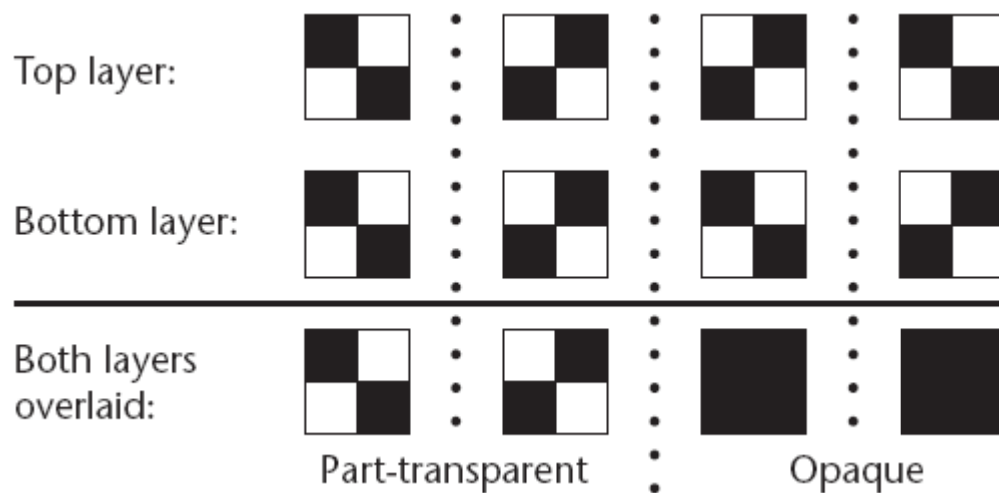


Figura 3.5: Camadas com os *pixels* que formam a imagem [CHAUM, 2004].

Para melhor visualizar a relação da figura 3.5, temos na figura 3.6 um exemplo claro e prático, no qual se pode perceber que a relação mútua das impressões em preto dos *pixels* em cada camada permite que o texto fique legível quando do alinhamento das camadas (faces).

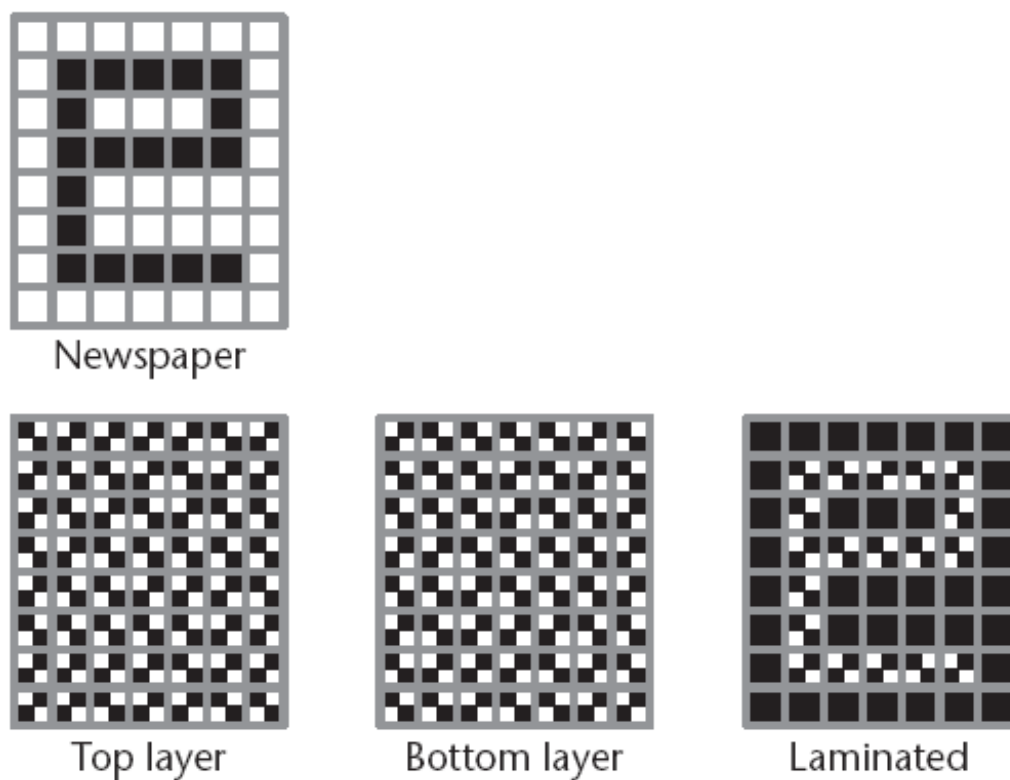


Figura 3.6: Recomposição da imagem a partir das duas camadas [CHAUM, 2004].

Esclarecida a questão da codificação da contraprova/recibo sem entrar no mérito do algoritmo, o que não é o escopo deste trabalho, fica a questão de como o eleitor fará a conferência do seu recibo (contraprova) após o término do pleito. Antes, deve ser esclarecido que o votante deve escolher entre uma das faces para que o mesmo a leve como recibo ou contraprova do voto, a outra camada deverá ser destruída pela Autoridade Eleitoral juntamente com o eleitor. A partir da escolha do eleitor, o sistema imprime em cada face informações indicando qual a face escolhida pelo votante e qual a face que deve ser destruída por um picotador de papéis ou algo similar.

Após a votação, a conferência do recibo ocorre a partir da publicação dos resultados na *World Wide Web*, na qual é divulgada uma cópia idêntica à do recibo, permitindo que o eleitor imprima o recibo divulgado e faça o alinhamento com o seu recibo, de forma a verificar se os pontos ou reticulados pretos que formam a imagem ou texto são iguais aos do recibo que possui. O ID que também é impresso na cédula deve ser o mesmo.

O SEV proposto utiliza, para fins de apuração, somente uma cópia eletrônica do recibo, a qual o eleitor optou por levar. A outra face (eletrônica) é destruída, tal como ocorre com a face física.

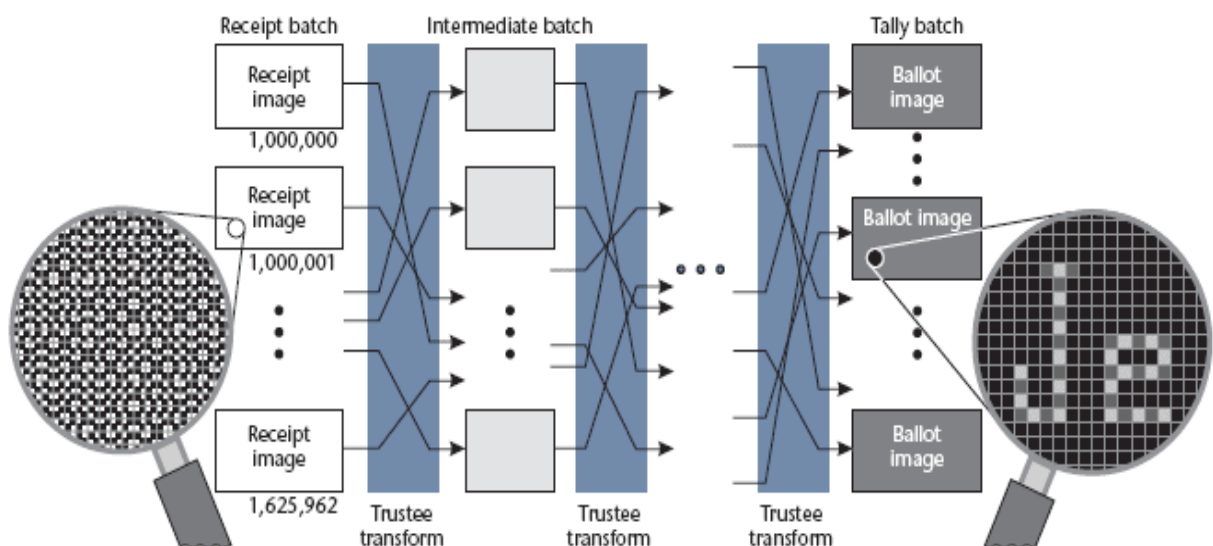


Figura 3.7: Processo de reconstrução da última plegada da cédula [CHAUM, 2004].

No processo de contagem dos votos, ocorre um esquema onde os recibos virtuais, que se encontram cifrados, passam por fases numa ordem casual (*mixnet*), nas quais, a cada uma delas, parte da cédula é decifrada. Uma fase alimenta a outra, possibilitando, ao final, recuperar a outra face do recibo, que complementa a informação codificada. Em cada ponto intermediário ou de transformação, é utilizada uma nova chave de decodificação, conforme o esquema criptográfico aplicado. A figura 3.7 apresenta todo esse mecanismo de recuperação da cédula e, portanto, possibilitará a obtenção da qualidade do voto em texto claro e permitirá a apuração por meio óptico.

A principal vantagem do modelo está no fato de a contraprova (recibo) se basear em algoritmos de criptografia visual, o que dificulta fraudes que comprometem a integridade do sistema, dada a criptografia empregada no esquema. Mesmo sendo o recibo a fonte codificada e que permite recuperação da informação do voto em texto claro, o uso de múltiplas chaves para a decodificação inviabiliza qualquer tentativa de quebra do processo criptográfico utilizado.

Em [CHAUM, 2004] é feita uma avaliação de três formas de modificar a cédula de forma ilícita, a partir de *software* corrupto e/ou malicioso, sem que a fraude seja detectada diretamente:

- Se for impressa uma face incorreta, que será utilizada na apuração, e o votante levar outra face, cuja codificação condiz com o seu voto;
- Se for utilizado o mesmo número de série para dois recibos diferentes, supondo que os dois eleitores escolherão a mesma face;
- Se for executado de forma incorreta um dos passos da contagem, considerando que esse item não será verificado no processo de auditoria.

O modelo apresenta dois pontos negativos, que são:

- A necessidade do uso de uma impressora e material de impressão especial, que encarecem o processo, além de demandar a fabricação de equipamento especial, dado que este não é produto de mercado;
- Uma das faces, a que não foi escolhida pelo eleitor como recibo/contraprova, deve ser destruída no local da votação por um picotador de papel ou algo similar que evite a sua reconstrução. No entanto, esse procedimento pode ser falho quanto à possibilidade de o “lixo” ser reaproveitado maliciosamente. Considerando que

cada seção necessitaria de um picotador de papel, tem-se um aumento do custo para a solução proposta.

3.1.3. Sistema baseado em HSM e documentos XML

Em [ROSSLER, 2005] é apresentado um sistema de votação eletrônica baseado em documentos XML [BENZ, 2003], assinatura digital e uso de um *Hardware Security Module* (HSM) como elemento fundamental que caracteriza a urna eletrônica e que visa agregar segurança à chave privada associada às assinaturas, e demais operações envolvendo criptografia.

O HSM, ou Módulo de Segurança de *Hardware*, é um dispositivo que gera, fornece e protege chaves criptográficas. Especificamente nessa proposta, o HSM armazena cédula com votos de eleitores, sendo um padrão da indústria para uso com sistemas criptográficos [ATTRIDGE, 2002].

A proposta tem como base assinatura e criptografia sobre documentos XML suprida pelo HSM e *Smart Card* com algoritmos RSA/DSA de 1024 bits.

Na proposta, em todo intercâmbio de documentos, seja entre sistemas ou internamente, a infra-estrutura de votação é feita utilizando documentos no padrão XML com assinatura e criptografia, com base no padrão do W3C.

O sistema apresenta quatro elementos: a **autoridade de registro**, que tem a função de verificar se o eleitor está autorizado a votar; a **autoridade de eleição**, que está associada às pessoas que conduzem o processo eleitoral na sessão eleitoral; a **urna eletrônica**, que possui o HSM como peça fundamental na codificação, decodificação, contagem e recontagem dos dados; e o **cartão do cidadão** (*Smart Card*), que provê os recursos de identificação, autenticação e execução do voto, com o objetivo de assinar digitalmente os procedimentos efetuados pelo eleitor durante a fase de votação.

O sistema opera em duas fases distintas. A primeira fase consiste no registro eletrônico do eleitor, quando o mesmo recebe um *Identity-Link*, que é uma estrutura XML baseada em *Security Assertion Markup Language* (SAML) que o identificará de forma única pelo uso de assinatura digital.

O eleitor poderá se autenticar e se credenciar à votação através do recebimento de uma mensagem XML assinada pela entidade eleitoral, contendo o seu identificador de eleitor, sua zona eleitoral e uma cédula digital contendo os candidatos elegíveis para o pleito. O

identificador é único e temporário e será utilizado para identificar o eleitor durante o processo de votação. O anonimato é mantido, visto que o identificador foi gerado a partir do nome do eleitor e com funções criptográficas de sentido único (*hash*).

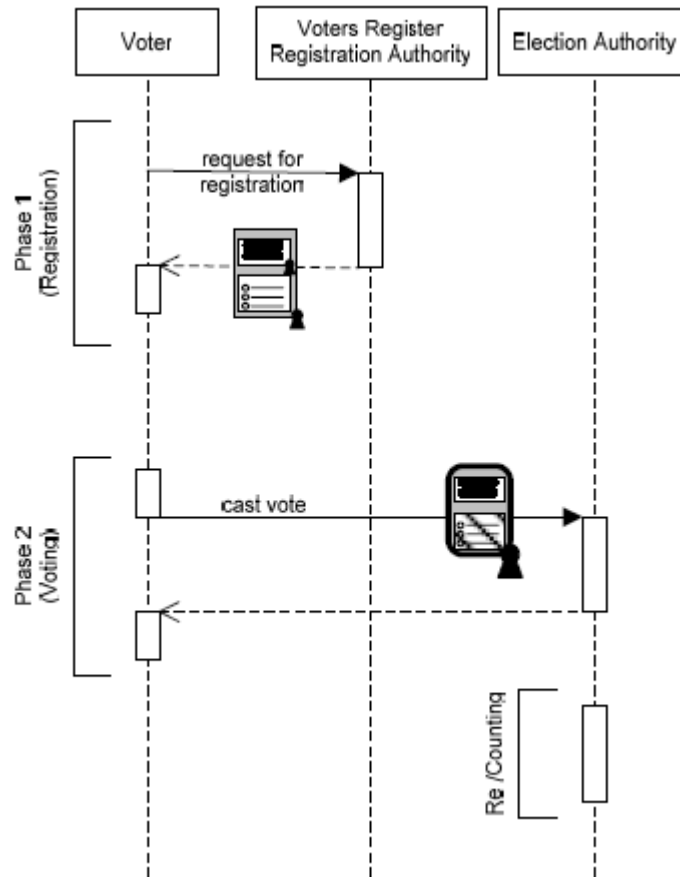


Figura 3.8: Diagrama de sequência das fases de registro e votação [ROSSLER, 2005].

O eleitor também recebe a chave pública (*Smart Card*) do HSM para que o voto do eleitor seja cifrado com a mesma, possibilitando que, na fase de apuração, o voto seja decifrado.

A segunda fase consiste no registro do voto pelo eleitor, utilizando a credencial presente no *Smart Card*. Neste tem-se a chave pública da urna e a cédula virtual fornecida na fase de registro/credenciamento, que figura a credencial propriamente. Proferido o voto, a cédula eletrônica é codificada e assinada, e o eleitor recebe uma confirmação eletrônica de que seu voto foi computado. A figura 3.8 apresenta um diagrama de sequência que permite visualizar de forma mais direta as fases de registro e votação e procedimentos de contagem/recontagem.

A cédula é composta de duas partes: a superior, que contém um identificador único e informações referentes ao pleito eleitoral, e a inferior, que contém a lista de candidatos.

A figura 3.9 demonstra a cédula sob um *template* XML com a visão anterior e posterior à votação. Antes da votação, quando a cédula já foi entregue ao eleitor, a mesma contém a assinatura da Autoridade Eleitoral em ambas as partes do documento e, depois da votação, os campos onde o eleitor proferiu seu voto é cifrado e assinado com a chave do HSM. Desta forma, garante-se a autenticidade e integridade do documento.

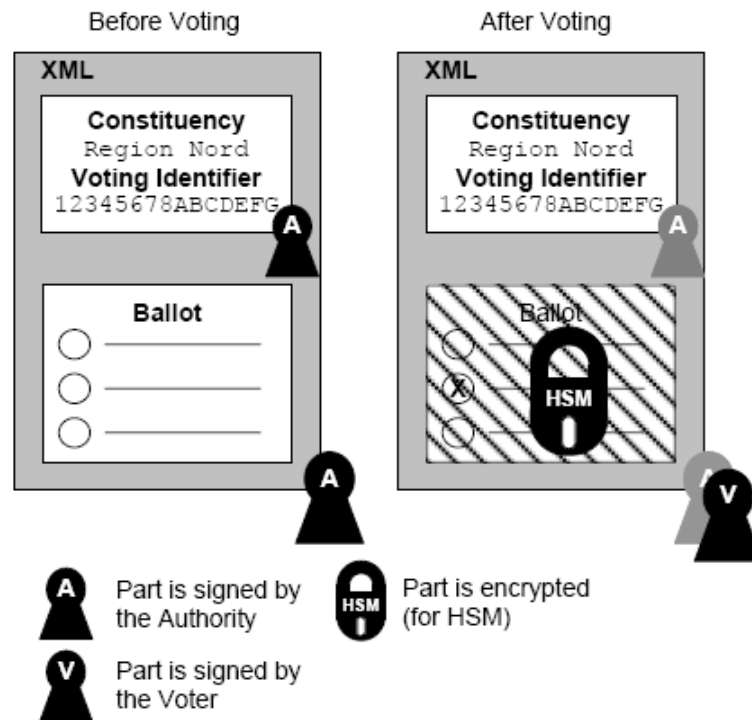


Figura 3.9: XML assinado e cifrado, antes e após a votação [ROSSLER, 2005].

Após a votação, o servidor de dados do sistema de eleição processa os votos, verificando as assinaturas dos eleitores. No fechamento do pleito, os votos são totalizados. No processo de totalização, a contagem é feita utilizando a chave privada presente no HSM e visa garantir que o voto somente será público nesse momento. Procedimentos de recontagem podem ser efetuados normalmente, visto que os votos criptografados encontram-se na urna e em meio persistente.

Deve-se observar que, na proposta, o identificador do voto não é criptografado, mas apenas assinado. Se a contagem puder ser pausada e conduzida passo a passo, pela sequência cronológica de votação pode-se chegar à autoria do voto.

A proposta não contempla a materialização do voto e não fornece contraprova do voto.

3.1.4. Sistema baseado em assinaturas às cegas

Em [KOFLE, 2003] é proposto um sistema de votação com a premissa de garantir o anonimato do eleitor utilizando uma arquitetura direcionada para a Internet. Basicamente, a proposta consiste em um protocolo de duas fases, registro e votação, no qual o anonimato é obtido através do esquema de assinaturas às cegas.

O problema relacionado ao anonimato do eleitor se situa entre os processos de registro e de votação. Isto significa que se não houver um dispositivo que desvincule a identificação do eleitor na fase em que o mesmo efetua o seu registro e a fase de votação, poderá haver violação do anonimato. Porém, para o eleitor votar, tem que existir algum tipo de habilitação emitida pela entidade que o autenticou e o credenciou a votar. Se não houver alguma forma de evitar que as duas entidades, a de registro e a de votação, identifiquem o eleitor, não é possível garantir a propriedade do anonimato. Para tal, esquemas de assinaturas às cegas têm sido úteis para esse tipo de necessidade, no qual o anonimato é necessário, como é o caso dos SEVs. Um exemplo de assinatura às cegas, exposto de forma didática, pode ser visto no Apêndice C.

A proposta apresenta um protocolo de duas fases, a de registro e a de votação. Abaixo, o esboço do protocolo na fase de registro:

- 1) O votante gera um *token* aleatório t , para que seja assinado cegamente pela entidade de registro. Monta uma mensagem contendo o *token* e uma solicitação de votação. O *token* t é assinado com a chave do votante e a mensagem cifrada, com a chave pública da entidade de registro, possuindo o formato $K_{pub}^R [S_{priv}^V (blinded(t), "I want to vote electronically")]$;
- 2) A entidade de registro, ao receber a mensagem, assina o *token* t às cegas com sua chave privada e cifra a mensagem com a chave pública do votante e encaminha ao mesmo a mensagem $K_{pub}^V [S_{priv}^R (\sigma_R(blinded(t)))]$;
- 3) De posse do primeiro *token*, o votante gera um segundo *token* (τ) e solicita que a entidade certificadora assine o mesmo às cegas. O *token* τ é assinado com a chave do votante e a mensagem cifrada com a chave pública da entidade de certificação e possui o formato $K_{pub}^T [S_{priv}^V (blinded(\tau))]$;
- 4) A entidade certificadora recebe a mensagem, assina o *token* τ às cegas, cifra a mensagem com a chave pública do votante e encaminha ao mesmo a mensagem $K_{pub}^V [S_{priv}^T (\sigma_T(blinded(\tau)))]$.

Concluído o processo, o votante possui dois *tokens* devidamente assinados às cegas pelas entidades do sistema de votação, fazendo com que as mesmas desconheçam o conteúdo do *token* e assim habilitem o votante à próxima fase, a de votação.

Os *tokens* são gravados no *Smart Card* como uma tupla no formato $(t, \sigma_R(t), \tau, \sigma_T(t), c)$.

Na realidade, a entidade de certificação também pode ser vista como um monitor de referência. A figura 3.10 representa os quatro passos apresentados acima.

Na fase de votação, o votante submete os *tokens* (sua habilitação ao voto) à entidade de votação (urna eletrônica) para obtenção da cédula e proferir seu voto. Antes, o votante gera um par de chaves simétricas (m, m') para cifrar/decifrar a cédula e monta uma mensagem contendo a tupla já citada, mais a chave m e a informação de localização da entidade de certificação (T) , conforme os passos abaixo:

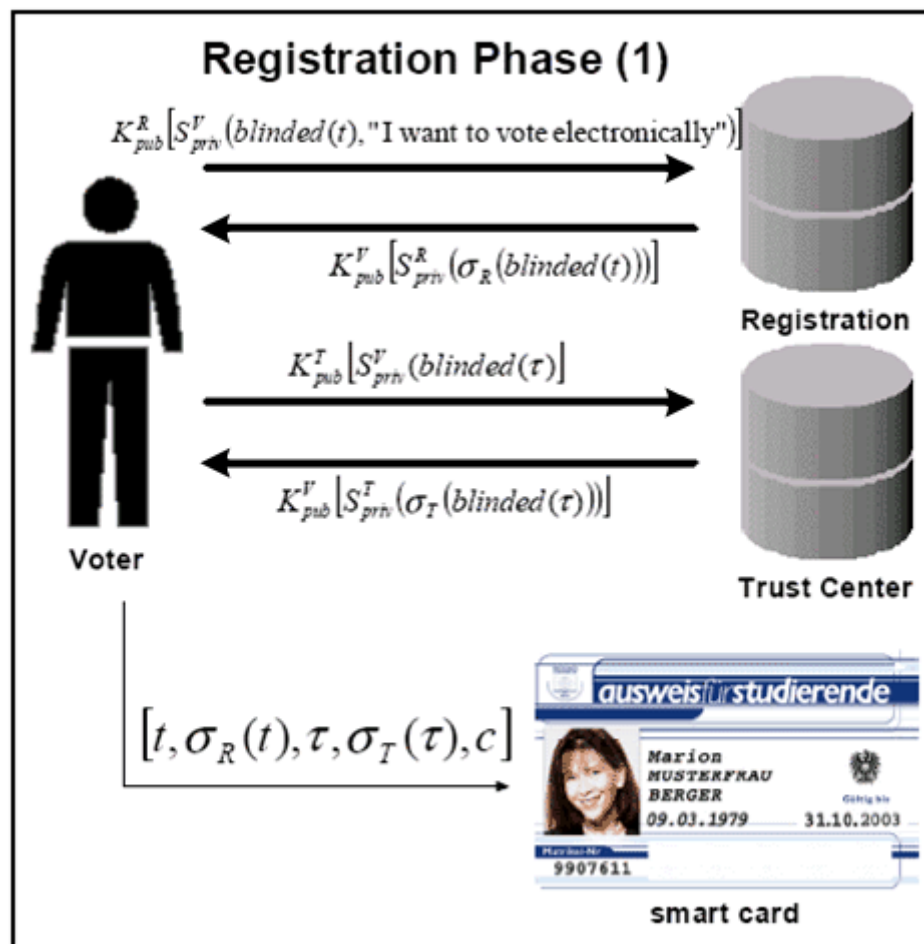


Figura 3.10: Mensagens da fase de registro [KOFLE, 2003].

- 1) O votante submete os *tokens* à entidade de votação através da mensagem

$$K_{pub}^B [c, T, m, t, \sigma_R(t), \tau, \sigma_T(t)];$$

- 2) A entidade de votação verifica as assinaturas de forma a verificar a autenticidade e encaminha a cédula (BS) assinada com sua chave privada e cifrada com a chave m : $m(S_{priv}^B(BS))$;
- 3) O Votante, ao receber a mensagem, decifra a mesma com a chave m' , preenche a cédula, cifra a mensagem com a chave pública da entidade e encaminha a mensagem $K_{pub}^B[c, T, m, t, \sigma_R(t), \tau, \sigma_T(\tau), BS]$.

Concluída a fase de votação, os votos estão prontos para serem totalizados. A figura 3.11 ilustra os passos da fase de votação.

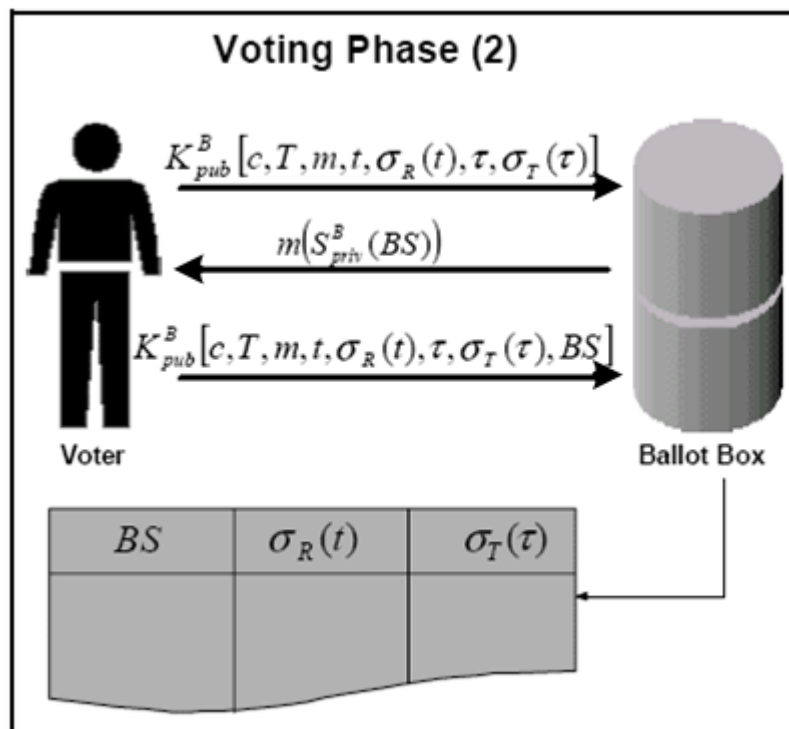


Figura 3.11: Mensagens da fase de votação [KOFLEER, 2003]

O modelo proposto possibilita, de fato, o anonimato, visto que ambas as entidades não têm como identificar o eleitor. Isso ocorre em decorrência das assinaturas às cegas sobre os *tokens* e da geração do par de chaves que não está associado à identificação do eleitor e que é utilizado para cifrar (chave privada m) e decifrar (chave pública m') a cédula. Como todas as mensagens são cifradas, assegura-se a propriedade de integridade. Há outras questões que devem ser analisadas quanto às demais propriedades aplicadas aos SEVs, mas não abordadas no modelo. Mas o objetivo da exposição desse protocolo é expor mais uma forma de utilização do anonimato com a utilização de assinaturas às cegas.

3.2. Relatórios técnicos

Em busca de solução para os problemas de segurança e falhas adversas apresentados em pleitos eleitorais, ou visando ao processo de prospecção, diversos estudos envolvendo especialistas, engenheiros e cientistas da comunidade acadêmica foram realizados mediante debates em workshops e outros eventos afins, cujos resultados produziram relatórios de significativo valor quanto à avaliação e melhoria de sistemas de votação.

O objetivo aqui não é apresentar o exposto nos relatórios, apenas apontar aspectos interessantes abordados nos mesmos.

3.2.1. Relatório Caltech/MIT

Em decorrência dos problemas ocorridos nas eleições presidenciais do ano de 2000 em diversos estados dos Estados Unidos da América (EUA), o *California Institute of Technology* (Caltech) e o *Massachusetts Institute of Technology* (MIT) juntaram-se de forma a discutir os problemas identificados e contribuir com soluções, visando evitar a ocorrência de problemas similares em eleições posteriores. Desse esforço conjunto surgiu o *Caltech-MIT Voting Technology Project* (<http://www.votingtechnologyproject.org>).

O projeto produziu o relatório [CALTECH-MIT, 2001], que apresentou diversas recomendações e propôs um *framework* para construção de futuras máquinas de votação (DREs) que sejam referência de uso em todo o país. Nos EUA não há uma unificação do sistema de votação, sendo que cada estado/município possui uma tecnologia de máquina de votar e/ou desenho de cédula diferente.

O relatório, entre as diversas recomendações pontuais, sugere a substituição das atuais e antigas máquinas de cartões perfurados e de alavanca em uso naquele país por outras devidamente aprovadas em testes de usabilidade e confiabilidade.

Como não há unificação do registro do eleitor em nível nacional, o relatório também sugere essa unificação. O projeto encontra-se ativo e, desde então, tem produzido outras contribuições na área.

3.2.2. Relatório CESC

Na Inglaterra, o voto é facultativo e, em decorrência do baixo quorum nos pleitos eleitorais, em 2002 o governo solicitou ao *National Technical Authority Information*

Assurance (CESG) o estudo [CROW, 2002] visando modernizar o processo eleitoral do país de forma a atrair o eleitor e evitar o grande número de ausências nos pleitos eleitorais.

O estudo teve como meta efetuar um levantamento de requisitos para o desenvolvimento de um SEV para eleições de porte nacional no qual fossem observados os seguintes requisitos:

- Infra-estrutura necessária;
- Receptividade do eleitor quanto ao novo sistema;
- Avaliação dos riscos de segurança e apresentação de contramedidas;
- Benefícios e vantagens agregadas na implantação de um SEV, em substituição ao sistema em uso;
- Implementação de projetos-piloto a partir de diversos dispositivos passíveis de serem utilizados, tais como telefones celulares (SMS/WAP/GRPS), PC/Quiosques (Internet/Linha discada), TV digital e o sistema tradicional de serviço postal (Correios).

O resultado do estudo foi um conjunto de premissas que visam garantir os requisitos e propriedades em um SEV com base nas tecnologias utilizadas. Mas o estudo revela que há consideráveis dificuldades na implantação de um SEV em nível nacional para uso em tempo real. Os fatores que inviabilizam a implantação do SEV estão relacionados aos seguintes aspectos:

- Os dispositivos de votação (DREs) que o eleitor utilizará para votar impõem diversos riscos à segurança;
- A infra-estrutura a ser utilizada seria de grande complexidade e de alto custo;
- O eleitor já possui uma cultura massificada sobre o atual sistema, gerando oposições à implantação do SEV;
- Há problemas para implantação de dispositivos para materialização do voto que são contemplados no sistema atualmente em uso.

3.2.3. Relatório Brennan

Em 2005, o Centro Brennan de Justiça, da Faculdade de Direito da Universidade de Nova Iorque, convocou renomados cientistas dos setores governamental, acadêmico e privado, especialistas em máquinas de votação (DREs) e profissionais de segurança computacional para que juntos formassem um força-tarefa para analisar as vulnerabilidades

nas três tecnologias de votação mais utilizadas em todo o mundo, especificamente nos EUA. Dessa força-tarefa resultou o “Relatório Brennan” [NORDEN, 2006], no qual diversos aspectos, do *hardware* ao *software* e infra-estrutura de comunicação relativa a ameaças e vulnerabilidades sobre tecnologias de votação do tipo DRE, DRE w/ VVPT e PCOS, foram avaliados, gerando, assim, diversas recomendações com vistas a minimizar os problemas que recaem sobre os SEVs.

Além das recomendações pontuais, o relatório mostra que todas as três tecnologias analisadas são vulneráveis a ataques e falhas, podendo ser violada a propriedade da integridade, e que, portanto, o resultado final de um pleito eleitoral está sujeito a fraudes. Considera, ainda, que se as autoridades envolvidas na administração do sistema e legisladores se orientarem pelas medidas de segurança recomendadas, os riscos de segurança mais sérios podem ser substancialmente reduzidos.

3.3. Conclusão

Foram apresentados, ao longo deste capítulo, diversos trabalhos desenvolvidos pela comunidade científica e por especialistas de várias áreas do conhecimento, os quais, a partir de estudos e debates, produziram modelos e recomendações visando resolver problemas ligados aos SEVs.

Capítulo 4

Um Sistema Seguro de Votação Eletrônica Multi-Cédula

Este capítulo apresenta a nossa proposta de um Sistema Eletrônico de Votação (SEV), com o objetivo de atender aos preceitos democráticos do voto, tendo como premissa os requisitos e as propriedades apresentadas no capítulo 2, resultando em um sistema confiável e robusto.

O sistema baseado em três cédulas proposto por [RIVEST, 2007] apresenta requisitos e propriedades interessantes que podem ser associadas a um SEV. O objetivo da nossa proposta é melhorar sua usabilidade, além de automatizá-lo para que se torne viável em sistemas reais.

As demais propriedades desejáveis aos SEV foram obtidas com o uso de tecnologias que incluem infra-estrutura de chaves públicas, tecnologia de documentos XML, EML (*Election Markup Language*), *Hash table*, base de dados XML nativa e tecnologia de serviços *web* (*Web Services*).

4.1. Motivação

As arquiteturas de SEVs têm tido dificuldades para garantir, de maneira incontestável, o anonimato do voto durante o processo de votação. Geralmente, é preciso confiar que uma determinada máquina não associe ilegalmente a identificação do votante a credenciais que o mesmo recebe para votar.

Os SEVs não têm provido de maneira satisfatória mecanismos que forneçam indícios ao eleitor de que seu voto foi efetivamente computado no processo de apuração, sem

possibilitar ao mesmo provar a terceiros em quem votou, objetivando inibir a prática de comércio do voto e coação do eleitor.

Os SEVs estão com dificuldades para prover mecanismos confiáveis de auditoria que produzam informações fidedignas de todo o procedimento operacional que ocorre nas urnas eletrônicas, servidores de rede, *software* e demais equipamentos de *hardware* do sistema, contudo tais trilhas de auditoria não podem infringir o anonimato do eleitor, a confidencialidade e integridade do voto.

A identificação do eleitor não tem sido abordada de modo a garantir de maneira irrefutável a autenticidade de um votante.

As soluções criptográficas adotadas para os SEVs têm mostrado questionável proteção ao anonimato do voto.

A materialização do voto não tem sido adotada na maioria dos SEV, dificultando qualquer processo de auditoria ou recontagem manual dos votos.

A usabilidade das urnas eletrônicas, com relação à facilidade de preenchimento da cédula e interface de operação, não tem mostrado recursos para atender às necessidades de idosos, deficientes auditivos e visuais e de eleitores com baixo nível de discernimento.

Observadores independentes que fiscalizam o processo eleitoral têm tido dificuldades para acompanhar a votação em alguns SEVs, por não terem mecanismos acessíveis para desempenhar a sua função.

Vários trabalhos foram propostos para dar segurança aos SEVs, porém nenhum é abrangente o suficiente para ser considerado em arquiteturas de SEV. Em geral, as propostas abordam uma pequena parte do problema.

Não há padronização suficiente para possibilitar o desenvolvimento de um sistema de *software* multi-versões para SEVs.

Há vários estudos e relatórios questionando a segurança de SEVs, mas há poucas soluções aceitáveis para o problema.

4.2. Objetivos

O objetivo deste trabalho é apresentar um modelo funcional, passível de implementação e que solucione os problemas relacionados à motivação deste trabalho, sem, contudo, agregar ao modelo altos níveis de complexidade. Mais especificamente, pretende-se:

- Garantir a propriedade do anonimato sem empregar a técnica de assinatura às cegas;

- Prover contraprova ou recibo do voto, baseado no esquema de três cédulas proposto por [RIVEST, 2007];
- Produzir rastros/trilhas de auditoria confiáveis, em nível de operação do sistema de votação, sem infringir o anonimato do eleitor, a confidencialidade e integridade do voto;
- Prover o sistema de um mecanismo de identificação do votante que minimize as possibilidades de personificação do eleitor;
- Prover um mecanismo de materialização do voto que não interfira diretamente no tempo de votação do eleitor;
- Automatizar o sistema de três cédulas para aumentar sua usabilidade e aplicação em sistemas reais;
- Prover confiabilidade ao *software* de votação.
- Prototipar a proposta para avaliar o modelo, visando o atendimento dos requisitos e propriedades inerentes aos SEVs;

Outro objetivo do trabalho é possibilitar o desenvolvimento/implementação da arquitetura proposta a partir de tecnologias de sistemas abertos e interoperáveis e com interfaces/serviços padronizados.

4.3. Arquitetura Proposta

A proposta consiste em definir uma arquitetura de SEV que implemente o esquema de três cédulas apresentado em [RIVEST, 2007]. Este esquema foi originalmente concebido como um sistema de votação baseado em papel, e implementá-lo em um ambiente computacional distribuído é uma tarefa complexa. Porém, o SEV foi desenvolvido com base no esquema de três cédulas para operar em uma estrutura distribuída, respeitando as exigências de segurança de tal sistema e melhorando sua usabilidade.

A arquitetura do SEV visa dividir as responsabilidades entre as entidades da mesma no sentido de diminuir a importância de cada uma delas. Ou seja, objetiva-se propor uma arquitetura onde, intrinsecamente, as entidades devem desempenhar suas funções sem que seja possível a obtenção não autorizada de informações sensíveis do SEV. É objetivo, também, minimizar os pontos únicos de falhas, vulnerabilidades ou de comprometimento do sistema.

A arquitetura do sistema de votação proposto é composta pelas seguintes entidades: Agente de Registro (AR), Console de Registro (CR), Gerente de Votação (GV), Console de Votação (CV), Urna Eletrônica (UE), Dispositivo de Contraprova (DC), Boletim de Resultados (BBS) e Infra-estrutura de Chaves Públicas (ICP). A arquitetura ainda possui o Votante (Vo), a Autoridade Eleitoral (AE) e os Representantes Eleitorais (REs), que são atores humanos e determinam ações de eleitor, do administrador do sistema e de fiscalização, respectivamente.

As entidades acima apresentadas se relacionam em três fases distintas: a Fase de Registro e Habilitação, a Fase de Votação e a Fase de Apuração. Cada fase e as entidades envolvidas serão descritas com detalhes nas seções que se seguem.

A arquitetura possui uma concepção modular que garante escalabilidade e robustez, visando seu uso a eleições de grande escala.

4.3.1. Visão Geral da Arquitetura proposta

A figura 4.1 mostra uma visão geral da arquitetura e os relacionamentos entre as entidades envolvidas, conforme esboço a seguir:

- **Fase de Registro e Habilitação:** o Vo efetua sua identificação e se autentica biometricamente através do CR (evento 1). Após a autenticação do Vo, o CR solicita ao AR uma credencial (evento 2) e a fornece ao Vo, armazenando-a em um cartão inteligente. O AR solicita (evento 3) ao GV três novos IDs para recompor seu repositório de IDs. Os IDs são utilizados para compor a credencial (três IDs por credencial) e um número aleatório desse é gerado na inicialização do sistema através do evento I;
- **Fase de Votação:** o Vo apresenta sua credencial ao CV (evento 4) e se autentica biometricamente; Validada a credencial, o Console solicita ao GV a(s) cédula(s) de votação (evento 5). Preenchida a cédula, a mesma é submetida ao GV que a deposita na UE através do evento 6. Armazenadas as cédulas, o CV habilita o DC a efetuar a impressão ou gravar a contraprova no cartão inteligente do Vo. Além disto, também é habilitada a materialização do voto, conferida pelo eleitor em Urna Física (evento 7). O *template* das cédulas é gerado na inicialização do sistema através do evento II;

- **Fase de Apuração e Divulgação dos Resultados:** concluída a votação, a apuração dos votos é iniciada pela Autoridade/Representantes Eleitorais através do uso de suas chaves privadas através do evento III que atua sobre a Unidade de Contagem da UE. O evento anterior gera o evento 8, que é o envio do resultados da UE para o BBS, os quais estarão disponíveis para consulta na *World Wide Web*.

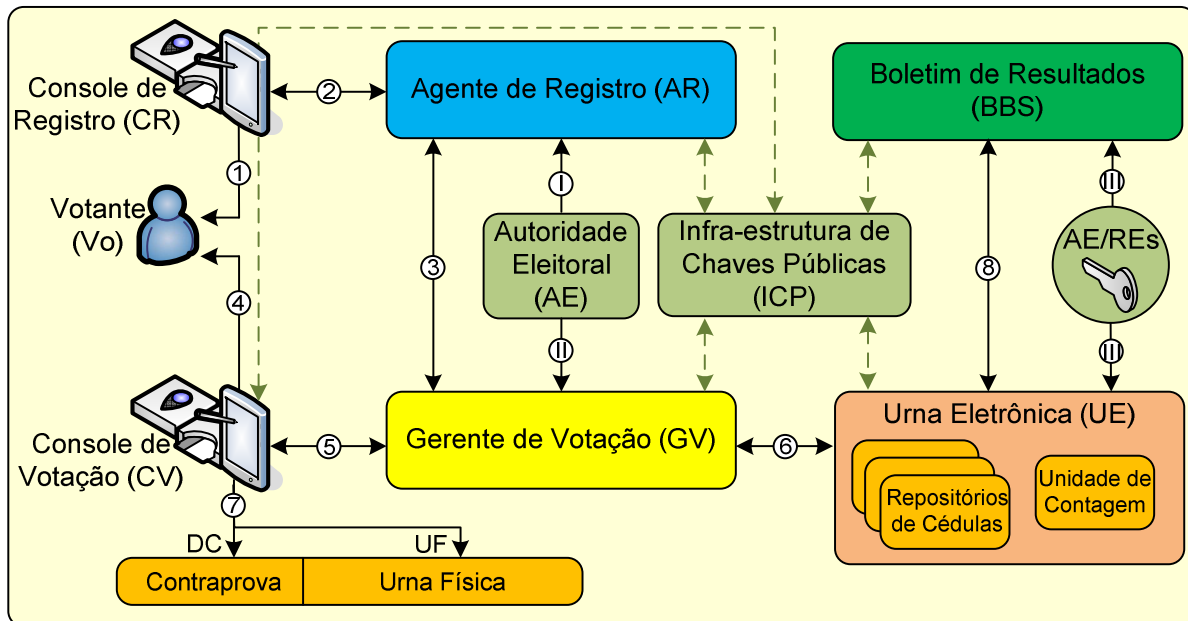


Figura 4.1: Diagrama da arquitetura proposta [COSTA, 2008].

A Infra-estrutura de Chaves Públicas em todos os procedimentos é responsável pela verificação das chaves envolvidas nas transações.

As seções seguintes apresentam, de maneira mais detalhada, as mensagens (primitivas de comunicação) envolvidas em cada fase do processo de votação e as respectivas entidades envolvidas.

4.3.2. Fase de Registro e Habilitação

A Fase de Registro e Habilitação tem por responsabilidade efetuar o registro e a habilitação do eleitor ao exercício do seu direito ao voto numa dada eleição. Em analogia ao sistema de votação eleitoral brasileiro, nessa fase o eleitor se dirige ao mesário em uma seção eleitoral.

As entidades envolvidas nessa fase compreendem o CR, o AR, a Infra-estrutura de Chaves Públicas (ICP), Repositório de Eleitores e *Ballot IDs* (REB) e o Repositório de *BallotID* (RBI) representados na figura 4.2.

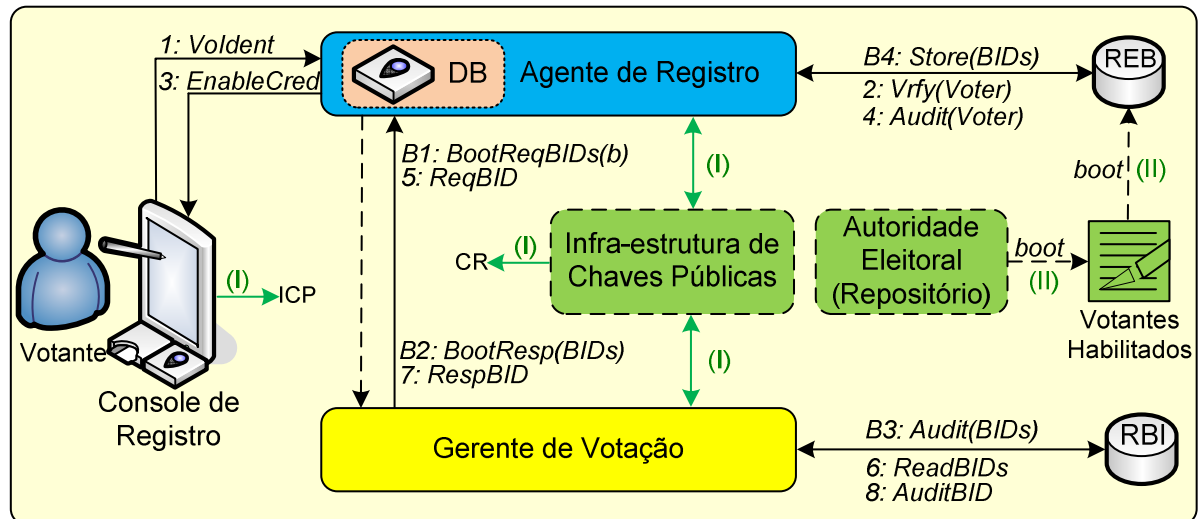


Figura 4.2: Diagrama de interação entre os módulos da Fase de Registro e Habilitação.

O CR é a entidade responsável por recepcionar eletronicamente o eleitor no ponto de votação (zona eleitoral, por exemplo), sendo a interface homem-máquina para interação com o eleitor e com o sistema no processo de registro e habilitação. Além dos dispositivos de entrada/saída de dados convencional, o CR possui um dispositivo de leitura biométrica para impressões digitais e um dispositivo de leitura/gravação de cartão inteligente (*Java Card*).

A AR é a entidade que efetua o controle do registro e habilitação do eleitor, fornecendo ao mesmo uma credencial para uso na fase de votação. O papel do GV nesta fase é fornecer os *Ballot IDs* (conjunto de três identificadores numéricos distintos e únicos num mesmo pleito eleitoral) ao AR para a composição da credencial.

A ICP tem como função validar as chaves/assinaturas criptográficas utilizadas nas mensagens entre as entidades envolvidas.

Os repositórios REB e RBI possuem dados dos eleitores/*Ballot IDs* e das cédulas/*Ballot IDs*, respectivamente.

Considera-se que, numa fase de pré-eleição, o eleitor se habilitou a participar do pleito perante a AE. A habilitação consiste em cadastrar sua identificação, senha e/ou dados biométricos na AE. Se, por questões adversas, o eleitor não pôde ter sua situação regulamentada, no banco de dados não constará esse registro e o mesmo estará impedido de votar. O uso da autenticação biométrica quando do registro/habilitação ao voto, garante a autenticidade do eleitor, evitando assim, a personificação do eleitor, por exemplo.

Considerando a figura 4.2, ainda no período de pré-eleição, o sistema de votação deve passar por um processo de *boot* onde o AR solicita ao GV *b Ballot IDs* (BIDs) através das

mensagens B1 e B2 e os armazena no repositório REB através da mensagem B4. O GV audita os BIDs enviados ao AR em seu repositório local RBI através da mensagem B3. Essa informação de auditoria será utilizada posteriormente na fase de votação, como um dos itens de validação da credencial do votante. Os BIDs armazenados no REB constituirão um *pool* de credenciais a serem fornecidas aos votantes. O AR, ao usar os BIDs para montar uma credencial, sempre os usará aleatoriamente, evitando assim que o GV associe uma ordem cronológica e/ou seqüencial das credenciais recebidas na fase de votação à ordem que o mesmo forneceu os BIDS ao AR. Para que a ordenação em seqüência não possa ser estabelecida, entende-se que no mínimo quinze BIDs devam ser solicitados pelo AR, por caracterizarem uma quantidade que garante a aleatoriedade no fornecimento de cinco credenciais – sempre disponíveis no repositório. Porém, b é sempre definido pela AE.

Também como operação de *boot* no período de pré-eleição, a AE deve popular o repositório de eleitores REB com a base de eleitores habilitados a votar, incluindo os seus dados de autenticação (*hash* da senha ou *template* biométrico da impressão digital).

Iniciada a eleição ou fase de registro, o Vo se identifica junto à CR utilizando algum tipo de identificação (título eleitoral, por exemplo) e a CR encaminha o mesmo ao AR por meio da mensagem *VoIdent* (evento 1, figura 4.2). O AR consulta, no repositório REB, se o Votante está habilitado a votar, através da mensagem *Vrfy(Voter)* (evento 2). Se habilitado, o Vo passa pelo processo de autenticação, e o AR obtém, do *pool* de BIDs armazenados no REB, três IDs aleatórios e constrói a credencial de votação, adicionando os dados de autenticação do Vo, e a encaminha ao Vo através da mensagem *EnableCred* (evento 3) – esses dados serão gravados em um cartão inteligente do Vo. Através da mensagem *Audit(Voter)* do evento 4, o AR registra que o eleitor, com a identificação processada, já recebeu uma credencial.

Como o *pool* de BIDs ficou reduzido em $b-3$, para manter o mesmo número de b BIDs, o AR solicita ao GV três BID, usando a mensagem *ReqBID* (evento 5). O GV obtém três novos BIDs em RBI (mensagem *ReadBID*, evento 6) e os retorna para o AR através da mensagem *RespBID* (evento 7). A auditoria do BID entregue ao AR ocorre na mensagem *AuditBID* (evento 8).

Para agregar segurança aos procedimentos desta fase, os itens abaixo relacionados são contemplados:

- Todas as mensagens entre os módulos são assinadas digitalmente e, em alguns casos cifradas (exposto abaixo), e a autenticidade das chaves é verificada na ICP através do evento (I);
- Todos os *Ballot IDs* entregues pelo GV ao AR são cifrados individualmente com a chave pública do CV, evitando que o AR os conheça;
- O dado de autenticação do Vo gravado na credencial é cifrado com a chave pública do CV e a credencial assinada por AR.

Concluída a Fase de Registro e Habilitação, pode-se observar que os mecanismos e esquema utilizados atenderam aos seguintes requisitos/propriedades de um SEV:

- **Habilitação/Autenticidade do eleitor:** o evento (1), associado ao evento (2), confere a habilitação do Votante, visto que a base de dados utilizada pelo AR e a base de registro de eleitores habilitados a votar e é devidamente populada (inicializada) pela AE. A autenticidade do Vo é verificada biometricamente através de sua impressão digital (aconselhável para evitar a personificação do eleitor) que afere ser ele próprio, de fato;
- **Unicidade:** quando o AR atualiza seu repositório de eleitores (REB) no passo (4), indicando que um dado eleitor já obteve uma credencial, está sendo garantido que este mesmo eleitor não terá mais permissão de obter uma segunda credencial para votar, visto já tê-la obtido;
- **Anonimato/Conluio:** quando o GV cifra os BIDs e o AR cifra a senha (*hash*) ou *template* biométrico do eleitor, ambos com a chave pública do CV, fica assegurado que somente o CV poderá decifrar a credencial. Assim, em momento algum do processo, quaisquer das entidades terão como associar o BID de uma cédula com os que foram fornecidos ao Votante por AR. Isso evita o conluio entre AR e GV e contribui para o anonimato; quando GV forneceu os BIDs ao AR, ele não poderá associar cronologicamente o eleitor que está votando no CV, visto que os BIDs são inseridos na credencial aleatoriamente e desvinculando qualquer forma de violação do anonimato;
- **Autenticidade, confidencialidade e integridade:** nesta fase, a confidencialidade é obtida quando as entidades cifram o conteúdo das mensagens com a chave pública do destinatário. Quando GV cifra os BIDs com a chave pública do CV, o AR não tem como conhecer quais foram os BIDs fornecidos. Quando o AR cifra o dado do eleitor

com a chave pública do CV e assina a credencial com sua chave privada, impossibilita que o eleitor possa falsificar a credencial e garante a autenticidade, confidencialidade e integridade.

4.3.3. Fase de Votação

A Fase de Votação é a fase responsável por prover ao eleitor as cédulas de votação para o exercício do voto no pleito eleitoral em curso, depositar o voto na urna eletrônica, fornecer o recibo de contraprova ao eleitor e materializar seu voto em uma urna física. O requisito necessário para o início dos procedimentos de votação é que o eleitor forneça ao sistema uma credencial válida, obtida na Fase de Registro e Habilitação.

Os módulos envolvidos nessa fase são o Console de Votação (CV), o Gerente de Votação (GV), a Urna Eletrônica (UE), a Infra-estrutura de Chaves Públicas (ICP) e o Repositório de Cédulas/*Ballot IDs* (RBI), este último vinculado ao GV, conforme representados na figura 4.3.

O CV é a entidade responsável por recepcionar eletronicamente o eleitor no ponto de votação (zona eleitoral, por exemplo), sendo a interface homem-máquina para a interação eleitor e sistema no processo de votação. Além dos dispositivos de entrada/saída de dados convencional, o CV possui um dispositivo de leitura biométrica para impressões digitais, um dispositivo de leitura/gravação de cartão inteligente (*Java Card*) e os dispositivos para impressão da contraprova e materialização do voto. Porém, o CV não possui nenhum meio de armazenamento persistente, no qual possa armazenar informações referentes a voto, votante ou ambos.

O GV provê o CV, a(s) cédula(s) de votação e o controle da votação, que incluem o estado (*status*) de uso de uma credencial e o depósito da(s) cédula(s) na UE. O GV utiliza seu repositório RBI para armazenar um *template* da(s) cédula(s) de votação do pleito em curso, controle e geração dos *Ballot IDs* e procedimentos de rastreamento e auditoria.

A UE tem como função receber os votos enviados pelo GV e armazená-los adequadamente nos repositórios de cédulas.

A ICP tem como função validar as chaves/assinaturas criptográficas utilizadas nas mensagens entre as entidades envolvidas.

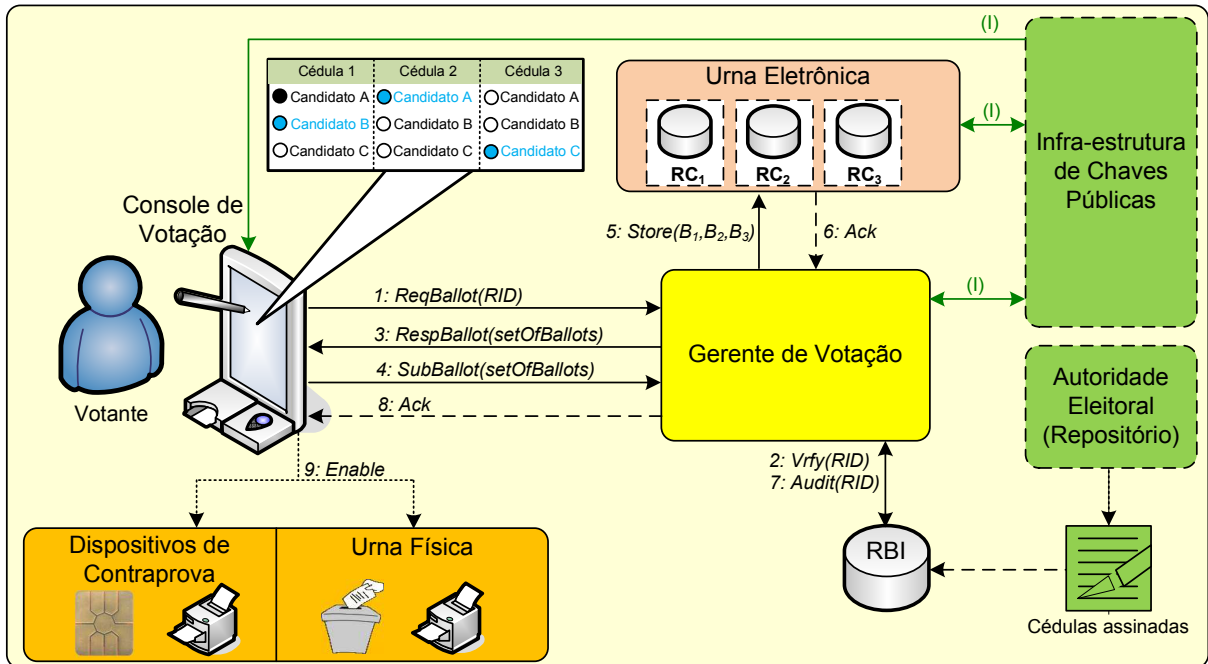


Figura 4.3: Diagrama interativo entre os módulos da Fase de Votação.

Tendo como referência a figura 4.3, funcionalmente, os procedimentos desta fase se iniciam quando o eleitor interage com o CV, fornecendo sua credencial através do cartão inteligente. O CV efetua a leitura da credencial, decifra a informação de autenticação (*hash* da senha ou *template* biométrico) e a utiliza para autenticar o eleitor.

Após a autenticação do eleitor, o CV recupera da credencial o primeiro ID (denominado de *Receipt ID*/RID) do conjunto de três e envia para o GV via mensagem *ReqBallot* (RID) (evento 1, figura 4.3). O GV, através da mensagem *Vrfy*(RID) (evento 2), verifica se o ID é válido, isto é, se o ID foi emitido por GV e o estado de votação do mesmo. O estado de votação do RID e a ação a ser tomada por GV dentro do pleito eleitoral podem ser os seguintes:

- O RID ainda não votou em nenhum cargo. O GV envia a cédula de votação do primeiro cargo eletivo;
- O RID já iniciou o processo de votação, mas ainda não votou em nenhum cargo ou não concluiu todos os cargos. O GV envia a cédula de votação correspondente ao ponto em que o Vo paralisou os procedimentos de votação. O estado de marcação da cédula não é recuperado, devendo o Vo remarcar o seu voto;
- O RID já votou em todos os cargos e GV notifica o CV que o Vo não tem direito a voto naquele pleito em curso.

As cédulas são enviadas ao CV através da mensagem *RespBallots(setOfBallots)*, possibilitando ao Vo proferir o seu voto (evento 3, figura 4.3). Como as cédulas são baseadas na proposta de [RIVEST, 2007], para agregar usabilidade no preenchimento das cédulas, o CV, a partir do *template* dos candidatos, gera aleatoriamente uma marca em cada cédula por candidato, conforme pode ser visualizado na cédula exemplo da figura 4.3. No caso, os candidatos marcados com tons mais claros foram pré-marcados, sendo necessário que o Vo faça apenas uma marca no candidato em que deseja votar. Neste exemplo, as marcas feitas por GV foram os “Candidatos” A, B e C, respectivamente nas cédulas 2, 1 e 3. Para escolher o candidato a ser votado, o Vo marcou o “Candidato A” na cédula 1 (marca mais escura).

Após o Vo terminar a escolha dos candidatos, o CV insere em cada cédula os IDs e permite que o Vo escolha uma das cédulas como contraprova do voto. Após a escolha, o CV submete o voto ao GV através da mensagem *SubBallots(setOfBallots)*, evento 4.

O GV, ao receber as cédulas, as envia à UE para serem armazenadas, através da mensagem *Store (B₁, B₂, B₃)*, evento 5 da figura 4.3. Cada cédula será armazenada em um repositório: RC₁, RC₂ e RC₃. Havendo sucesso no armazenamento, a UE retorna ao GV a mensagem *Ack* (evento 6) e GV audita em seu repositório RBI a informação de que os BIDs da transação em curso já votaram, através da mensagem *Audit (RID)*, evento 7 da figura 4.3.

Armazenados os votos e a transação auditada, o GV informa ao CV o sucesso da transação com a mensagem *Ack* (evento 8). Ao receber o *Ack*, o CV aciona os procedimentos para o armazenamento/impressão da contraprova do voto e da materialização do voto através da mensagem *Enable* (evento 9). A materialização do voto pode ser feita de várias formas. Uma alternativa é o CV gerar um resumo das cédulas, contendo apenas o voto com o nome do candidato escolhido pelo eleitor, por exemplo, e conferido pelo mesmo antes de a cédula ser automaticamente depositada na Urna Física. Evidentemente, nenhum tipo de identificação será admitido na cédula. Havendo mais cargos a serem votados, os procedimentos são cíclicos e recomeçam a partir do evento 3.

Para agregar segurança nos procedimentos desta fase, os itens abaixo relacionados são contemplados:

- Todas as mensagens entre os módulos são assinadas digitalmente e em alguns casos cifradas (exposto abaixo), e a autenticidade das chaves é verificada pela ICP através do evento (I);

- A credencial apresentada pelo Vo ao CV não possui nenhum tipo de identificação que o associe à mesma. A informação de autenticação não é armazenada no CV e nem no GV. O CV somente obtém essa informação através do cartão inteligente para autenticar o eleitor em tempo real. As informações pessoais do votante devem estar criptografadas ou protegidas por senha – só o votante deve ter acesso a essas informações;
- Antes de o CV enviar a(s) cédula(s) ao GV para armazenamento, cada cédula é cifrada com a chave pública da AE e de dois Representantes Eleitorais, de forma que somente esses três atores poderão iniciar o processo de apuração ao término da votação.

Concluída a Fase de Votação, pode-se observar que os mecanismos e esquemas propostos atenderam aos seguintes requisitos/propriedades de um SEV:

- a) **Autenticidade:** a credencial que o Vo apresenta ao CV foi assinada pelo AR. Antes de abrir a credencial, o CV verifica essa assinatura, aferindo, assim, a autenticidade da credencial. Para o Vo, a autenticidade é verificada no processo de autenticação biométrica, devendo, então, não serem utilizadas senhas, evitando a personificação do eleitor;
- b) **Unicidade:** quando GV verifica a validade da credencial, o requisito da unicidade é assegurado, pois se os BIDs já foram utilizados e a votação está com estado finalizado, é porque o Vo já votou em todos os cargos. Se o pleito eleitoral constitui-se de mais de um candidato e o Vo, por alguma falha, não conseguiu votar em todos os candidatos, o GV verifica e permitirá que continue a votar a partir do ponto em que houve a interrupção. Assim, é assegurado que o Vo somente votará uma única vez dentro do pleito eleitoral em curso;
- c) **Contraprova e comercialização do voto:** após a finalização da votação com sucesso, o Votante deve ter escolhido para cada cargo uma das cédulas para levar como contraprova do voto, conforme [RIVEST, 2007]; e o GV, no evento 9, habilitou em DC a impressão ou a gravação da imagem da cédula escolhida no cartão inteligente. Essa contraprova não fere a propriedade de **Não-coação e Comercialização do Voto**, visto não ser possível revelar a terceiros a qualidade do voto proferido pelo eleitor com a parte que o Vo detém. Ainda, para o próprio Vo, a contraprova é apenas um documento que traz indícios de que o voto foi contabilizado na apuração e que está correto. A contraprova é divulgada publicamente ao término da apuração;

- d) **Materialização do voto:** Dentro do mesmo posicionamento do item anterior, o GV, no evento 9 da figura 4.3, habilita a impressão do voto do Vo. O voto impresso e conferido pelo Vo é depositado automaticamente na UF. A materialização do voto garante a recontagem, caso haja contestação do resultado eletrônico, e pode ser desenhado para ser lido utilizando em *scanners* ópticos.
- e) **Anonimato do eleitor:** a propriedade do anonimato também é garantida, visto que o GV, ao receber o RID, não tem como associar a identidade real do Vo para quem o AR forneceu esses RIDs. Ainda, a credencial recebida por CV não traz nenhuma informação que identifique diretamente o Vo; por exemplo, o número identificador (constante do título eleitoral) que foi utilizado na fase de registro/habilitação;
- f) **Autenticidade, confidencialidade e integridade:** nesta fase, quando cada cédula é cifrada com a chave pública da AE e dos REs e assinada pelo GV, o voto passa a ser secreto em todo o processo em curso, garantido, assim, a autenticidade, confidencialidade e integridade das mensagens e do voto proferido pelo Vo.

4.3.4. Fase de Apuração

A Fase de Apuração é a responsável pela apuração dos resultados (contagem dos votos) e divulgação dos resultados em um serviço de boletim eletrônico.

Os módulos envolvidos nesta fase são a UE, o BBS, a AE e os REs.

A UE é a entidade responsável por armazenar as cédulas enviadas pelo GV. A UE tem, em sua estrutura, três repositórios: um para cada cédula e o sub-módulo Unidade de Contagem (UC), que permite que os votos presentes em cada cédula sejam totalizados e enviados ao módulo BBS, para publicação. A UC possui uma interface homem-máquina que provê a interação entre o sistema e a AE/REs, para os procedimentos de apuração. Além dos dispositivos de entrada/saída de dados convencional, a UC possui um dispositivo de leitura biométrica para impressões digitais e um dispositivo de leitura/gravação de cartão inteligente (*Java Card*).

A UE é protegida por um *trigger*, que mistura os votos a cada inserção, e a UC por uma *constraint*, que só habilita a contagem ao término da eleição e com a inserção de três chaves privadas, da AE e dos REs.

O BBS é a entidade responsável por receber da UE os votos já totalizados por candidato e disponibilizá-los ao público. Uma vez iniciado o processo de totalização pela UE,

os dados são automaticamente enviados à base de dados do BBS, que publica os resultados em uma página da *World Wide Web*. Da mesma forma que a UE, a publicação só é habilitada ao término do pleito e através de ações da AE.

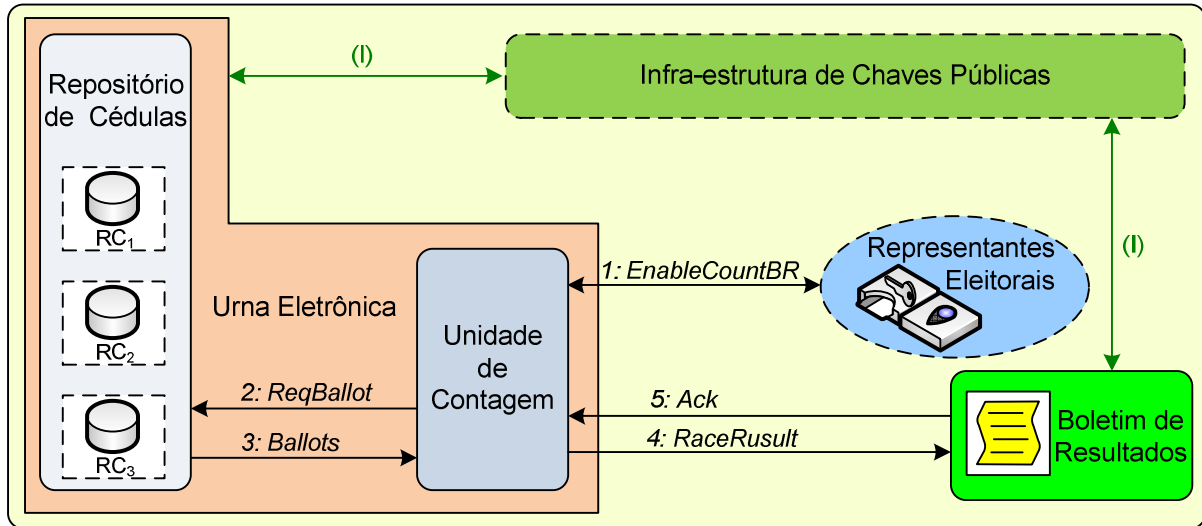


Figura 4.4: Diagrama interativo entre os módulos da Fase de Apuração.

A ICP tem como função validar as chaves criptográficas utilizadas nas mensagens entre as entidades envolvidas.

Tendo como referência a figura 4.4, o procedimento de apuração se inicia quando os atores humanos AR e REs se autenticam biometricamente através do dispositivo de leitura de digital e inserem seus cartões inteligentes no respectivo leitor. O cartão de cada ator possui a chave privada, que é par da chave pública na qual as cédulas foram cifradas pelo GV na fase de votação. A inserção desses dados gera a mensagem *EnableCountBR* (evento 1), que efetivamente inicia o processo de contagem pela UC.

A UC, ao receber o evento 1 (figura 4.4.), recupera dos repositórios (RC₁ a RC₃) todas as cédulas, contabilizando todos os votos associados aos cargos do pleito eleitoral. Para tal, a UC envia ao Repositório de Cédulas a mensagem *ReqBallot* (evento 2) e obtém desse a sequência ordenada das cédulas, via mensagem *Ballots* (evento 3).

A UC totaliza internamente os votos por cargo e envia o resultado ao BBS, através da mensagem *RaceResult* (evento 4); e o BBS, ao receber o resultado, responde com a mensagem *Ack* (evento 5). Esse procedimento ocorre para todos os cargos do pleito eleitoral, os quais estarão disponíveis para consulta pública através da *World Wide Web* (Internet).

Para agregar segurança nos procedimentos da dessa fase, os itens abaixo relacionados são providos:

- Todas as mensagens entre os módulos são assinadas digitalmente e em alguns casos cifradas (exposto abaixo) e a autenticidade das chaves são verificadas pela ICP, através do evento (I);
- As cédulas só podem ser decifradas quando ocorrer o término da eleição e com o uso de três chaves privadas distintas.

4.3.5. Infra-estrutura de Chaves Públicas

A Infra-estrutura de Chaves Públicas (ICP) é a entidade de certificação digital baseada na arquitetura de chaves públicas (criptografia assimétrica) e permite que os diversos módulos envolvidos verifiquem a autenticidade das assinaturas digitais e chaves utilizadas no sistema para o processo de cifragem/decifragem.

4.4. Conclusão

Este capítulo apresentou uma proposta de arquitetura para um Sistema Eletrônico de Votação Multi-Cédulas que atende aos diversos requisitos intrínsecos a esse tipo de sistema, tais como anonimato do eleitor, autenticidade das transações envolvidas, integridade do voto, mecanismos contra coação e/ou comércio do voto, contraprova e materialização do voto.

Em decorrência do crescente avanço da área governamental (*E-Gov*) quanto à pretensão de utilizar assinaturas digitais para aferir a autenticidade no fluxo de documentos entre governo e cidadão, optou-se pelo uso do cartão inteligente (*Smart Card*, mais especificamente *Java Card*) como mecanismo para aferir a autenticidade do eleitor de forma eletrônica e visual. Assim, o cartão inteligente deve conter a chave privada dos atores humanos (eleitor, AE e REs), seus dados de autenticação biométrica e uma foto estampada no próprio cartão, possibilitando provar, de forma mais fidedigna, sua identidade e evitando a personificação do eleitor.

A arquitetura apresentada foi concebida de forma modular e, espera-se, com a robustez necessária para o seu uso em eleições de larga escala ou através da Internet. Para o uso na Internet, o problema da coação/comércio do voto ainda é uma barreira.

Capítulo 5

Aspectos de Implementação

Para o desenvolvimento do protótipo, este capítulo aborda o protocolo de comunicação entre as entidades com base na proposta apresentada no Capítulo 4. Apresenta um esboço da infra-estrutura de serviços utilizado, aspectos de implementação do protótipo, resultados de testes com o protótipo e os módulos conforme foram implementado usando a linguagem Java.

A implementação visa aferir as funcionalidades da arquitetura proposta, cujo resultado é a produção de um protótipo. O protótipo foi desenvolvido utilizando a linguagem Java, podendo ser executado em computadores com Windows ou Unix, conferindo sua portabilidade.

A comunicação protocolar, processos de autenticação e autorização entre o eleitor/sistema e entre os diversos módulos serão providos pelo modelo definido como Serviços Web (*Web Services*) e normatizados pelas entidades W3C (*World Wide Web Consortium*) e OASIS (*Organization for Structured Information Standards*). Para maiores detalhes sobre Serviços Web, consultar Apêndice A.

5.1. Protocolo Proposto

O protocolo define as mensagens de comunicação entre os atores humanos (Votante e Representante Eleitoral) e as demais entidades, sendo base para a implementação do protótipo da arquitetura proposta no Capítulo 4. A comunicação entre as entidades da arquitetura é cifrada e assinada, utilizando criptografia de chaves públicas cuja convenção é a descrita a seguir:

- $\{m\}_A^{priv}$: representa a mensagem “m” cifrada com a chave privada de “A”;
- $\{m\}_A^{pub}$: representa a mensagem “m” cifrada com a chave pública de “A”;
- $[m]_A$: representa a mensagem “m” assinada com a chave privada de A.

Como exemplo, considere a expressão $Auth_Vrfy[\{(voterID, AuthData)\}_A^{pub}]_B$, que representa a mensagem *Auth_Vrfy*, cujo conteúdo *(voterID, AuthData)* foi cifrado com a chave pública de “A” e assinado com a chave privada de “B”. Nesse caso, “B” é a origem da mensagem e “A”, o destino final. Nesse exemplo, são contempladas a confidencialidade do conteúdo da mensagem, mediante a cifragem, e a autenticidade/integridade, pela assinatura.

Acompanhando o esboço da arquitetura proposta, o protocolo que se segue é descrito conforme as fases envolvidas.

5.1.1. Fase de Registro e Habilitação

O Console de Registro (CR) e o Agente de Registro (AR) são as entidades responsáveis pela Fase de Registro/Identificação. Nessa fase, há um procedimento de inicialização (*boot*) que ocorre antes de iniciar a eleição, consistindo na inicialização da base de dados local (Repositório de Eleitores) do AR com informações geradas pela Autoridade Eleitoral. No repositório de eleitores há registros dos votantes habilitados a votar e dados de autenticação. O AR mantém também o repositório de *Ballot IDs*, que é inicializado por

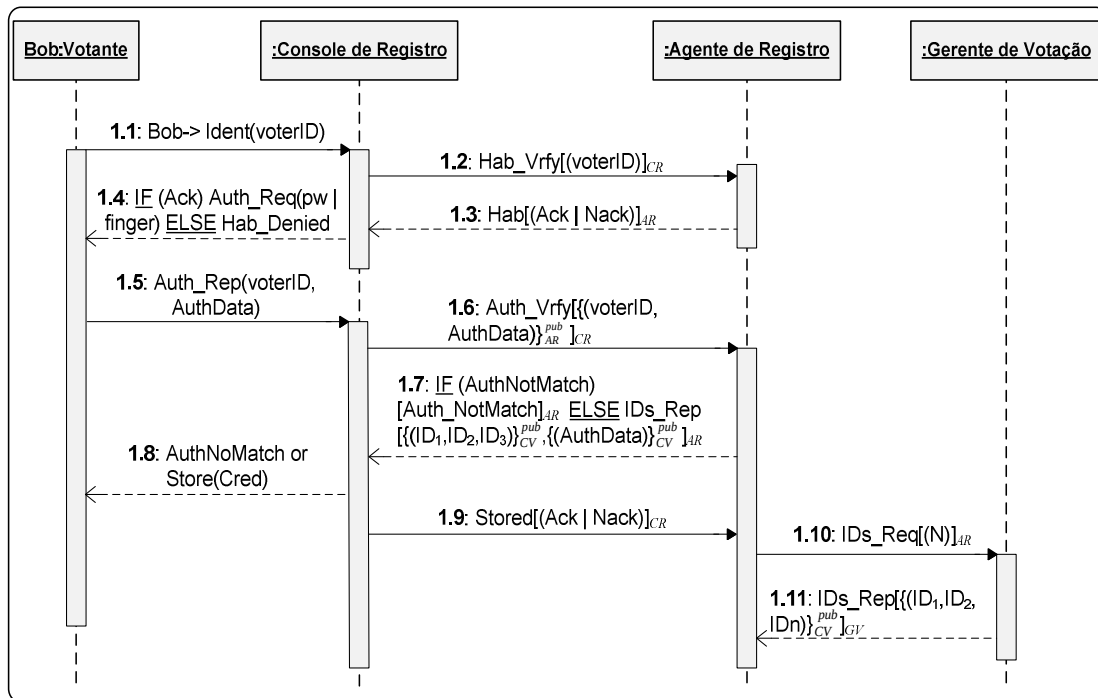


Figura 5.1: Troca de mensagens na Fase de Registro/Habilitação.

solicitações ao Gerente de Votação (GV) com N *Ballot IDs* (que permite emitir $N/3$ credenciais de votação). Os eventos 1.10 e 1.11 mostram como o número N de *Ballot IDs* é mantido constante no repositório; N é definido pela Autoridade Eleitoral. Quando o AR gera uma credencial, ele escolhe aleatoriamente três *Ballot ID* para compor a credencial. Com isso, evita-se que o Gerente de Votação associe IDs ao votante a partir da sequência cronológica de fornecimento dos mesmos.

As principais mensagens protocolares envolvidas nesta fase são mostradas no diagrama da figura 5.1 e, na Tabela 5.1, a descrição.

Tabela 5.1: Descrição das mensagens protocolares na Fase de Registro

Evento	Descritivo
1.1	O Votante Bob se identifica junto ao CR usando a mensagem <i>Ident(voterID)</i> , onde <i>voterID</i> é um identificador numérico (número do título eleitoral, por exemplo);
1.2	O CR, ao receber a identificação do Votante, verifica se o mesmo está habilitado a votar, enviando ao AR a mensagem <i>Hab_Vrfy</i> ;
1.3	O AR, ao receber a solicitação de verificação de habilitação, consulta seu Repositório de Eleitores. Estando o <i>voterID</i> com status OK é retornada ao CR a mensagem <i>Hab(Ack)</i> , indicando que o Votante está habilitado a votar e ainda não obteve nenhuma credencial anteriormente. Em caso contrário, é retornada a mensagem <i>Hab(Nack)</i> , indicando que o Votante não está habilitado a votar ou já obteve uma credencial anteriormente;
1.4	Se a resposta ao passo anterior for um <i>Nack</i> , o RC envia a mensagem <i>Hab_Denied</i> ao Votante, informando que o mesmo não está apto a votar. Em caso contrário, envia a mensagem <i>Auth_Req(pw)</i> ou <i>Auth_Req(finger)</i> solicitando ao Votante que se autentique para obtenção da credencial, utilizando senha (<i>pw</i>) ou impressão digital (<i>finger</i>);
1.5	Após o Votante ter entrado com a senha ou a informação biométrica, é enviada ao CR a mensagem <i>Auth_Resp(voterID, AuthData)</i> como resposta à solicitação de autenticação, sendo o <i>voterID</i> a identificação do Votante e <i>AuthData</i> o dado de autenticação (senha ou <i>template</i> ¹ biométrico capturado por um <i>Fingerscan</i> ²);

¹ O **template** é a representação matemática dos dados biométricos da impressão digital.

² O **Fingerscan** é um dispositivo que captura a impressão digital do votante, que, quando processada, gera o *template* biométrico.

Evento	Descritivo
1.6	O RC, ao receber o dado de autenticação do Votante, envia ao AR a mensagem <i>Auth_Vrfy</i> , solicitando a verificação de autenticidade da mensagem. No Repositório de Votantes, os dados de autenticação armazenados são apenas o <i>hash</i> da senha do votante e o <i>template</i> biométrico cifrado;
1.7	Se no evento 1.6 a verificação de autenticação for negativa, o AR responde ao CR com a mensagem <i>Auth_NotMatch</i> . Havendo sucesso no processo de autenticação, o AR monta a Credencial contendo os dados de autenticação do Votante (<i>template</i> ou <i>hash</i> da senha) e três IDs escolhidos aleatoriamente. Os dados são cifrados com a chave pública do Console de Votação, assinado pelo AR e encaminhado para o CR através da mensagem <i>IDs_Resp</i> ;
1.8	Se no passo anterior o votante não se autenticou com sucesso, a mensagem <i>Auth_NotMatch</i> é encaminhada ao Votante, caso contrário o mesmo receberá a Credencial de votação. O armazenamento da Credencial em meio persistente (<i>Java Card</i> ³) é feito através da mensagem <i>Store</i> ;
1.9	Havendo sucesso no armazenamento da Credencial em meio persistente, o CR envia ao AR a mensagem <i>Stored(Ack)</i> , ou <i>Stored(Nack)</i> se houver falha. No caso de recebimento de <i>Ack</i> , o AR registra no Repositório de Eleitores que o <i>voterID</i> já recebeu uma credencial;
1.10	Ao receber o <i>Ack</i> do passo anterior, o AR solicita ao Gerente de Votação três IDs para manter o número <i>N</i> de <i>Ballot IDs</i> em seu repositório, usando a mensagem <i>IDs_Req(1)</i> , onde “1” corresponde a um <i>Ballot ID</i> , ou seja, três IDs;
1.11	O GV recupera do seu Repositório de <i>Ballot IDs</i> três IDs, cifra-os com a chave pública do Console de Votação e envia ao AR através da mensagem <i>IDs_Resp</i> .

5.1.2. Fase de Votação

A fase de votação contempla um procedimento de inicialização (*boot*) que consiste no armazenamento do “*template* das cédulas”, o qual vem assinado do repositório de candidatos elegíveis da Autoridade Eleitoral. Além disso, no *boot* é mostrada uma tela ao operador do CV antes da abertura da votação em um ponto de votação (*polling station*), solicitando que o mesmo faça a escolha do *software* que será executado naquele CV.

³ **Java Card** é um cartão inteligente (Smart Card) com processador e memória. Possui internamente a JVM (Java Virtual Machine) para a execução de aplicativos do usuário (Applets).

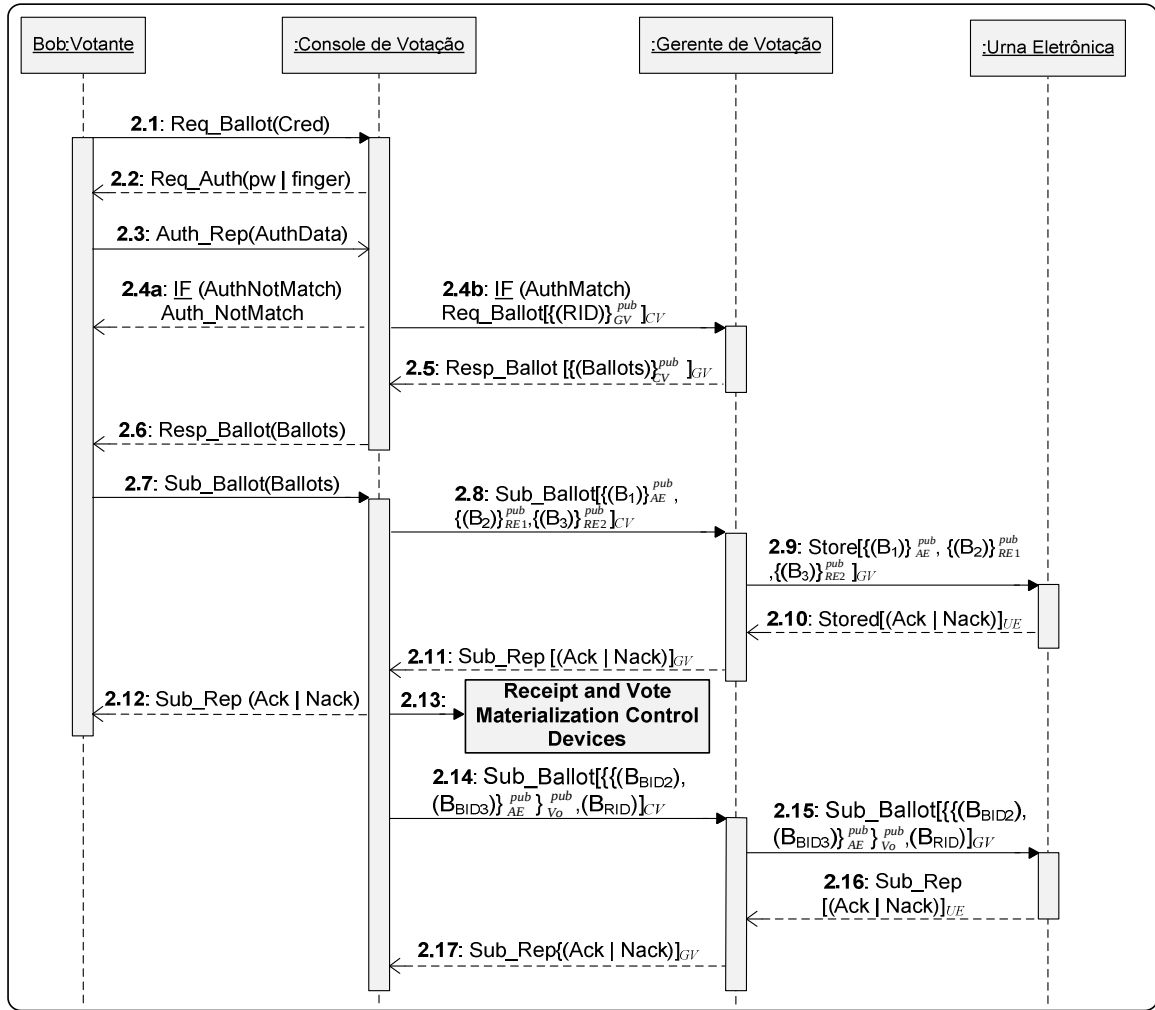


Figura 5.2: Troca de mensagens na Fase de Votação.

Após a escolha, o operador receberá um número que deverá anotar no relatório do ponto de votação. O CV enviará para o Gerente de Votação a escolha do operador e o número mostrado no CV para ser gravado em *log*. Ao término da eleição, será verificado se o número (*hash* do programa que realizou a eleição) mostrado no CV corresponde à escolha feita pelo operador. Esse procedimento visa à utilização da técnica de multiversão, homologada pela autoridade eleitoral sem o conhecimento prévio de ninguém. Após a eleição, confronta-se o número mostrado no CV com o *hash* do programa que realizou a eleição no CV. Se ambos forem iguais, o programa utilizado estava íntegro.

A Fase de Votação é a mais importante do processo e envolve diretamente três entidades, o Console de Votação (CV), que é a interface com o votante, o Gerente de Votação (GV), que coordena os procedimentos da fase de votação e a Urna Eletrônica (UE), que provê o repositório de cédulas. As principais mensagens protocolares envolvidas nesta fase são mostradas no diagrama da figura 5.2 e, na Tabela 5.2, a descrição de cada uma.

Tabela 5.2. Descrição das mensagens protocolares na Fase de Votação

Evento	Descrição
2.1	O Votante Bob apresenta a Credencial obtida na fase de registro/habilitação ao CV, requisitando as cédulas de votação, utilizando a mensagem Req_Ballot ;
2.2	O CV decifra a Credencial do Votante, obtém os dados de autenticação e os <i>Ballot IDs</i> e solicita ao Votante que se autentique enviando a mensagem Req_Auth(pw) , para autenticação via senha, ou Req_Auth(finger) para autenticação via biometria. É importante notar que o uso de biométrica praticamente inviabiliza a falsificação de documentos que permitem a personificação de votantes, portanto é a recomendação para a autenticação;
2.3	O Votante responde à solicitação de autenticação com a mensagem Auth_Resp(Auth_Data) , sendo que <i>Auth_Data</i> contém o <i>hash</i> da senha digitada ou o <i>template</i> biométrico, gerado pelo <i>Fingerscan</i> ;
2.4a/2.4b	Ao receber a informação de autenticação, o CV confere o <i>hash</i> ou o <i>template</i> constante em <i>Auth_Data</i> , com a informação de autenticação obtida através da Credencial no passo 2.2. Se as informações de autenticação forem diferentes o CV informa o Votante via mensagem Auth_NoMatch (2.4 ^a). Caso contrário, o CV solicita ao GV as cédulas de votação enviando a mensagem Req_Ballot(RID) (2.4b), sendo que RID (<i>Receipt ID</i>) é o ID ₁ da Credencial (evento 1.7 da figura 3). O RID constará na cédula que o Votante escolher como contraprova. Adicionalmente, o RID será registrado em <i>log</i> do GV para fins de auditoria. O único meio de saber se um votante concluiu a fase de votação é através do RID. O RID denota que um votante autenticado está em algum estágio do processo de votação, mas não o identifica;
2.5	Em atendimento ao evento 2.4b, o GV verifica em seu repositório de RIDs se o mesmo é válido e se já não foi utilizado em um processo de votação anterior. Caso negativo, envia as três cédulas pré-preenchidas ao CV através da mensagem Resp_Ballot . De acordo com o esquema de três cédulas proposto em [RIVEST, 2007], cada candidato deve ter uma marca em uma das três cédulas, para facilitar o preenchimento para o Votante.

Evento	Descrição
2.5	Antes de enviar as cédulas ao CV, o GV escolhe aleatoriamente uma das três cédulas e marca uma única vez cada candidato. Assim, o Votante terá que efetuar somente uma marca (em uma cédula não marcada) no candidato que deseja votar. Com o pré-preenchimento das cédulas, o Votante pode observar visualmente os locais onde poderá efetuar sua marca, e evita erros de preenchimento. Além disso, o pré-preenchimento melhora significativamente a usabilidade do sistema de votação baseado em três cédulas;
2.6	O CV, ao receber as cédulas do GV, as encaminha ao Votante para o devido preenchimento através da mensagem Resp_Ballot ;
2.7	O Votante preenche as cédulas de votação, escolhe uma das três como contraprova e as submete ao CV através da mensagem Sub_Ballot ;
2.8	O CV, ao detectar a opção do Votante, insere o <i>Receipt ID</i> na cédula escolhida como contraprova e atribui aleatoriamente os outros dois <i>Ballot IDs</i> às demais cédulas. Em seguida, é feita a cifragem aleatória de cada cédula em uma das três chaves públicas distintas, sendo uma da Autoridade Eleitoral (AE) e duas dos Representantes Eleitorais (REs). As cédulas cifradas são encaminhadas ao VM através da mensagem Sub_Ballot . O Console de Votação também mantém consigo uma cópia das três cédulas; a contraprova será posteriormente enviada ao Dispositivo de Contraprova (DC) tão logo se tenha o resultado positivo do GV que as cédulas foram armazenadas na UE. A cópia das outras duas cédulas será explicada no evento 2.14;
2.9	O VM, ao receber as cédulas do CV, as assina e as deposita na UE através da mensagem Store ;
2.10	A urna (UE), ao receber o pedido para o armazenamento, o faz gerando o <i>hash</i> do voto como índice para evitar qualquer tipo de violação do anonimato do voto por seqüencialização de armazenamento. Se o <i>Store</i> for com sucesso, é retornado para GV um <i>Ack</i> ; caso contrário, é retornado um <i>Nack</i> ;
2.11	O Gerente de Votação encaminha o retorno da operação de armazenamento na UE ao CV. Quando o GV recebe um <i>Ack</i> da eu, registra essa informação em seu repositório de <i>Ballot IDs</i> , para fins de auditoria e para relatar que esses IDs já foram utilizados em uma votação concluída com sucesso.

Evento	Descrição
2.11	Caso contrário, quando a votação ficou incompleta, a Credencial contendo esses IDs pode ser utilizada para que o votante reinicie a fase de votação do ponto em que o processo foi interrompido;
2.12	Se o CV receber Sub_Resp(Ack) , informa ao Votante que o processo de votação foi encerrado com sucesso. Caso contrário, recebe um Sub_Resp(Nack) e é solicitado que a votação seja reiniciada;
2.13	Havendo sucesso no processo de votação, o CV armazena a contraprova no <i>Java Card</i> do Votante. Alternativamente, um resumo do voto é impresso como materialização do voto e depositado (<i>cast</i>) na Urna Física (UF) automaticamente depois de conferido pelo votante. O resumo do voto consiste em uma listagem contendo apenas os candidatos votados sem nenhum tipo de identificação. Evidentemente, no resumo do voto podem ser produzidas marcas ou códigos que facilitem a leitura em dispositivo óptico (<i>scanner</i> , por exemplo) para acelerar um possível processo de recontagem manual, se necessário;
2.14/ 2.15	Como impressoras e <i>Smart Cards</i> estão sujeitos a falhas, o CV, no evento 2.8, faz uma cópia das cédulas, que servirão como backup do voto, caso a impressora ou <i>Java Card</i> não funcione no momento da impressão do voto ou armazenamento da contraprova, ou mesmo para o caso do <i>Java Card</i> ser perdido. As cópias das cédulas que não têm como <i>Ballot ID</i> são cifradas na chave pública da AE e o resultado da cifragem é cifrado novamente na chave pública do votante. As duas cédulas duplamente cifradas, junto com a contraprova, serão então enviadas a um repositório da AE na UE, através do CV, por meio da mensagem Sub_Ballot e reenviado por GV (evento 2.15). Com a dupla cifragem, o voto só pode ser aberto com as chaves privadas do Votante e da AE. Caso seja necessário, ambos podem definir um local adequado para que o votante tenha acesso ao voto armazenado pela AE;
2.16/ 2.17	Em resposta aos eventos 2.14 e 2.15, a UE responde (evento 2.16) com <i>Ack</i> , se houve sucesso no armazenamento, ou <i>Nack</i> , em caso de falha. O GV recebe o evento 2.16 e encaminha ao CV através do evento 2.17.

5.1.3. Fase de Apuração

A Fase de Apuração compreende os procedimentos de contagem dos votos armazenados na Urna Eletrônica (UE) e a divulgação do resultado no Boletim de Resultados (BBS).

A UE é a entidade responsável por armazenar as cédulas enviadas pelo GV e processar a apuração. A UE se divide em dois módulos: O Repositório de Cédulas e a Unidade de Apuração (UA). A Unidade de Apuração (UA) tem como propósito gerenciar a totalização dos votos e enviá-los ao módulo do BBS, para publicação.

Como cada cédula foi cifrada com a chave pública de um Representante Eleitoral (RE), para que o UA proceda com a apuração é necessário que sejam inseridas as chaves privadas dos REs. As chaves dos REs só são válidas para uma única eleição. A apuração somente é habilitada após o término da eleição pela Autoridade Eleitoral (AE). Para assegurar a democracia e transparência do processo eleitoral são indicados como RE, por exemplo, a própria Autoridade Eleitoral (TSE/TRE, no caso do Brasil), mais um representante da sociedade civil e um representante dos partidos políticos, os quais, ao fornecerem suas chaves privadas ao módulo de apuração, concordam em dar início ao processo de apuração. Esse procedimento também evita apuração parcial.

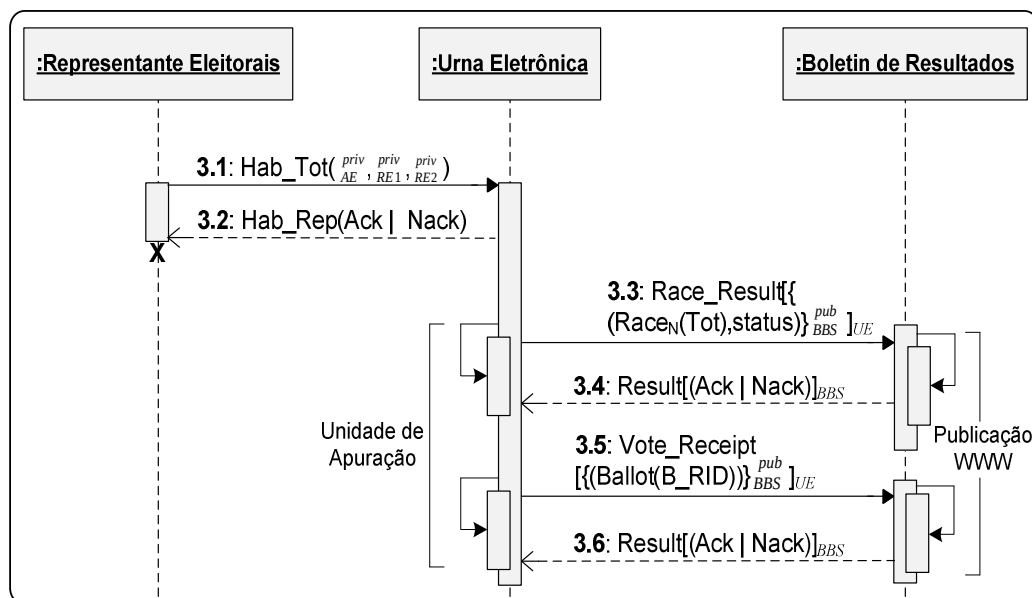


Figura 5.3. Troca de mensagens na Fase de Apuração.

O Boletim de Resultados (BBS) é a entidade responsável por receber da Unidade de Apuração a listagem de candidatos com os votos totalizados individualmente. Uma vez iniciado o processo de apuração, as listagens vão sendo automaticamente enviadas à base de dados do

BBS e os resultados publicados em uma página no formato da *Wide World Web*. Da mesma forma que a apuração só começa ao fim da eleição, a publicação só acontece com o início da apuração.

As principais mensagens protocolares envolvidas nesta fase são mostradas no diagrama da figura 5.3 e, na Tabela 5.3, a descrição das mesmas.

Tabela 5.3. Descritivo das mensagens protocolares na Fase de Apuração

Evento	Descrição
3.1	Dando início ao processo de apuração dos votos, os REs, incluindo uma AE, fornecem para a UA as três chaves privadas – as cédulas no processo de votação foram cifradas com as chaves públicas desses atores no Console de Votação. A UA pode assim decifrar as cédulas, para contagem e geração da totalização dos resultados, usando a mensagem <i>Hab_Tot</i> ;
3.2	A UA, ao receber a primitiva solicitando o início do processo de apuração, responde ao REs com a mensagem <i>Hab_Resp(Ack)</i> , se o início de contagem foi reconhecido, ou <i>Hab_Resp(Nack)</i> , caso contrário. O reconhecimento do início do procedimento depende de alguns fatores, como, por exemplo, se a eleição já foi finalizada;
3.3	Estando habilitado o início da apuração, a UA efetua seu processamento interno e envia ao BBS os resultados já totalizados por cargo eletivo, por meio da mensagem <i>Race_Result</i> , assinada pela UE. Essa mensagem possui a informação dos candidatos por cargo eletivo e seus respectivos votos totalizados;
3.4	Se o BBS recebeu a mensagem anterior com sucesso, responde com a mensagem <i>Result(Ack)</i> ; caso contrário, responde com <i>Result(Nack)</i> . Os eventos 3.3 e 3.4 se repetem até que os resultados sejam concluídos;
3.5	Finalizando a fase de apuração, são enviados pela UA ao BBS as cédulas que foram escolhidas pelos votantes como contraprova do voto, através da mensagem <i>Result_Vote_Receipt</i> ;
3.6	O BBS responde com a mensagem <i>Result(Ack)</i> , aferindo o sucesso no recebimento da mensagem, ou com <i>Result(Nack)</i> , se não houver sucesso.

5.2. Infra-estrutura de Serviços

Visando ao uso do sistema sobre infra-estrutura de redes privadas ou da Internet, e possibilitando interoperação e escalabilidade, um *framework* para Serviços Web será utilizado como apoio na implementação do sistema. O *framework* consiste em prover as interfaces homem-máquina para a interação dos eleitores e administradores com o sistema, prover a comunicação e registro dos serviços fornecidos pelos módulos e os mecanismos de autenticação e autorização a seguir descritos com maior nível de detalhes.

5.2.1. Interfaces homem-máquina

A interação do eleitor e a autoridade eleitoral com as entidades/módulos do sistema é feita utilizando uma aplicação cliente/servidor baseado em navegadores Internet e servidores Web, conforme diagrama da figura 5.4.

Nesse contexto, cada módulo do sistema terá o seu servidor *web* que atenderá a requisições utilizando um canal de comunicação seguro (cifrado) fim-a-fim com base nos protocolos HTTPS/SSL. Todos os módulos disponibilizarão interfaces de administração e configuração através de Web Services. Os módulos em questão são: Agente de Registro, Gerente de Votação, Urna Eletrônica e Boletim de Resultados.

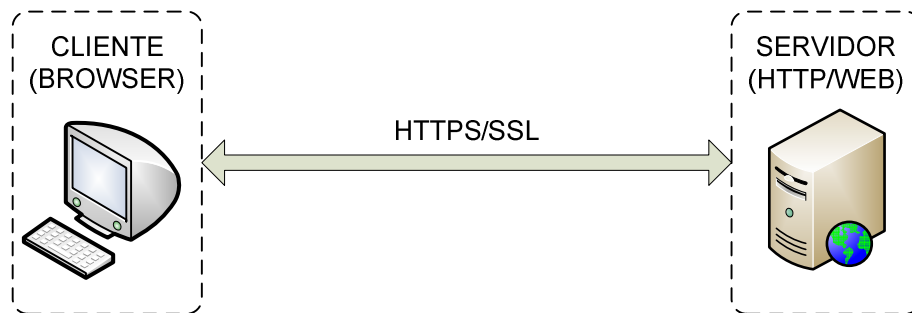


Figura 5.4: Interface com o eleitor/administrador (cliente/servidor)

5.2.2. Comunicação e registro entre entidades/módulos

As primitivas do protocolo de comunicação (Apêndice F) entre os diversos módulos que compõem o sistema são encapsuladas em documentos XML e transportadas por SOAP sobre HTTP. O objetivo é garantir a interoperabilidade oferecida por *Web Services* (WS). Além disto, os WS disponibilizam mecanismos que facilitam o processo da troca de mensagens e do registro dos serviços. Abaixo, uma descrição de cada mecanismo:

- **Protocolo SOAP (*Simple Object Access Protocol*)** [HENDRICKS, 2002]: o SOAP será o protocolo padrão a ser utilizado entre os módulos para a troca de mensagens XML e utilizará o HTTP como meio de transporte. A autenticidade e integridade serão apoiadas pelos padrões de documentos *XML-Signature* e *XML-Encryption*, respectivamente;
- **Linguagem WSDL (*Web Service Description Language*)** [HENDRICKS, 2002]: o WSDL será a linguagem que descreverá a semântica dos serviços e interfaces oferecidos por cada módulo do sistema, de forma que em um sistema distribuído e num processo de “*discovery*”, qualquer módulo possa facilmente determinar os serviços e suas propriedades;
- **UDDI (*Universal Description, Discovery and Integration*)** [HENDRICKS, 2002]: o UDDI, dentro do sistema, terá como função permitir que qualquer principal identifique a URL (*Uniform Resource Locate*) na qual se encontra a WSDL de cada módulo do sistema. A utilização da UDDI mantém o sistema dinâmico e prove interoperabilidade.

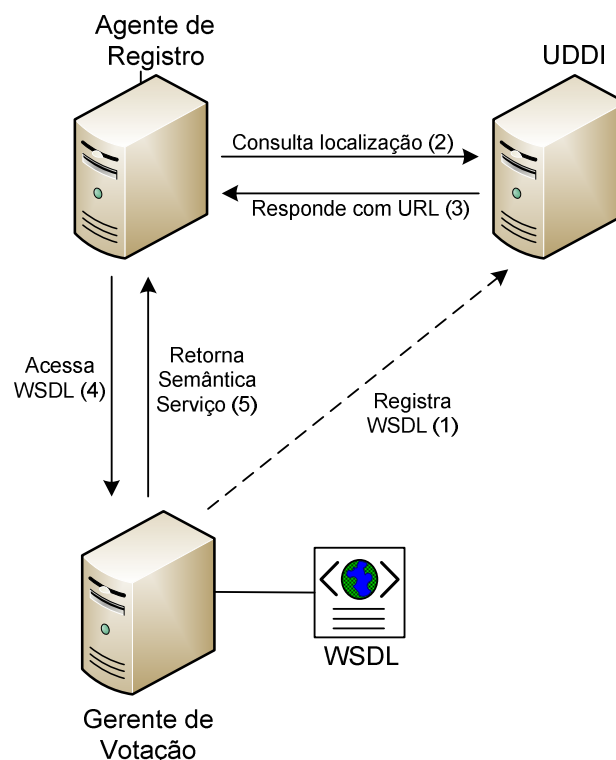


Figura 5.5: Processo de registro e recuperação de informações WSDL

Para exemplificar, a figura 5.5 ilustra o processo de registro e requisição de um documento WSDL, devendo ser considerado que toda a comunicação ocorre através do protocolo SOAP sobre HTTP. Abaixo, a descrição de cada passo conforme enumeração:

- 1) O módulo Gerente de Votação, como todos os demais módulos, registra na UDDI a WSDL dos serviços disponíveis. Na realidade, o que é registrado não é o conteúdo do documento WDSL, mas sim o caminho onde se encontra o documento; nesse caso, no Gerente de Votação;
- 2) O módulo Agente de Registro consulta no UDDI informações de localização do serviço que deseja acessar;
- 3) O UDDI, tendo a informação em seus registros, responde com o caminho onde se encontra a WSDL referente ao serviço, passando assim, a URL do mesmo;
- 4) O Agente de Registro, de posse da URL, efetua um *request* da WSDL armazenando-a no Gerente de Votação;
- 5) O Gerente de Votação responde com os dados do documento WSDL que contém a semântica dos serviços oferecidos pelo mesmo.

5.2.3. Mecanismos de autenticação e autorização

Os mecanismos de autenticação, autorização e políticas serão providos com mecanismos baseados nas especificações do W3C/OASIS, WS-Trust, WS-Policy e por validação de assinaturas digitais conforme descritos abaixo:

- **O WS-Trust (Web Services Trust) [NADALIN, 2006]:** a especificação WS-Trust tem como objetivo prover a interoperação entre diferentes mecanismos de autenticação, como, por exemplo, atuar como terceira parte confiável entre um sistema de autenticação biométrica (usado pelo eleitor), baseado em *templates* e certificados X.509 (usado nos módulos); a entidade *Security Token Service* (STS) será responsável por interoperar as requisições, validação e renovação de *tokens* entre as entidades envolvidas, quando os mecanismos de autenticação forem diferentes, por exemplo. Os métodos utilizados no protocolo são transportados em envelopes do protocolo SOAP;
- **O WS-Policy (Web Services Policy) [BAJAJ, 2006]:** o controle de acesso dos recursos disponíveis em cada módulo do sistema é definido e implementado sobre documentos WSDL, utilizando as especificações *WS-Policy* em conjunto com o *WS-SecurityPolicy* e *WS-PolicyAttachment*;

- **XML Signature [BARTEL, 2002]:** todos os módulos identificarão e autenticarão a origem, quando aplicável, através da assinatura XML encapsulada e associada ao documento XML na forma *enveloped*;
- **Certificados X.509 [ADMS, 2002]:** como mecanismo de segurança adicional, os canais de comunicação entre módulos são providos por certificados X.509, de forma a autenticar as origens e, indiretamente, reforçar a integridade no canal de transporte;
- **XKMS (XML Key Management Specification) [HALLAN-BAKER, 2005]:** em decorrência do uso de chaves assimétricas, o XKMS proverá o mecanismo de infraestrutura de chaves públicas, realizando procedimentos de localização, validação, registro de chaves, entre outros.

5.3. O Protótipo e Aspectos de Implementação

A seguir, serão apresentadas as ferramentas utilizadas no protótipo e a linguagem para descrição dos dados da eleição (EML).

5.3.1. Ferramentas, Frameworks e APIs

O protótipo da versão eletrônica do sistema de votação baseado em papel desenvolvido por [RIVEST, 2007] foi desenvolvido em linguagem Java⁴ e as entidades da arquitetura fazem uso de serviços, ferramentas, frameworks e/ou APIs para os seguintes fins:

a) Transporte dos dados

Os dados trocados entre as entidades são codificados em documentos XML, encapsulados em pacotes SOAP (*Simple Object Access Protocol*) e transportados por HTTP (*Hipertext Transfer Protocol*) provido pelo *Apache Axis*⁵ – aplicação do *Apache Tomcat*⁶. Além do uso do SOAP, o protótipo usa o serviço de pedido/resposta (HTTP/JSP) sobre SSL (*Security Socket Layer*), provido pelo *Apache Tomcat*, para implementar os Consoles de Registro e Votação – executado a partir de um *browser* HTTP.

⁴ <http://java.sun.com>

⁵ <http://ws.apache.org/axis2>

⁶ <http://tomcat.apache.org>

b) Autenticidade, integridade e confidencialidade

Para assinatura e cifragem das mensagens XML, foi utilizada a API Apache *XML-Security*⁷, que implementa as especificações *XML-Signature* e *XML-Encryption*.

c) Banco de Dados

Todas as mensagens e dados referentes ao processo de votação são armazenados no formato XML usando o *Oracle*⁸ *Berkeley DB XML*, base de dados XML nativa.

d) Infra-estrutura de Chaves Públicas

O cliente e servidor da ICP é baseado na iniciativa Open XKMS⁹, que interpreta documentos XML implementando as funções de verificação, registro e revogação de certificados X.509.

Dos diversos algoritmos assimétricos, entre o RSA, *ElGmal*, *Diffie-Hellman* e outros baseados em Curvas Elípticas, a arquitetura utiliza RSA como algoritmo para cifras com chaves de 1024 bits. Considerando uma implementação mista, o uso do algoritmo DSA desenvolvido pelo NIST para assinaturas digitais foi adotado entre as opções disponíveis.

Ainda, para estarem em consonância com os padrões, as especificações W3C-DSIG (*XML Signature*) [BARTEL, 2002] e W3C-XENC (*XML Encryption*) [IMAMURA, 2002], respectivamente para assinaturas e cifragem de documentos padrão XML, são utilizadas no sistema. Com o uso do XML em todas as mensagens, a ICP utilizada baseia-se na especificação XKMS (*XML Key Management Specification*) [HALLAN-BAKER, 2005].

e) Interface do usuário e hardware

Os Consoles de Registro e Votação são baseados em interface *Web* e adicionalmente empregam *Applets* para os processos de autenticação biométrica e leitura/escrita da credencial, e contraprova do voto armazenada em um cartão tipo *Java Card*.

O *Microsoft Fingerscan Reader* da Microsoft, em conjunto com a *API Griaule Fingerprint SDK* foram utilizados na implementação da autenticação biométrica.

⁷ <http://santuario.apache.org>

⁸ <http://www.oracle.com/technology/products/berkeley-db/xml>

⁹ <http://sourceforge.net/projects/xkms>

O IBM Gemplus GemPC Smart Card Reader com cartões Java Card GEM Xpresso Pro r3.2 PK da Gemalto foram utilizados para prover a leitura/escrita da credencial e a contraprova.

5.3.2. Uso da EML

Os esquemas EML foram empregados para as fases de pré-eleição, eleição e pós-eleição. A figura 5.6 mostra os esquemas EML utilizados pelas entidades da arquitetura em cada uma delas.

Na fase de pré-eleição, a base de dados de candidatos elegíveis é construída utilizando os esquemas 210 (*Candidate Nomination*) e 230 (*Candidate List*). A lista de candidatos elegíveis, gerada no esquema 230, associado a informações da eleição – esquemas 110/330 (*Election Event/Election List*) – são fontes de informações para o esquema 410 (*Ballot*) – *template* da cédula.

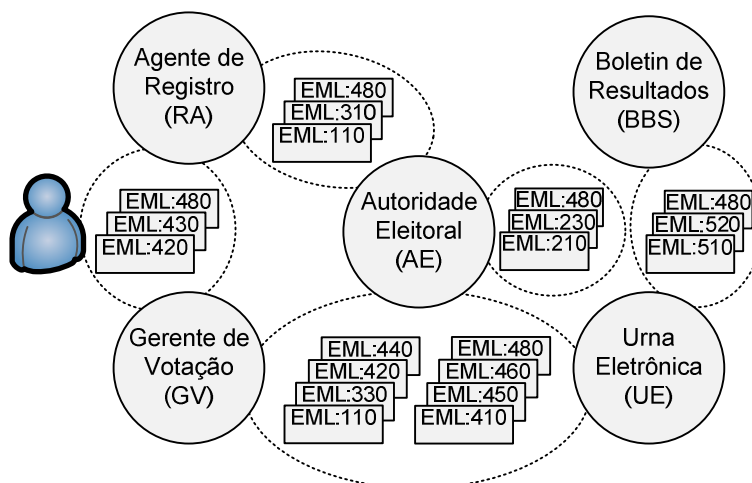


Figura 5.6. Esquemas EML utilizados no protótipo.

Ainda na fase de pré-eleição, foi utilizado o esquema 310 (*Voter Registration*) associado ao esquema 330 para efetuar o controle de registro e a habilitação dos votantes.

Os procedimentos envolvidos na fase de eleição são providos pelos esquemas 440 (*Cast Vote*), 445 (*Retrieve Vote*) e 450 (*Vote Confirmation*), sendo utilizados pelo Console de Votação, pelo Gerente de Votação e pela Urna Eletrônica.

Na fase de pós-eleição, fase de contagem e na divulgação dos resultados, os esquemas 460 (*Votes*), 510 (*Count*) e 520 (*Result*) foram usados pela Urna Eletrônica/Unidade de Apuração e pelo Boletim de Resultados, respectivamente.

Os procedimentos de autenticação são suportados pelos esquemas 420 (*Authentication*) e 430 (*Authentication Response*) e providos pelo dispositivo de assinaturas em documentos XML, usando ICP.

A auditoria do sistema utiliza o esquema 480 (*Audit Log*) auxiliado pelo sistema de LOGs do *Apache Tomcat*.

5.4. Descrição dos Módulos Implementados

Segue abaixo o descritivo dos módulos do protótipo da versão eletrônica desenvolvido neste trabalho e que teve como referência o sistema de votação baseado em papel, proposto em [RIVEST, 2007]. A descrição é esboçada por fase de votação, acompanhando os textos anteriores.

Os módulos desenvolvidos contemplam páginas JSP/JSF e Serviços Web providos pelo servidor *Servlet Apache Tomcat* e por *applets*.

5.4.1. Módulos da Fase de Registro e Habilitação

Abaixo os módulos envolvidos na Fase de Registro e Habilitação e suas classes Java:

- a) **Console de Registro (CR):** provido por páginas JSP/JSF e duas *applets*, uma para prover a autenticação biométrica do eleitor e outra para efetuar a gravação da credencial no cartão inteligente (*Smart Card* com sistema operacional *Java Card*). O CR faz comunicação com o Agente de Registro utilizando o protocolo SOAP conforme exposto no Capítulo 5. Cada item abaixo está associado a uma classe Java e seu respectivo código JSP/JSF, com exceção das classes das *applets* indicadas apropriadamente:
 - **Index:** provê a interação inicial entre eleitor e sistema, solicitando o número de identificação do eleitor, e efetua a autenticação utilizando senha, ou ativa a *applet* para autenticação biométrica. O modo de autenticação é configurado administrativamente;
 - **ElectionStatus:** informa ao eleitor o período da eleição quando esse tenta utilizar o sistema fora do período permitido;
 - **VoterDisable:** informa ao eleitor que o mesmo não está desabilitado a votar quando o mesmo insere o seu código de identificação;

- **AuthFingerprint:** provê a autenticação biométrica do eleitor através da *applet* **RAFingerApplet**;
 - **DataConfirmation:** confirma os dados do eleitor quando autenticado, apresentando, inclusive, a foto do mesmo;
 - **ReqCredential:** solicita ao Agente de Registro uma credencial de votação para o eleitor;
 - **SaveCredential:** grava no cartão inteligente do eleitor a credencial de votação através da *applet* **SESFileWriteApplet**;
 - **EndRegistration:** finalizado o processo de registro e habilitação do eleitor;
 - **RAFingerApplet:** *applet* que efetua a leitura da impressão digital do eleitor, visando à autenticação do mesmo;
 - **SESFileWriteApplet:** *applet* que efetua a gravação da credencial do eleitor no cartão inteligente.
- b) **Agente de Registro (AR):** baseado em Serviço Web, provê o controle do registro e habilitação do eleitor. Possui apenas a classe **RAService**, que é executada sobre o *Tomcat/Axis* e seus métodos provêm serviços para o Console de Registro e é cliente do serviço *VMService* (Gerente de Votação). Utiliza um banco de dados XML nativo e as transações ocorrem sobre *threads*, visando ao aumento de desempenho do sistema.

5.4.2. Módulos da Fase de Votação

Abaixo os módulos envolvidos na Fase de Votação e suas classes Java:

- a) **Console de Votação (CV):** provido por páginas JSP/JSF e três *applets*, uma para prover a autenticação biométrica do eleitor, outra para efetuar a leitura da credencial e outra para apresentar as cédulas de votação e efetuar a gravação da contraprova do voto. As duas últimas *applets* se utilizam do cartão inteligente (*Smart Card* com sistema operacional *Java Card*). O CV faz comunicação com o Gerente de Votação utilizando o protocolo SOAP, conforme exposto na seção anterior. Cada item abaixo está associado a uma classe Java e seu respectivo código JSP/JSF, com exceção das classes das *applets* indicadas apropriadamente:
- **Index:** provê a interação inicial entre eleitor e sistema, para os procedimentos de votação. O eleitor apresenta a credencial através do cartão inteligente, e o

sistema solicita a autenticação do eleitor. Essa classe invoca a *applet* **SESFileReadApplet**, que faz a leitura da credencial no cartão. A autenticação através de senha é provida pela própria *applet* e por biometria, através da *applet* **RAFingerApplet**;

- **AuthFingerprint**: provê a autenticação biométrica do eleitor através da *applet* **VMFingerApplet**;
 - **RequestBallot**: chamada após autenticação do eleitor, comunica-se com o Gerente de Votação para prover procedimentos de verificação do *Receipt ID* (RID) proveniente da credencial, inicia a *applet* **SESBallotApplet** e essa apresenta a cédula de votação para o eleitor;
 - **SESBallotApplet**: *Applet* que apresenta a cédula de votação ao eleitor e procede com o processo de votação fim-a-fim, incluindo a gravação da contraprova no cartão inteligente e a impressão da materialização do voto. Ela se comunica diretamente com o Gerente de Votação, efetuando operação do recebimento e envio da(s) cédula(s).
- b) **Gerente de Votação (GV)**: baseado em Serviço Web, provê o controle da votação e o depósito da cédula na Urna Eletrônica. Possui apenas a classe **VMService**, que é executada sobre *Tomcat/Axis* e seus métodos provêm serviços para o Console de Votação. Utiliza um banco de dados XML nativo e as transações ocorrem sobre *threads*, visando ao aumento de desempenho do sistema;
- c) **Urna Eletrônica (UE)**: baseado em Serviço Web, provê o armazenamento das cédulas de votação através de três repositórios distintos. Possui apenas a classe **BBSERVICE**, que é executada sobre *Tomcat/Axis* e seus métodos provêm serviços para o Gerente de Votação. Não utilizada nesta fase, a UE possui o módulo Unidade de Apuração (UC) com interface homem-máquina utilizada na Fase de Apuração. Utiliza um banco de dados XML nativo e as transações ocorrem sobre *threads*, visando ao aumento de desempenho do sistema.

5.4.3. Módulos da Fase de Apuração

Abaixo os módulos envolvidos na Fase de Apuração e suas classes Java:

- a) **Console de Apuração (CA)**: provido por páginas JSP/JSF e a *applet* **SESKeyCardApplet**, o CA não ficou explícito na exposição da arquitetura, mas é

a interface entre os atores, Autoridade Eleitoral (AE) e os Representantes Eleitorais (REs), e representa a Unidade de Contagem (UC), provendo a leitura das chaves privadas para o início da apuração a partir do cartão inteligente de cada ator. Esse módulo possui somente a classe ***index***, responsável pela chamada à *applet*. Mantém comunicação com os Repositórios de Cédulas (RCs) da Urna Eletrônica e com o serviço **BBSService** do módulo Boletim de Resultados (BBS);

- b) **Console do BBS (CBBS)**: provido por páginas JSP/JSF e a interface pública para divulgação dos resultados da eleição e comunica-se com o serviço **BBSService** para prover as requisições do usuários através do protocolo HTTP/HTTPS;
- c) **Boletim de Resultados (BBS)**: baseado em Serviço Web, armazena os resultados da eleição enviados pelo Console de Apuração e atende as requisições desses dados pelo Console do BBS. Possui apenas a classe **BBSService** que é executada sobre *Tomcat/Axis*, utilizando o protocolo SOAP.

5.5. Resultados obtidos

Visando avaliar a viabilidade do protótipo em processos eleitorais de grande escala, foram efetuados alguns testes de desempenho. O objetivo foi obter o tempo de execução dos procedimentos de habilitação, de votação e obtenção dos resultados/contagem dos votos. Cada teste foi efetuado 30 vezes e os resultados representam o tempo médio para cada caso. O coeficiente de variação das observações durante as medidas foram inferiores a 5%.

Para o teste de habilitação foi considerado o tempo entre a solicitação da credencial (evento 1.6, figura 5.1) e a resposta à mesma (evento 1.7).

Para o teste de votação foi considerado o tempo entre a solicitação da cédula (evento 2.4b, figura 5.2) e o recebimento da mesma (evento 2.5); o tempo entre a submissão da cédula (evento de 2.8, figura 5.2) e a resposta da Urna Eletrônica (evento 2.11).

O cenário de execução dos testes foi composto por quatro PCs ligados em rede local (*fast ethernet*), cujos serviços/funções foram instalados separadamente, conforme mostra a Tabela 5.4.

A participação dos eleitores nos procedimentos de habilitação e de votação foi simulada através da execução concorrente de 40 *threads* atendendo 40 eleitores simultaneamente. No processo de votação foram considerados três cargos e a marcação do voto foi definida aleatoriamente.

Tabela 5.4: Recursos utilizados nos testes

Recurso	Configuração	Serviço
PC1	Celeron 1.5 Ghz, 1GB RAM, Windows XP SP2	Console de Registro; Console de Votação; Unidade de Apuração
PC2	Pentium 4, 2.8 Ghz HT, 1 GB RAM, Disk SATA 2, Windows Vista	Axis2/Tomcat Agente de Registro
PC3	Pentium 4, 2.8 Ghz HT, 1 GB RAM, Disk SATA 2, Windows Vista	Axis2/Tomcat Gerente de Votação
PC4	AMD x64 Dual Core 4800, 1 GB RAM, Disk SATA2, Windows Vista	Axis2/Tomcat Urna Eletrônica

Para o procedimento de votação (fase mais crítica do processo), o tempo médio observado (ver Tabela 5.5) mostra que é possível atender cada eleitor em aproximadamente 147,5 ms. Assim, cada Gerente de Votação poderá atender aproximadamente seis eleitores por segundo ou 21.600 eleitores por hora.

Tabela 5.5: Desempenho na fase de Habilitação/Votação

Fase	Operações Simultâneas	Tempo Médio (ms)
Habilitação	40	7100
Votação	40	5900

Para dar escalabilidade ao sistema, é só aumentar o número de Gerentes de Votação – com 50 Gerentes de Votação, por exemplo, é possível atender 10.800,000 eleitores num período de 10 horas.

Para a Fase de Apuração, foram simulados 500 eleitores votando em 3 cargos, o que gerou 1500 cédulas por repositório, sendo que o tempo médio de contagem foi de 3,6 segundos.

Em complementação a este capítulo, o apêndice G apresenta um descritivo dos módulos desenvolvidos no protótipo.

O protótipo atualmente tem 11.500 linhas de código, 14 formulários com interface *web* (JSF/JSP), 11 formulários com interface Java *Swing*, 30 bases de dados de documentos XML (sob Oracle *Berkley DB XML*).

5.6. Conclusão

Este capítulo apresentou os aspectos de implementação do protótipo da arquitetura proposta e resultados de desempenho.

Os resultados mostrados na avaliação do protótipo foram alcançados com o uso de tecnologia padrões de mercado, aliados às melhores práticas de segurança aplicados a SEVs.

O uso dos principais esquemas da EML (*Election Markup Language*) foi contemplado no protótipo, garantindo, assim, a padronização para o intercâmbio de dados, possibilitando que, por exemplo, o Boletim de Resultados possa receber consultas por entidades externas através de *Web Services*.

Os resultados nos testes aplicados ao protótipo mostraram que a proposta é viável em eleições de larga escala.

Capítulo 6

Conclusão

Este trabalho apresentou uma proposta de um sistema de votação eletrônico confiável, robusto e que atende os preceitos democráticos do voto sem o uso de complexos esquemas criptográficos.

Na arquitetura apresentada, foram contemplados os requisitos do anonimato do eleitor, a privacidade e integridade do voto, utilizando-se o sistema de criptografia assimétrica.

A autenticidade do eleitor é aferida utilizando biometria através da impressão digital, e um mecanismo de contraprova do voto foi provida através do esquema de “Três Cédulas” [RIVERST, 2007].

A usabilidade, deficiente no sistema baseado em papel, foi efetivamente resolvida computacionalmente através do preenchimento parcial das cédulas. O uso de um dispositivo de impressão acionado pelo eleitor e controlado pela entidade de votação possibilita, de forma alternativa, a materialização do voto, com conferência do eleitor e de forma segura.

A unicidade no processo do voto e rastros de auditoria, sem que comprometam o anonimato do eleitor, a confidencialidade e integridade do voto foram contempladas em todos os procedimentos operacionais que envolvem as entidades da arquitetura proposta.

O protótipo desenvolvido confirmou sua confiabilidade, robustez e interoperabilidade, esta última garantida pela especificação EML (*Election Markup Language*).

Conforme os resultados demonstrados na Seção 5.4, onde se utilizou recursos pessoais, sem infra-estrutura de servidores, o uso da arquitetura mostrou-se satisfatório.

Associada aos resultados apresentados, a construção modular da arquitetura garante escalabilidade; e, assim, o seu uso em eleições de larga escala se mostra viável.

Este trabalho não contempla todos os aspectos de segurança associados aos sistemas de votação eletrônica, devendo ser desenvolvidas novas pesquisas que visem aprimorá-los e aumentar sua reputação, tais como pesquisas para evitar *software* fraudulento; produção de mecanismos de contraprova mais simples e eficientes; sistema de auditoria de código em tempo de votação; sistema para uso na Internet que coíbam a coação do eleitor e comércio do voto.

Referências Bibliográficas

- [ADMS, 2002] ADAMS, C. e LLOYD, S. **“Understanding PKI: Concepts, Standards, and Deployment Considerations”**. Editora Addison Wesley, 2002.
- [AMADO, 1999] AMADO, G. **“Eleição e Representação”**. Conselho Editorial do Senado Federal. 1999.
- [ATTRIDGE, 2002] ATTRIDGE, J. **“An Overview of Hardware Security Modules”**. SANS Institute, Information Security Reading Room, 2002.
- [BAJAJ, 2006] BAJAJ, S. et al. **“Web Services Policy Framework”**. Disponível em <http://specs.xmlsoap.org/ws/2004/09/policy/ws-policy.pdf>. Último acesso em Junho/2008.
- [BARNES, 2002] BARNES, C. et al. **“Hack Proofing Your Wireless Network”**. Editora Syngress Publishing, 2002.
- [BARTEL, 2002] BARTEL, M., BOYER, J., FOX, B., LAMACCHIA, B. e SIMON, E. **“XML-Signature Syntax and Processing”**. World Wide Web Consortium - W3C, 2002.
- [BENALOH, 1996] BENALOH, J. **“Verifiable Secret-Ballot Election”**. Tese de Doutorado, Yale University, 1996.
- [BENZ, 2003] BENZ, B. e DURANT, J. **“XML Programming Bible”**. Editora Wiley Publishing. 2003.
- [BRUNAZO, 2006] BRUNAZO, A. e CORTIZ, M. **“Fraudes e Defesas no Voto Eletrônico”**. Editora All Print, 2006.
- [BYRNE, 2007] BYRNE, M., GREENE, K. e EVERETT, S. **“Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines”**. CHI 2007 Proceedings, Politics & Activism, Association for Computing Machinery Inc., Vol 1, p. 171-180, 2007.
- [CALTECH-MIT, 2001] CALTECH-MIT. **“Voting – What is, What could be”**. The Caltech-MIT Voting Technology Project, 2001.

- [CHAPPEL, 2002] CHAPPEL, D. e JEWELL, T. "**Java Web Services**". Editora O'Reilly, 2002.
- [CHAUM, 1981] CHAUM, D. "**Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms**". Communications of ACM, vol. 24, no. 2, p. 84–88, 1981.
- [CHAUM, 2004] CHAUM, D. "**Secret Ballot Receipts: True Voter-Verifiable Election**". IEEE Security and Privacy, Jan/Fev 2004, p.38-47.
- [CHAUM, 2006] CHAUM, D. "**Punchscan Voting System**". Disponível em <http://punchscan.org>. Último acesso em Junho/2008.
- [COOL, 2001] COOL, T. "**Voting Theory for Democracy**". Thomas Cool Consultancy & Econometrics, p. 340, 2001.
- [COSTA, 2008] COSTA, R. G., SANTIN, A. O. e MAZIERO, C. A. "**A Three-Ballot-Based Secure Electronic Voting System**". IEEE Security & Privacy, v. 6, p. 14-21, 2008.
- [CROW, 2002] CROW, T. "**e-Voting Security Study**". Communications Electronics Security Group of European Committee for Standardisation, 2002.
- [CYBERTRUST, 2005] CYBERTRUST. "**Managing Digital Identities and Signatures through Public / Private Partnership**". Customer Case Study, Cybertrust, 2005.
- [DAUGHERTY, 2004] DAUGHERTY, Z. "**An Introduction to Voting Theory**". Tese de Graduação em Matemática, Mathematics Harvey Mudd College, 2004.
- [ELGAMAL, 1985] ELGAMAL, T. "**A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms**". IEEE Transactions on Information Theory. 31 (1985), p.469-472.
- [FERREIRA, 2001] FERREIRA, M. R. "**Evolução do Sistema Eleitoral Brasileiro**", Secretaria de Informação e Documentação do TSE/Senado Federal, 392p, 2001.
- [FISCHER, 2003] FISCHER, E. "**Election Reform and Electronic Voting Systems (DREs) Analysis of Security Issues**". CRS Report, Congressional Research Service, 2003.
- [FLANDERS, 2006] FLANDERS. "**Programme Architecture – Local Elections Flander 2006**". Disponível em <http://www.oasis-open.org/committees/download.php/20745/LocalElectionsFlanders2006.pdf>. Último acesso em Junho/2008.
- [FUJIOKA, 1992] FUJIOKA, A., OKAMOTO, T. e OHTA, K. "**A Practical Secret Voting Scheme for Large Scale Elections**". Proc. of Advances in Cryptology – AUSCRYPT '92, LNCS 718, p. 244-251, 1992.

- [GANESAN, 2007] GANESAN, C. "**EML Voting Project**". Disponível em <http://emlvoting.org>. Último acesso em Junho/2008.
- [GOLDWASSER, 1989] GOLDWASSER, S., MICALI, S. e RACKO, C. "**The Knowledge Complexity of Interactive Proof Systems**", SIAM Journal on Computing, Vol 18, p.186-208, 1989.
- [GOTTERBARN, 2006] GOTTERBARN, D. "**E-Voting: A Failure of Professionalism**". Inroads, The SIGCSE Bulletin, v..38, n. 4, p. 7-8, 2006.
- [HALLAN-BAKER, 2005] BAKER, P. e MYSORE, S. "**XML Key Manager Specification (XKMS 2.0)**".
- [HENDRICKS, 2002] HENDRICKS, M. et al. "**Professional Java Web Services**". Editora Alta Books, 2002.
- [IEEE-SCC38, 2007] IEEE-SCC38. "**Voting Standards**". IEEE, Standard Coordinating Committee 38. Disponível em <http://grouper.ieee.org/groups/scc38>. Último acesso em Junho/2008.
- [IMAMURA, 2002] IMAMURA, T., DILLAWAY, B. e SIMON, E. "**XML Encryption Syntax and Processing**", World Wide Web Consortium - W3C, 2002.
- [ISO/IEC, 1999] ISO/IEC9126. "**Guia Para Utilização das Normas Sobre Avaliação da Qualidade de Produtos de Software - ISO/IEC 9126 e ISO/IEC 14598**". ABNT – Associação Brasileira de Normas Técnicas, 1999.
- [ISO/IOC, 1997] ISO7498. "**ISO/IEC 7498-x Open Systems Interconnection - Basic Reference Model. OSI**", 2ª edição, 1997.
- [JAKOBSKIND, 2002] JAKOBSKIND, M. A. e MANESCHY, O. "**Burla Eletrônica - a máquina que faz seu voto sumir**". I Seminário do Voto Eletrônico, Câmara dos Deputados, Editado pela Fundação Alberto Pasqualini, 2002.
- [KIAYIAS, 2006] KIAYIAS, A., KORMAN, M. e WALLUCK, D. "**An Internet Voting System Supporting User Privacy**". Computer Security Applications Conference, IEEE, 2006.
- [KOFER, 2003] KOFER, R., KRIMMER, R. e PROSSER, A. "**Electronic Voting: Algorithmic and Implementation Issues**". 36th Hawaii International Conference on System Sciences, IEEE, 2003.
- [LAMPSON, 1971] LAMPSON, B. W. "**Protection**". 5th Princeton Conference on Information Sciences and Systems, p. 437, 1971.

- [LANDWEHR, 01] LANDWEHR, C. E. **“Computer Security”**. Publicação Online, Springer-Verlag, 2001.
- [LIETOLD, 2005] LIETOLD, H., HOLLOSI, A. e POSCH, R. **“Security Architecture of the Austrian Citizen Card Concept”**, Secure Information Technology Center – Austria, 2005.
- [MERCURI, 2001] MERCURI, R. **“Electronic Vote Tabulation Checks & Balances”**. Tese de Doutorado. University of Pennsylvania, 2001.
- [MOORE, 2001] MOORE, D., VOELKER, G. M. e SAVAGE, S. **“Inferring Internet Denial-Of-Service Activity”**. Proceedings of the 10th conference on USENIX Security Symposium, 2001.
- [MOHEN, 2001] MOHEN, J. GLIDDEN, J. **“The Case for Internet Voting”**. Communications of the ACM, n. 1, v. 44, Janeiro 2001.
- [NADALIN, 2006] NADALIN, A., GOODNER, M., GUDGIN, M., BARBIR, A. e GRANQVIST, H. **“Web Ser-vices Trust Language v1.3”**, Organization for the Advancement of Structured Information Standards - OASIS.
- [NAOR, 1994] NAOR, M. e SHAMIR, A. **“Visual Cryptography”**, Advances in Cryptology, Eurocrypt’94, Springer Berlin / Heidelberg, Volume 950, p. 1–12, 1995.
- [NORDEN, 2006] NORDEN, L. e et al. **“The Machinery Of Democracy: Voting System Security, Accessibility, Usability, and Cost”**. The Brennan Center for Justice, p. 29, 2006.
- [O’CONNOR, 2002] O’CONNOR, J. J. e ROBERTSON, E. F. **“The history of Voting”**, Em <http://www-gap.dcs.st-and.ac.uk/history/HistTopics/Voting.html>. Último acesso: Junho/2008.
- [OASIS, 2007] OASIS Open **“EML v5.0 - Process and Data Requirements & Schema Descriptions”**, OASIS Consortium. Disponível em <http://www.oasis-open.org/committees/election>. Último acesso em Junho/2008.
- [RIVEST, 1978] RIVEST, R.; SHAMIR, A. e ADLEMAN, L. **“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”**. Communications of the ACM, v. 21, n.2, p. 120-126, 1978.
- [RIVEST, 1992] RIVEST, R. **“The MD5 Message-Digest Algorithm”**. RFC 1321, IETF, 1992.

- [RIVEST, 2007] RIVEST, R. e SMITH, W. "**Three Voting Protocols: Three Voting Protocols: ThreeBallot, VAV, and Twin**". USENIX/ACCURATE Electronic Voting Technology Workshop, 16th USENIX Security Symposium, 2007.
- [RODRIGUEZ, 2002] RODRIGUEZ, V. "**Secure Programming Standards Methodology Manual**". The Institute for Security and Open Methodologies, 2002.
- [ROSSLER, 2005] ROSSLER, T., LEITOLD, H. e POSCH, R. "**E-Voting A Scalable Approach using XML and Hardware Security Modules**". IEEE International Conference on e-Technology, e-Commerce and e-Service 2005, p. 480-485, 2005.
- [SANTIN, 2004] SANTIN, A. "**Teias de Federações: uma abordagem baseada em cadeias de confiança para autenticação, autorização e navegação em sistemas de larga escala**". Tese de Doutorado, Universidade Federal Santa Catarina, 2004.
- [SCHNEIER, 1996] SCHNEIER, B. "**Applied Cryptography**". Editora John Wiley & Sons, 2ª edição, 1996.
- [STALLMAN, 1991] STALLMAN, R. E et al; "**GNU General Public License**", Free Software Foundation. Disponível em <http://www.gnu.org/licenses>. Último acesso em Junho/2008.
- [VLADIMIROV, 2004] VLADIMIROV A.; GAVRILENKO, K. e MIKHAILOVSKY, A. "**Wi-Foo - The Secrets of Wireless Hacking**". Editora Addison-Wesley, 2004.
- [WANG, 2003] WANG, H.; WANG, C. "**Addressing Security Threats and Risks Through Software Quality Design Factors**". Communications of the ACM, v. 46, n. 6, 2003.

Apêndice A

Esquemas Criptográficos

Os desafios para garantir as propriedades de **autenticidade, unicidade, anonimato, não-coação, integridade e auditabilidade**, alicerces da segurança em Sistemas Eletrônicos de Votação (SEVs), têm levado inúmeros cientistas da área de ciências exatas a se direcionarem em pesquisas para o desenvolvimento de métodos para implementação de SEVs que atendam as propriedades citadas e que são anseios de toda uma sociedade que clama por confiabilidade, transparência e lisura dos processos eleitorais envolvendo esses sistemas.

A baixa reputação dos SEVs por parte da sociedade está diretamente associada a dúvidas quanto aos resultados dos pleitos eleitorais, que devem atender os desejos dos eleitores voto-a-voto. Os SEVs, por princípio, têm que estar sincronizados com os alicerces de segurança acima citados, a leis e “regras de negócio” instituídos no país no qual o mesmo é implantado. Além disso, devem ser preparados para coibir qualquer probabilidade de fraude através de *software* malicioso que venha burlar os alicerces de segurança e vir a favorecer algum candidato em especial. Tem-se aí um motivo óbvio para que se cobre das autoridades sistemas que agreguem transparência, sejam passíveis de auditoria e possibilitem a averiguação de burlas, conluíus ou erros do sistema de forma pró-ativa a qualquer momento.

Na área de *e-voting*, esses esquemas em sua maioria têm como base os criptosistemas associados à infra-estrutura de chaves públicas providas pelo RSA Criptosystem [RIVEST, 1978]. Seus pontos de segurança são a dificuldade de se fatorarem grandes números primos e o *El-Gamal Criptosystem* [ELGAMAL, 1985], além de compreender um algoritmo cuja assimetria se baseia na dificuldade de computar logaritmos discretos em corpos finitos.

Atualmente, os estudos para o desenvolvimento de SEVs seguros se direcionam em esquemas de **assinatura cegas**, **criptografia homomórfica**, **redes de mistura**, **canais anônimos**, **prova de conhecimento zero** e, em muitos casos, o uso híbrido desses esquemas. A seguir será apresentado cada um desses esquemas criptográficos.

A.1. Assinaturas às Cegas

O anonimato do eleitor em sistemas de votação, quanto à qualidade de seu voto, é uma propriedade necessária, pois não é permitido, em momento algum, associar a identificação real do votante e qualidade de seu voto. A falta do anonimato do eleitor pode incidir na prática de comércio de votos e burla da propriedade de não-coação, prática que fere os princípios legais dos processos eleitorais em todo o mundo.

Introduzido pela primeira vez por [CHAUM, 1982] para o uso na área financeira e [FUJIOKA, 1992] na área da votação eletrônica, o esquema de assinaturas às cegas permite que o usuário obtenha a assinatura digital de uma determinada entidade, sem que a mesma tenha condições de saber o conteúdo do que está assinando, o qual pode conter informações que identifiquem o votante. Baseados nesse esquema, diversos SEVs têm utilizado essa técnica para garantir a propriedade do anonimato.

Em termos pedagógicos, e para melhor entendimento do esquema de assinaturas às cegas, será feita uma analogia, utilizando duas folhas (A e B) e um papel carbono. Digamos que o ator Bob deseja que a entidade X assine cegamente a folha A, que contém informações. Assim, Bob coloca o papel carbono sobre a folha A e sobre o papel carbono coloca a folha B, e esse conjunto é entregue para a entidade X assinar. A entidade X assina sobre a folha B que está em branco e, portanto, não permite que X veja o conteúdo em A. A entidade X devolve o conjunto para Bob e este retira a folha B e o papel carbono, passando a ter na folha A, a assinatura da entidade X em decorrência da propriedade do papel carbono que transferiu para a folha A a assinatura de X.

Em termos computacionais, e usando criptografia assimétrica (RSA), a entidade X possui uma chave pública “e”, a privada “d” e o módulo “n”. Bob envia uma mensagem “m” para ser assinada por X, mas antes adiciona um fator de cegamento aleatório “r” à mensagem no seguinte formato: $msg = mr^e \bmod n$. A entidade X recebe a mensagem e a assina, retornando para Bob $msg^d = (mr^e) \bmod n$. Bob, ao receber, descega msg^d usando $msg^d/r \bmod n$, que resulta em $m^d \bmod n$.

A.2. Criptografia Homomórfica

Atualmente, o esquema de criptografia homomórfica [BENALOH, 1996] tem sido alvo de estudos quanto à sua utilização em SEVs, com o objetivo de obter a soma dos votos sem conhecer a qualidade dos votos individualmente.

Basicamente, esse tipo de criptografia pode ser formulado como $F(a) + F(b) = F(a + b)$, onde a soma de dois valores cifrados é igual à soma cifrada dos valores.

A.3. Redes de Mistura (Mixnets)

As redes de mistura, ou *mixnets*, foi introduzida por [CHAUM, 1981] com o objetivo de prover um canal de comunicação anônimo para aplicações que demandassem tais necessidades, ou seja, o emissor envia uma mensagem e tem a garantia de que o receptor, ao recebê-la, não terá como descobrir a origem da mesma.

A rede de mistura compreende em um emissor cifrar “N” vezes a mensagem e enviá-la para o primeiro misturador de “N” misturadores. A cada misturador, a mensagem é decifrada e encaminhada numa ordem casual e assim sucessivamente até o receptor da mensagem.

Em um SEV, podemos fazer uma analogia a um conjunto de cédulas que são submetidas à *mixnet* em uma ordem seqüencial de entrada. Através das primitivas criptográficas que compõem a *mixnet*, obtém-se na saída a produção das mesmas cédulas em ordem diferente da ordem de entrada, evitando, assim, qualquer relação entre a cédula que entrou e a que saiu.

O uso de um único misturador garante a mistura, mas não garante o anonimato por completo, pois passa a ser ter um elemento que conhece toda a ordem das mensagens. Quando se aumenta para dois misturadores, o segundo misturador não conhece a ordem em que o primeiro misturador recebeu as mensagens e o primeiro misturador não sabe a ordem em que o segundo entregou a mensagem. Porém, a partir de um conluio entre os misturadores, essa ordem pode ser conhecida.

Assim, quanto maior o número e o paralelismo de “agentes de mistura” ao longo da rede, maior a garantia do anonimato da mensagem.

Nesse esquema, observa-se que é necessário agregar um lote de cédulas para que então a *mixnet* faça o seu processamento e, de fato, a saída venha ser em uma ordem aleatória e/ou por múltiplos canais. É desejável que as mensagens tenham o mesmo tamanho, evitando-se que haja uma análise da relação entrada e saída e o tamanho de cada mensagem. Porém, esse problema pode ser resolvido adicionando à mensagem caracteres nulos, de forma a manter um comprimento fixo para todas as mensagens.

Em SEVs, esse processo seria utilizado para efetuar o armazenamento de cédulas, de forma que o mesmo não ocorra na mesma ordem em que o voto foi proferido, e através de canais aleatórios, evitando, assim, qualquer relação entre o votante e a cédula armazenada. A figura A.1 esboça uma representação conceitual de uma *mixnet*, onde Mx é a mensagem.

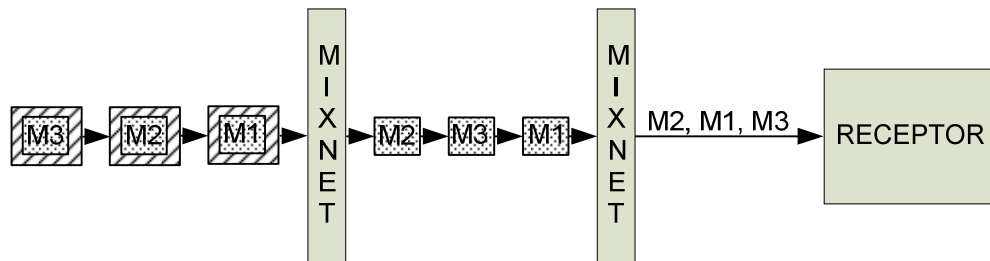


Figura A.1: Representação simples de uma rede de mistura.

Uma proposta que compreende uma sequência de múltiplas *mixnets*, agregando ainda mais o fator de mistura, direcionada ao SEV e utilizando *mixnets* de forma mais elaborada foi feita em [CHAUM, 2004]. Outras questões referentes ao processo das primitivas de mistura não serão apresentadas, por ser extenso e não ser o objetivo deste trabalho.

A.4. Canais Anônimos

Introduzido no trabalho de [CHAUM, 1981] em conjunto com o conceito de redes de mistura, permite a um emissor enviar uma mensagem a um receptor sem que este tenha como identificar a origem da mensagem, com a diferença que o receptor da mensagem tem como responder à mensagem, de forma a manter um canal de comunicação bidirecional, preservando o anonimato do emissor.

Conceitualmente, os procedimentos de reordenamento e retenção de lotes de mensagens permanecem conforme as redes de mistura. Porém, o emissor cifra a mensagem somente uma vez com a chave do primeiro *mixnet*. Este, ao receber a mensagem decifra-a, monta outra mensagem contendo a mensagem original mais um identificador, cifra a mensagem montada e encaminha à próxima *mixnet*, sendo que esse procedimento se repete ao

longo da rede de mistura, onde o último *mixnet* entrega ao receptor a mensagem em texto claro e seu identificador.

O receptor, ao receber a mensagem, poderá respondê-la utilizando o identificador, onde o processo inverso ocorre, sendo o identificador a referência de endereçamento para o retorno da mensagem. A figura A.2 representa o esquema utilizado nos canais anônimos sem representar o processo de mistura/reordenamento, no qual M é a mensagem e o IDx, o identificador.

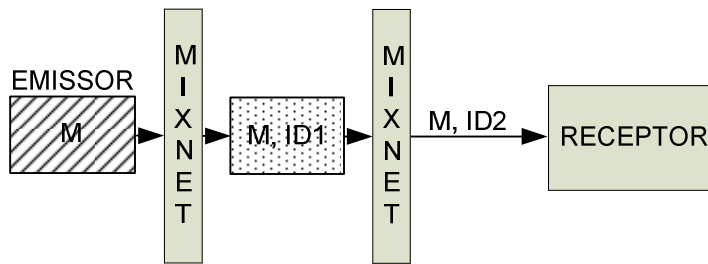


Figura A.2: Representação simples de canais anônimos.

A.5. Prova de Conhecimento Zero

Alguns esquemas criptográficos utilizam a técnica de Prova de Conhecimento Zero [GOLDWASSER, 1989], que permite mostrar o conhecimento de uma dada informação sem ter que revelá-la.

Em sistemas de votação, essa propriedade pode ser usada no processo de apuração/verificação, onde se pode determinar o total de votos, sem saber a qualidade do voto individualmente.

Ainda, associando Prova de Conhecimento Zero, podemos ter a impossibilidade de transferência da prova, que ocorre quando o ator A prova para B que conhece a informação C e B não tem como provar que teve a demonstração do conhecimento por A. Assim, essa propriedade poderá ser aplicada em protocolos de comunicação envolvendo diversas entidades e onde o anonimato deve ser preservado.

Apêndice B

Normas e padrões

Com o advento da globalização da Comunidade Européia e das diferentes leis que regem estados e municípios em um país, estabelecer padrões na definição dos componentes de um sistema de votação é uma necessidade iminente.

Assim, para possibilitar a troca de informações e interoperação entre os diversos sistemas e equipamentos existentes, e tendo como premissas a segurança, a exatidão e o cumprimento das regras e leis eleitorais, diversas instituições de renome internacional têm se direcionado na definição desses padrões.

Nas seções seguintes, são apresentadas algumas referências de projetos de órgãos de padronização de nível internacional, que têm trabalhado no sentido de prover uma unificação dos métodos e da infra-estrutura de equipamentos aplicados aos Sistemas de Votação Eletrônica, possibilitando, assim, que fabricantes possam desenvolver os seus produtos conforme os padrões definidos e, portanto, garantir uma interoperabilidade global.

B.1. IEEE P-1622 (Voting Systems Electronic Data Interchange)

O IEEE (*Institute of Electrical and Electronic Engineers*) mantém, desde 2002, o projeto denominado P-1622 [IEEE-SCC38], que tem como objetivo estabelecer padrões para a troca de dados e interoperabilidade entre os diversos componentes presentes em um sistema de votação, tais como o sistema de registro do eleitor, o processo de armazenamento de dados do candidato, definições da cédula, votação, classificação, entre outros.

A especificação EML descrita na seção seguinte deverá ser um dos padrões a serem adotados para promover essa interoperabilidade e troca de informações entre os sistemas.

Essa iniciativa permitirá que diversas empresas que desenvolvem produtos para sistemas de votação se balizem nos padrões para que ocorra uma interoperação, independente do estado ou país, como é o caso dos Estados Unidos, onde cada estado tem sua legislação e, portanto, pode ter um sistema de votação diferente.

B.2. Election Markup Language (EML)

A EML (*Election Markup Language*) é uma linguagem especificada pela OASIS (*Organization for the Advancement of Structured Information Standards*) e foi concebida com o intuito de estabelecer um padrão interoperável para sistemas de votação com suporte a múltiplos idiomas, adaptável aos diversos segmentos (privado e público) e que fosse seguro, conforme as exigências das leis e regras do sistema eleitoral de cada país.

A estrutura da EML foi modelada com base nos atuais sistemas eleitorais e define um dicionário de dados e esquemas de mensagens que utilizam estruturas de dados (71 tipos, entre simples e complexos) e 53 elementos/atributos definidos na linguagem para formar uma estrutura funcional.

Com semântica herdada da tecnologia XML, hoje, em sua versão 5 (março/2007) especifica processos e requisitos de dados (*Process and Data Requirements*), a descrição de esquemas (*Schema Description*), mecanismos de segurança e controle de erros.

Um conjunto de processos foram definidos e divididos em três áreas: a **PRÉ-ELEIÇÃO**, a **ELEIÇÃO** e a **PÓS-ELEIÇÃO**. Cada área é composta por grupos de processos e estes por esquemas EML.

B.2.1. Processos envolvidos na PRÉ-ELEIÇÃO

A área definida como pré-eleição contempla os seguintes grupos de processos:

a) Grupo “Candidates (200)”:

Este grupo concentra processos relacionados a pessoas nomeadas como candidatos elegíveis em uma eleição. Um candidato neste contexto pode ser um indivíduo ou um partido político. A figura B.1 ilustra os processos envolvidos.

Abaixo, descrição dos esquemas para troca de mensagens entre os processos:

- **Election Event (110):** É utilizado para mensagens de intercâmbio de informação em uma eleição, provendo, aos serviços do sistema, informações provenientes da Autoridade Eleitoral;

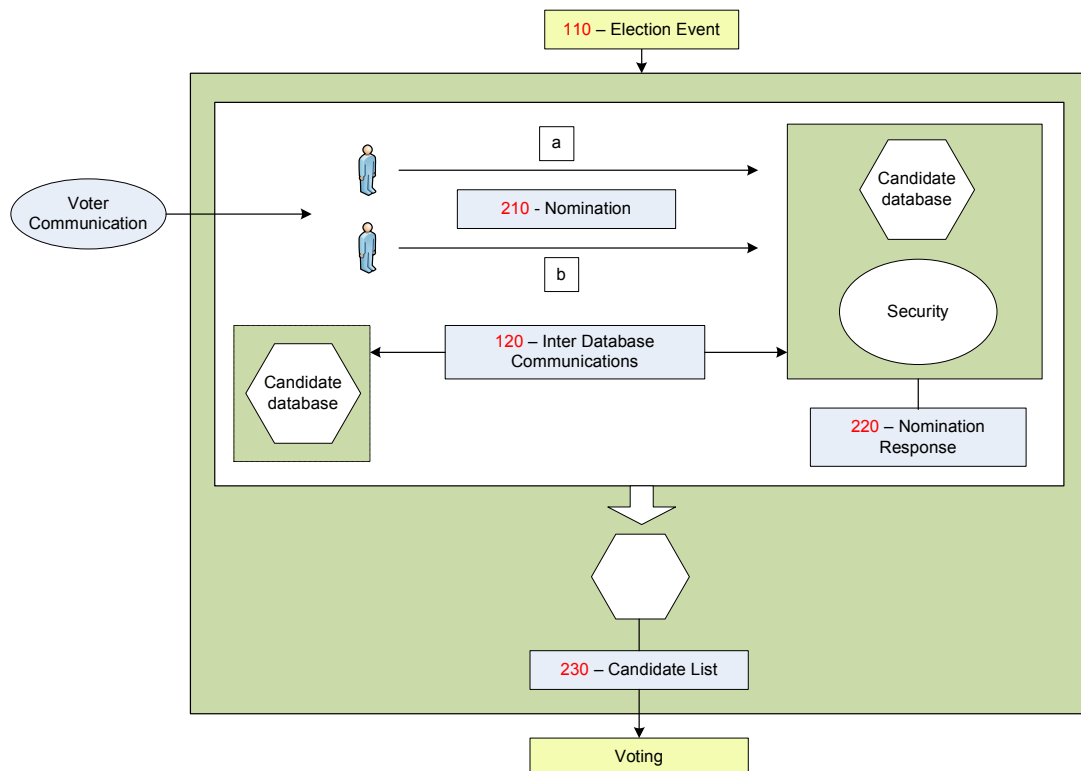


Figura B.1: EML - Processo de nomeação de candidatos [OASIS, 2007]

- **Inter Database (120):** Utilizado para a interoperação com banco de dados de outros sistemas de votação;
- **Candidate Nomination (210):** Mensagem utilizada para nomear candidatos, partidos, aceitar nomeação e retirar nomeação. O consentimento de candidato pode ser combinado em uma mensagem única, com uma nomeação do candidato ou do partido. A mensagem não cobre a nomeação de referendos;
- **Response to Nomination (220):** Mensagem enviada do organizador da eleição, ao candidato ou autoridade de nomeação de um partido, para informar que a nomeação foi aceita;
- **Candidate List (230):** Utilizada para transferir lista de candidatos.

b) **Grupo “Options (600)”:**

Este processo se relaciona com as opções a serem apresentadas aos eleitores em um referendo. As opções podem ser SIM ou NÃO, uma pergunta única, ou pode compreender um nível mais complexo de perguntas. A figura B.2 ilustra os processos envolvidos. Segue abaixo descrição dos esquemas para troca de mensagens entre os processos:

- **Election Event (110):** É utilizado para mensagens de intercâmbio de informação em uma eleição, provendo, aos serviços do sistema, informações provenientes da Autoridade Eleitoral;
- **Options Nomination (610):** Este esquema é usado para submeter propostas para um referendo. Utiliza o elemento de proposta genérica para definir a própria proposta. Um ou mais proponentes podem ser denominados e podem assinar a nomeação;
- **Options Nomination Response (620):** Esta mensagem é enviada pela Autoridade Eleitoral ao proponente para informar se a nomeação foi aceita ou não;
- **Options List (630):** Este esquema é usado para mensagens que transferem as listas de propostas de um referendo. Ele pode identificar o evento da eleição e fornece detalhes sobre a eleição. Cada proposta em um referendo conta como uma eleição, portanto, cada eleição identificada manterá uma proposta única.

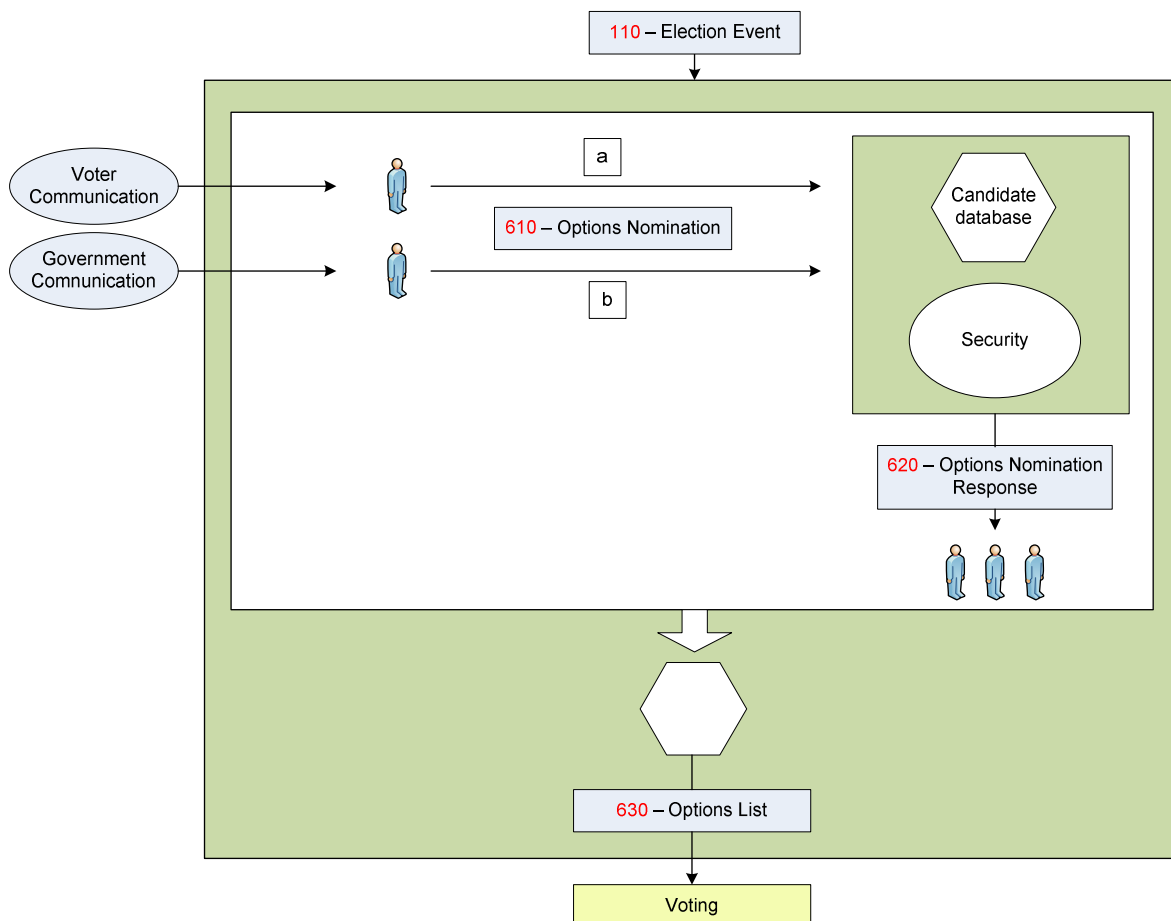


Figura B.2: EML - Processo de nomeação de Opções de Referendo [OASIS, 2007].

c) **Voters (300):**

A base deste processo é o Banco de Dados de Eleitores. Os dados armazenados no banco de dados são provenientes de informações oficiais fornecidas pelo Eleitor à Autoridade Eleitoral. Os procedimentos incluem registro, exclusão e alteração de dados do eleitor. Essa ação pode ser direta com a Autoridade Eleitoral ou através de um sistema online. A figura B.3 ilustra os processos envolvidos.

Segue abaixo descrição dos esquemas para troca de mensagens entre os processos:

- **Election Event (110):** É utilizado para mensagens de intercâmbio de informação em uma eleição, provendo, aos serviços do sistema, informações provenientes da Autoridade Eleitoral;
- **Inter Database (120):** Utilizado para a interoperação com banco de dados de outros sistemas de votação;
- **Voter Resgistration (310):** Utilizada nos procedimentos de registro do eleitor;

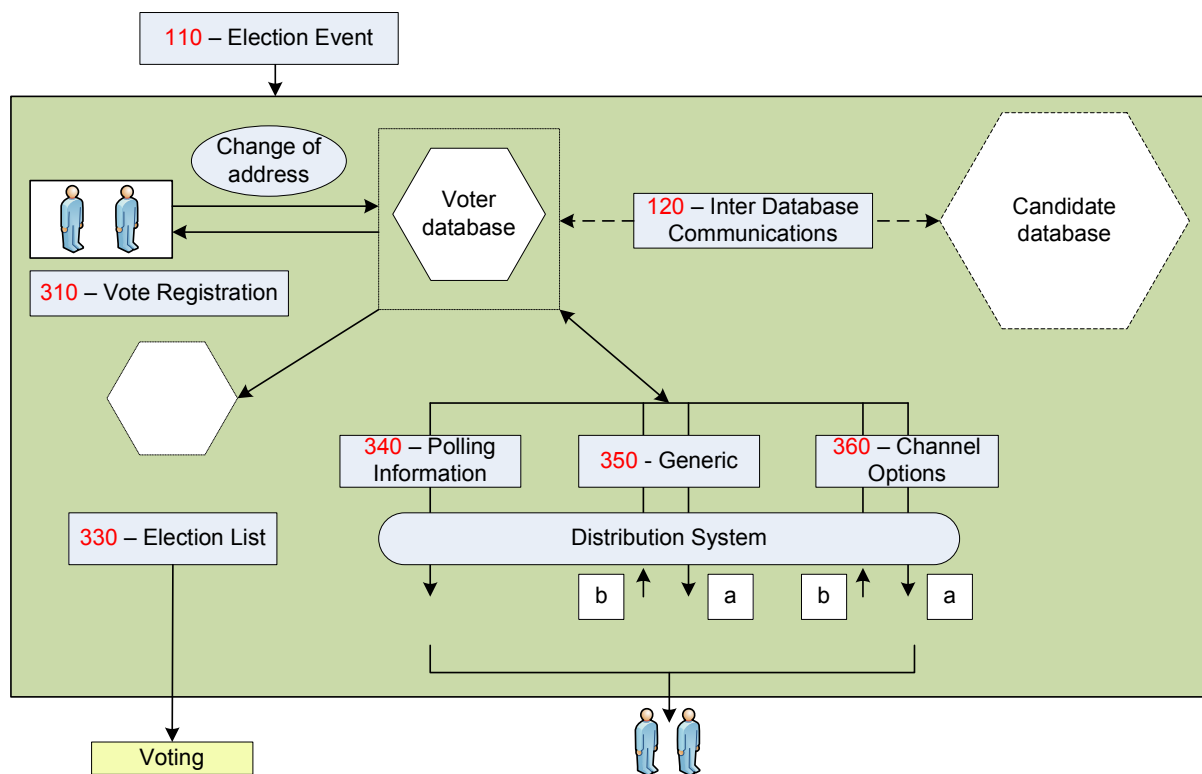


Figura B.3: EML - Processos relacionados ao registro do eleitor [OASIS, 2007].

- **Election List (330):** Utilizada para transferir lista de eleitores elegíveis;
- **Polling Information (340):** A mensagem definida para este esquema tem como objetivo apresentar ao eleitor um conjunto de informações instruindo como o

mesmo deve votar, entre outros eventos relacionados à votação. Essas informações incluem o dispositivo que será utilizado (DREs), o número do telefone SMS a ser utilizado, se aplicável, o endereço de votação para situações presenciais, a URL para votações via Internet, informações sobre cédula, entre outros.

- **Outgoing/Incoming Generic Communication (350a/b):** Provê a estrutura de comunicação com o eleitor;
- **Incoming/Outgoing Channel Options (360a/b):** É uma extensão do esquema 350a/b e suas mensagens têm a função de solicitar ou responder (*outgoing/incoming*, conforme o caso) um ou mais canais de votação. Inclui uma lista de canais habilitados e de opções gerais do pleito eleitoral.

B.2.2. Processos envolvidos na ELEICÃO

A área definida como eleição contempla os esquemas do grupo **Voting (400)** e envolve processo de autenticação do eleitor e depósito do voto. A figura B.4 ilustra o processo de votação.

Segue abaixo a descrição dos processos envolvidos na votação:

- **Election Event (110):** É utilizado para mensagens de intercâmbio de informação em uma eleição, provendo, aos serviços do sistema, informações provenientes da Autoridade Eleitoral;
- **Candidate List (230):** Utilizada para transferir lista de candidatos;
- **Election List (330):** Utilizada para transferir lista de eleitores elegíveis;
- **Ballots (410):** Utilizado para a apresentação das cédulas ao eleitor, posicionamento e esquema para impressão;
- **Authentication (420):** Utilizado nos procedimentos de autenticação do eleitor;
- **Authentication Reply (430):** Mensagem de resposta de autenticação quando do recebimento de uma mensagem 420, informa se o sujeito foi autenticado ou não;
- **Cast Vote (440):** Essa mensagem representa a efetivação do voto e que, opcionalmente, necessita de um *token* de votação para assegurar que o voto está sendo depositado por um eleitor autorizado, e gera um conjunto de informações de auditoria;
- **Retrieve Vote (445):** Esta mensagem é utilizada em sistemas de votação que contemplam urna de pré-cédulas, na qual os votos podem ser recuperados antes de

serem contados. Quando um voto é recuperado, deve ser eliminado da urna de pré-cédulas;

- **Vote Confirmation (450):** É uma mensagem de confirmação de voto e pode ser utilizada para informar se o voto foi contabilizado, e ainda fornece um número de referência (recibo) para o caso de questionamentos futuros;
- **Votes (460):** Esse esquema é utilizado para definir uma mensagem que compreende um conjunto de votos utilizado para a apuração. É um conjunto do esquema “Cast Vote (440)”. Nesse processo, informações de auditoria são geradas;
- **VToken Log (470):** Formato de mensagem para armazenar, em arquivos de *log*, informações dos *tokens* de votação;
- **Audit Log (480):** Formato de mensagem para gravações gerais em arquivos de *log*;
- **Options List (630):** Esse esquema é usado para mensagens que transferem as listas de propostas de um referendo. Ele pode identificar o evento da eleição e fornece detalhes sobre a eleição. Cada proposta em um referendo conta como uma eleição, portanto cada eleição identificada manterá uma proposta única.

A área definida como **PÓS-ELEIÇÃO** contempla os esquemas dos grupos *Results* (500) e *Audit* e envolve o processo de contagem e divulgação dos resultados do pleito eleitoral e, por fim, processos definidos para prover a auditoria do sistema. Abaixo, a descrição dos processos envolvidos na contagem e divulgação dos resultados:

- **Count (510):** Essa mensagem é responsável pelo esquema de contagem e ainda provê a comunicação dos resultados para o esquema 520. A mensagem inclui um identificador do evento relacionado à eleição;
- **Result (520):** As mensagens descritas por esse esquema são utilizadas para publicar os resultados do pleito eleitoral.

A figura B.5 ilustra o processo de contagem e divulgação de resultados.

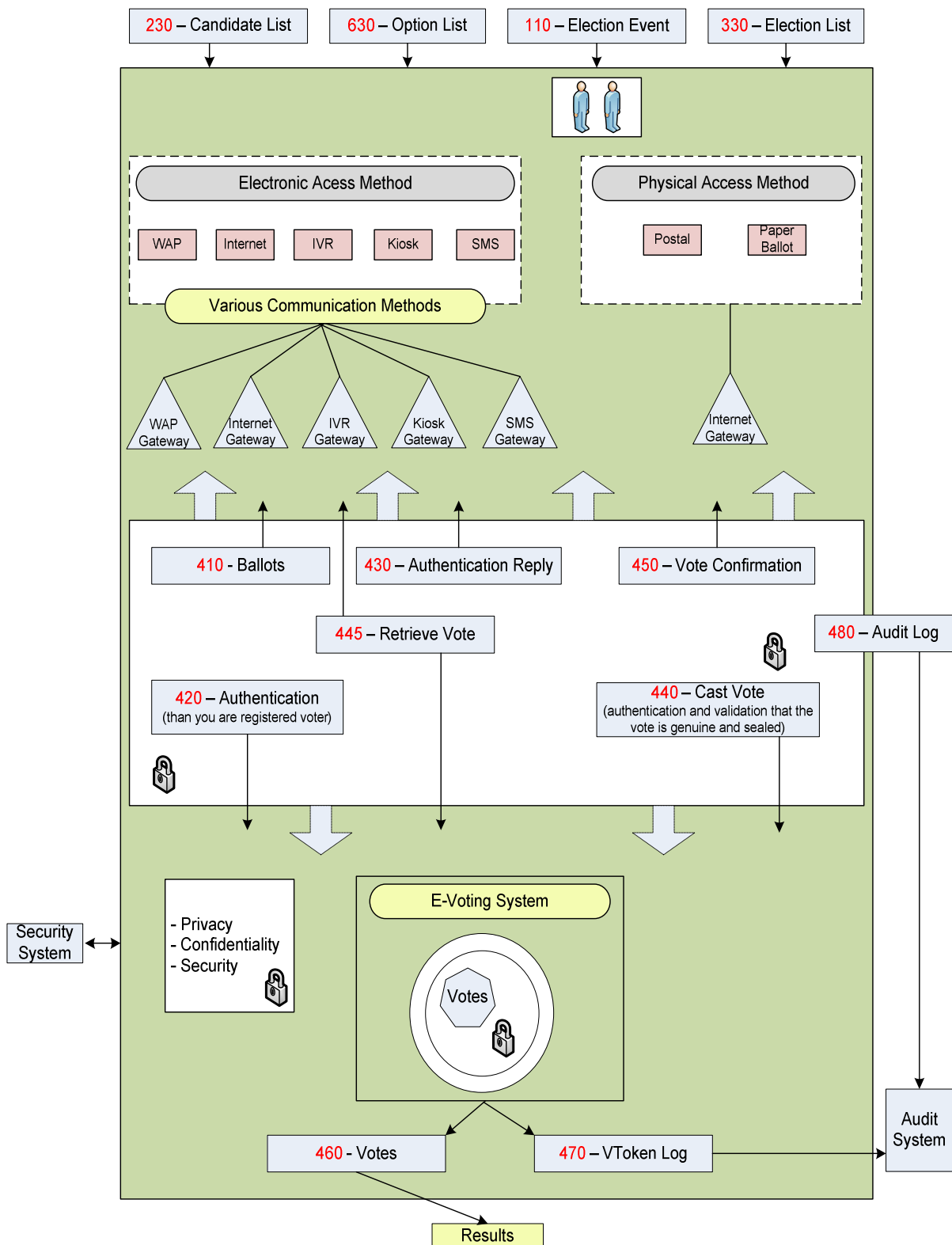


Figura B.4: EML - Processo de Votação [OASIS, 2007]

A área definida como **PÓS-ELEIÇÃO** contempla os esquemas dos grupos *Results* (500) e *Audit* e envolve o processo de contagem e divulgação dos resultados do pleito eleitoral e, por fim, processos definidos para prover a auditoria do sistema. Segue abaixo a descrição dos processos envolvidos na contagem e divulgação dos resultados:

- **Count (510):** Essa mensagem é responsável pelo esquema de contagem e ainda provê a comunicação dos resultados para o esquema 520. A mensagem inclui um identificador do evento relacionado à eleição;
- **Result (520):** As mensagens descritas por esse esquema são utilizadas para publicar os resultados do pleito eleitoral.

A figura B.5 ilustra o processo de contagem e divulgação de resultados.

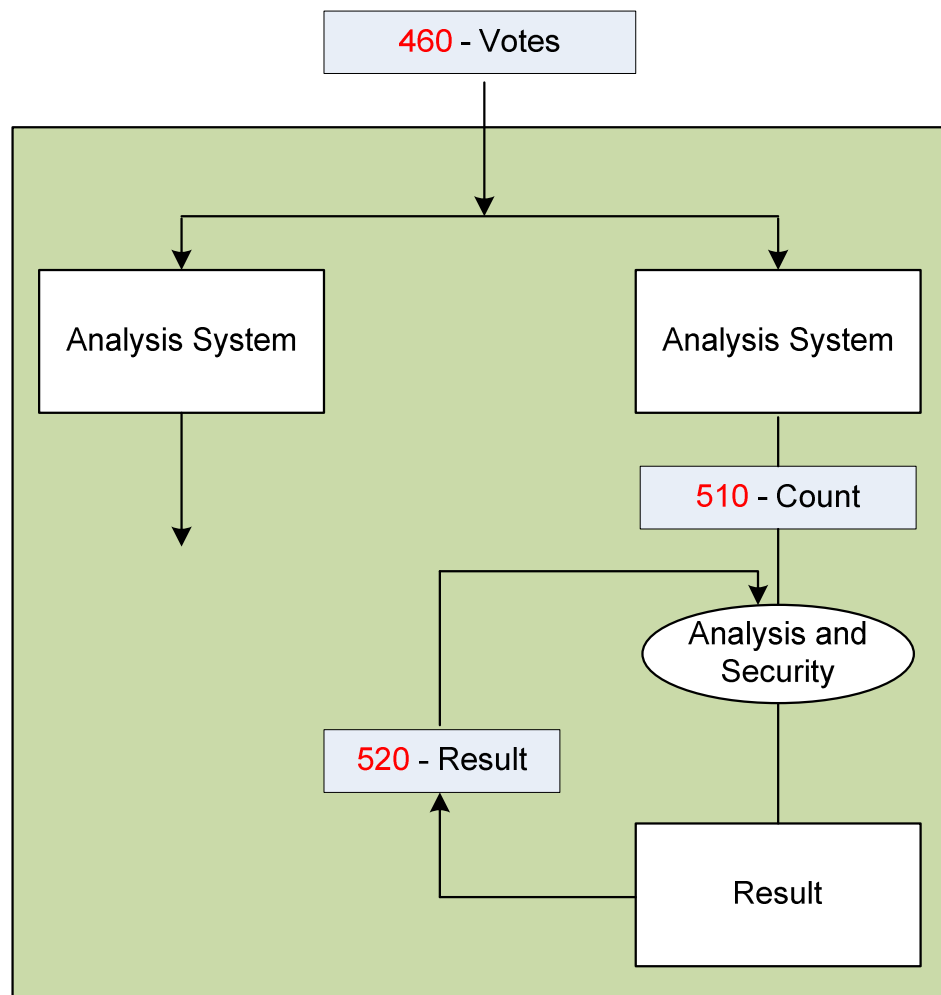


Figura B.5: EML – Processo de contagem e de divulgação de resultados [OASIS, 2007].

B.2.3. Processos envolvidos na PÓS-ELEICÃO

Ainda na área definida como pós-eleição temos os processos relacionados à auditoria do sistema, abaixo descritos:

- **VToken Log (470):** Formato de mensagem para armazenar, em arquivos de *log*, informações dos *tokens* de votação;
- **Audit Log (480):** Formato de mensagem para gravações gerais em arquivos de *log*;

A figura B.6 ilustra os processos envolvidos na auditoria.

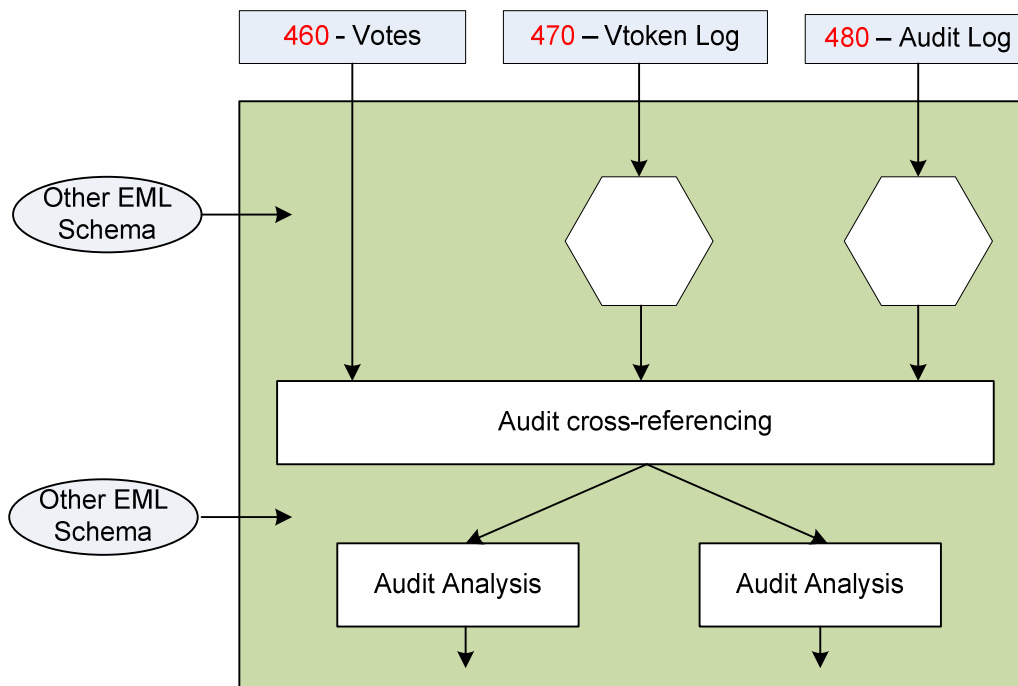


Figura B.6: EML – Processos envolvidos na auditoria [OASIS, 2007].

A EML também especifica mecanismos de segurança para os diversos processos envolvidos num pleito eleitoral, tendo sempre como premissa garantir o direito do voto ao eleitor devidamente habilitado, levando em consideração os requisitos de autenticação, confidencialidade/privacidade, integridade e não-repúdio, integridade e os requisitos de segurança impostos a um Sistema Eletrônico de Votação, conforme exposto na Seção 2.2.2.

Para prover os mecanismos de segurança citados, a EML especifica uma **Arquitetura de Segurança** que engloba identificação e registro do eleitor, direitos para votar baseado em autenticação, proteção de troca de eleitor quando o mesmo está votando remotamente, validação do direito ao voto, confidencialidade do voto, integridade da lista de candidatos,

apuração dos votos com exatidão e controle de segurança do sistema de votação. A figura B.7 ilustra a arquitetura de segurança proposta pela EML.

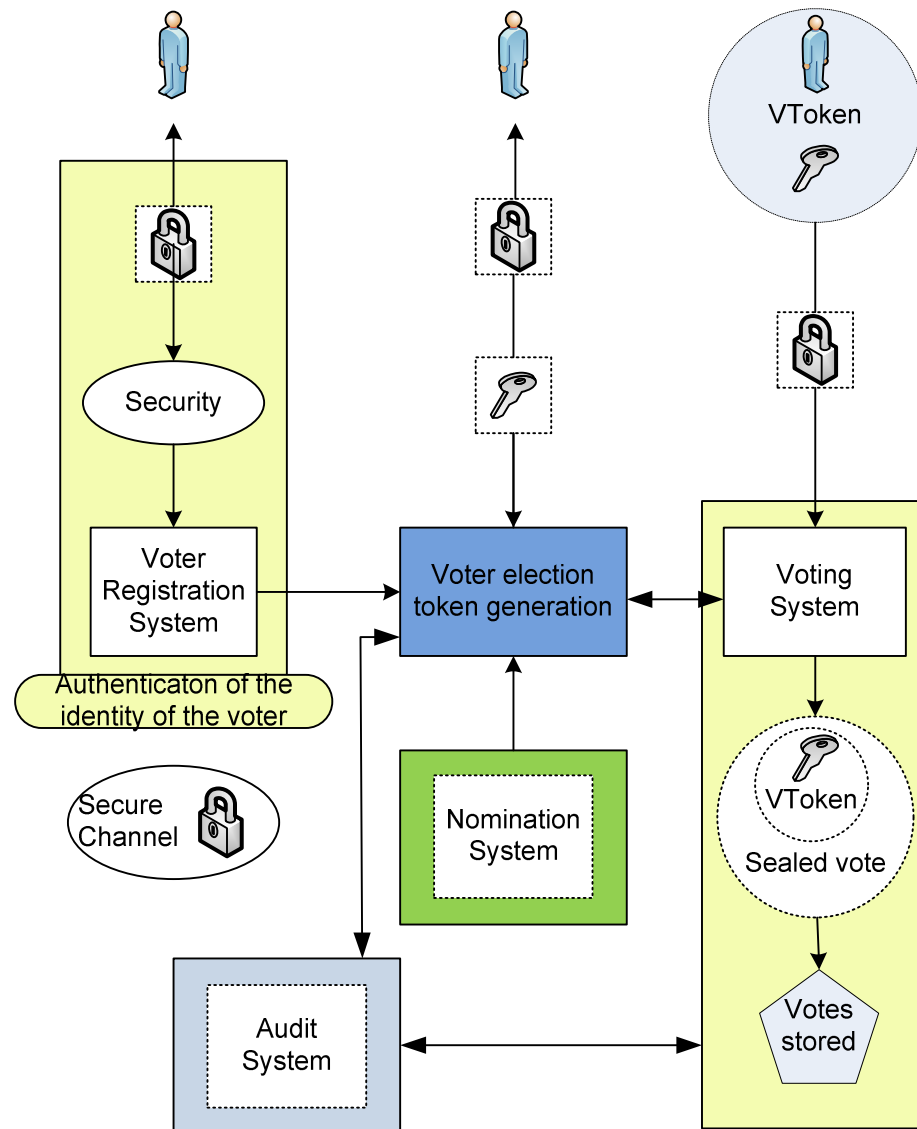


Figura B.7: EML – Arquitetura de segurança [OASIS, 2007]

A EML se mostra uma forte aliada ao projeto de interoperação do IEEE P-1622 (ver Seção anterior), sendo um avanço quanto à especificação de padrões.

Na prática, a EML tem sido pouco utilizada, mas já é objeto de projetos-piloto de *e-Voting*.

A especificação da EML foi utilizada em todas as suas áreas, PRÉ-ELEIÇÃO, ELEIÇÃO E PÓS-ELEIÇÃO, nas eleições que ocorreram em outubro/2006 em Flanders, no

norte da Bélgica, cujo relatório [FLANDERS, 2006] da arquitetura de votação denota o uso maciço dessa tecnologia.

Para desmistificar a EML, um *framework* “Open Source” para *e-Voting* foi desenvolvido e denominado de “EML Voting Project” [GANESAN, 2007], e sua implementação se baseia em Java e pode ser utilizado em modo “*standalone*” ou através de um módulo que pode ser agregado ao *framework* Axis da *Apache Foundation*, que deverá ser aproveitado em consonância com as regras de licenciamento, na implementação da proposta deste trabalho.

Apêndice C

Introdução a Serviços Web

Uma vez que a implementação da proposta apresentada neste trabalho tem como suporte a infra-estrutura de Serviços Web, comumente conhecida com *Web Services* (WS), este apêndice traz uma pequena introdução a essa classe de serviço que a cada dia toma novas frentes junto às implementações práticas desenvolvidas na *Web*.

Disponibilizar um sítio na Internet é um dos Serviços Web pioneiros na rede e, por ser tão comum, talvez o mesmo já não se aplique à classe de Serviços Web aqui apresentado. Os Serviços Web advêm da necessidade de se disponibilizar serviços, provendo uma interoperação padronizada, de forma que qualquer provedor de serviços possa oferecê-lo em qualquer parte do mundo e a comunicação entres as entidades usuário e provedor ocorra sob protocolos com padrões definidos e abertos, agregando aos mesmos mecanismos funcionais e com a segurança necessária. Basicamente, a infra-estrutura opera orientada a serviços sobre uma infra-estrutura similar à arquitetura cliente/servidor.

Os Serviços Web, criados por uma demanda de grupos de trabalhos de diversas empresas ligadas a serviços Internet, têm trabalhado nessa padronização, que inclui o W3C (*World Wide Web Consortium*) e OASIS (*Organization for the Advancement of Structured Information Standards*).

Para melhor entender o que de fato faz os WS e o que os diferenciam da simples disponibilização de páginas HTML na Internet, pode-se dar como exemplo uma agência de venda de passagens aéreas pela Internet. Em tempo real, ela obtém autorização da compra proveniente de um cartão de crédito, conecta-se à administradora através de protocolos de WS sem se preocupar com que plataforma de programação o provedor trabalha (nesse caso, a administradora). No caso específico do sistema de votação, os resultados das eleições podem

ser disponibilizados através do módulo BBS (Boletim de Resultados, ver Capítulo 4) a todos os provedores de informação, com o simples uso de WS, que consiste numa plataforma única e possibilita o uso de serviços distribuídos, tais como os citados.

A seções a seguir apresentam uma explanação das tecnologias e protocolos associados aos Serviços Web que são implementados a partir de diversos *frameworks*, tal como o *Axis*, da *Apache Foundation*, e usado na implementação do modelo proposto neste trabalho.

C.1. Entidades

Os Serviços Web pertencem à classe de Serviços Orientados à Arquitetura (SOA) e sua funcionalidade se baseia em três entidades básicas: o SOAP, que provê a comunicação e interoperação entre as entidades, aplicativos e serviços; a WSDL, que descreve os serviços disponíveis; e a UDDI, que publica os serviços descritos pela WSDL. Nos subitens a seguir, será explanada cada uma dessas entidades. A figura C.1 ilustra essas entidades e suas relações.

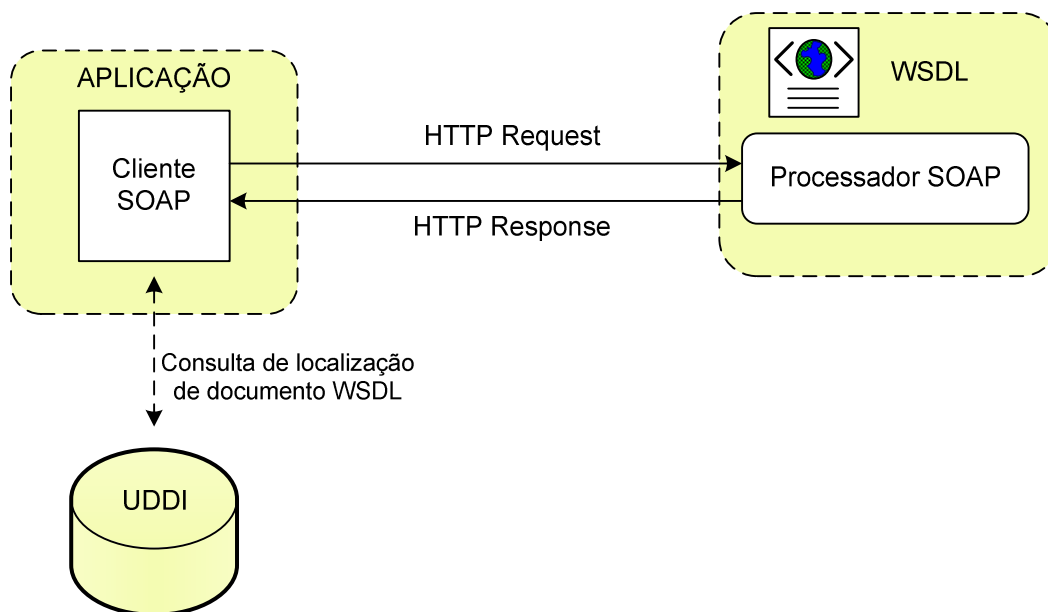


Figura C.1: Relações entre as entidades dos *Serviços Web* [CHAPPEL, 2002].

C.1.1. O protocolo SOAP

O protocolo SOAP (*Simple Object Access Protocol*) [HENDRICKS, 2002] foi desenvolvido para prover o envelopamento de documentos XML na troca de mensagens entre os diversos sistemas. É composto por três campos: um envelope, cabeçalho e o corpo descrito a seguir:

- **Envelope:** Campo obrigatório, demarca o início e o fim da mensagem SOAP (`<SOAP-ENV:Envelope></SOAP-ENV:Envelope>`);
- **Cabeçalho:** Não é um campo obrigatório e pode ser utilizado para recursos de autenticação e gerenciamento (`<SOAP-ENV:Header></SOAP-ENV:Header>`);
- **Corpo:** Campo obrigatório, contém efetivamente os dados a serem enviados/recebidos pelas entidades envolvidas na comunicação (`<SOAP-ENV:Body></SOAP-ENV:Body>`).

O mecanismo do protocolo SOAP se baseia basicamente em duas primitivas: solicitação e resposta. A solicitação tem como base a invocação de procedimentos remotos, cujo retorno é a resposta proveniente do processamento do procedimento invocado. Para garantir a interoperabilidade, o protocolo SOAP, apesar de não estar vinculado a nenhum protocolo da camada de transporte, normalmente é encapsulado sobre o protocolo HTTP, cuja segurança no nível de transporte pode ser provida pelo SSL/TLS.

C.1.2. A linguagem WSDL

A linguagem WSDL (*Web Service Description Language*) [HENDRICKS, 2002] é utilizada pelo provedor de serviço para descrever as funcionalidades de cada serviço por ele disponibilizado, e figura um documento com gramática XML que pode ser acessado diretamente via HTTP.

Um documento WSDL é composto por um conjunto de portas que se ligam às sintaxes das mensagens, operações e tipos de dados a serem utilizados na comunicação com o serviço, possibilitando que o cliente interopere adequadamente com os procedimentos remotos do provedor de serviço. De certa forma, é uma autodocumentação das chamadas que podem ser efetuadas sobre aquele serviço.

C.1.3. Serviço UDDI

O serviço UDDI (*Universal Description, Discovery and Integration*) [HENDRICKS, 2002] é um componente do WS para descrever o conjunto de informações de negócio, no qual figura o provedor de serviços, tais como:

- **Negócio:** contém informações como o nome do provedor, contato, classificação comercial do provedor, entre outros;

- **Serviço:** contém a relação dos diferentes serviços disponibilizados pelo provedor, incluindo uma classificação dos serviços de acordo com o seu uso comercial;
- **Especificação técnica:** contém detalhes técnicos sobre o serviço disponível, incluindo a localização do documento que descreve as sintaxes dos serviços disponibilizados pelo provedor de serviço, ou seja, a UDDI manterá um registro com a URL da WSDL do serviço. Observa-se que o documento WSDL não é armazenado nessa entidade de registro, apenas o caminho na qual a mesma se encontra. A responsabilidade do registro da WSDL é da entidade que provê o serviço.

C.2. Linguagem XML e Mecanismos de Segurança

A Linguagem de Marcação extensível, ou XML (*Extensible Markup Language*) [BENZ, 2003], é uma das bases da interoperação em WS, visto que toda comunicação entre cliente e provedor de serviços se baseia na serialização de documentos XML sobre o protocolo SOAP, explanado anteriormente.

A tecnologia de WS concebida para utilizar meios de comunicação de baixo acoplamento, como a Internet, provê alguns dispositivos de segurança associados a documentos XML que fazem parte do grupo *WS-Security* e consiste em agregar aos documentos uma assinatura e a cifragem dos dados, que compreende o *XML Signature* e o *XML Encryption*, cuja especificação é do W3C.

C.2.1. XML Signature

A tecnologia de WS utiliza a especificação *XML Signature* [BARTEL, 2002], que compreende uma forma de garantir a autenticidade, a integridade e o não-repúdio da mensagem entre cliente e provedor. A assinatura é efetuada sobre o conteúdo de um documento XML, podendo ser nas formas *enveloped*, *enveloping* e *detached*:

- **Enveloped:** A assinatura se encontra dentro do conteúdo que é assinado, ou seja, a assinatura é um elemento do documento XML assinado;
- **Enveloping:** O conteúdo assinado estará dentro da assinatura, ou seja, o conteúdo do documento XML assinado é um elemento da assinatura XML;
- **Detached:** A assinatura ocorre externamente ao documento XML, apenas sendo referenciada por ele.

C.2.2. XML Encryption

A especificação *XML Encryption* [IMAMURA, 2002] tem como objetivo garantir a confidencialidade do conteúdo de documentos XML, podendo o processo de cifragem ocorrer em todo o documento ou em partes dele, seja sobre conteúdo texto ou binário.

C.3. O WS-Security

O *WS-Security* (*Web Services Security*) especificado pela OASIS tem como objetivo prover mecanismos de segurança aos Serviços Web. A segurança agregada aos Serviços Web através do *WS-Security* consiste em estender ao protocolo base, o SOAP, mecanismos de segurança. A figura C.2 ilustra a arquitetura do *WS-Security*, onde outras especificações a complementam. No entanto, essa introdução aos Serviços Web restringe-se às entidades envolvidas no modelo/protótipo.

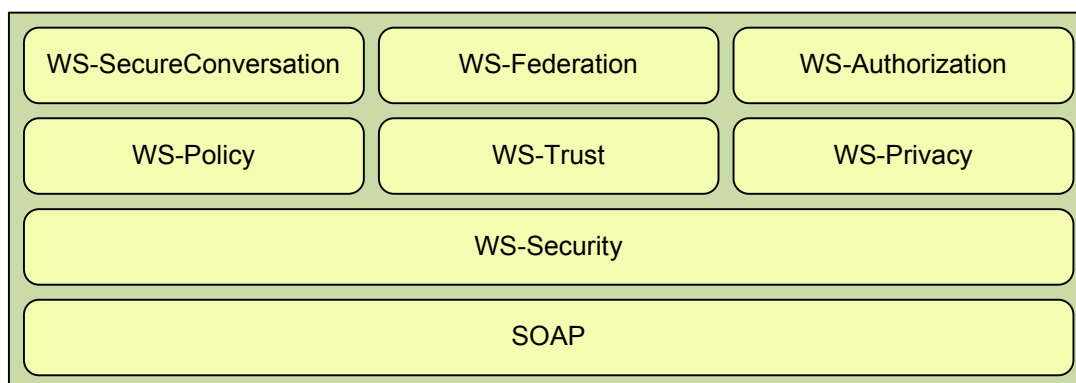


Figura C.2: Arquitetura do WS-Security

O *XML-Signature* e o *XML-Encryption*, já explanados, classificam-se como mecanismos associados ao *WS-Security*, no que tange a procedimentos de assinatura digital e criptografia dos dados, respectivamente sobre SOAP. Para a camada de transporte, o mecanismo utilizado é o SSL/TLS. No entanto, ambos os recursos podem ser utilizados em conjunto, elevando o nível de confiabilidade fim-a-fim.

A especificação ainda prevê o uso de credenciais de autenticação através da *tag/namespace* `<wsse:Username>`, que figura credenciais do tipo *UsernameToken*, nas quais podem ser considerados como autenticação simples, ou credencial do tipo *BinarySecurityToken* para uso com certificados X.509, *ticket Kerberos*, asserções SAML, entre outros modelos de autenticação. Qualquer diretiva do *WS-Security* é encapsulada na *tag/namespace* `<wsse:Security>`.

C.4. O WS-Policy

O *WS-Policy* agrega aos Serviços Web uma gramática descritiva de políticas de direitos de acesso e forma de uso de serviços e recursos, tais como modo de autenticação, tipos de algoritmos, tipo de canal seguro a ser utilizado, tendo como foco agregar segurança no acesso aos recursos e serviços. Essas políticas são representadas através de documentos XML e compreendem um conjunto de asserções que se iniciam a partir do elemento `<wsp:Policy>`.

As asserções do *WS-Policy* são efetivadas através de dois operadores, o *ExactlyOne*, que limita a política a uma única asserção, e o operador *All*, que permite o uso de todas as asserções de forma combinada, cujo elemento possui a sintaxe `<wsp:[ExactlyOne][All]>`.

As políticas definidas através do *WS-Policy* podem ser anexadas dentro de um documento WSDL através do elemento *PolicyReference*. Adicionalmente temos o *WS-PolicyAttachment*, que permite que as políticas sejam anexadas diretamente dentro de um documento XML. Não é necessário que a especificação do recurso e da política esteja dentro do mesmo documento XML.

A especificação associada, o **WS-SecurityPolicy**, apresenta os mecanismos de como os atores dos Serviços Web podem utilizar as políticas, que incluem direitos e *capabilities*.

C.5. O WS-Trust

O *WS-Trust* é uma especificação que permite a interoperabilidade dos múltiplos formatos de *tokens* de segurança e/ou autenticação, definindo um protocolo do tipo *request/response*. Para tal, é utilizada uma terceira entidade confiável, o STS (*Security Token Service*), que produz o intercâmbio de confiança para o acesso de um *principal* aos recursos de cada entidade/serviço.

O *WS-Trust* agrega, no cabeçalho de segurança de uma mensagem SOAP, três relações que são objeto de emissão/troca de *tokens* de segurança pelo STS a solicitações de *principals*. São elas:

Formato (*Format*): o receptor de uma mensagem SOAP pode receber uma mensagem com a sintaxe do *token* incompatível, ou seja, ele recebe um *token* de autenticação baseado em *tickets Kerberos*, porém ele só trata certificados X.509;

Confiança (*Trust*): o receptor pode não ter condições de estabelecer uma relação de confiança de forma autônoma para conversão de *tokens*;

Espaço de nomes (*Namespace*): o receptor pode não compreender um conjunto de diretivas que se encontram no *token*, visto as diferenças de sintaxe.

Assim, para que seja feita a troca de um *token* a partir da relação de confiança provida pelo STS entre serviços/entidades distintas, o protocolo request/response é utilizado da seguinte forma: um *principal* envia um *RequestSecurityToken* (e que contém o *token* na qual se deseja trocar) para o STS e este responde com um *RequestSecurityTokenResponse* (que contém o novo *token* que seja confiável/compatível com o serviço/recurso que o *principal* deseja acessar). A figura C.3 ilustra o procedimento protocolar de um *principal* que solicita um *token* ao STS que mantém uma relação de confiança como serviço. Após a posse do *token*, o *principal* solicita ao serviço o acesso ao recurso, utilizando o *token* obtido via STS.

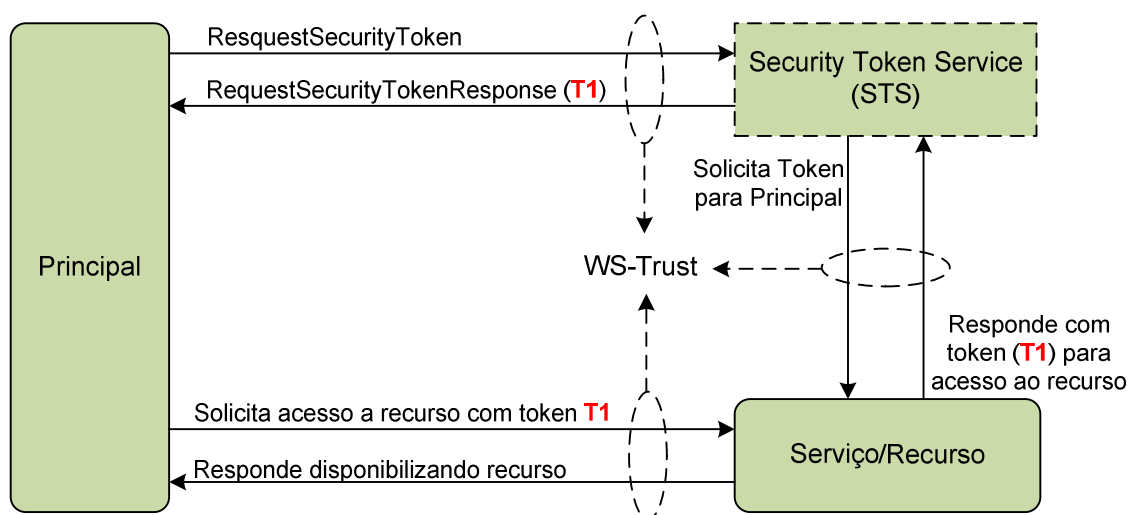


Figura C.3: Protocolo Request/Response do STS

C.6. O XML Key Management Specification

O XKMS (*XML Key Management Specification*) é uma especificação do W3C (*World Wide Web Consortium*) e compreende um protocolo com funções de validação, registro e distribuição de chaves públicas para o suporte a documento XML. O XKMS se subdivide em duas outras entidades: o X-KISS (*XML Key Information Service Specification*) e o X-KRSS (*XML Key Registration Service Specification*).

O X-KISS provê mecanismos para localização e validação de chaves associados a documentos XML assinados e cifrados. O X-KRSS provê mecanismo para o registro, emitir/re-emitir, revogar e recuperar chaves com base em certificados no padrão X.509. Nesse contexto, o XKMS se apresenta como uma Infra-Estrutura de Chaves Pública (ICP) associada às chaves utilizadas nas especificações *XML-DSig* e *XML-Enc*.

C.7. O WS-AtomicTransaction

A especificação *WS-Atomic Transaction* indica os mecanismos para transações atômicas em Serviços Web e está subordinada ao grupo *WS-Coordination*. A especificação define três protocolos de coordenação, de acordo com os tipos específicos de transação atômica a ser realizada: a completa, a com *commit* volátil de duas fases e a com *commit* não-volátil de duas fases.

Essa especificação se direciona para o uso de aplicações que são executadas em ambientes distribuídos e mecanismos transacionais atômicos que se fazem necessários, de forma a garantir a integridade e correteza dos dados.

O protocolo para transação **Completa** consiste em processar o *commit* com base nos participantes que se encontram registrados em cada protocolo, ou seja, o coordenador inicia com *commit* volátil de duas fases e depois com *commit* durável de duas fases, e o resultado final é enviado a quem iniciou a transação.

De forma geral, os protocolos com *commit* de duas fases consistem nos participantes registrados efetuarem o *commit* ou abortar, de forma a assegurar que todos os participantes conheçam o resultado final, conforme variações abaixo:

- **Commit volátil de duas fases:** os participantes gerenciam os recursos voláteis num registro em *cache*;
- **Commit não-volátil de duas fases:** os participantes gerenciam os recursos não-voláteis num banco de dados.

O protocolo permite que um participante possa se registrar em mais de um protocolo.

