

Estudo dos Requisitos para um Sistema de Votação Electrónica

RUI ROCHA PINTO

FILIPE SIMÕES

PEDRO ANTUNES

DI-FCUL

TR-04-2

MARÇO 2004

Departamento de Informática
Faculdade de Ciências da Universidade de Lisboa
Campo Grande, 1700 Lisboa
Portugal

Technical reports are available at <http://www.di.fc.ul.pt/tech-reports>. The files are stored in PDF, with the report number as filename. Alternatively, reports are available by post from the above address.

SUMÁRIO

1. INTRODUÇÃO	4
1.1. OBJECTIVOS	4
2. PROPRIEDADES DO SISTEMA DE VOTAÇÃO ELECTRÓNICO	5
3. SISTEMA	8
4. SUBSISTEMAS	
4.1. RECENSEAMENTO DE ELEITORES	9
4.2. VOTAÇÃO	9
4.3. CONTAGEM	9
5. ACTORES	
5.1. AUDITOR	10
5.2. ELEITOR	10
5.3. MEMBRO DA MESA ELEITORAL	10
5.4. MEMBRO OFICIAL	10
5.5. POTENCIAL ELEITOR	10
5.6. PÚBLICO EM GERAL	10
5.7. RECENSEADOR	10
5.8. RESPONSÁVEL PELO ESTABELECIMENTO PÚBLICO	10
5.9. SERVIDOR DE ELEITORES	11
5.10. SERVIDOR DE RESULTADOS	11
5.11. SERVIDOR DE VOTAÇÃO	11
6. DIAGRAMA DE CONTEXTO	
6.1. SISTEMA DE VOTAÇÃO ELECTRÓNICA - NÍVEL 1	12
6.2. SISTEMA DE VOTAÇÃO ELECTRÓNICA - NÍVEL 2	13
6.3. RECENSEAMENTO DE ELEITORES	13
6.4. VOTAÇÃO	14
6.5. CONTAGEM	14
7. CASOS DE USO	
7.1. RECENSEAMENTO DE ELEITORES	15
7.1.1. <u>Recenseamento de Eleitores – Remoto</u>	15
7.1.2. <u>Recenseamento de Eleitores – Presencial</u>	17
7.2. VOTAÇÃO	18
7.2.1. <u>Votação - Via Acesso Remoto</u>	18
7.2.2. <u>Votação – Local Público</u>	19
7.2.3. <u>Votação – Recinto Controlado</u>	20
7.3. CONTAGEM	21
8. DIAGRAMAS DE SEQUÊNCIA	
8.1. RECENSEAMENTO DE ELEITORES – REMOTO	22
8.2. RECENSEAMENTO DE ELEITORES – PRESENCIAL	23
8.3. VOTAÇÃO – VIA ACESSO REMOTO	24
8.4. VOTAÇÃO – LOCAL PÚBLICO	25
8.5. VOTAÇÃO – RECINTO CONTROLADO	26
8.6. CONTAGEM	27
9. DIAGRAMAS DE COLABORAÇÃO	
9.1. RECENSEAMENTO DE ELEITORES – REMOTO	28
9.2. RECENSEAMENTO DE ELEITORES – PRESENCIAL	28
9.3. VOTAÇÃO – ACESSO REMOTO	29
9.4. VOTAÇÃO – LOCAL PÚBLICO	30
9.5. VOTAÇÃO – RECINTO CONTROLADO	31
9.6. CONTAGEM	32

10. DIAGRAMA DE INSTALAÇÃO	
10.1. RECENSEAMENTO DE ELEITORES	33
10.2. VOTAÇÃO - ACESSO REMOTO	33
10.3. VOTAÇÃO - LOCAL PÚBLICO	34
10.4. VOTAÇÃO - RECINTO CONTROLADO	35
11. DIAGRAMA DE ROBUSTEZ	
11.1. RECENSEAMENTO DE ELEITORES	36
11.2. VOTAÇÃO	36
11.3. CONTAGEM	36
12. DIAGRAMA DE CLASSES	37
13. REALIZAÇÕES	
13.1. RECENSEAMENTO DE ELEITORES	38
13.2. VOTAÇÃO	38
13.3. CONTAGEM	39
14. PROPRIEDADES VS RECINTOS DE VOTAÇÃO	40
15. BIBLIOGRAFIA	41

1. INTRODUÇÃO

Os Sistemas de Votação Electrónica (SVE) são sistemas que, quer pelas suas características e limitações quer pelo seu impacto social, estão actualmente em estudo e desenvolvimento intensivos em todo o mundo, encontrando-se já em utilização em alguns países, contudo com algumas limitações [10].

São de certo modo nobres os objectivos que levam ao desenvolvimento de SVE, sobretudo após um decréscimo significativo do interesse na participação em processos eleitorais que se tem vindo a verificar nas democracias ocidentais [6] [10].

Proporcionar um aumento das oportunidades de voto (maior número de lugares onde se torna possível exercer o direito de voto e não obrigatoriedade de o eleitor se apresentar em determinado local), redução de votos “nulos” não intencionais, maior rapidez e exactidão na contagem dos votos, etc., são alguns dos objectivos de qualquer SVE.

Apesar de concordamos que esta questão trata da aplicação de tecnologia já existente a um processo corrente nos nossos dias em democracia, deve-se dar redobrada ênfase de que deverá sempre ser mantida, ou mesmo reforçada, a confiança dos eleitores e do público em geral em todo o processo de introdução desta tecnologia.

Do ponto de vista da ciência informática, a questão fundamental que se coloca está em identificar qual a combinação optima entre tecnologia e processos sociais que garanta um conjunto muito vasto de propriedades que a sociedade considera como adquiridas relativamente ao processo de votação. Os desafios são portanto inúmeros, desde a necessidade de garantir que um SVE funciona em grande escala, sem problemas de fiabilidade e segurança que coloquem uma votação em causa; que o sistema será capaz de garantir o aumento das oportunidades de voto e ao mesmo tempo o anonimato, a integridade dos votos e outras propriedades; que o sistema será acessível e utilizável por uma imensa diversidade de pessoas; e, finalmente, que o sistema e processos eleitorais serão facilmente compreensíveis para os utilizadores comuns e entidades administrativas e políticas.

Este relatório pretende constituir apenas um contributo parcial e preliminar na abordagem a este problema. Em concreto, pretende-se identificar, a partir da revisão do estado da arte, quais são as propriedades requeridas para os SVE e, em seguida, identificar um conjunto de elementos arquitecturais e colaborações entre objectos que permitem garantir essas propriedades.

1.1. OBJECTIVOS

Este relatório analisa as propriedades inerentes a um SVE, sendo complementado com um conjunto de esquemas desenvolvidos na linguagem UML que descrevem os diversos subsistemas e processos que compõem o sistema global, de forma a tentar contribuir tecnicamente para um estudo mais detalhado dos requisitos exigidos a um SVE.

Este relatório irá numa primeira fase identificar as propriedades que são recomendadas pela literatura relacionada para estudo e elaboração de um SVE.

O sistema apresentado neste relatório será subdividido em três subsistemas: recenseamento de eleitores, votação e contagem.

Serão analisados todos os actores envolvidos no sistema e esquematizados os diagramas de contexto.

O sistema permitirá o recenseamento remoto (“via Internet”) ou presencial de eleitores, e a votação poderá ser efectuada de três formas distintas: presencial e controlada, presencial num local público e remotamente.

O documento irá permitir estudar, através de descrições em UML, os diversos CASOS DE USO identificados e respectivos DIAGRAMAS DE SEQUÊNCIA, de COLABORAÇÃO, de INSTALAÇÃO, de ROBUSTEZ e de CLASSES, cruzando no final as propriedades desejáveis aos SVE com os diversos tipos de votação em estudo.

2. PROPRIEDADES DE UM SISTEMA DE VOTAÇÃO ELECTRÓNICA

Um SVE deve garantir, além das propriedades inerentes ao processo eleitoral tradicional, mais um conjunto de propriedades justificadas pela sua implementação utilizando sistemas electrónicos.

O que se descreve seguidamente são todas as propriedades discutidas na literatura a que o sistema proposto deve obedecer para cada um dos tipos de votação: presencial e controlado, presencial num local público e remotamente.

Anonimato [2] [3] [9] [11]

A associação entre o voto e a identidade do eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam manutenção do sistema) quer após a votação (mesmo que por ordem judicial).

Auditabilidade [2] [3] [6] [8]

O sistema deverá poder ser auditado quer por observadores externos – através por exemplo da análise do registo de logs, quer pelo próprio sistema – com a confrontação dos diversos dados.

Autenticação do Operador [2] [3]

Os utilizadores autorizados a operar o sistema devem ter mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjunção de alguns dos tipos de autenticação existentes (Smartcard + PIN + Password, ou ainda autenticação bio-métrica – impressões digitais, retina ocular, voz, etc).

Autenticidade [2]

Autenticar o indivíduo é o meio pelo qual a identificação de um votante é validada e confirmada. Apenas os eleitores autorizados devem poder votar.

Exemplos de tipos de autenticação são [10]: Presencial, PIN, Password, Certificados Digitais, Smartcard, bio-métrica.

Certificabilidade [2]

O sistema deve poder ser testado e certificado por agentes oficiais.

Confiabilidade [2] [3] [5] [6] [8]

O SVE deve funcionar de forma robusta, sem perda de votos, tornando-se confiável ao olhos dos diversos actores que nele participam.

Conveniência [1] [2] [4] [6] [8] [9]

O sistema só será útil se permitir aos votantes exercerem o seu direito de voto de forma rápida, com o mínimo de equipamento, treino e sem necessidades específicas adicionais.

Detectabilidade

O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.

Direito de Voto

O Direito de Voto será atribuído a um eleitor sempre que ele verifique simultaneamente as propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de ele poder votar.

Disponibilidade do Sistema [2] [3]

O SVE deve estar sempre disponível durante o período eleitoral, para que o processo decorra normalmente.

Documentação [2]

Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema deve estar documentado, devendo não conter ambiguidades e ser coerente.

Flexibilidade [1] [2] [4] [7] [9]

Os equipamentos de votação que fazem parte do SVE devem suportar uma variedade de questões relacionadas com o processo de votação, com por exemplo a utilização por pessoas com necessidades especiais, etc.

Integridade do Pessoal [3]

O pessoal envolvido no projecto, implementação, administração e operação do SVE deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.

Integridade do Sistema [2] [3]

O sistema deve poder ser posto à prova, depois de validado e certificado por auditores externos.

Integridade dos Votos [3] [9]

Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.

Invulnerabilidade [4]

A invulnerabilidade do SVE é garantida se se verificarem as condições de Autenticidade e Singularidade.

Mobilidade [1] [4]

O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.

Não-Coercibilidade [1] [2] [7] [10]

O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.

Precisão [3]

As eleições podem ser decididas por apenas um voto. O sistema não pode tolerar margens estatísticas de erro durante a sua operação. Até o erro involuntário de um eleitor, mal treinado para votar em dado equipamento, pode inverter ou modificar o resultado eleitoral.

Privacidade [2] [4] [7] [8] [11] [13]

O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.

Rastreabilidade

O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir “logs” de entrada e saída de utilizadores, bem como registos do envio e recepção de dados, que obviamente não comprometam as restantes propriedades (Anonimato e Privacidade).

Recuperabilidade

O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.

Singularidade (Não Reutilização) [2]

O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.

Tolerância a Ataques [3] [5] [12]

A principal característica que diferencia um SVE de outros sistemas de alto risco é que este poderá ser alvo privilegiado de ataques mal intencionados. Medidas de defesa contra fraudes, inclusive vindas dos próprios agentes que projectaram e desenvolveram o sistema, devem ser rigorosas e redundantes.

Tolerância a Falhas [3]

É desejável a existência de métodos de detecção de falhas no equipamento. A troca de um bit num total de um candidato pode ser a diferença entre ganhar ou perder a eleição.

Transparência do Processo [2] [7] [12]

Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.

Transparência do Sistema [2] [3]

Todo o software, documentação, equipamento, micro-código e circuitos especiais devem poder ser abertos para inspecção e auditoria a qualquer instante.

Usabilidade [2] [3]

O sistema deve ser de fácil uso quer para eleitores quer para operadores.

Viabilidade (Custo/Benefício) [6] [7]

O SVE deve ser eficiente e viável economicamente.

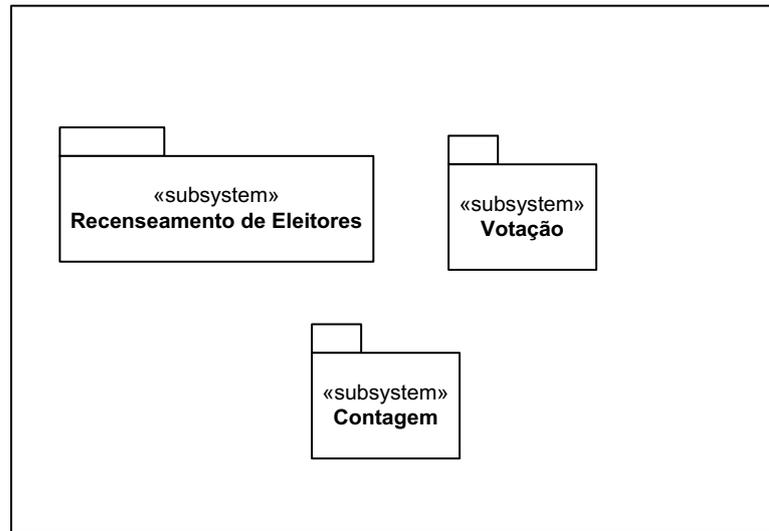
Verificabilidade [1] [2] [4] [7] [8] [11] [13]

O sistema deve permitir a verificação de que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a Autenticidade dos registos dos votos sem no entanto quebrar outras propriedades como o Anonimato ou a Privacidade.

3. SISTEMA

O SVE em estudo decompõe-se em 3 subsistemas que constituem todo o edifício eleitoral:

- Recenseamento de Eleitores;
- Votação;
- Contagem.



Os subsistemas que constituem todo o sistema serão descritos e desenvolvidos nos capítulos seguintes.

4. SUBSISTEMAS

4.1. RECENSEAMENTO ELEITORAL

O subsistema de “Recenseamento Eleitoral” realiza o registo pr vio de Eleitores, uma funcionalidade que   equivalente ao processo de recenseamento das pessoas que perfazem as condi es de serem eleitoras. Este registo   obrigat rio sendo fornecido ao eleitor recenseado um mecanismo de comprova o, que pode consistir num cart o de eleitor, Smartcard, envelope com um c digo de acesso ao processo de vota o (PIN, ou Password) ou qualquer outra forma de identifica o de forma inequ voca perante o SVE ou membro da mesa eleitoral (cf. mais abaixo), nomeadamente atrav s de caracter sticas bio-m tricas.

O recenseamento (registo) dos eleitores pode ser realizado presencialmente (por exemplo numa Junta de Freguesia) ou atrav s de um processo remoto (por exemplo atrav s de uma interface disponibilizada via Internet).

4.2. VOTA O

O subsistema de “Vota o” realiza o processo de vota o propriamente dito. Este subsistema dever  permitir a identifica o do eleitor, valida o de condi es de vota o (Autenticidade e Singularidade) e, caso possa votar, o sistema disponibiliza uma interface onde o eleitor escolhe a sua op o de voto.

Neste documento ser  estudado o caso da vota o electr nica em tr s ambientes distintos:

- Presencial e em recinto controlado:

Os eleitores ter o a possibilidade de votar presencialmente em recinto controlado,   semelhan a do que hoje acontece, mas substituindo o voto em papel por outro em formato electr nico;

- Presencial e em local p blico:

Os eleitores poder o exercer o seu direito de voto num local p blico pr -determinado (quiosques, super-mercados, lojas do CTT ou outras ou salas/locais preparadas para o efeito);

- Via acesso remoto:

Os eleitores poder o votar remotamente, ou seja, atrav s da Internet a partir de qualquer ponto onde seja poss vel o acesso ao SVE.

4.3. CONTAGEM

O subsistema de “Contagem” tem como finalidade o apuramento e contagem de todos os votos, bem como a publica o e divulga o dos seus resultados.

5. ACTORES

Os actores representam todos os utilizadores que interagem com o SVE. No entanto um actor não é necessariamente um utilizador no sentido restrito de termo – pessoa que utiliza o sistema – podendo ser um equipamento informático, como por exemplo um servidor.

5.1. AUDITOR

Elemento/equipamento/serviço/entidade que tem como objectivo auditar em cada momento as transacções que estão a decorrer no SVE, ou seja, registar todos os eventos pertinentes para o sistema (acessos, envio/recepção de dados, criação de novos registos, alteração de dados, etc.) para que a informação registada permita detectar deficiências de funcionamento e/ou a presença de eventuais erros.

5.2. ELEITOR

Os eleitores são as pessoas previamente registadas no sistema, ou seja, qualquer pessoa com condições de participar no acto eleitoral para o qual o SVE está preparado. Caso as pessoas tenham direito a participar no processo eleitoral mas não estejam registadas no SVE não poderão exercer o seu direito.

5.3. MEMBRO DA MESA ELEITORAL

Elemento nomeado pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, com o objectivo de verificar a autenticidade dos eleitores no processo de votação presencial em recinto controlado.

5.4. MEMBRO OFICIAL

Elemento designado pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, para acompanhar o processo de contagem, publicação e divulgação dos resultados eleitorais.

5.5. POTENCIAL ELEITOR

Todo o cidadão que esteja em condições legais para participar no processo eleitoral e que pretenda registar-se como Eleitor, para posteriormente exercer o seu direito de voto.

5.6. PÚBLICO EM GERAL

Todos os interessados (órgãos de comunicação social, partidos políticos, candidatos, população, etc.) na obtenção dos resultados parciais/finais de um processo de votação.

5.7. RECENSEADOR

Elementos, nomeados pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, com o objectivo de poderem aceder ao sistema para efectuar presencialmente o Recenseamento de Eleitores.

5.8. RESPONSÁVEL PELO ESTABELECIMENTO PÚBLICO

Elementos responsáveis pelos diversos estabelecimentos públicos, onde se poderá exercer o direito de voto presencial em lugar público.

5.9. SERVIDOR DE ELEITORES

Equipamento informático onde permanecerão armazenados os dados que constituem a identificação de todos os eleitores recenseados, bem como se já efectuou a votação num determinado acto eleitoral, com o objectivo de não poder efectuar novamente a votação (Não Reutilização). Poderá existir mais do que um servidor de eleitores, sendo que todos eles não são mais que “espelhos” do servidor de eleitores inicial. Esta técnica deve ser utilizada para evitar o congestionamento do servidor e por questões de mobilidade, disponibilidade do sistema, tolerância a faltas e tolerância a ataques.

5.10. SERVIDOR DE RESULTADOS

Equipamento informático onde ficarão armazenados os resultados apurados do processo eleitoral. Poderá existir mais do que um servidor de resultados, sendo que todos eles não são mais que “espelhos” do servidor de resultados inicial. Esta técnica deve ser utilizada para evitar o congestionamento do servidor e por questões de disponibilidade do sistema, tolerância a faltas e tolerância a ataques.

5.11. SERVIDOR DE VOTAÇÃO

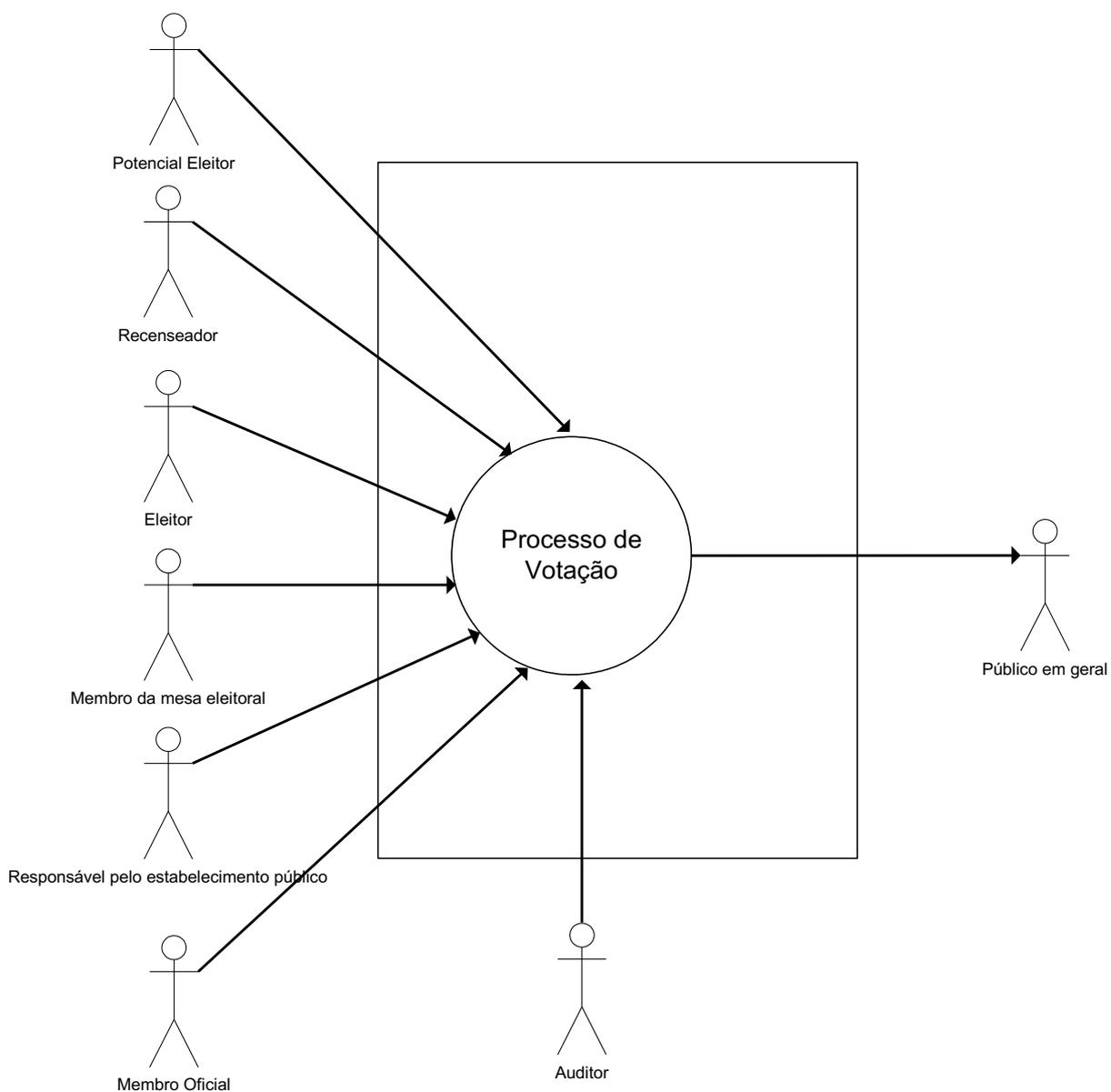
Equipamento informático onde permanecerão armazenados os dados que constituem os votos de cada eleitor, de uma forma perfeitamente anónima. É com base nestes dados que se efectuará o processo de contagem dos votos. Poderá existir mais do que um servidor de votação, seja por razões de decomposição ou hierarquização (por exemplo, em locais de voto) seja por questões de disponibilidade do sistema, tolerância a faltas e tolerância a ataques.

6. DIAGRAMA DE CONTEXTO

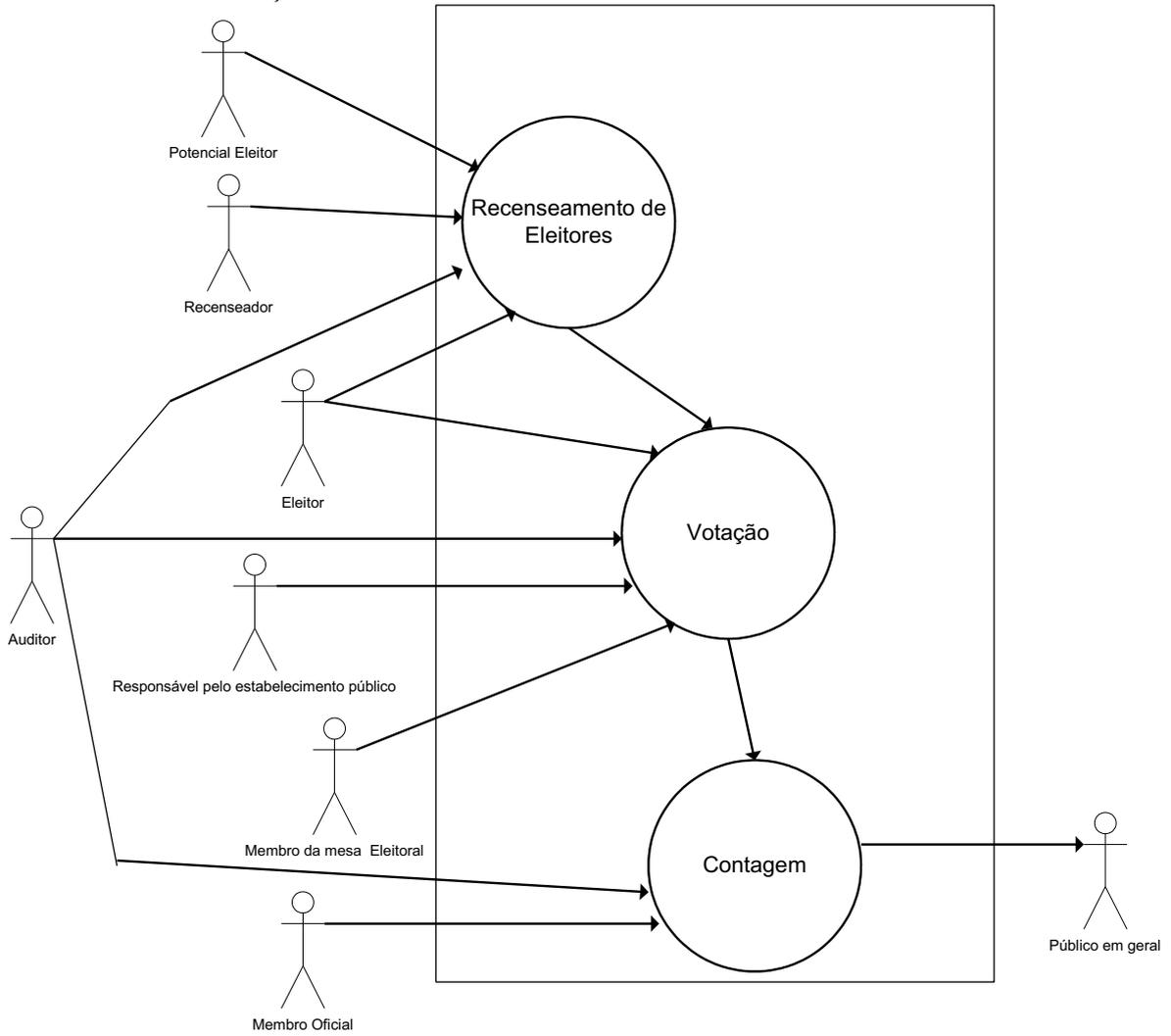
O Diagrama de Contexto pretende ilustrar, de uma forma bastante generalista mas objectiva, o contexto em que o SVE está inserido. São assim apresentados os seguintes diagramas:

- Sistema de Votação Electrónica - Nível 1
- Sistema de Votação Electrónica - Nível 2
- Recenseamento de Eleitores
- Votação
- Contagem

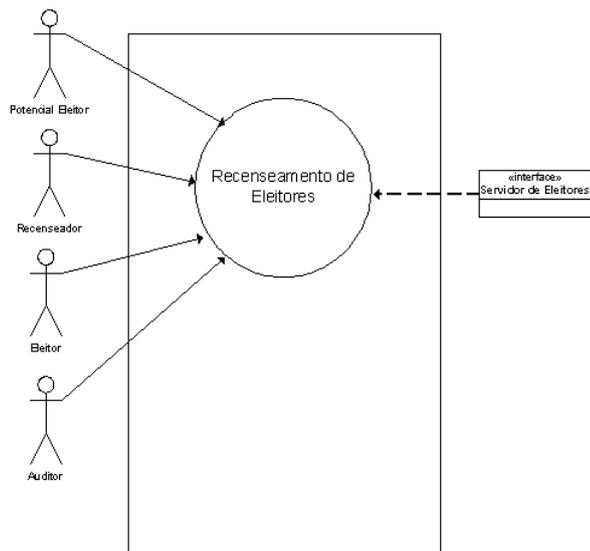
6.1. SISTEMA DE VOTAÇÃO ELECTRÓNICA - NÍVEL 1



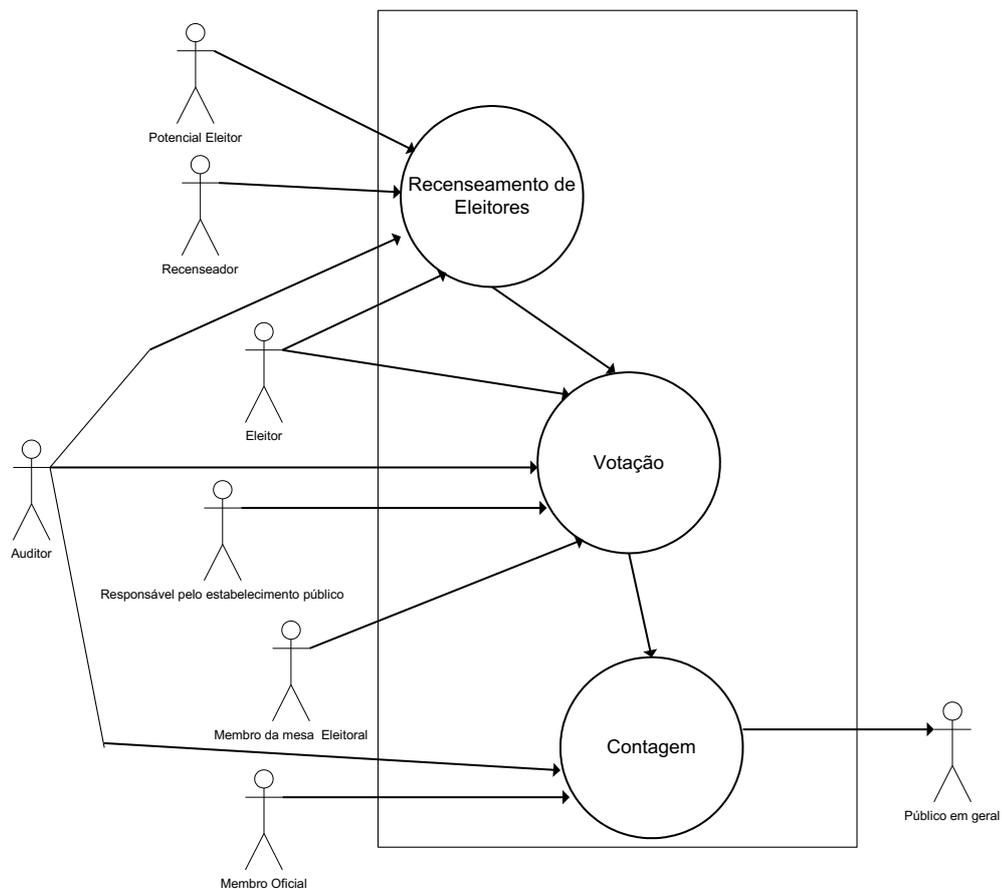
6.2. SISTEMA DE VOTAÇÃO ELECTRÓNICA - NÍVEL 2



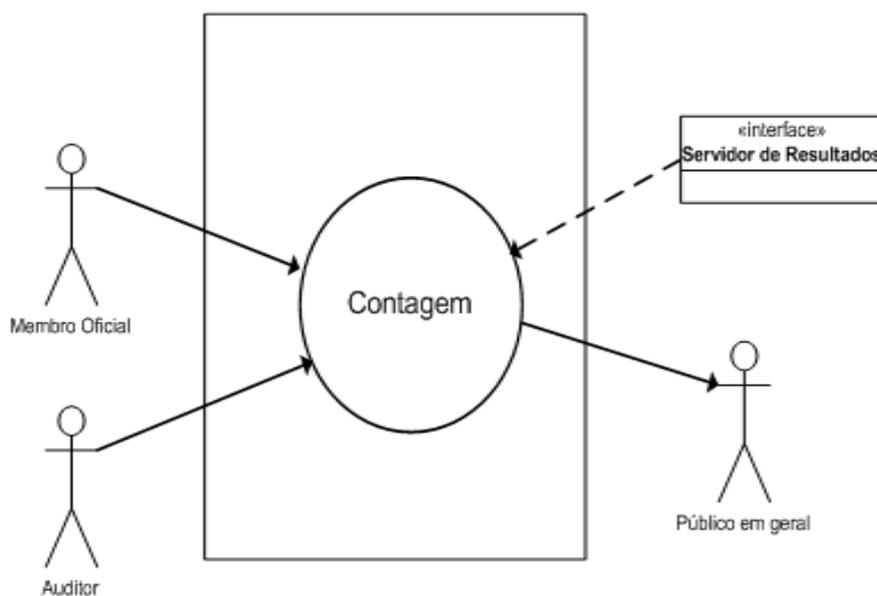
6.3. RECENSEAMENTO DE ELEITORES



6.4. VOTAÇÃO



6.5. CONTAGEM



7. CASOS DE USO

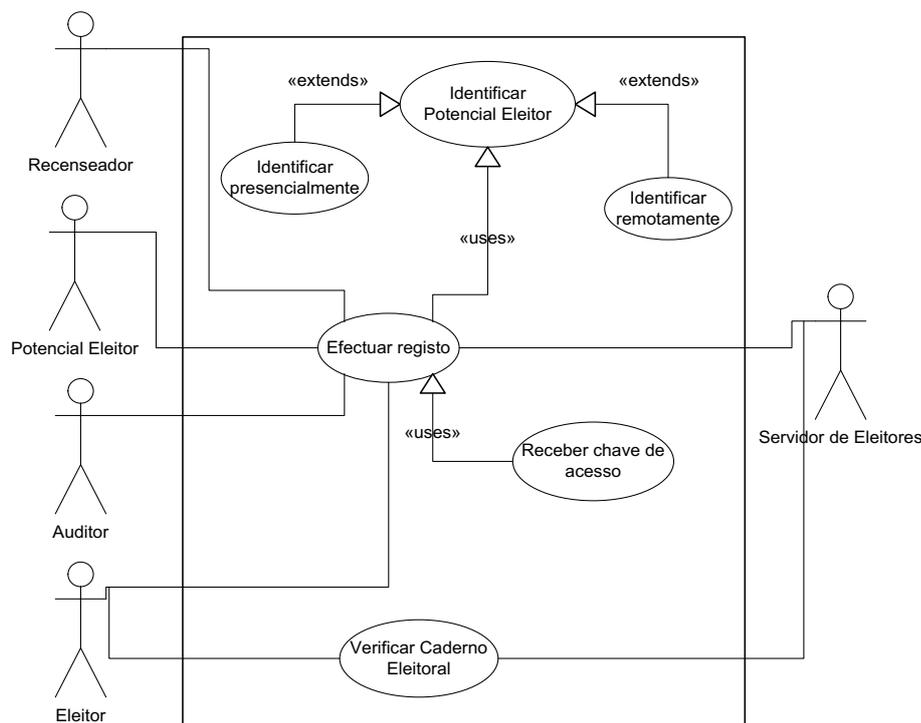
Os Diagramas de Casos de Uso são utilizados para identificar as fronteiras do sistema e descrevem quais os serviços que devem ser disponibilizados aos utilizadores (Actores). São apresentados os seguintes Diagramas de Casos de Uso:

- Recenseamento de Eleitores
 - Recenseamento de Eleitores – Remoto
 - Recenseamento de Eleitores – Presencial
- Votação
 - Votação – Recinto Controlado
 - Votação – Local público
 - Votação – Via Acesso Remoto
- Contagem

7.1. RECENSEAMENTO DE ELEITORES

O subsistema “Recenseamento do Eleitores” permite que se possam recensear pessoas com capacidade legal de poder exercer, em período eleitoral, o seu direito de voto. Consideram-se duas formas de se efectuar o recenseamento: presencial, em local especificado para o efeito (por exemplo, Juntas de Freguesia, Câmaras Municipais, etc.), sendo neste caso o registo executado com o auxílio de um recenseador (funcionário autárquico com competência para tal), ou remotamente através de uma interface específica para o efeito, disponibilizada através da Internet.

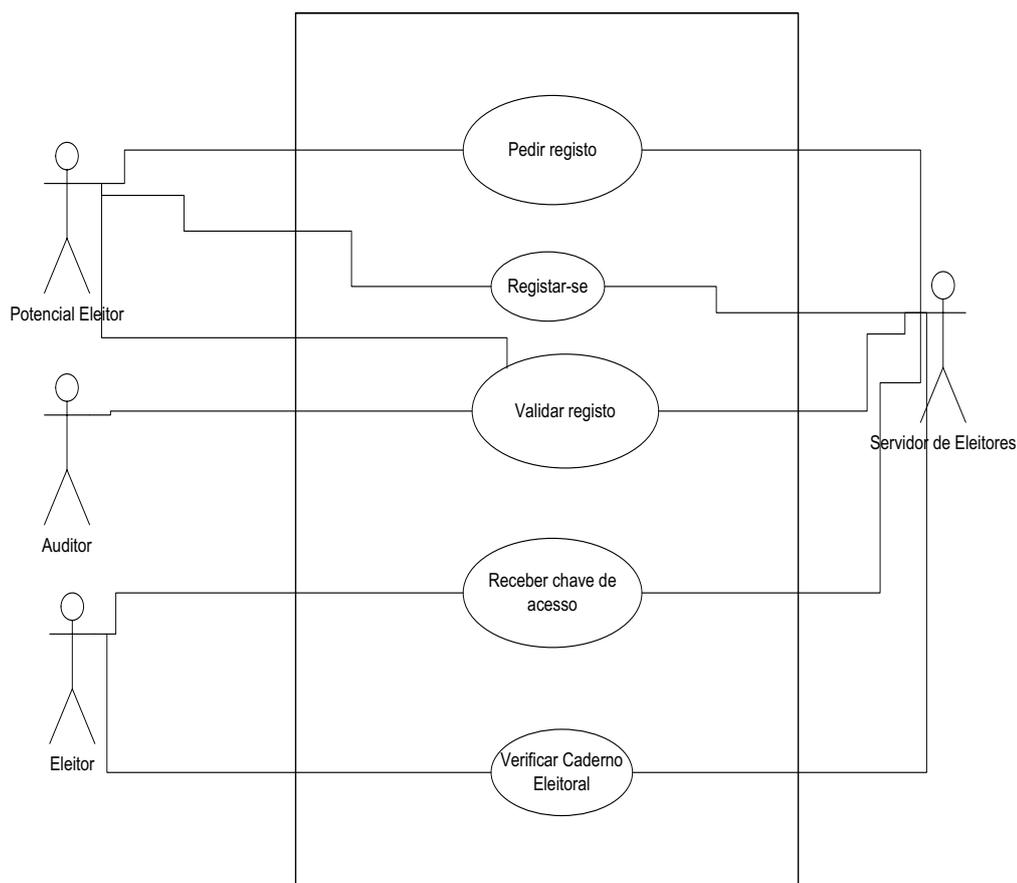
Neste diagrama, mais abrangente, podemos apresentar todos os “Actores” envolvidos no subsistema.



7.1.1. Recenseamento de Eleitores – Remoto

O subsistema “Recenseamento de Eleitores – Remoto” é um processo suportado por um Servidor de Eleitores ao qual é solicitado remotamente – via Internet – um pedido de registo por parte de pessoas com capacidade legal de serem eleitores, sendo-lhes disponibilizado uma interface gráfica para que possam efectuar esse registo.

O processo é concluído com a validação dos dados e com a recepção, por parte do eleitor, de um mecanismo de acesso ao sistema, para posterior participação no processo de votação.

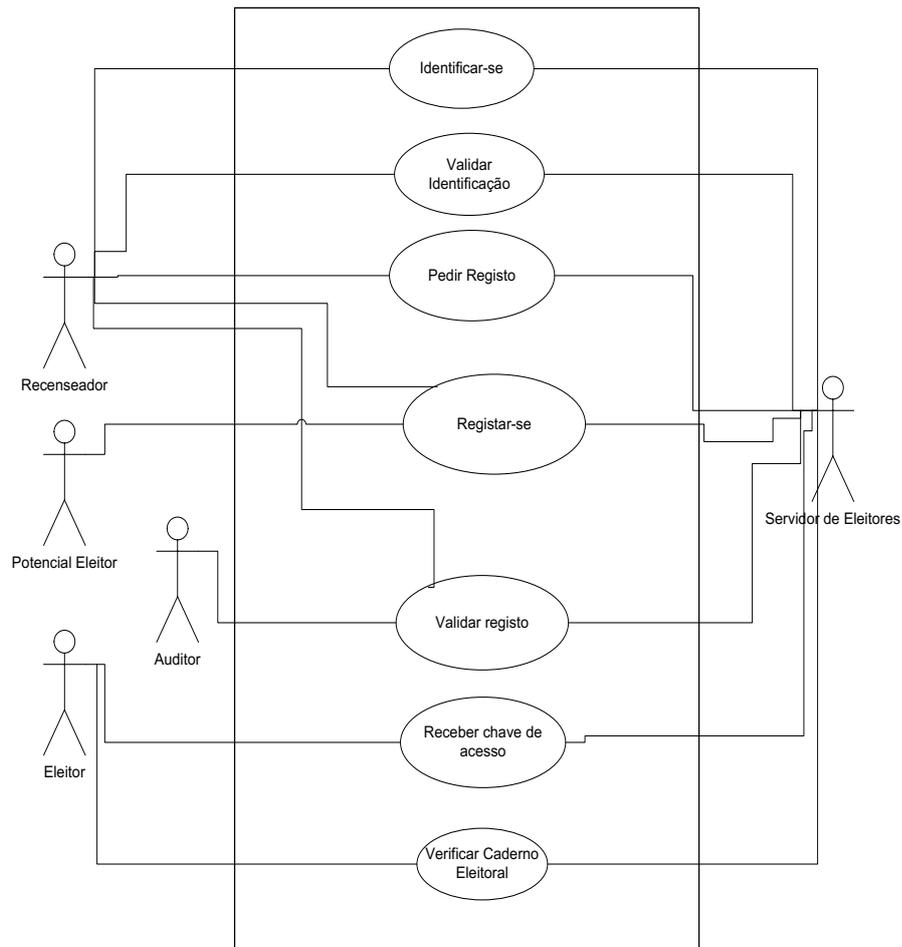


7.1.2. Recenseamento de Eleitores - Presencial

O subsistema “Registo de Eleitores - Presencial” é um processo suportado por um Servidor de Eleitores em que um intermediário (Recenseador) solicita um pedido de registo para pessoas com capacidade legal de serem eleitores, sendo-lhe disponibilizada uma interface gráfica para que possa ser efectuar o registo.

Este processo é sempre utilizado quando o registo de eleitores (recenseamento eleitoral) tenha que ser feito de forma presencial, utilizando-se para tal o “actor” Recenseador (que poderá, por exemplo, ser um funcionário autárquico com competência para tal).

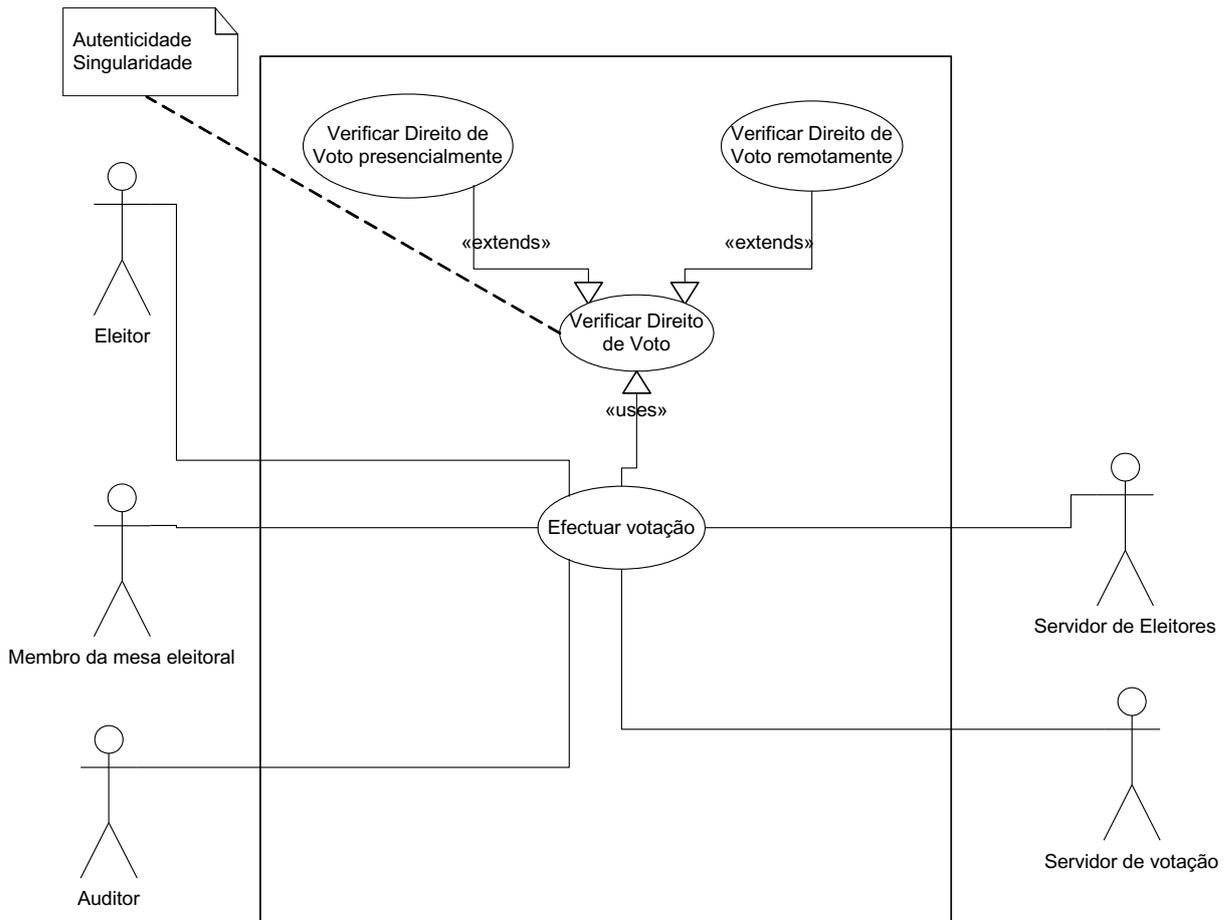
O processo é concluído com a validação dos dados e com a recepção, por parte do eleitor, de um mecanismo de acesso ao sistema para posterior participação no processo de votação.



7.2. VOTAÇÃO

O subsistema “Votação” realiza o processo em que os eleitores podem exercer o seu direito de voto. Esse direito pode ser exercido de forma presencial – em local público ou recinto controlado – ou de forma remota – a partir de qualquer ponto com acesso remoto ao SVE. Em qualquer dos casos, só após a verificação de que os eleitores estão aptos a exercer o seu direito de voto é que o sistema disponibilizará os mecanismos para que o mesmo se realize.

A entrega do boletim de voto compreende a fase de anonimização do voto, ou seja, a fase do processo de votação em que o voto seleccionado é separado do seu autor, verificando assim as propriedades de anonimato, privacidade e não rastreabilidade, tendo como objectivo não se poder, futuramente, associar o voto ao votante.

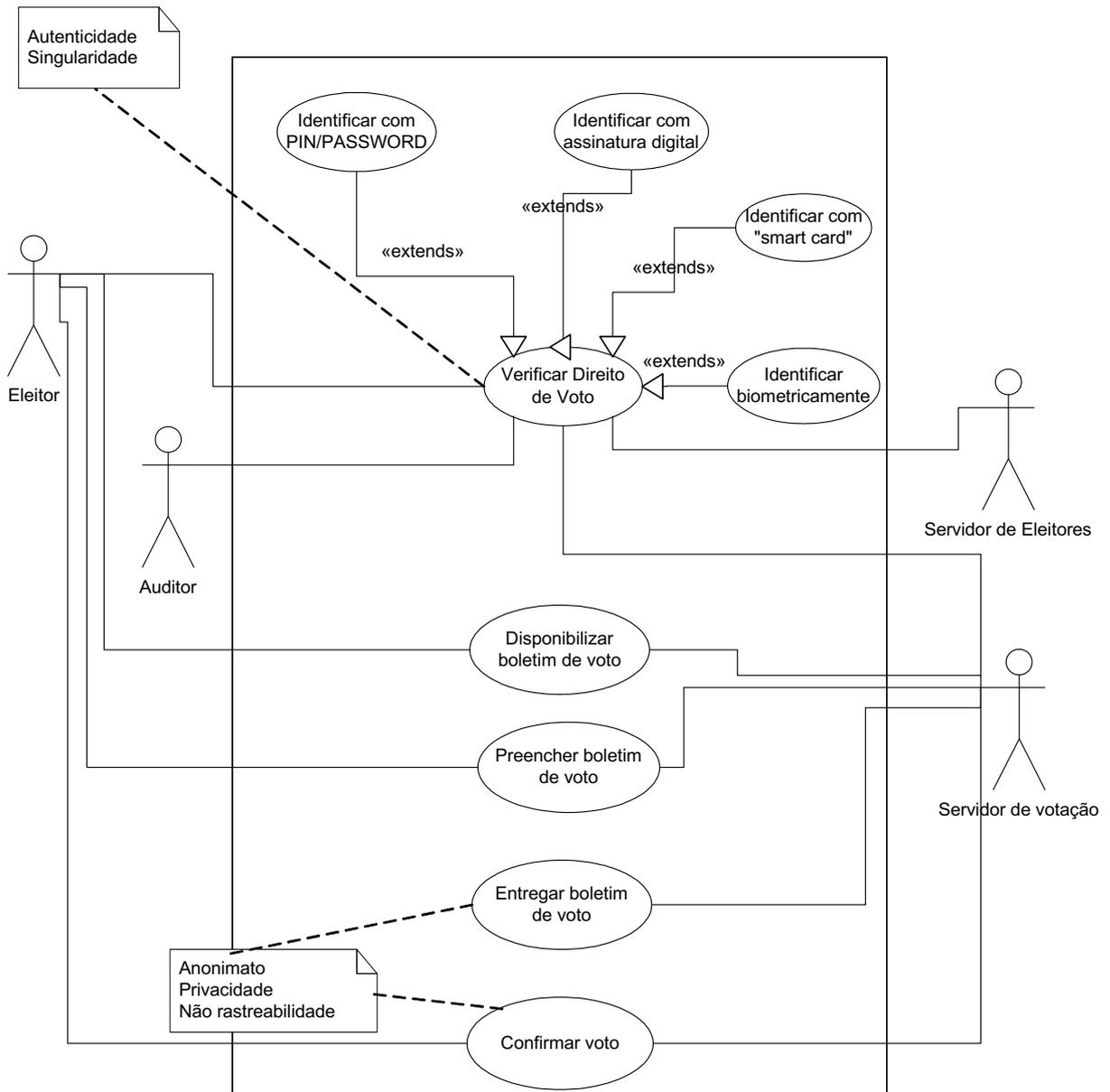


7.2.1. Votação – Via Acesso Remoto

No subsistema “Votação – Via Acesso Remoto” os eleitores terão que se identificar ao sistema, que verificará se podem exercer o seu direito de voto. Das diversas formas de identificação perante o sistema podemos salientar: PIN/Password, Assinatura Digital, Smartcard ou dados bio-métricos.

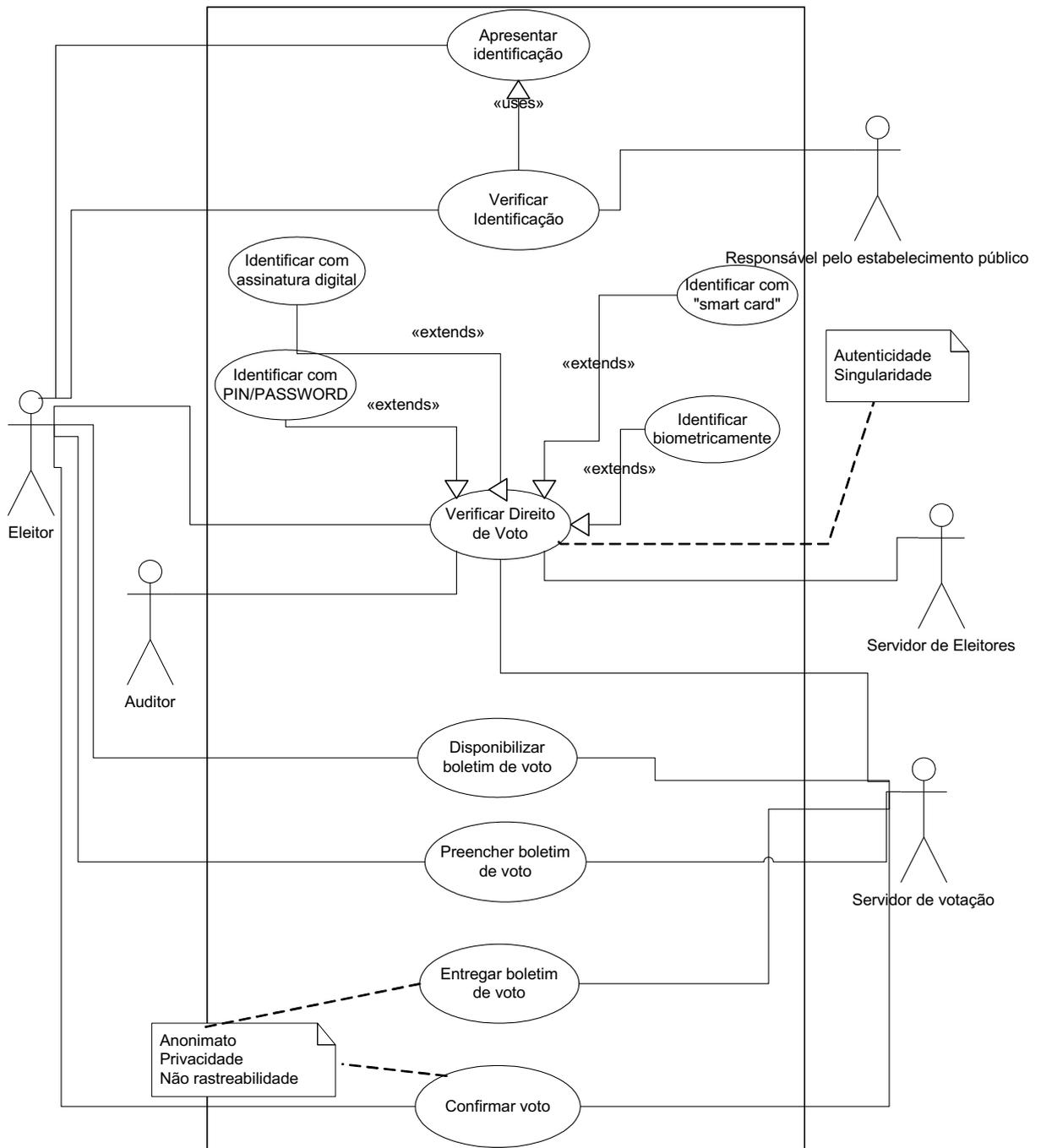
Depois de verificados todos os requisitos, é disponibilizada uma interface gráfica com o boletim de voto que o eleitor preenche e envia (de forma semelhante à entrega do voto em papel).

A entrega do boletim de voto compreende a fase de anonimização do voto, ou seja, a fase do processo de votação em que o voto (opção escolhida pelo eleitor) é separado do seu autor, verificando assim as propriedades de anonimato, privacidade e não rastreabilidade do voto.



7.2.2. Votação – Local Público

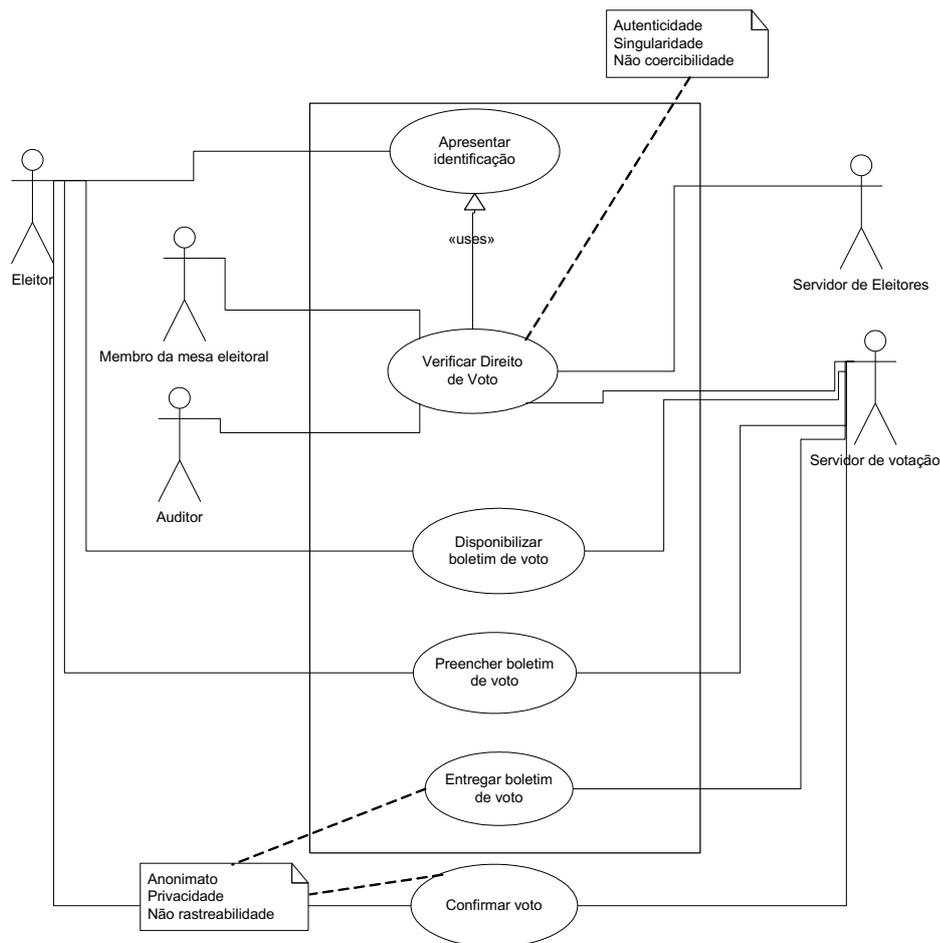
No subsistema “Votação – Local Público” os eleitores terão à sua disposição, em locais públicos (quiosques, Loja do Cidadão, lojas dos CTT, supermercados, etc.) mecanismos de acesso ao SVE onde poderão exercer o seu direito de voto. Neste caso, o votante terá apenas que se identificar junto do responsável pelo local público para que possa proceder ao voto. O processo de verificação e validação do eleitor é a partir deste instante igual ao subsistema “Votação – Via Acesso Remoto”.



7.2.3. Votação – Recinto Controlado

No subsistema “Votação – Recinto Controlado” os eleitores terão que se identificar junto do Membro da Mesa Eleitoral ao qual compete verificar a identidade do eleitor e confirmar a sua condição de eleitor.

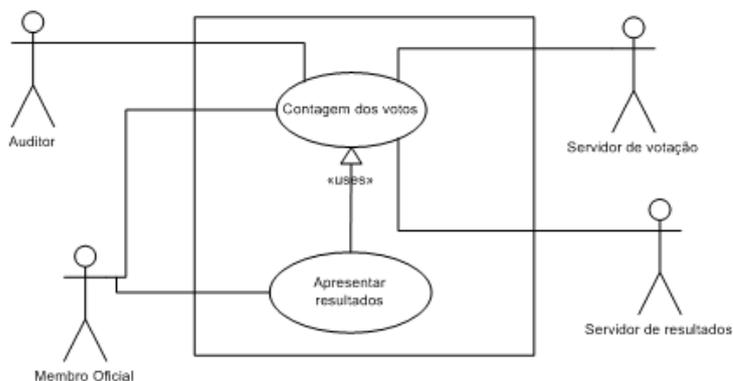
Depois de verificados todos os requisitos, é disponibilizada uma interface gráfica com o boletim de voto que o eleitor preenche e envia (semelhante à entrega do voto).



7.3. CONTAGEM

O subsistema “Contagem” realiza a contagem dos votos, disponibilização e publicação dos resultados eleitorais. Os resultados apurados são agrupados por parâmetros previamente estabelecidos (totais por freguesia/concelhos/distritos, partidos, eleitos, etc.) sendo os mesmos colocados no servidor de resultados.

Ao Membro Oficial compete dar início ao processo de Contagem, quer essa contagem seja parcial ou final.

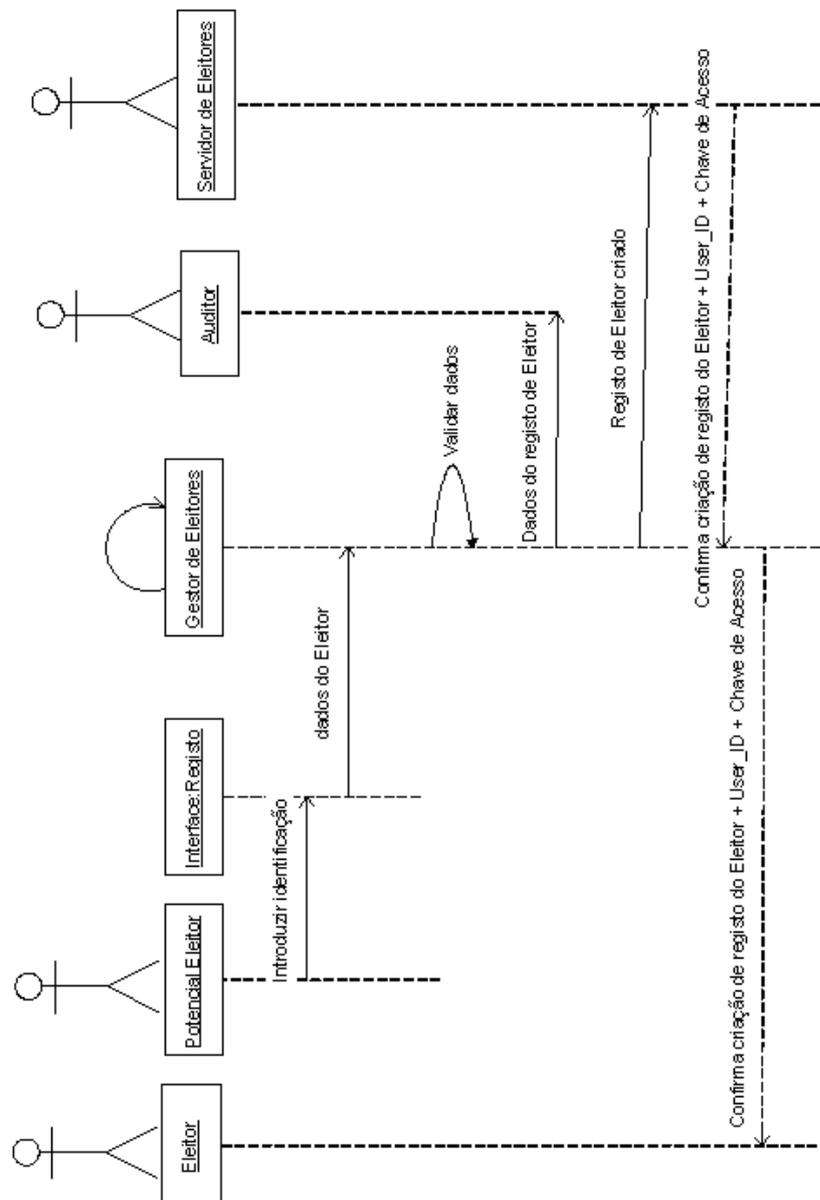


8. DIAGRAMAS DE SEQUÊNCIA

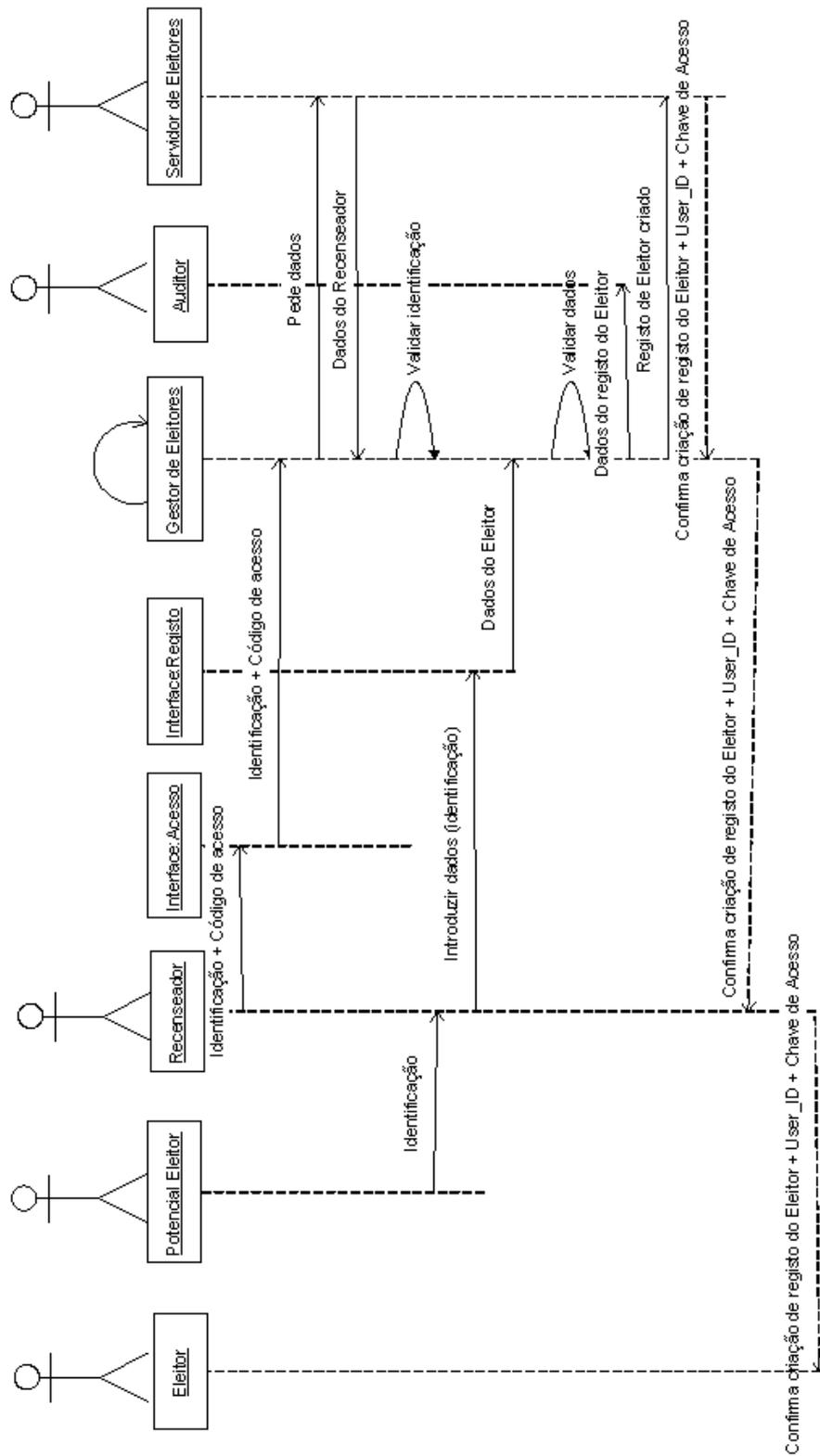
O Diagrama de Sequência descreve as interações entre os elementos do SVE segundo uma visão temporal. São apresentados os seguintes diagramas:

- Recenseamento de Eleitores - Remoto
- Recenseamento de Eleitores - Presencial
- Votação - Via Acesso Remoto
- Votação – Local Público
- Votação - Recinto Controlado
- Contagem

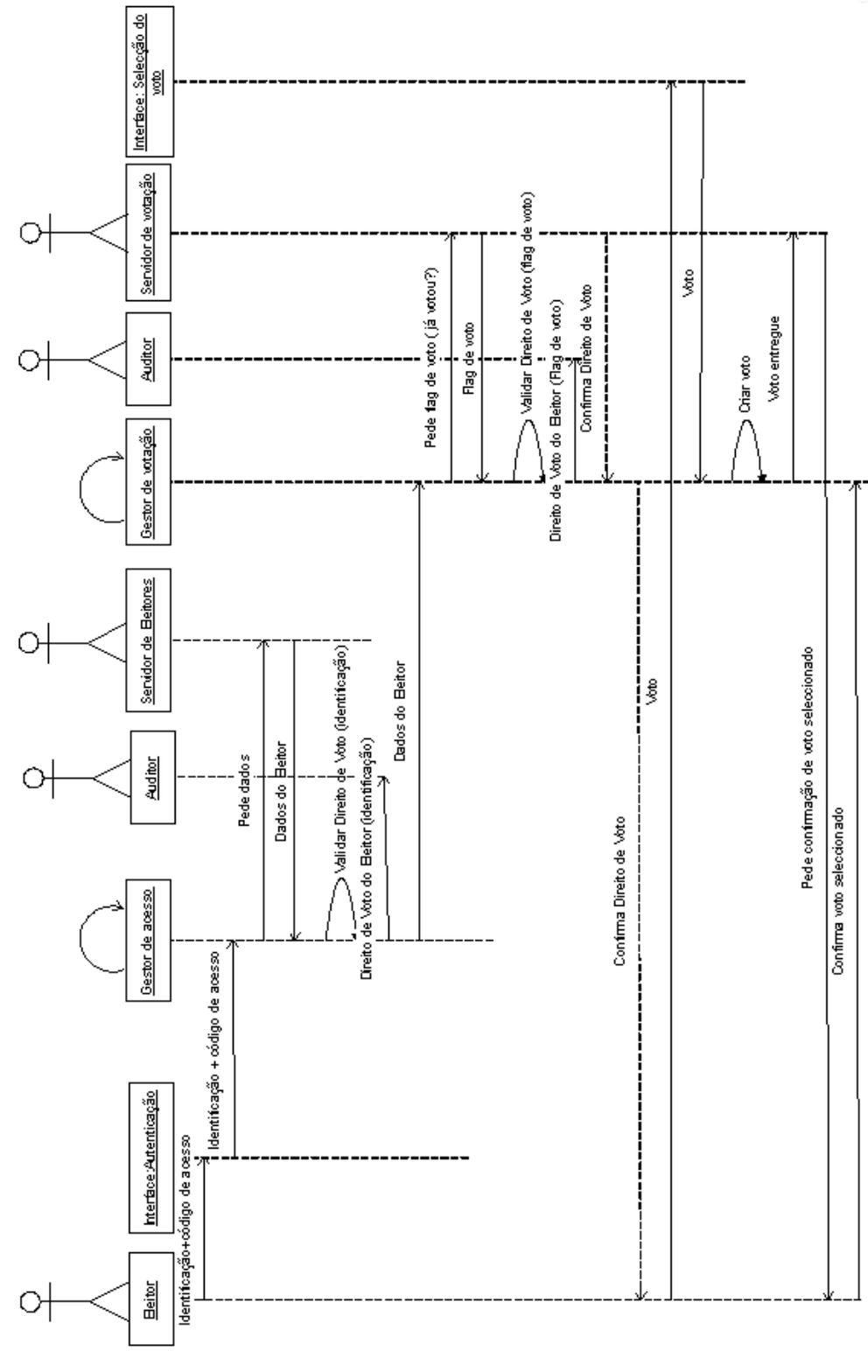
8.1. RECENSEAMENTO DE ELEITORES – REMOTO



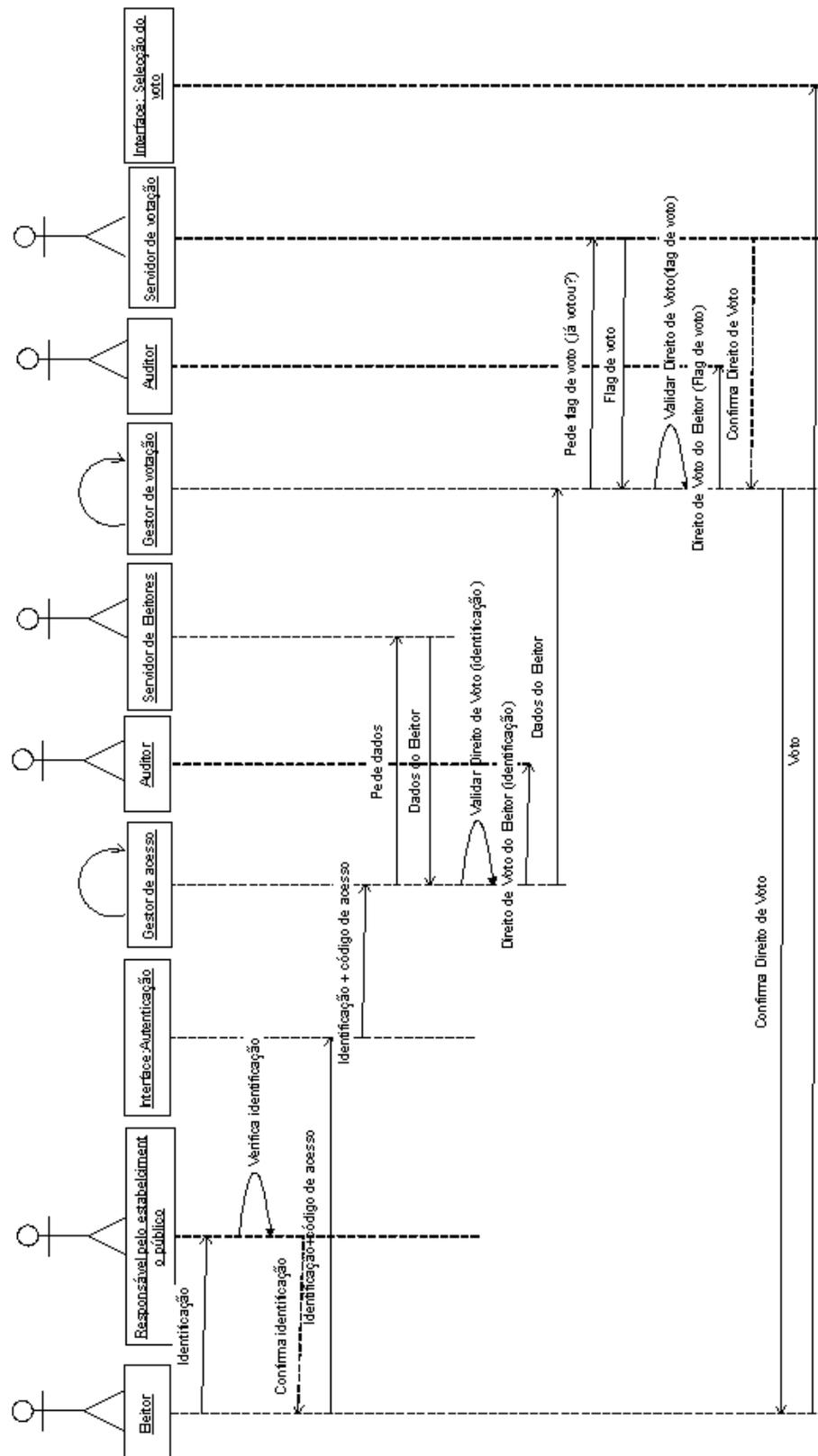
8.2. RECENSEAMENTO DE ELEITORES - PRESENCIAL



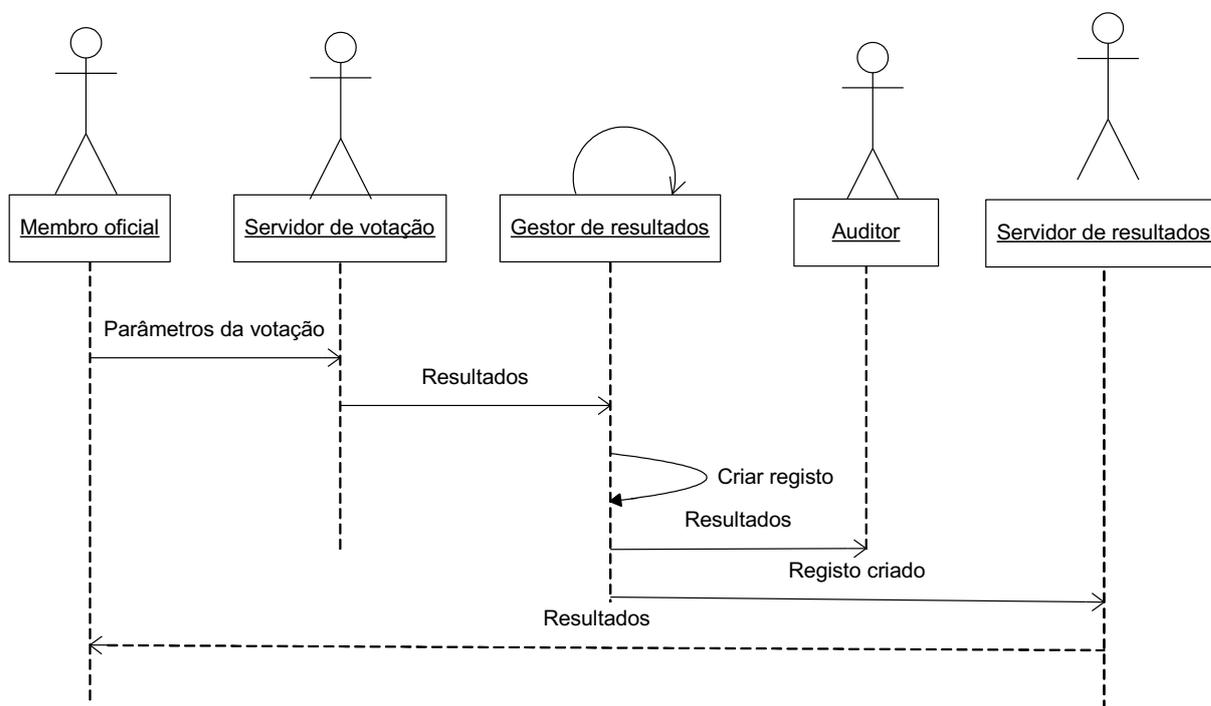
8.3. VOTAÇÃO – VIA ACESSO REMOTO



8.4. VOTAÇÃO – LOCAL PÚBLICO



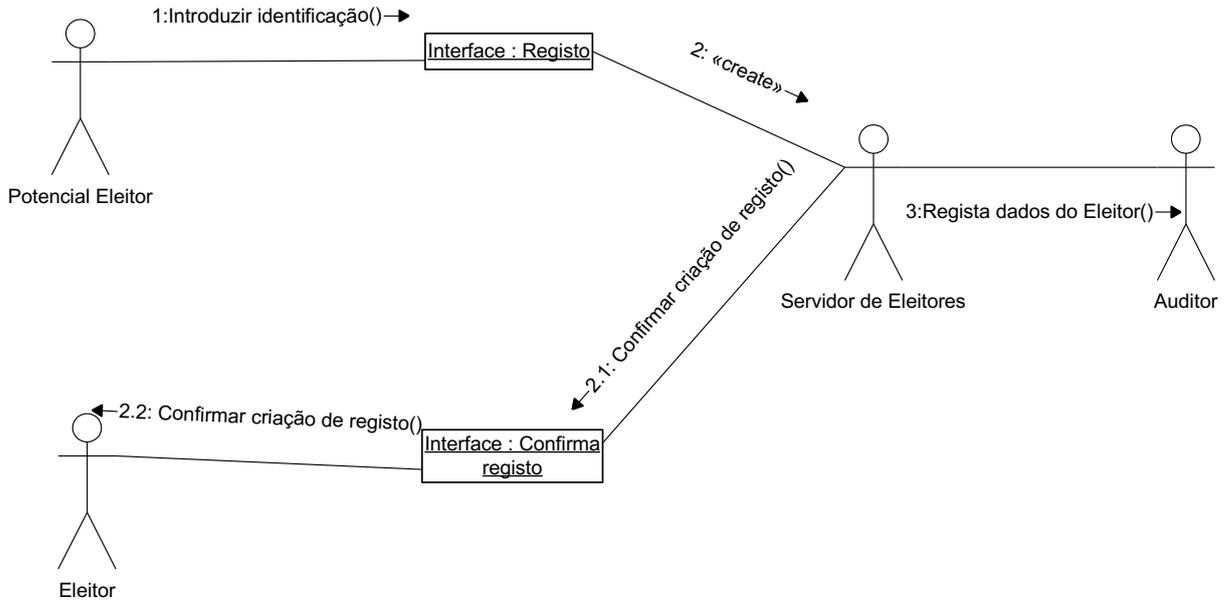
8.6. CONTAGEM



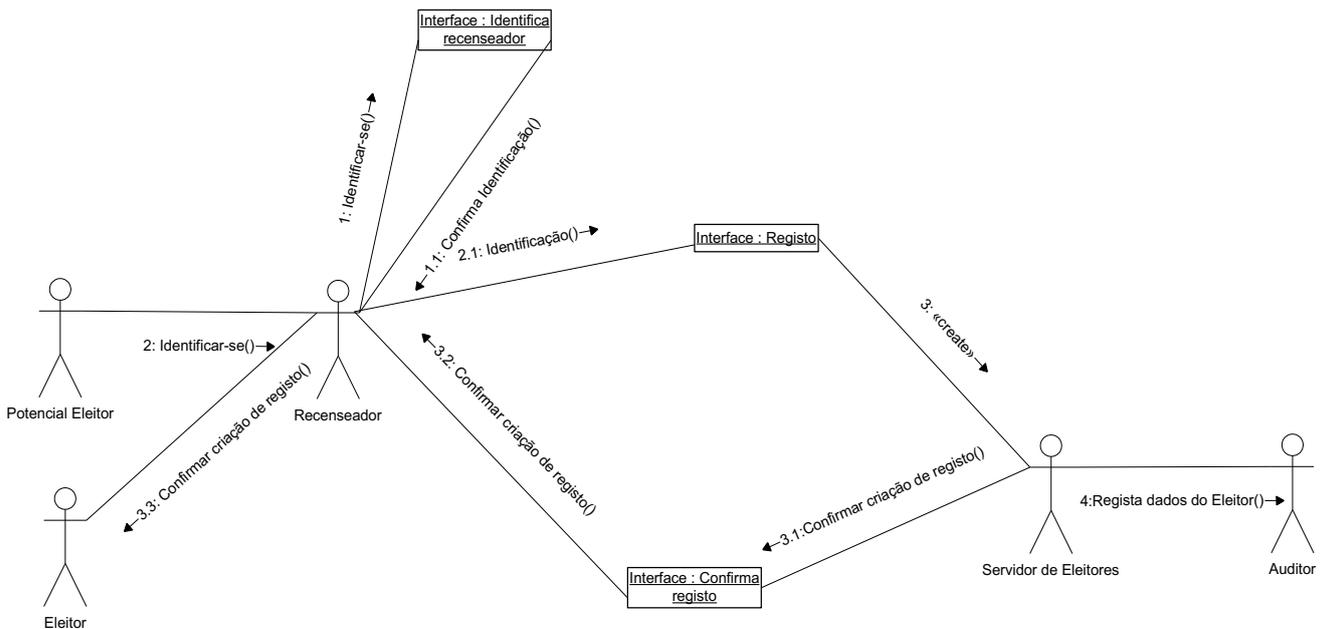
9. DIAGRAMAS DE COLABORAÇÃO

Os Diagramas de Colaboração mostram as relações entre elementos do SVE que desempenham diferentes papéis.

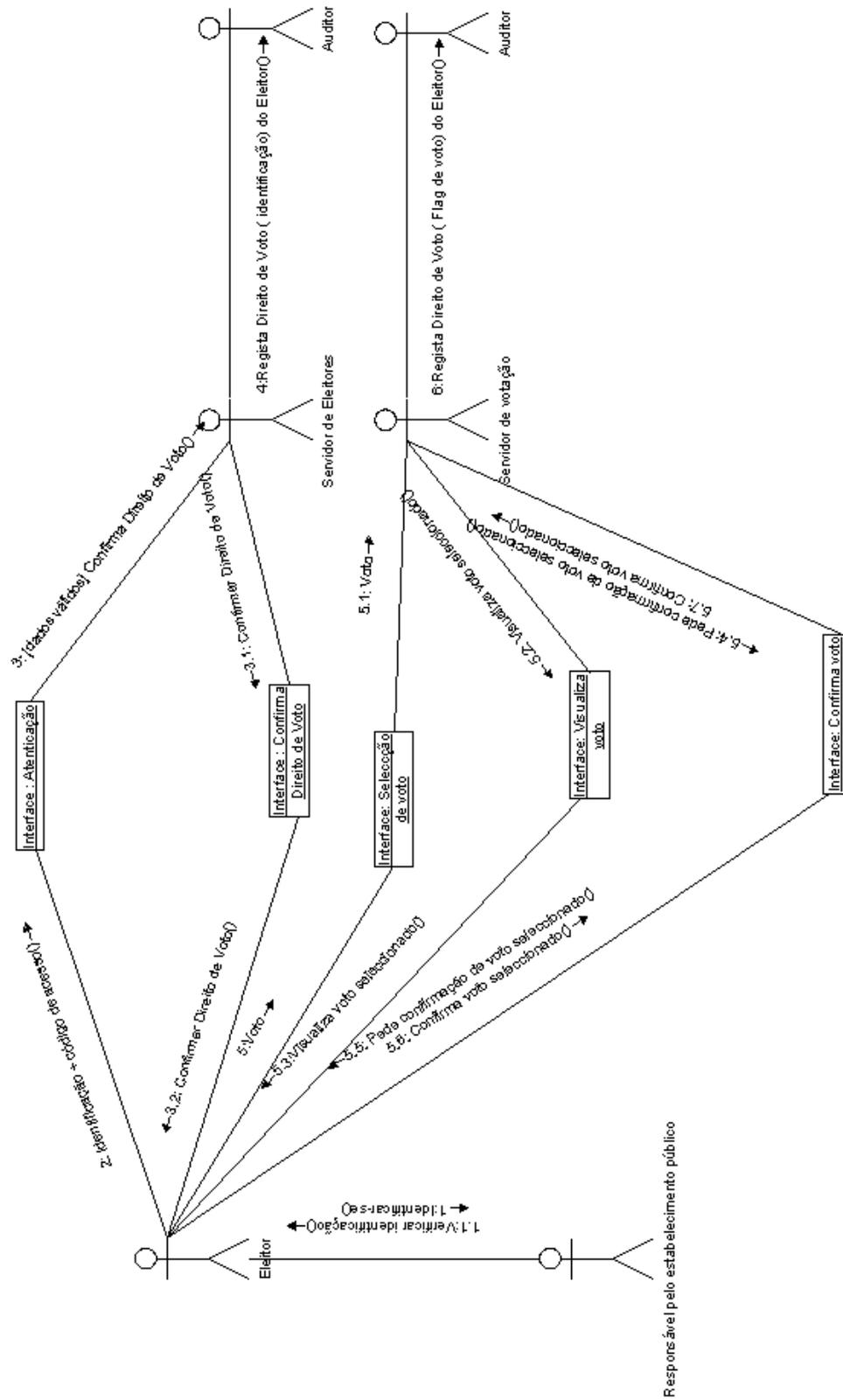
9.1. RECENSEAMENTO DE ELEITORES – REMOTO



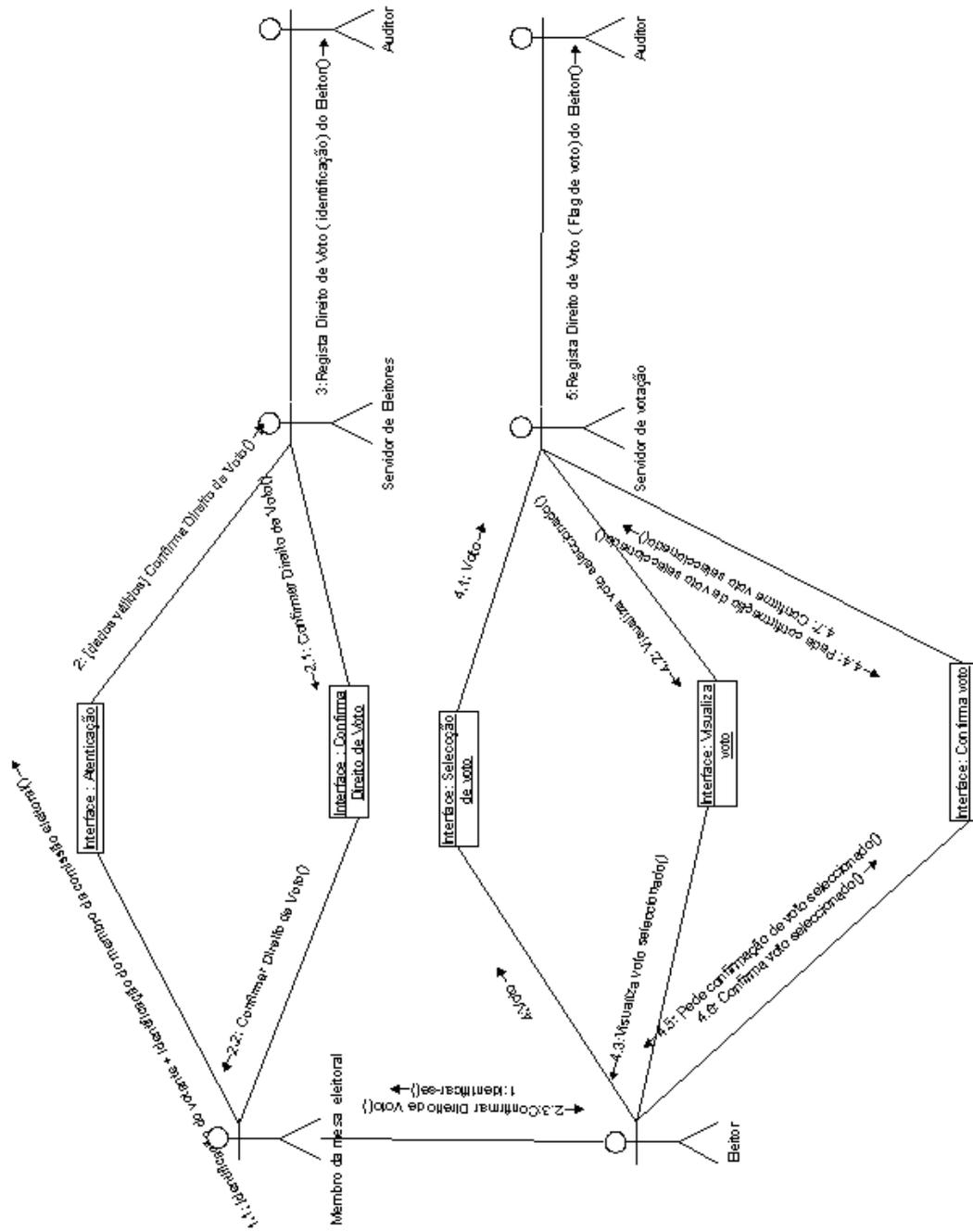
9.2. RECENSEAMENTO DE ELEITORES – PRESENCIAL



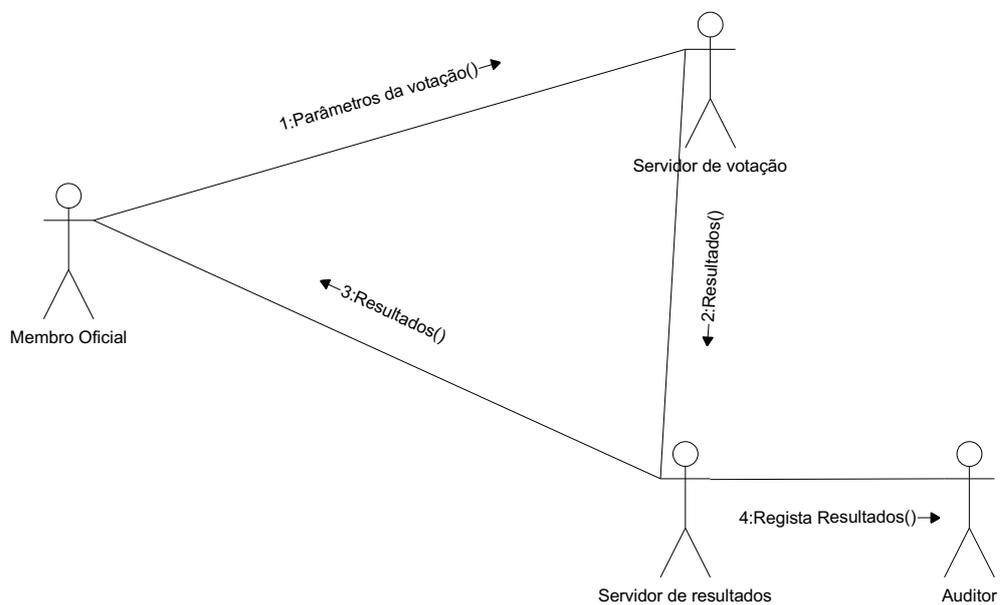
9.4. VOTAÇÃO – LOCAL PÚBLICO



9.5. VOTAÇÃO – RECINTO CONTROLADO

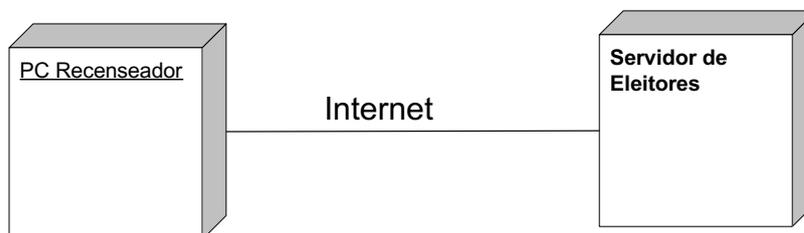


9.6. CONTAGEM

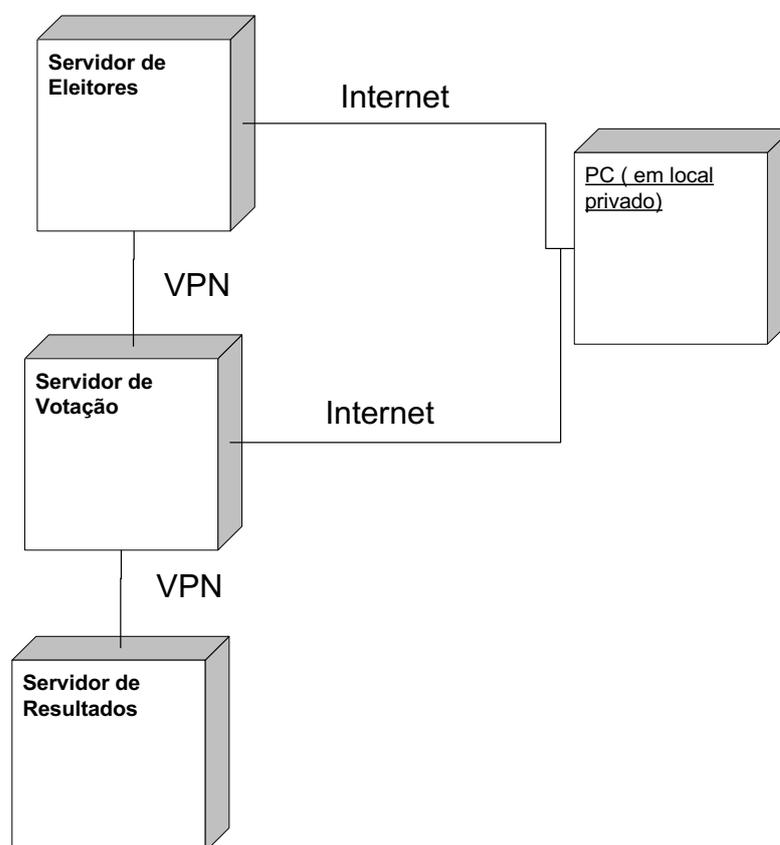


10. DIAGRAMA DE INSTALAÇÃO

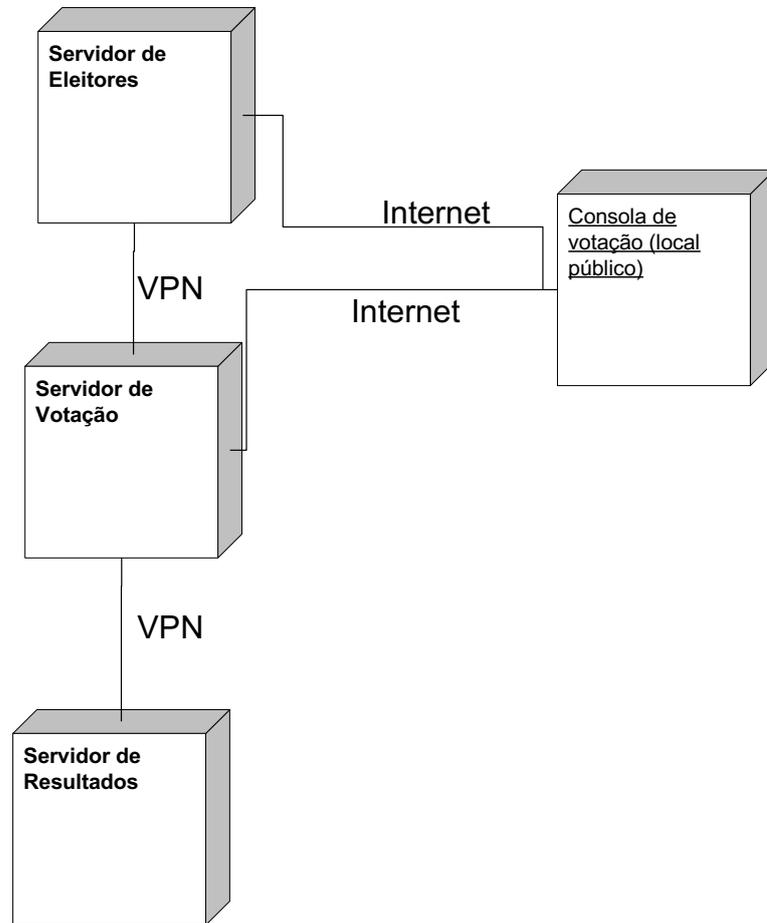
10.1. RECENSEAMENTO DE ELEITORES



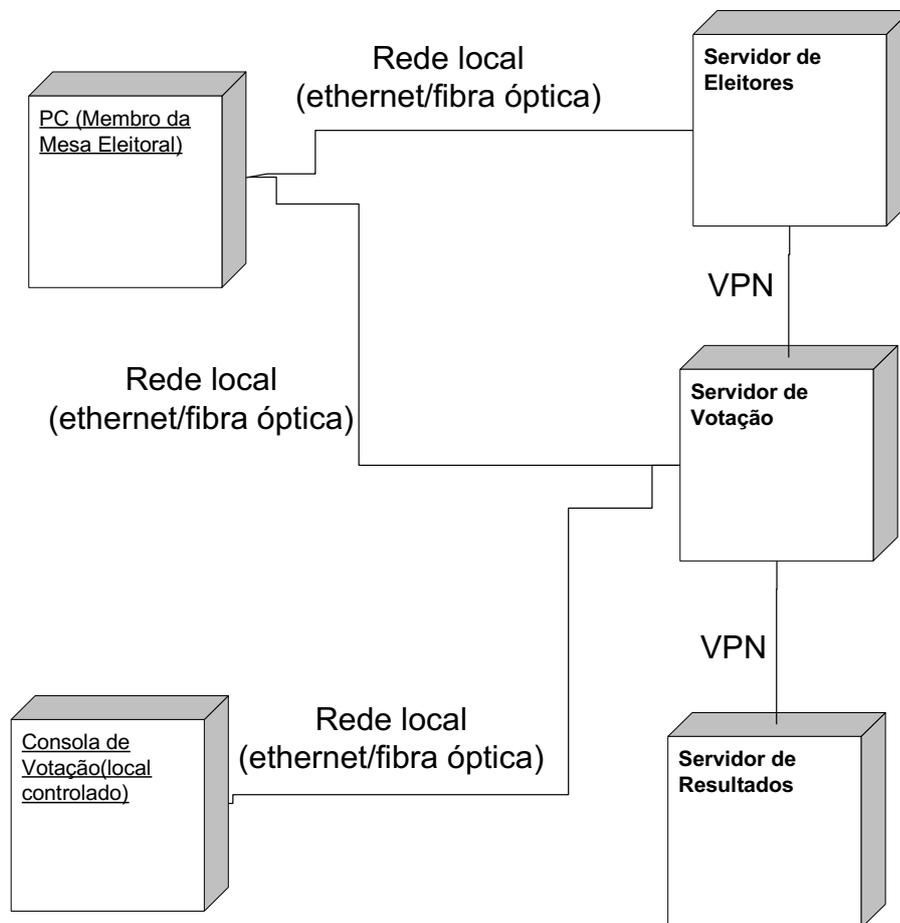
10.2. VOTAÇÃO – ACESSO REMOTO



10.3. VOTAÇÃO - LOCAL PÚBLICO

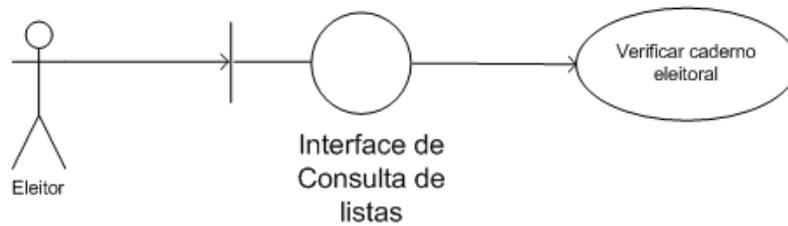
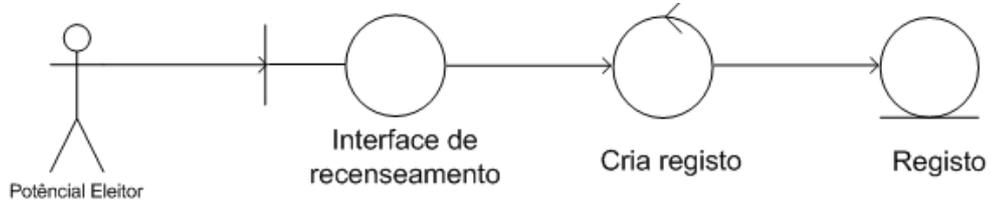


10.4. VOTAÇÃO – RECINTO CONTROLADO

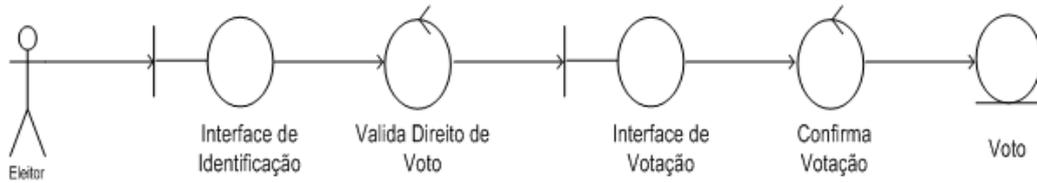


11. DIAGRAMA DE ROBUSTEZ

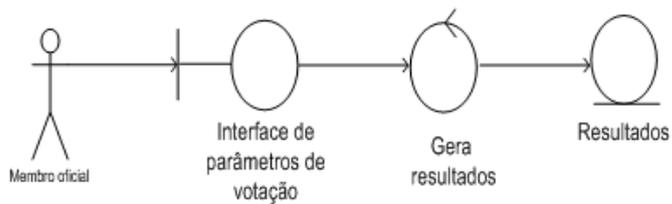
11.1. RECENSEAMENTO DE ELEITORES



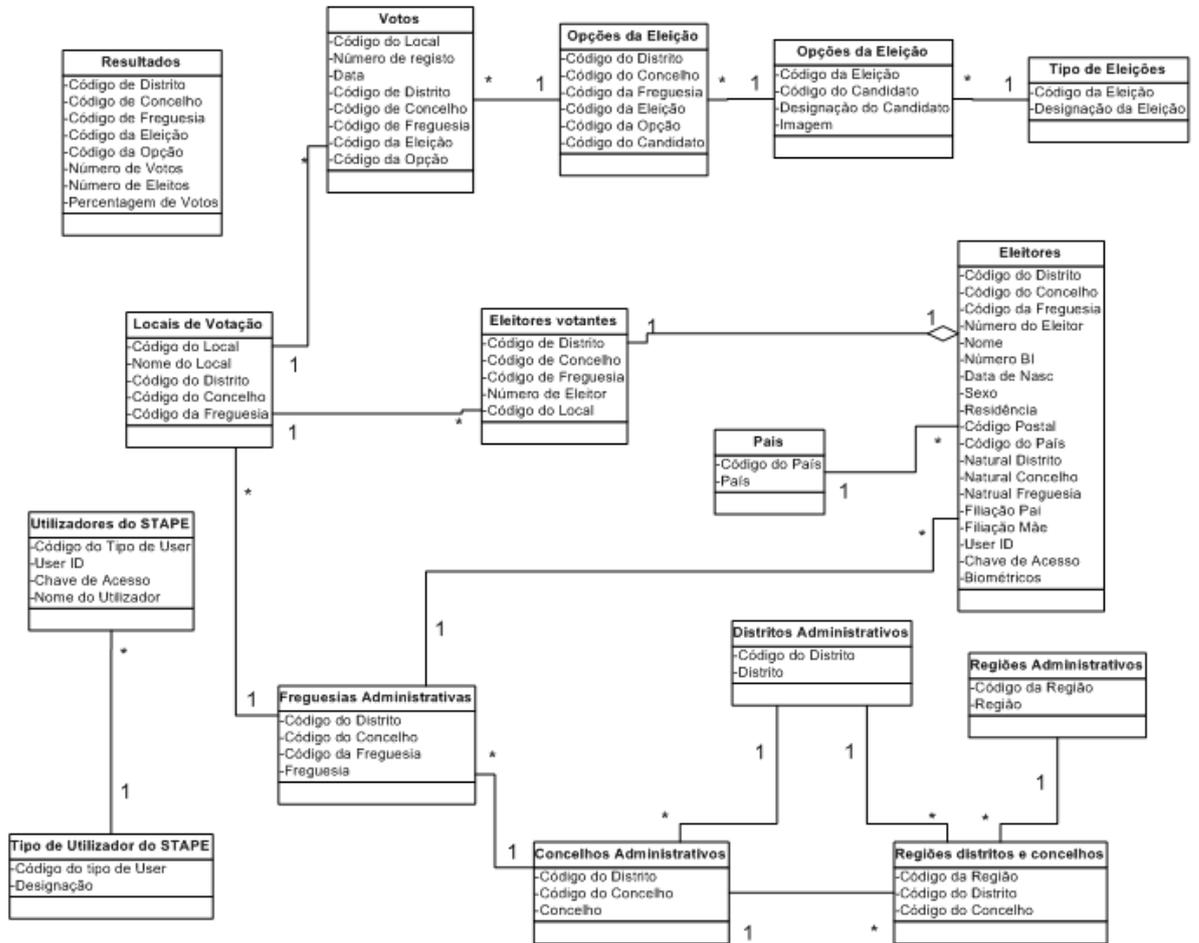
11.2. VOTAÇÃO



11.3. CONTAGEM

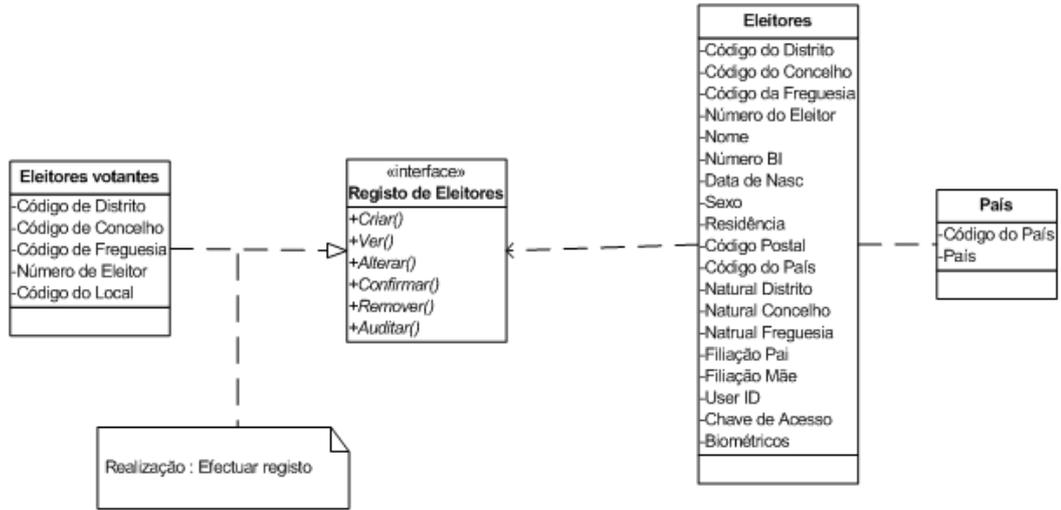


12. DIAGRAMA DE CLASSES

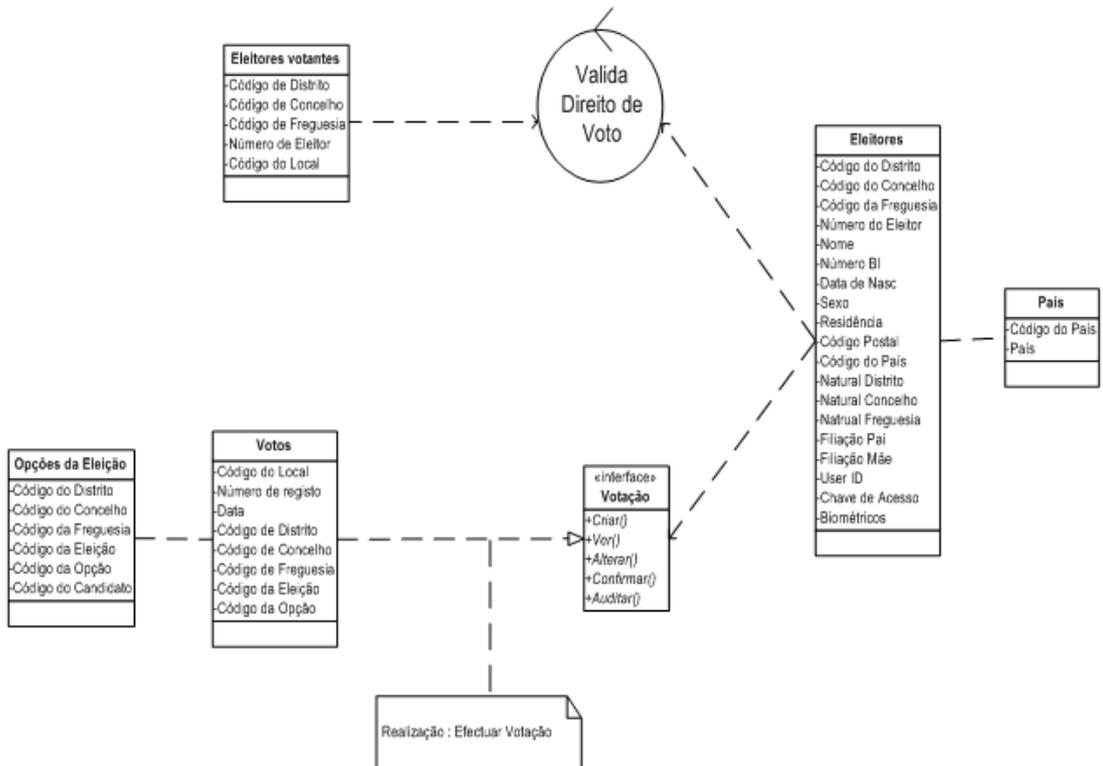


13. REALIZAÇÕES

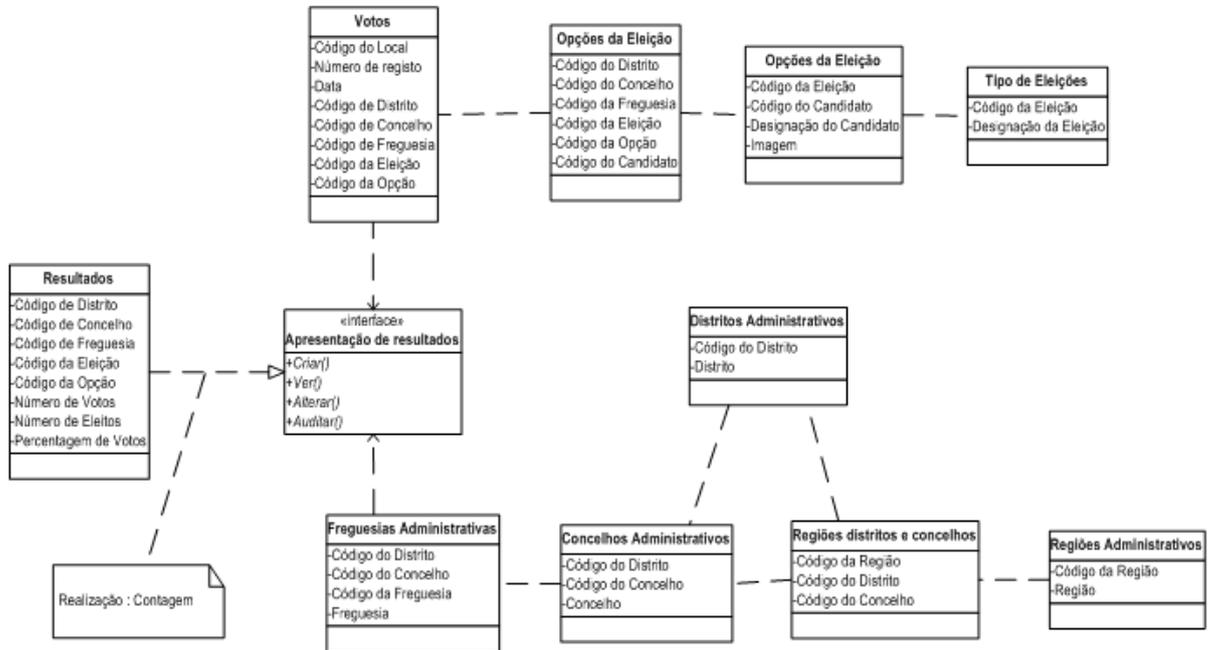
13.1. RECENSEAMENTO DE ELEITORES



13.2. VOTAÇÃO



13.3. CONTAGEM



14. PROPRIEDADES VS RECINTOS DE VOTAÇÃO

Propriedades	Votação		
	Recinto Controlado	Local Público	Via Acesso Remoto
Anonimato	X	X	X
Auditabilidade	X	X	X
Autenticação do operador	X	-	-
Autenticidade	X	X	X
Certificabilidade	X	X	X
Confiabilidade	X	X	X
Conveniência	-	X	X
Detectabilidade	X	X	X
Disponibilidade do sistema	X	X	X
Documentação	X	X	X
Flexibilidade	-	X	X
Integridade do pessoal	X	-	X
Integridade do sistema	X	X	X
Integridade dos votos	X	X	X
Invulnerabilidade	X	X	X
Mobilidade	-	X	X
Não-coercibilidade	X	-	-
Precisão	X	X	X
Privacidade	X	X	-
Rastreabilidade	X	X	X
Recuperabilidade	X	X	X
Singularidade (não reutilização)	X	X	X
Tolerância a ataques	X	X	X
Tolerância a faltas	X	X	X
Transparência do processo	X	X	X
Transparência do sistema	X	X	X
Usabilidade	X	X	X
Verificabilidade	X	X	X

15. BIBLIOGRAFIA

- [1] Adler, J. (2000) "Online Voting Primer", VoteHere.net
- [2] Antunes, P., Monteiro, A., Soares, N., Oliveira, R. (2001) "Sistemas Electrónicos de Votação", DI-FCUL
- [3] Brunazo, A. (2001) "Critérios para Avaliação da Segurança do Voto Eletrónico", Workshop em Segurança de Sistemas Computacionais WSEG '2001, UFSC, Florianópolis, SC
- [4] Cranor, L., Cytron, R. (1997) "Sensus: A Security-Conscious Electronic Polling System for the Internet", Proceedings of the Thirtieth Hawaii International Conference on System Sciences, HICSS '30, IEEE Computer Society
- [5] CSEG (2002) "E-Voting Technical Security Requirements", Issue 1.0, X/10049/4600/6/21, HM Government, UK, November
- [6] Gerk, Ed, (2001) "Voting Systems: From Art to Science", Voting Technology Conference, Caltech/MIT
- [7] Internet Policy Institute (2001) "Report of the National Workshop on Internet Voting: Issues and Research Agenda"
- [8] Jefferson, D., (2000) "Internet Voting", Compac System Research Center, Technical Committee of the California Secretary of State's Task Force on Internet Voting, California Internet Voting Advisory Committee, California Voter Foundation
- [9] Kofler, R., Krimmer, R., Prosser, A. (2002) "Electronic Voting: Algorithmic and Implementation Issues", Department Production Management, Vienna University for Business Administration and Economics
- [10] Pratchett, L. (2002) The Implementation of Electronic Voting in the UK, De Montfort University of Essex, May
- [11] Radwin, M., Klein, P. (1995) "An Untraceable, Universally Verifiable Voting Scheme", Seminar in Cryptology, December
- [12] Rubin, A. (2002) Security Considerations for Remote Electronic Voting, Communications of the ACM, V. 45, N. 2, December
- [13] Tzeng, Zhi-Jia, Tzeng, Wen-Guey, (2001), "Practical and Efficient Electronic Voting Schemes", Department of Computer and Information Science, National Chiao Tung University