

**ADILSON AVELINO CONDE MORGADO**

**E-VOTO COM RECURSO AO  
CARTÃO DE CIDADÃO**

**Orientador: José Quintino Rogado**

**Universidade Lusófona de Humanidades e Tecnologias**

**ECATI**

**Lisboa**

**2016**

**ADILSON AVELINO CONDE MORGADO**

**E-VOTO COM RECURSO AO  
CARTÃO DE CIDADÃO**

Dissertação defendida em provas públicas na Universidade Lusófona de Humanidades e Tecnologias no dia 03/05/2016), perante o júri, nomeado pelo Despacho de Nomeação n.º: 153/2016, com a seguinte composição:

Presidente: Prof<sup>a</sup>. Doutora Inês Isabel de Pimentel Oliveira (ULHT)

Arguente: Prof. Doutor Rui Pedro Nobre Ribeiro (ULHT)

Orientador: Prof. Doutor José Luís de Azevedo Quintino Rogado (ULHT)

**Universidade Lusófona de Humanidades e Tecnologias**

**ECATI**

**Lisboa**

**2016**

## **DEDICATÓRIA**

Beto Morgado (meu pai).

Criaste cinco filhos numa casa de um quarto, eram tempos difíceis. Muitas vezes, faltava o dinheiro para o candongueiro ou para uns ténis novos (recorrendo às botas militares), mas graças a Deus nunca deixaste faltar o dinheiro para o caderno e os livros, e mais tarde para as propinas nas Universidades privadas, para mim e para os meus irmãos. Dizias que quando partisses, a única coisa que nos ias deixar era a educação, por isso não mediste esforço para nos formares, nem para fazeres de nós melhores alunos, a cada novo dia que passava.

Beto tirei 15. Didi, tu podes tirar 18. 19, é para o professor e 20 é perfeição, tu só estudas, 15 é bom, mas tu consegues mais.

Lá eu me punha a estudar, e no próximo teste... Beto tive 18. Eu te disse meu filho, tu consegues. Parabéns!

Fiz tudo para te honrar com o meu diploma de mestrado, mas o destino foi traiçoeiro, e levou-te antes que eu pode-se realizar este sonho. Foi difícil, porém, continuei por ti meu pai. Estejas onde estiveres, saiba que além de formação, me deixaste um grande vazio.

Foi sempre por ti...

Adilson Avelino Conde Morgado

## AGRADECIMENTOS

Agradeço a Deus todo-poderoso pela força, sabedoria e coragem que me deu para deixar a minha terra (Angola), e rumar a Portugal para fazer esta formação.

Agradeço:

À minha esposa Yeda Aleixo Morgado, pela paciência e sabedoria que teve para encarar os meus momentos, dormir sozinha (porque eu estava a programar, e programa chato que não saía) e muitas vezes preocupada, pois o homem está o dia todo a frente do computador. Enfim, agradeço a Deus por existires.

Ao meu filho Kevin Morgado, tão pequenino mas já sabe que o pai está a estudar, e então tem que “chatear” a mãe. Louvo a Deus pela tua vida

Aos meus pais Leonor & Beto Morgado, muito obrigado pela força que sempre me deram. Mesmo a morrerem de saudades, tal como eu, sempre me encorajaram. Deus vos abençoe.

Aos meus irmãos Alberto, Edivaldo, Solange e Waler Morgado, equipa de alta competição, eu sou resultado das nossas discussões/debates. Somos um cordão de 3 nós. Deus vos guarde.

Ao meu primo e amigo Vladimir Gaspar, és parte importante nesta caminhada, te serei eternamente grato pelo apoio. Que Deus ilumine o teu caminho.

À minha madrinha Luzia Morgado (tia Gigi), o nosso amor é divino (e está a passar para a Tany, ☺). Tinha que abrir um capítulo para falar de ti. Deus te abençoe

Aos meus sogros Amaral Aleixo e Herminia Tiny, meus pais adjuntos. Foi Deus que vos trouxe para a minha vida. Deus vos cuide.

Aos meus professores José Rogado (meu mestre, sem ti não seria possível), Inês Oliveira, Sérgio Guerreiro, Lino Santos. Mais do que professores, grandes motivadores. Que Deus vos abençoe.

Aos meus amigos, Nilton 07, Mulembele, Carlos Mendes, Kiese Kanito (meu mano), Alexandre Ernesto, Nice Zulo, Walter Abel, Cotita, Samora Sobrinho (Mtr. Nice), Yuri Van-Dunenn, Paulino Santos, Xuxu. Obrigado pelo apoio. Vocês são, e sempre serão, irmãos que a vida me deu.

Escrever sobre estas pessoas, significa que esta jornada está a chegar ao fim. Que Deus vos abençoe, rica e poderosamente.

## RESUMO

Os diferentes métodos de autenticação existentes, atualmente, conferem diferentes níveis de segurança aos sistemas que protegem. Métodos como, credenciais guardadas em *smartcards* podem atingir um elevado nível de segurança. Em simultâneo, assiste-se a um decréscimo significativo de interesse na participação em processos eleitorais, que se tem verificado sobretudo, nas democracias ocidentais. Proporcionar um aumento das oportunidades de voto (maior número de lugares onde se torna possível exercer esse direito) passou a ser mais do que um desejo, uma necessidade.

Para colmatar esta necessidade e explorar as potencialidades do Cartão de Cidadão (CC), foi criado o [E-voto com recurso ao Cartão de Cidadão](#), que é um sistema de voto eletrónico com recurso a uma autenticação baseada no CC. Uma abordagem teórica/prática foi levada a cabo, para identificar indicadores que levam a crer que esta implementação traz ganhos significativos e grande impacto social.

A fundamentação teórica deste trabalho apresenta aspetos fundamentais relativos à *Gestão de identidade* e ao CC. Inicialmente, são apresentados os conceitos, as propriedades, os componentes e a arquitetura do sistema associado ao CC. Em seguida, os agentes da gestão de identidade são descritos através de suas características, categorias e aplicações, com o intuito de demonstrar a viabilidade do uso desta tecnologia no processo eleitoral.

Palavras-chave: Cartão de Cidadão, Sistema de Gestão de Identidade, criptografia, autenticação, certificado digital, sistema de voto eletrónico.

## ABSTRACT

The different existing authentication methods currently provide different levels of security for authentication systems. Methods such credentials stored in *smartcards* can achieve a high level of security. Parallel to this is seen in a significant decrease of interest in participation in electoral processes that have occurred in Western democracies. Providing increased opportunities to vote (as many places where it is possible to exercise the right to vote) became more than a desire, a need.

To address this need and to explore the potential of Citizen Card e- voting using the citizen card, which is an electronic voting system using the citizen card to authenticate was created. A theoretical approach / practice was taken in charge to identify indicators that suggest that this implementation brings significant gains and great social impact.

The theoretical foundation of this work presents fundamental aspects of identity management and citizen card. Initially the concepts, properties, components and architecture of the citizen card is presented. Then the agents of identity management are described by their characteristics, categories and applications, with the aim of demonstrating the feasibility of using this technology in the electoral process.

**Keywords:** Citizen Card, identity management, digital certificate authentication, electronic voting system, encryption system.

## **ABREVIATURAS E SÍMBOLOS**

CC – Cartão De Cidadão

E-Voto – Voto Eletrónico com Recurso ao Cartão De Cidadão

DRE- Direct Recording Electronic

E-Government – Governo Eletrónico

Ivonting – Voto Eletrónico (Estónia)

DES- Data Encryption Standard

AES- Advanced Encryption Standard

RSA- Rivest Shamir Adleman

MD5 – Message Digest Algorithm 5

SHA – Secure Hashing Algorithm

TTP – Trustet Third Party

CA – Certification Authority

EC – Entidade Certificadora

ER – Entidade Registo

CRL – Lista De Certificados Revogados

CL – Lista de Certificados

OCSP – Entidade De Certificação

URL – Uniform Resource Locator

HTTPS - Hyper Text Transfer Protocol Secure

SSH – Secure Shell

SSL – Secure Socket Layer

TLS - Transport Layer Security

OTP – One Time Password

PKI – Public Key Infrastructure

IP – Internet Protocol

DAC – Discretionary Access Control

MAC – Mandatory Access Control

RBAC - Role Based Access Control

TIC – Tecnologia de Informação e Comunicação

BD – Base de Dados

SOD – Separation Of Duties

SSO - Single Sign-On

IDP – Identity Provider

SP – Service Provider

SALM - Security Assertion Markup Language

IML - Linguagem de Modelagem Unificada

INFOSEC – Segurança de Informação

DDoS - Ataques de negação de serviço distribuído

IDS - Intrusion Detection System



## ÍNDICE

<b>1. Introdução.....</b>	<b>1</b>
<b>1.1 Sistemas de Voto .....</b>	<b>2</b>
<b>1.2 Voto Eletrónico no Brasil .....</b>	<b>2</b>
<b>1.3 Sistema de Voto Eletrónico na Estónia .....</b>	<b>3</b>
<b>1.4 Objetivos .....</b>	<b>4</b>
<b>2. Segurança da Informação.....</b>	<b>6</b>
<b>2.1 Introdução .....</b>	<b>6</b>
<b>2.2 Conceitos.....</b>	<b>7</b>
<b>2.3 Mecanismos de Segurança .....</b>	<b>8</b>
<b>2.4 Identidade .....</b>	<b>10</b>
<b>2.5 Privacidade .....</b>	<b>12</b>
<b>2.6 Assinatura.....</b>	<b>17</b>
<b>2.7 Certificados Digitais .....</b>	<b>19</b>
<b>2.8 Enquadramento Legal .....</b>	<b>24</b>
<b>3. Modelos de Autenticação .....</b>	<b>27</b>
<b>3.1 Credenciais .....</b>	<b>27</b>
<b>3.2 Autenticação Simples.....</b>	<b>27</b>
<b>3.3 Challenge - Response .....</b>	<b>28</b>
<b>3.4 Sistemas Híbridos .....</b>	<b>30</b>
<b>3.5 Autenticação Mútua .....</b>	<b>31</b>
<b>3.6 Autenticação com Múltiplos Fatores.....</b>	<b>33</b>
<b>3.7 Autorização e Controlo de Acessos .....</b>	<b>34</b>

3.8	Políticas de Controlo de Acessos.....	35
4.	Sistemas de Gestão de Identidade.....	40
4.1	Modelo local / centralizado .....	
4.2	Modelo Federado .....	43
5.	E-voto com recurso ao CC.....	46
5.1	Arquitetura da Solução .....	46
5.2	Diagramas de Sistema .....	47
5.3	Protótipo .....	52
6.	Análise de Risco.....	55
6.1	Identificação e Análise de Riscos .....	55
6.2	Tratamento dos Riscos .....	56
6.3	(Riscos inerentes ao CC, Java e Applet) .....	58
7.	Conclusão e Perspetivas.....	60
7.1	Trabalhos Futuros .....	61
8.	Bibliografia .....	63
	ANEXOS .....	67

## Índice de Figuras

<b>Fig. 1 – Urna Eletrónica Brasileira (fonte: Agência para a sociedade do conhecimento)</b>	<b>2</b>
<b>Fig. 2 – Portal de voto da Estónia (Fonte: Vabarrigi, “site” do governo da estónia)</b>	<b>3</b>
<b>Fig. 3 – Triângulo de Segurança da Informação</b>	<b>7</b>
<b>Fig. 4 – Transações (Visão Alto nível)</b>	<b>8</b>
<b>Fig. 5 – Segurança Física</b>	<b>9</b>
<b>Fig. 6 – Frente e verso do Cartão de Cidadão</b>	<b>11</b>
<b>Fig. 7 – Informações residentes no chip</b>	<b>18</b>
<b>Fig. 8 – Princípio de criptografia</b>	<b>19</b>
<b>Fig. 9 – Criptografia</b>	<b>19</b>
<b>Fig. 10 – Cifra de César</b>	<b>20</b>
<b>Fig. 11 – Cifra por Bloco</b>	<b>14</b>
<b>Fig. 12 – Cifra Contínua</b>	<b>14</b>
<b>Fig. 13 – Cifra Simétrica</b>	<b>14</b>
<b>Fig. 14 – Attack man-in-the-middle .</b>	<b>15</b>
<b>Fig. 15 – Cifra Assimétrica</b>	<b>15</b>
<b>Fig.16 – Aproximação quadrado e multiplicação.</b>	<b>17</b>
<b>Fig.17 – Calcular cifra e assinatura com chave Assimétrica.</b>	<b>18</b>
<b>Fig.18 – Processo de assinatura e confirmação de um documento</b>	<b>18</b>
<b>Fig. 19 – Hierarquia de Confiança</b>	<b>20</b>
<b>Fig. 20 – Hierarquia de Confiança no CC</b>	<b>20</b>
<b>Fig. 21 – Gestão de certificados digitais</b>	<b>23</b>
<b>Fig. 22 – Login USER/PASSWORD</b>	<b>28</b>
<b>Fig. 23 – Challenge Response</b>	<b>29</b>
<b>Fig. 24 – Sniffer (Challenge – Response)</b>	<b>30</b>
<b>Fig. 25 – Tunel TLS com certificado de Alice</b>	<b>37</b>

<b>Fig. 26 – Captura do Certificado</b>	<b>38</b>
<b>Fig. 27 – Protocolo genérico de autenticação mútua com desafio-resposta</b>	<b>39</b>
<b>Fig. 28 – Protocolo genérico de autenticação mútua com desafio-resposta</b>	<b>39</b>
<b>Fig. 28 – A identificação utilizada no sistema de autenticação Multibanco.</b>	<b>40</b>
<b>Fig. 29 – Controlo de acessos (relação entre autenticação, autorização e auditoria)</b>	<b>35</b>
<b>Fig. 30 – Políticas de controlo de acesso (DAC, MAC e RBAC).</b>	<b>36</b>
<b>Fig. 31 – RBAC (permissões para determinadas acções)</b>	<b>37</b>
<b>Fig. 32 – Um Role.</b>	<b>37</b>
<b>Fig. 33 – Groups</b>	<b>38</b>
<b>Fig. 34 – (Hierarquias de Roles).</b>	<b>38</b>
<b>Fig. 35 – Gestão de Identidades</b>	<b>47</b>
<b>Fig. 36 – Modelo Centralizado</b>	<b>48</b>
<b>Fig. 37 – Centralização</b>	<b>49</b>
<b>Fig. 38 – SSO Centralizado</b>	<b>50</b>
<b>Fig. 39 – Service Provider (1) e Identity Provider (2)</b>	<b>50</b>
<b>Fig. 40 – Funcionamento de uma Federação [20]</b>	<b>51</b>
<b>Fig. 41 – Funcionamento de uma Federação</b>	<b>47</b>
<b>Fig. 42 – Diagrama de Caso de Uso (Votação)</b>	<b>48</b>
<b>Fig. 43 – Diagrama de Caso de Uso (Votação)</b>	<b>48</b>
<b>Fig. 44 – Diagrama de Atividades</b>	<b>49</b>
<b>Fig. 45 – Diagrama de Classes</b>	<b>50</b>
<b>Fig. 46 – Diagrama de Sequência</b>	<b>51</b>
<b>Fig. 47 – Estrutura simplificada do User:E-voto</b>	<b>53</b>
<b>Fig. 48 – Estrutura simplificada da Serv-E-voto</b>	<b>54</b>
<b>Fig. 49 – Individos dos 10 aos 74 anos que usam telemóvel (26)</b>	<b>61</b>

## **Índice de Tabelas**

**Tabela 1: Comparação de cifras simétricas vs cifra assimétrica 15**

**Tabela 2: Algoritmo de cifra assimétrica RSA 16**

**Tabela 3: Autenticação mútua em diversos protocolos cliente > servidor 32**

**Tabela 4: Análise de risco 56**

**Tabela 5: Níveis de alta disponibilidade 57**

## 1. Introdução

“Cada um vale pouco e todos valem exatamente o mesmo”.

*Democracia (do grego demo= povo e cracia=governo, ou seja, governo do povo) é um sistema em que as pessoas de um país podem participar na vida política. Esta participação pode ocorrer através de eleições. Numa democracia, as pessoas possuem liberdade de expressão e de manifestação de suas opiniões. A maior parte das nações do mundo atual seguem o sistema democrático.*

A Eleição, é todo processo pelo qual um grupo designa um ou mais dos seus integrantes para ocupar um cargo, por meio de votação. Na democracia representativa, este processo consiste na escolha de determinados indivíduos para exercerem o poder soberano, concedido pelo povo através do voto, devendo estes, assim, exercer o papel de representantes da nação. A eleição pode se processar com o voto de toda a comunidade ou de apenas uma parcela da comunidade (os chamados eleitores) (1). Contudo, tem-se verificado um decréscimo significativo do interesse na participação em processos eleitorais nas democracias ocidentais. Assim, proporcionar um aumento das oportunidades de voto (maior número de lugares onde se torna possível exercer o direito de voto), uma redução de votos “nulos” não intencionais, a possibilidade de permitir, com privacidade, o direito de voto a pessoas com necessidades especiais, a diminuição de reclamações/acusações de fraude em alguns países, uma maior rapidez e “exatidão” na contagem dos votos, são dilemas dos governos atuais em todo mundo.

Para colmatar estes problemas, várias soluções de voto eletrónico (2) (3) estão em estudo. Contudo, o voto eletrónico está na linha da frente, quer pelas suas características e limitações quer pelo seu impacto social, pois acredita-se que reúne os principais requisitos para colmatar as principais lacunas do voto “tradicional”. Porém, na opinião de vários autores (4), ainda está longe de ser uma realidade global. A opinião destes autores baseia-se nas falhas de segurança sentidas nas recentes implementações de sistemas de voto eletrónico (Brasil e Finlândia por ex.), que provocam desconfiança nos eleitores. Neste contexto, a segurança é um aspeto fundamental a considerar, sendo por isso exigido um cuidado muito especial na escolha e implementação das tecnologias de suporte para a votação eletrónica. Tal como os sistemas de informação das organizações, estas exigem um levantamento de requisitos, a identificação de todos os intervenientes, uma descrição de todos os processos e a escolha de um leque de tecnologias adequadas, cada uma exigindo medidas de segurança ou administrativas devidamente ajustadas.

Para a implementação da segurança associada ao sistema de voto eletrónico (E-VOTO com CC), um dos aspetos fundamentais é a utilização de *Smart Cards* para uma autenticação forte e segura, bem como a definição de políticas de segurança que envolvam também outras componentes, tais como: acesso físico, catástrofes naturais, entre outros aspetos não tecnológicos que embora abordados (sem aprofundar) estão fora do âmbito deste trabalho.

## 1.1 Sistemas de Voto

O voto eletrónico, genericamente considerado, tem vindo por todo o mundo e nas suas diversas vertentes (presencial e não presencial), a ser objeto de ensaios ou experiências piloto. Os Sistemas de Voto Eletrónico são sistemas que quer pelas suas características e limitações quer pelo seu impacto social, têm sido desenvolvidos e aprimorados em todo o mundo. Apesar de muitos países estarem a testar alguns destes sistemas de voto eletrónico (incluindo Portugal nos anos 1997, 2001, 2004 e 2005 respetivamente, todas elas não vinculativas) (5), os mais representativos são porventura os usados no Brasil e na Estónia, por se tratar do país pioneiro na matéria e do país, que penso, que tem o sistema de voto eletrónico mais robusto, respetivamente (egov).

Essa vontade dos Estados assenta na necessidade de desenvolvimento de processos eleitorais mais modernos e entronca na categoria do designado "Governo Eletrónico".

## 1.2 Voto Eletrónico no Brasil

Desde a década de 80, na altura do regime militar, que decorreram no Brasil “os primeiros” estudos para a realização de eleições informatizadas, com a motivação de tornar as eleições mais fáceis e rápidas de apurar. Estudos que tiveram frutos no começo da década seguinte, levaram à conceção da máquina de votar denominada *Direct Recording Electronic* (6) (DRE) em 1990. No ano seguinte, realizou-se o primeiro pleito oficial que utilizou voto eletrónico no Brasil. Em 1996 o Tribunal Superior Eleitoral (TSE), iniciou a implementação da urna eletrónica em todo o país, desde então, esta tecnologia tem sido aprimorada. Em 2008 esta entidade implantou a urna eletrónica com reconhecimento biométrico das impressões digitais do cidadão eleitor (fig.1), integrada num sistema informatizado que tem gerado muita controvérsia. Pois, o TSE considera que o sistema reúne todas as condições para ser considerado “seguro” (7), já os analistas de segurança consideram-no “extremamente inseguro”. (8) Isto porque, se acredita que possa existir fraude, quer por agentes internos quer por agentes externos ao equipamento, e uma vez que o TSE não divulga os mecanismos de segurança utilizados para garantir a robustez do equipamento, levantam-se algumas dúvidas sobre a transparência existente naquele país (9).

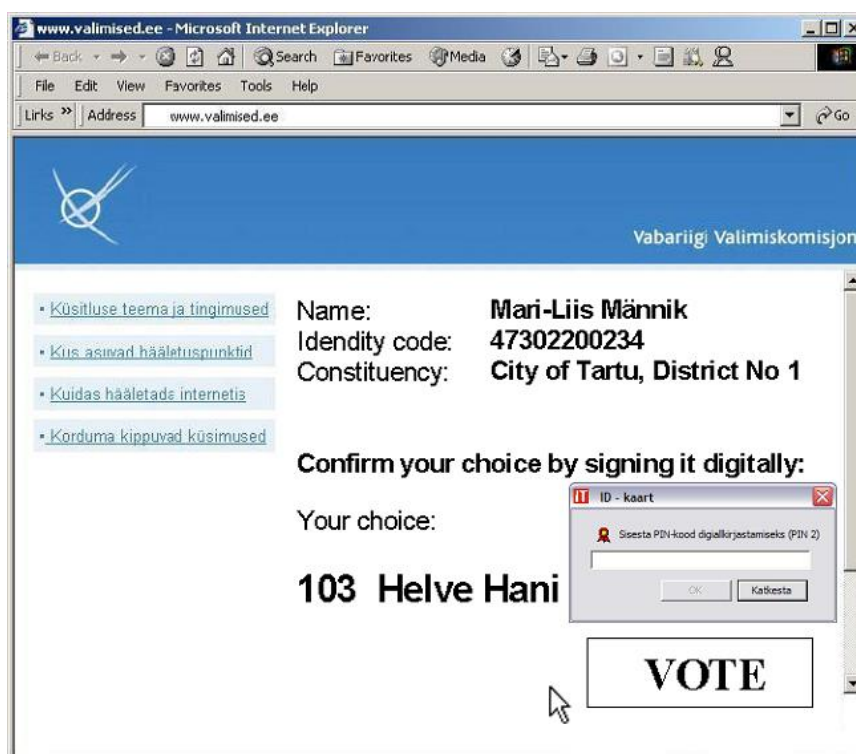


**Fig. 1 – Urna Eletrónica Brasileira (fonte: Agência para a sociedade do conhecimento)**

Entre críticas e elogios pelo mundo fora, a verdade é que o modelo DRE continua a ser usado no Brasil, porém, o modelo DRE foi excluído das normas técnicas norte-americanas (2007) (10), foi proibido na Holanda (2008) (11), abandonado no Paraguai (2008) (12) e declarado inconstitucional na Alemanha (2009) (13).

### 1.3 Sistema de Voto Eletrónico na Estónia

Neste pequeno país da Europa, presidido por um programador (Toomas Hendrik Ilves), a realidade tecnológica não podia ser outra, pois a paixão pela tecnologia é um modo de vida. Em 2005, a comissão eleitoral nacional da Estónia deu um importante passo rumo ao desenvolvimento do Governo Eletrónico (e-Government). Pela primeira vez no mundo, a votação *online* não presencial “segura” através da Internet foi organizada à escala nacional. De acordo com a lei, o *iVoting* (como o sistema é conhecido no idioma da Estónia) estará disponível em todas as eleições. O *iVoting* visa oferecer aos eleitores um canal adicional através do qual podem expressar o seu voto, com o objetivo de aumentar a participação eleitoral por meio de uma melhor acessibilidade.



**Fig. 2 – Portal de voto da Estónia (Fonte: Vabarrigi, site do governo da estónia)**

Para votar eletronicamente através da Internet, os eleitores precisam apenas de ter um bilhete de identidade (que mais parece um multibanco) para efetuarem a autenticação eletrónica. O que não aumenta a complexidade da solução, uma vez que quase 100% dos cidadãos da Estónia, com idades compreendidas entre 15 a 74 anos, têm o bilhete de identidade válido. A votação pela internet não substitui o processo convencional de votação com cédula de papel nos centros de votação na Estónia, mas é uma alternativa complementar a este. Em 2007, 3,13% dos cidadãos com direito a votar fizeram-no *online*. Nas eleições europeias em Junho



de 2009, 15% dos cidadãos com direito a votar fizeram-no online. Em Março de 2011, 25% dos votos foram eletrónicos. O procedimento leva, em média, dois minutos e foi fortemente adotado nas últimas eleições pelos eleitores com mais de 55 anos de idade.

Na Estónia, as eleições duram 7 dias e o cidadão pode dentro desta baliza de tempo votar e alterar o seu voto se necessário, sendo que só o último voto é considerado/contabilizado pelo sistema. Acredita-se que esta medida seja um fator de segurança, uma vez que combate a compra de votos. Para além desta inovação, a possibilidade de se utilizar o telemóvel ou Tablet para se autenticar e votar, fazem do *iVoting* o sistema de voto eletrónico mais robusto do “mercado”, e colocam-no na linha da frente das aplicações que visam o desenvolvimento do governo eletrónico.

O *iVoting* já com 10 anos desde a sua primeira utilização, ainda é objeto de estudo por parte de analistas de segurança um pouco por todo mundo, o que surpreende os estonianos, pois para eles trata-se somente de mais um aplicativo, o que não deixa de ser curioso. A cultura de conectividade e de segurança eletrónica existente naquele país, sempre apoiada pelo primeiro-ministro Taavi Rõivas e pelo presidente Toomas Ilves, é sem dúvida um fator crítico de sucesso.

## 1.4 Objetivos

Considerando a diversidade de temas no domínio da Gestão de Identidade e Segurança de Informação, nesta tese de mestrado pretendo focar-me na questão que me parece emergir da generalidade das restantes temáticas.

Estudar as potencialidades do CC e tirar partido da vertente eletrónica do mesmo, possibilitando a leitura dos dados de identificação dos titulares neste mesmo documento digital.

Neste sentido, o principal objetivo desta tese de mestrado é dar um contributo na Identificação Digital de um sujeito bem como a caracterização e conceção de um sistema de autenticação forte com base no CC, que será essencial para elaboração de um sistema de voto eletrónico construído de raiz [protótipo em JAVA (Portal de voto) onde se aplica os conceitos de segurança abordados nesta tese e se tem uma experiência prática do trabalho realizado] denominado: E-voto com recurso ao cartão de cidadão.

Do ponto de vista tecnológico, a questão fundamental que se coloca é identificar qual a combinação “perfeita” entre tecnologia e processos sociais que garantam um conjunto muito vasto de propriedades que a sociedade considera como adquiridas relativamente ao processo de votação.

Os desafios são inúmeros, desde a necessidade de garantir que o Sistema de Voto Eletrónico funcione em grande escala sem problemas de fiabilidade e segurança, que possam colocar uma votação em causa.

O sistema deverá ser capaz de garantir: o aumento das oportunidades de voto e ao mesmo tempo o anonimato, a integridade dos votos devendo ser acessível e utilizável por uma imensa diversidade de pessoas, e finalmente, o sistema e os processos eleitorais deverão ser facilmente compreensíveis para os utilizadores comuns e entidades administrativas e políticas.

O E-voto (com recurso ao cartão de cidadão), permitirá a coexistência do voto presencial e remoto, incluindo:

- » Voto eletrónico em ambiente Internet (*on-line*).
- » Voto eletrónico em ambiente presencial (*on-line*).
- » Estação de Apuramento de Resultados que permita a contagem dos votos realizados via Internet e presencialmente.

## 2. Segurança da Informação

*"Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (14)*

### 2.1 Introdução

Informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe (15).

É sabido que o mundo caminha para uma “informatização” total, onde todo tipo de informação estará armazenado em sistemas digitais. Quando a evolução tecnológica iniciou, há cerca de 50 anos atrás, a necessidade de uma atuação na área da segurança dos dados contidos nos sistemas não era levada a sério. Inicialmente os sistemas eram puramente de processamento, onde entravam e saíam dados processados, não havia nenhum tipo de retenção permanente dos dados.

Com a evolução das tecnologias de informação foram sendo criados novos modelos de processamento, de armazenamento, de transmissão, de integração, tudo aquilo que hoje em dia está naturalmente associado a um computador. Com isso, dados e informações começaram a circular entre sistemas, sendo processados e armazenados, agora é “algo que está dentro” dos computadores. Sendo assim, temos que nos certificar que estas informações são disponibilizadas somente para quem tem esse direito.

*Cerveira* (16), menciona a complexidade do mundo moderno e a sua evolução, e considera que o homem depende “quase exclusivamente das informações que recebe e da rapidez com que pode contar com essas informações”.

*Le Coadic* (17), refere que o valor da informação varia consoante o indivíduo, as necessidades e o contexto em que é produzida e partilhada. Uma informação pode ser altamente relevante para um indivíduo e simultaneamente pode não ter qualquer significado para outro indivíduo.

Em pouco tempo, com a evolução tecnológica, a informação passou a ser algo mutável da noite para o dia. O que era contemporâneo passou a ficar cada vez mais obsoleto. Se grande parte dessa informação migrou para a Internet nos últimos anos, o mesmo aconteceu com os crimes e fraudes. Ano após ano, os casos de cibercrimes aumentam, principalmente quando o assunto gira em torno do universo corporativo ou devassa da vida privada. Esta realidade trouxe à tona a discussão sobre segurança e gestão da informação, deixando cada vez mais claro a necessidade de procurar proteção adequada contra essa ameaça “invisível”. Se há alguns anos atrás a preocupação era o vírus deixar o computador lento, agora o que preocupa é a quantidade de ameaças virtuais a que estamos sujeitos. Diante dessa realidade, ter a **informação segura** pode ser considerado um diferencial de mercado perante a concorrência.

A segurança da informação é alicerçada em 3 fundamentos principais: integridade (I), confidencialidade (C) e disponibilidade (D) de um ativo, de modo a preservar o seu valor para uma pessoa individual ou para uma organização. Esta informação pode ser digital ou não, aplicando-se no entanto as mesmas características de proteção.



**Fig. 3 Triângulo de Segurança da Informação**

Além destes 3 princípios base de segurança associada à informação, acima referenciados, o E-voto com recurso ao CC deve ter mais um conjunto de propriedades para que se justifique a sua implementação, tais como: Unicidade, Privacidade, Anonimato, Autenticidade, Transacionalidade, Disponibilidade e Não Repúdio.

## 2.2 Conceitos

Estas propriedades são importantes para garantir a credibilidade e a confiança dos eleitores no Sistema de Voto Eletrónico [SVE].

**Integridade** - propriedade que garante que a informação manipulada mantém todas as características originais estabelecidas pelo proprietário da informação, incluindo o controlo de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição) (18).

O SVE deve garantir que tanto no decorrer do processo eleitoral como depois do mesmo, os votos não podem ser alterados, forjados ou eliminados do sistema.

**Confidencialidade** - propriedade que limita o acesso à informação unicamente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação (18).

O SVE deve apresentar esta propriedade basilar, dado que em todas as fases do processo eleitoral existe troca de informação crítica que apenas deve ser perceptível para as entidades/atores devidamente autorizados pelo sistema.

**Disponibilidade** - propriedade que garante que a informação está sempre disponível para o uso legítimo, ou seja, para aqueles utilizadores autorizados pelo proprietário da informação (18).

O SVE deve estar disponível para o eleitor, enquanto decorrer o processo eleitoral e/ou até que o tenha utilizado, e deste modo, evitar a negação do direito ao voto (De acordo com o disposto no artigo 72.º da Lei nº 7/2007, de 5 de Fevereiro (19)).

**Unicidade** – O SVE só poderá permitir que cada eleitor vote uma vez (1 eleitor = 1 voto. De acordo com o disposto no artigo 71.º da Lei nº 7/2007, de 5 de Fevereiro), o que é uma regra da democracia e um direito constitucional.

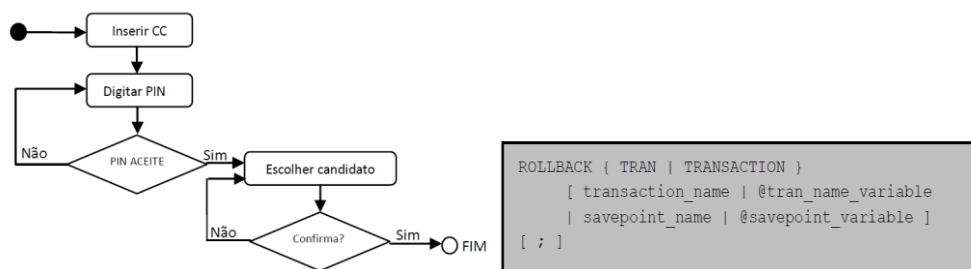
**Privacidade** - A privacidade, mais do que uma propriedade de segurança, é um direito (20), O SVE deve manter o secretismo pessoal da informação, livre de monitorização, bem como

do acesso a atores não autorizados, tendo em linha de conta a confidencialidade e integridade da informação em causa.

**Anonimato** - Designa o ato de manter uma identidade escondida. O SVE deve garantir que ninguém tenha acesso ao voto de nenhum cidadão, o que é um direito eleitoral (21).

**Autenticidade** - Autenticar o indivíduo e o sistema de voto, a identificação de um votante é validada e confirmada assim como o servidor aplicacional. Apenas os eleitores autorizados devem poder votar no SVE (maior de 18 anos por ex.).

**Transacionalidade** – No SVE, cada transação deve ter sucesso ou não ser tida em conta (0-1), devendo ser um “sistema de informação transacional”. Toda a alteração dos dados deverá ser efetuada dentro de uma “transação”, que ou grava todos os dados pertinentes ou, em caso de erro, retorna ao estado anterior, garantindo assim que a base de dados permanece sempre num estado de integridade (não permite gravar dados incompletos). “Se qualquer parte da transação falhar antes de ser confirmada, estas cópias são usadas para restaurar o banco de dados para o estado em que estava antes do início da transação (*Rollback*)”.



**Fig. 4 Transações (Visão Alto nível)**

**Irretratibilidade ou Não Repúdio** - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

O SVE deve conseguir provar caso necessário que o eleitor exerceu o direito de voto.

## 2.3 Mecanismos de Segurança

Para prover e garantir estes requisitos, foram adaptados e desenvolvidos os mecanismos de segurança que, quando corretamente configurados e utilizados, podem garantir a proteção/prevenção dos riscos associados ao SVE.

### 2.3.1 Segurança Física e Ambiental

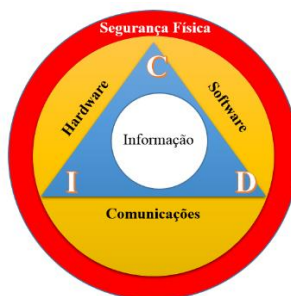
O ataque de 11 de Setembro de 2001 ao *World Trade Center* foi talvez o maior evento de impacto mundial dos últimos anos, que chamou a atenção dos especialistas de segurança para a lacuna existente entre sistemas de segurança física e informática.

Desde então dados acerca da segurança física de edifícios, portos, aeroportos, incluindo projetos e diagramas de sistemas e cablagem passaram a ser informação com caráter de

elevada confidencialidade pelo que têm de ser protegidos de acordo com as melhores práticas da segurança informática.

Devemos atentar para as ameaças sempre presentes mas nem sempre lembradas; incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede elétrica, acesso indevido de pessoas ao centro de processamento de dados, formação inadequada de funcionários, etc.

Segurança física ou ambiental são barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta (fig. 5), com o objetivo de prevenir o acesso físico não autorizado, os danos e as interferências na informação e nos recursos de processamento da informação da organização [NP\_ISO\_IEC\_27001\_213 Controlo A.11] (18). (Não aprofundado nesta tese).



**Fig. 5 Segurança Física**

Todo e qualquer sistema deve possuir um nível de segurança física, nível este que será obtido de acordo com o tipo da informação e dados que serão armazenados nestes sistemas. Por exemplo, a sala técnica onde estiverem os servidores de suporte aplicacional do SVE, tem de ser considerada um sistema de segurança física de grau de risco 4 (instalações de alto risco) e onde estiverem os terminais (Recinto de voto controlado) grau de risco 3 (instalações de médio/alto risco), isto segundo a norma EN50131-1 (22).

Por mais seguro que um sistema seja, ele não estará protegido da pessoa que o deseja invadir se ele(a) tiver acesso físico ao mesmo. Com base nesta máxima existem algumas “regras” ou boas práticas que devem ser tidas em consideração.

### **2.3.2 Recomendações/Boas Práticas para Segurança Física**

Deve-se instituir formas de identificação capazes de distinguir funcionários de visitantes e categorias diferenciadas de funcionários, se for o caso.

Solicitar a devolução de bens de propriedade da empresa (crachás, chaves, etc.), quando o visitante se retira ou quando o funcionário é retirado das suas funções.

Controlo de entrada e saída de materiais, equipamentos, pessoal, etc. registando a data, horários e responsável.

Supervisionar a atuação de equipas terceirizadas (limpeza, manutenção predial, vigilância, etc.)

Utilizar mecanismos de controlo de acesso físico em salas e áreas de acesso restrito (fechaduras eletrônicas, câmaras de vídeo, alarmes, etc.)

Proteger fisicamente as unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

Quanto maior o investimento em prevenção menor será o prejuízo em caso de Sinistro. O investimento não se refere apenas ao uso de tecnologia avançada, mas à forma como a empresa lida com a consciencialização dos seus funcionários.

### 2.3.3 Segurança Lógica

A *Segurança lógica* atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, backup desatualizados, violação de senhas, furtos de identidades, etc. (23). Considera-se segurança lógica a forma como um sistema é protegido (seja por *softwares* ou regras de restrições de acesso) ao nível do sistema operativo e aplicações. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de arquivos importantes de sistema ou aplicação.

As principais ameaças no que diz respeito à segurança lógica estão ligadas aos **acessos indevidos**, erros provocados e a perda de dados decorrente desses erros, falhas na rede provocadas por *software* estranho, fraudes e sabotagens.

Para implementar os mecanismos de segurança que apoiam os controlos lógicos são essenciais: **Identidade**, **Autenticação** (controlo de acessos), **Privacidade** (tecnologia de encriptação, políticas de segurança efetiva), **Autorização** (políticas de acesso) e **Assinatura**.

## 2.4 Identidade

*A identidade digital é a representação digital dos dados relacionados com uma pessoa, empresa, sistema, máquina, acessível através de meios técnicos.*  
[Wikipedia]

A filosofia contemporânea, principalmente a fenomenologia, tem tratado da identidade como o fundamento do ser: a identidade é o que permite ao **sujeito** tomar consciência de sua existência, o que se dá através da tomada de consciência de seu corpo, do seu saber (seus conhecimentos sobre o mundo), dos seus julgamentos (suas crenças), das suas ações (seu poder fazer). A identidade implica, então, a tomada de consciência de si mesmo.

As sociedades em geral têm tido uma grande atenção à **gestão da identidade** dos sujeitos, pois desde o tempo dos papiros que o sujeito tem registos de si mesmo. Ao longo do tempo a identidade tem sofrido grandes transformações, tal como o mundo. Hoje com a substituição do papel para o digital, implica que a gestão seja cada vez mais direcionada para as **identidades digitais** (*Infraestruturas de Autenticação e Autorização (AAI)*) (24).

Com a criação da **Lei n.º 7/2007** (25) onde a Assembleia da República decreta, nos termos da alínea c) do artigo 161º da Constituição, a criação do CC, representado na fig.6.

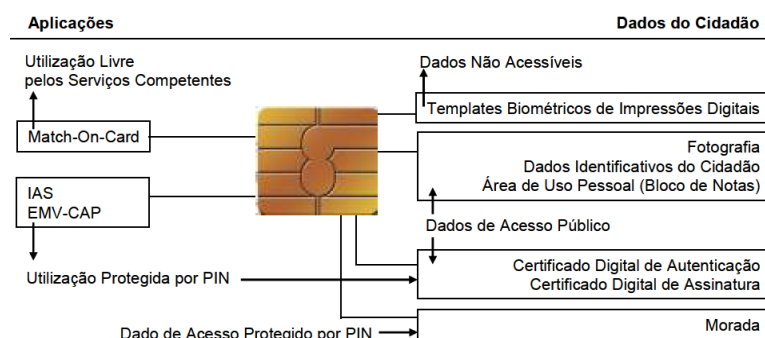
O CC como documento físico substitui cinco outros documentos: Bilhete de Identidade, Cartão de Eleitor, Cartão do Contribuinte, Cartão da Segurança Social e Cartão de Utente. Desta forma, reduzir os identificadores afetos a cada cidadão.



**Fig. 6 Frente e verso do Cartão de Cidadão**

O CC como documento digital é um documento de identificação múltipla que inclui uma zona destinada a leitura ótica e incorpora um circuito integrado (fig. 7) [Artigo 6.º, da Lei n.º 7/2007]. Dados como **número do cartão de cidadão** e data de nascimento contidos no mesmo, serão verificados no SVE, para garantir que se trata de um sujeito maior de idade e essencialmente garantir a **Unicidade** de voto. Esta informação consta no *chip* (escrito) para leitura eletrónica ou digital.

A zona específica destinada a leitura ótica contém os seguintes elementos de identificação do titular: apelidos e nomes próprios, nacionalidade, data de nascimento e sexo. Contém ainda a menção “República Portuguesa”, o tipo e o número de documento e a data de validade (artigo 7º, nº4, da Lei n.º 7/2007, de 5 de Fevereiro).



**Fig. 7 – Informações residentes no chip**

No âmbito da reforma das normas que regem a elaboração do recenseamento eleitoral, será considerada a eliminação do cartão de eleitor passando a ser utilizado apenas o cartão de cidadão. [Nota Informativa].



## 2.5 Privacidade

Quando uma entidade (B) garante que a informação recebida não será nunca disponibilizada a terceiros sem o acordo de (A), Pode ser também entendido como o direito de controlar a exposição e a disponibilidade de informações acerca de si.

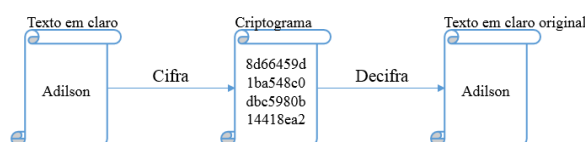
Para se manter o secretismo da informação, livre de monitorização bem como do acesso a atores não autorizados, tendo em linha de conta a confidencialidade e integridade da informação em causa, deverá ser feita em todas as fases do processo (comunicação e armazenamento):

- Criptografia (Túnel de comunicação e armazenamento cifrado).
- Assinatura Digital.

### 2.5.1 Criptografia

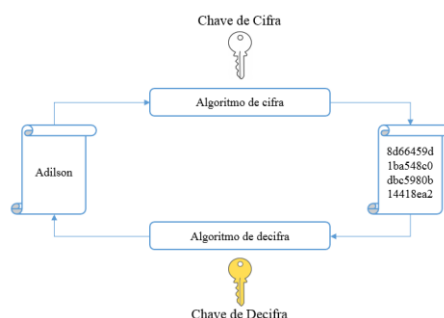
A criptografia é a arte ou ciência que permite escrever de forma a ocultar conteúdos (do grego *krypthós* – oculto + *graph* – raiz de *graphein*, escrever). O objetivo da criptografia é permitir que duas entidades possam trocar informação que é ininteligível para terceiros.

A criptografia baseia-se no uso de cifras. Uma cifra é uma técnica concreta de criptografia, isto é, uma forma específica de ocultar informação. Assim, uma cifra transforma um texto em claro num texto cifrado ou criptograma. A operação inversa é a decifra, que transforma o criptograma no texto original em claro.



**Fig. 8 – Princípio de criptografia**

A operação da maioria das cifras e decifras é definida através da especificação de um algoritmo e de uma chave fig. 9. O algoritmo define o modelo genérico de transformação de dados; a chave é o parâmetro do algoritmo que permite variar o seu comportamento de forma complexa.



**Fig. 9 – Criptografia**

Apesar de ter uma vital importância nos dias de hoje, a criptografia já estava presente no sistema de escrita hieroglífica dos egípcios. Inicialmente muito utilizada, principalmente para fins militares e diplomáticos (conhecida como **criptografia clássica**) como a **cifra de César** (**fig.10**) por exemplo.



**Fig. 10 – Cifra de César Criada por Júlio César para assegurar confidencialidade das mensagens escritas trocadas com os seus generais, é uma cifra de substituição muito simples e baseava-se em deslocar cada letra 3 posições para a direita, ficando conhecida como ROT3**

No âmbito da computação é importante que se possa garantir a segurança em todo o ambiente computacional (Computador, *PDA*, telemóvel, *smartcard*, etc.) que necessite de sigilo em relação às informações que manipula. O que exige o desenvolvimento de técnicas criptográficas cada vez mais avançadas e complexas, fortemente alicerçadas em funções matemáticas, a que se chama **criptografia moderna**, para garantir a privacidade.

A criptografia moderna pode classificar-se segundo dois critérios, são estes:

- Segundo as suas **características operacionais** podem ser:

Cifras por blocos.  
Cifras contínuas.

- Segundo o **tipo de chave** estas podem ser:

Cifras simétricas.  
Cifras assimétricas.

Estas classificações não são exclusivas entre si.

Não é objetivo desta tese fazer uma análise pormenorizada de todos os tipos de cifras usadas. É contudo, interessante realçar alguns aspetos de cada uma delas.

### 2.5.2 Modo de operação

**Cifras por Blocos** - A mensagem original é dividida em blocos de tamanho fixo. Cada bloco individual é tratado como uma mensagem original independente, cifrada com uma cifra monoalfabética.

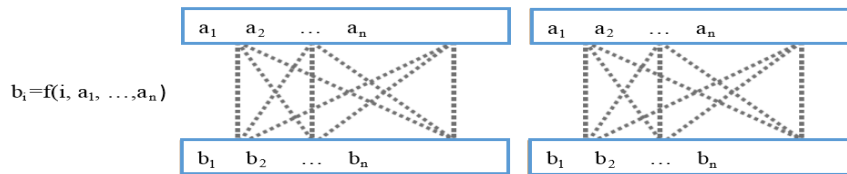


Fig. 11 – Cifra por Bloco

**Cifras Contínuas** – São Cifras polialfabéticas construídas por um gerado pseudoaleatório seguro cuja saída é somada com o texto original ou o criptograma. Deste modo cada carater do texto original, seja qual for a sua dimensão, será sempre traduzido para outro character de igual dimensão, mas a tradução do estado de operação da cifra contínua.

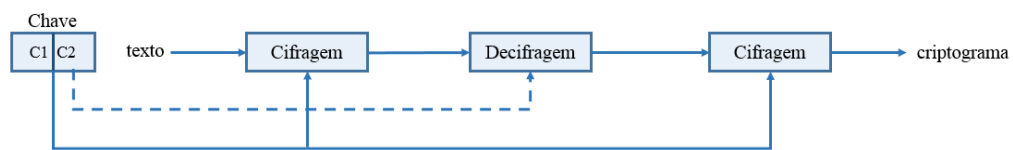


Fig. 12 – Cifra Contínua

### 2.5.3 Tipo de chaves

#### Cifras Simétricas

As cifras simétricas ou de chave privada são aquelas que empregam a mesma chave tanto para cifrar como para decifrar (fig. 13). Apresenta o inconveniente de que, para ser usada em comunicações, a chave deve estar tanto no emissor como no recetor, o que nos leva a perguntar **como transmitir a chave de forma segura?** DES, 3DES, AES e RC4 são alguns dos algoritmos que usam criptografia simétrica.

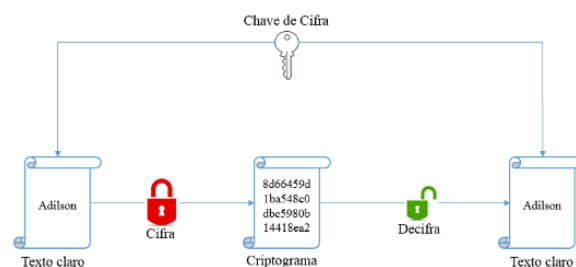
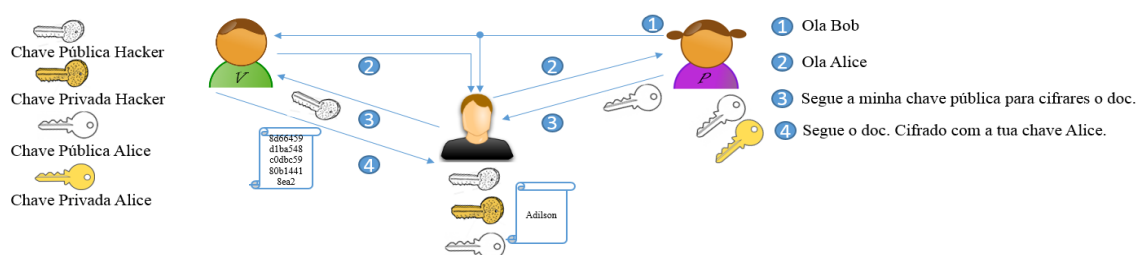


Fig. 13 – Cifra simétrica

O primeiro algoritmo baseado nestes princípios é o de *Diffie-Hellman* (26), que tem a seguinte vantagem: embora toda a troca de informação tenha sido feita em claro, a chave calculada é secreta. No entanto, este algoritmo não identifica os intervenientes, logo **quem**

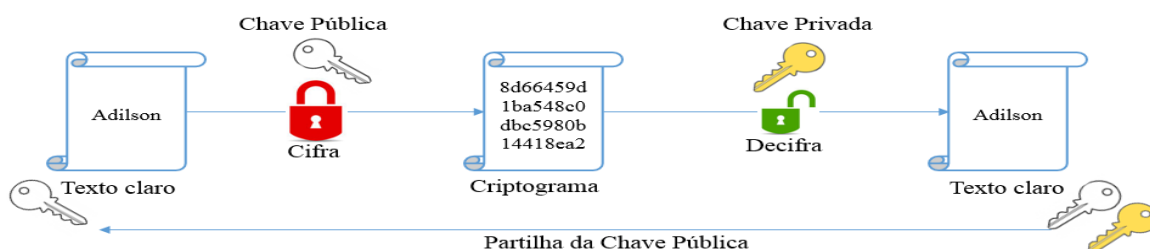
garante que o tráfego entre Alice e Bob na troca de chaves não teve um intercetor e o fez com cada um deles? O denominado *Man-in-the-Middle Attack* (27) fig.14.



**Fig. 14** Attack man-in-the-middle é uma forma de ataque em que os dados trocados entre duas partes, por exemplo (Alice e Bob), são de alguma forma interceptados, registados e/ou alterados pelo atacante sem que as vítimas se apercebam.

## Cifras Assimétricas

**Cifras assimétricas** ou de chave pública, que empregam uma chave privada e uma chave pública. Uma delas serve para cifrar e a outra para decifrar. Estes sistemas devem garantir que o conhecimento da chave pública não permita calcular a chave privada. Oferecem um leque mais amplo de possibilidades, podendo usar-se para estabelecer comunicações seguras por canais inseguros o que resolve o problema da troca de chaves. RSA, DSS e CURVAS ELÍPTICAS são alguns dos algoritmos que usam criptografia assimétrica.



**Fig. 15 – Cifra Assimétrica**

## Cifra Simétrica vs Cifra Assimétrica

Simétrica	Assimétrica
Numa comunicação entre dois intervenientes ambos necessitam assegurar a confidencialidade da chave.	Numa comunicação entre dois intervenientes apenas o destinatário necessita assegurar a confidencialidade da chave (privada).
Numa comunidade de N intervenientes, cada um necessita de gerir e proteger (N – 1) chaves.	Numa comunidade de N intervenientes, cada um necessita apenas de proteger a sua chave privada, podendo obter as chaves (públicas) de terceiro sem repositórios públicos.
Extremamente eficientes.	Complexidade computacional várias ordens de grandeza superior.
Tamanho de chaves muito inferior (por exemplo, 256bits).	Tamanho das chaves muito superior (por exemplo, 2.048bits).
É conveniente alterar frequentemente a chave (secreta) utilizada.	As chaves são de longa duração, dado que a sua substituição implicaria a reemissão dos seus certificados.

--	--

**Tabela 1** Comparação de cifras simétricas vs cifra assimétrica

Contudo estes dois tipos de criptografia não são antagónicos, mas sim complementares.

- A criptografia de chave pública é utilizada para autenticação e validação de documentos (algoritmos pesados e pouco adaptados a mensagens grandes).
- A criptografia de chave simétrica é utilizada para estabelecer canais de comunicações cifrados (algoritmos mais adequados à cifra de dados em larga escala)

Por exemplo o protocolo SSL utiliza uma combinação dos dois tipos de algoritmos.

#### 2.5.4 RSA: o Algoritmo utilizado no CC

O *RSA* é um algoritmo de criptografia de dados (**usado na chave assimétrica do CC para autenticação do titular**), que deve o seu nome a três professores do Instituto MIT (fundadores da atual empresa *RSA Data Security, Inc.*), *Ronald Rivest*, *Adi Shamir* e *Leonard Adleman*, que inventaram este algoritmo. Este algoritmo baseia a sua segurança na complexidade da factorização e cálculo de algoritmos modulares (de grandes números). O algoritmo funciona tal como mostra a tabela abaixo.

Valores públicos	$n$	Valor de grande dimensão, produto de dois grandes números primos $p$ e $q$ secretos.
Chave pública	$e$	$e < n$ , coprimo de $\phi(n) = (p - 1)(q - 1)$
Chave privada	$p, q, d$	$d < n$ , $e.d \equiv 1 \pmod{\phi(n)}$
Cifra	$C = P^e \pmod n$	
Decifra	$P = C^d \pmod n$	

**Tabela 2:** Algoritmo de cifra assimétrica RSA

Para decifrar um valor cifrado com a chave pública  $e$ , é preciso conhecer a chave privada  $d$ . O valor de  $d$  é fácil de calcular a partir de  $e$  para quem conhecer  $p$  e  $q$ , os fatores de  $n$ , porque  $\phi(n)$ , a função  $\phi$  de Euler, é igual a  $(p - 1)(q - 1)$ , mas a factorização de  $n$  é uma operação complexa. A outra forma de decifrar é inverter a exponenciação modular, isto é, calcular o algoritmo modular de  $C$  dados  $e$  e  $n$ , o que também é uma operação complexa. Assim, a função não pode ser invertida por quem só conhecer  $n$  e  $e$  (o valor público e a chave pública) e o alçapão são os valores  $p$  e  $q$ , usados para calcular  $n$ ,  $e$  e  $d$ .

A dimensão de  $n$  condiciona o tempo de execução do algoritmo de forma polinomial. No caso da exponenciação modular não se efetuam  $e$  ou  $d$  multiplicações, mas apenas  $2.l$ , onde  $l$  é o número de bits de  $e$  ou  $d$ . Para isso usa-se um método conhecido por quadrado e multiplicação fig.16.

$$\begin{aligned}
 a &= \sum_{i=0}^{l-1} a_i 2^i \\
 x^a &= x^{\sum_{i=0}^{l-1} a_i 2^i} = \prod_{i=0}^{l-1} (x^{2^i})^{a_i} \\
 x^a \pmod n &= 1 \cdot x^{2a_1} \cdot x^{4a_2} \dots x^{2^{l-2}a_{l-2}} \cdot x^{2^{l-1}a_{l-1}} \pmod n
 \end{aligned}$$

**Fig.16 – Aproximação quadrado e multiplicação para efetuar exponenciação modular com o número reduzido de operações (imagem feita com base no Livro do prof. Zúquete).**

O RSA pode igualmente ser usado como um algoritmo de assinatura. Com efeito:

$$(x^e \bmod n)^d \bmod n = x^{e \cdot d} \bmod n = (x^d \bmod n)^e \bmod n = x$$

Se usar-se  $d$  para cifrar  $x$ , assina-se este último porque só o detentor da chave privada  $d$  pode efetuar a cifra. A assinatura não esconde  $x$ , porque o valor público  $e$  serve para o revelar, mas garante a sua correção e autoria. O tema das assinaturas digitais será abordado em pormenor na secção a seguir.

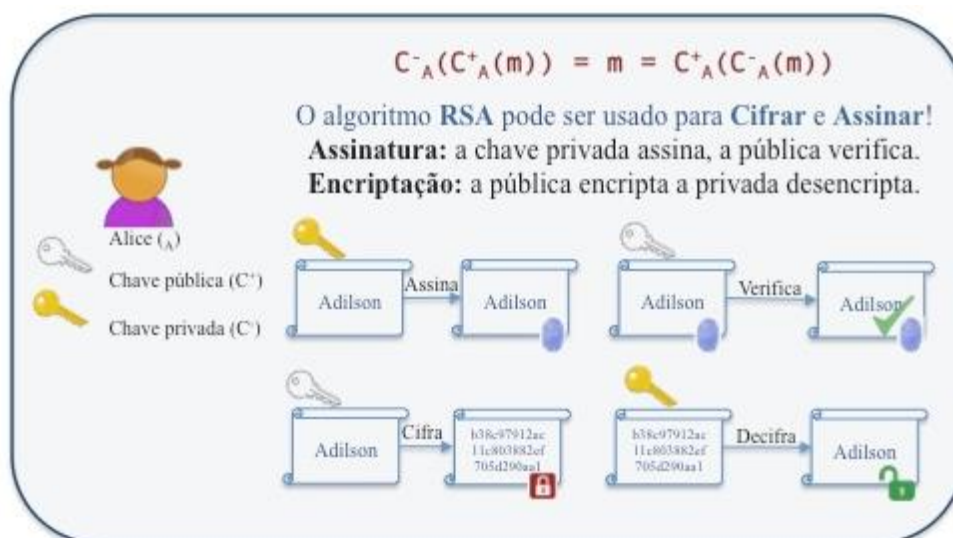
## 2.6 Assinatura

*Uma **assinatura** é uma marca ou escrito em algum documento que visa a dar-lhe validade ou identificar a sua autoria.*  
[Wikipedia]

O objetivo das assinaturas digitais é ir mais longe na garantia da origem e assegurar a autoria (autenticidade e a integridade) de uma mensagem para terceiros. Uma mensagem assinada digitalmente deverá ser associável a uma e uma só entidade e a sua assinatura deverá poder ser validada universalmente.

Por exemplo o *smartcard* do CC possui um par de chaves assimétricas de assinatura digital, as quais podem ser usadas por diversas aplicações para assinar documentos.

Tecnicamente, e de forma resumida, uma assinatura digital de um documento consiste na cifra do mesmo com a chave privada do autor ou subscritor do documento. O criptograma resultante não serve para esconder o documento original mas sim para garantir, a quem o decifra com a chave pública correspondente, que o texto recuperado, caso esteja igual ao original, está correto e foi assinado pelo detentor da chave privada.



**Fig.17 – Calcular cifra e assinatura com chave Assimétrica.**

### 2.6.1 Validação da Assinatura



**Fig.18 – Processo de assinatura e confirmação de um documento**

Na realidade, a certificação por encriptação simples é dispendiosa do ponto de vista informático, pois encriptar com *RSA* consome muito *CPU*,

Por isso utiliza-se primeiro uma função de *Hash* que cria um *Digest* (resumo) do documento a certificar, e só este é encriptado com a chave privada do remetente.

Uma função de *Hash* tem as seguintes propriedades:

- A partir de uma mensagem  $m$  de qualquer tamanho, produz um *digest*  $x = H(m)$  de tamanho fixo
- Se  $m \neq m'$  então  $H(m) \neq H(m')$
- Dado um *digest*  $x$ , é “impossível” computacionalmente deduzir  $m$ , tal que  $x = H(m)$ . Assim, o *digest* funciona como a impressão digital de uma mensagem.
- Funções matemáticas muito eficientes capazes de mapear mensagens de qualquer tamanho, em valores de tamanho fixo, denominados de valor de *hash*.

#### Funções de Hash mais utilizadas:

##### MD5: Message-Digest algorithm 5 (Rivest 1991)

- *Digest* de 128 *bits*. Não é considerada completamente segura (dado terem sido descobertas vulnerabilidades graves de segurança que permitem encontrar facilmente duas mensagens com o mesmo valor de *hash*).

## SHA: Secure Hashing Algorithm (NSA 1995)

- **SHA-1** produz um *digest* de 160 *bits* (Apesar de ainda bastante popular, a sua utilização é desaconselhada dado terem sido descobertas vulnerabilidades teóricas que tornam computacionalmente tratável a procura de duas mensagens com o mesmo valor de *hash*).
- **SHA-2** Produz um valor de *hash* de 32 *bytes* (256 *bits*) e 64 *bytes* (512 *bits*), respetivamente.

## 2.7 Certificados Digitais

### O problema

Da cifra de chave pública, tanto para encriptar mensagens como para validar assinaturas, resume-se no seguinte:

Como o titular de uma chave pública pode disseminá-la a terceiros com quem pretende interagir?

- Meios físicos, por exemplo entregando-a em mão nem sempre é prático e/ou possível
- Meios eletrónicos, por exemplo disponibilizando-a para *download* ou enviando-a por correio eletrónico, como é que o destinatário poderia ter a certeza de que o titular é quem diz ser?

### A Solução...

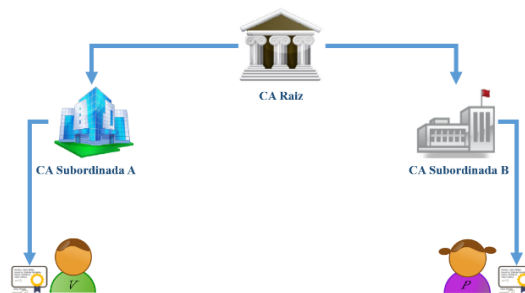
Certificados resolvem ambos estes problemas ao...

- Associarem a identidade do titular à sua chave pública
- Serem emitidos e assinados digitalmente por uma Entidade Certificadora confiável, ou seja, criar uma relação de confiança entre três entidades:

1. O sujeito a quem pertence a chave pública (i.e.: Alice)
2. O público em geral (i.e.: Bob)
3. Uma entidade em que ambos confiam (*Trusted Third Party*) Fig. 19.

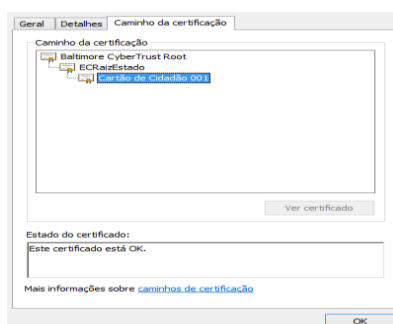
A prova de posse da chave pública é assegurada por um Certificado Digital que contém a chave da Alice e é assinado por uma Autoridade de Certificação (*CA - Certification Authority*). Para obter o reconhecimento automático das aplicações, usualmente as *CA's* necessitam de Ser certificadas por *CA's* de raiz que já sejam reconhecidas pelas aplicações (hierarquia de confiança) Fig. 19.





**Fig. 19 – Hierarquia de Confiança**

As CA's de Raiz (*Baltimore CyberTrust Root* no CC abaixo) emitem diretamente os certificados (terceiro confiável) enquanto as CA's Intermediárias (*ECRaizEstado* no CC abaixo) cujos certificados são emitidos indiretamente pelas CA de Raiz. Podemos pensar no caminho entre a CA de Raiz e o Cliente (Cartão de Cidadão 001 no CC abaixo) como uma ramificação, já que existem as CA de Raiz, que emitem os certificados para as CA's Intermediárias, se existirem, até ao Cliente ou utilizador final que aplica o certificado.



**Fig. 20 – Hierarquia de Confiança no CC**

O formato mais utilizado pelos certificados digitais é definido pela norma X.509 v3 (28) (Utilizado por exemplo no CC).

Existem outros formatos para utilizações mais específicas por exemplo os certificados CVC (29) utilizados nos Passaportes Eletrónicos e outros documentos de viagem ICAO.

### 2.7.1 Gestão dos Certificados Digitais

Os Certificados Digitais são geridos por Autoridades de Certificação quer públicas (Portugal SCEE por exemplo), quer privadas (*Multicert*, *VeriSign* por exemplo) que são responsáveis por:

- Receber pedidos de certificados validados pela Entidade de Registo e emitem o correspondente certificado digital.
- Definir e publicar a Política de Certificação (CPS) e as Políticas de Certificados (PC's).
- Gerir o ciclo de vida dos certificados digitais que emitem emissão, renovação, suspensão, ativação e revogação.
- Publicar em repositórios os certificados digitais e as CRL's (listas de certificados revogados) que emitem.
- Estabelecer as regras e procedimentos operacionais a observar, quer internamente quer nas Entidades de Registo que as representam.

### 2.7.2 Entidades Registo (RA)

- Recebe pedidos de utilizadores, com a respetiva documentação para emitir, renovar, revogar, etc.
- Valida e arquiva a documentação entregue pelos utilizadores que necessitam de provar a sua identidade, a propriedade de um determinado domínio, etc.
- Comunica com a CA utilizando canais privilegiados/autenticados, faz chegar a esta os pedidos aprovados
- Cumpre e faz cumprir as Políticas de Certificados e as demais regras definidas pela CA.

### 2.7.3 Entidades de Validação (OCSP)

Disponibilizam um serviço de valor acrescentado que permite validar se um certificado digital se encontra revogado/suspensão.

- Mais fiável do que a consulta das CRL's, dado que estas apenas são emitidas periodicamente.
- Entidades de certificação não são obrigadas a disponibilizar este serviço mas...
- Caso o façam, devem incluir o respetivo URL nos certificados emitidos.
- Caso não o façam, devem emitir CRL's com mais frequência, no sentido de minimizar o risco de aceitação indevida de certificados revogados.

#### 2.7.4 **Políticas de Certificados (PCs)**

Informam o público em geral sobre a utilização autorizada, responsabilidades inerentes e garantias associadas a cada tipo de certificado emitido por uma determinada CA.

Por exemplo, assinaturas digitais realizadas usando certificados de autenticação não vinculam o titular.

Para cada tipo de certificado...

- Definem as respetivas regras de emissão e utilização
- Por exemplo, necessidade de verificação presencial de identidade
- Especificam o perfil de certificado correspondente

Por exemplo, período de validade, utilizações permitidas para a chave privada, extensões incluídas, etc.

#### 2.7.5 **Declaração de Práticas de Certificação (CPS)**

Informam os interessados sobre o modo de funcionamento geral da CA, incluindo:

- Processos de emissão, renovação, suspensão, ativação, revogação e publicação de certificados.
- Estrutura interna e segregação de funções.
- Procedimentos de validação de identidade, documentação de suporte e respetivo arquivo.
- Medidas de segurança física, ambiental e processual.
- Perfis de certificados suportados.
- Certificações e programas de auditoria.
- Responsabilidades legais da CA.

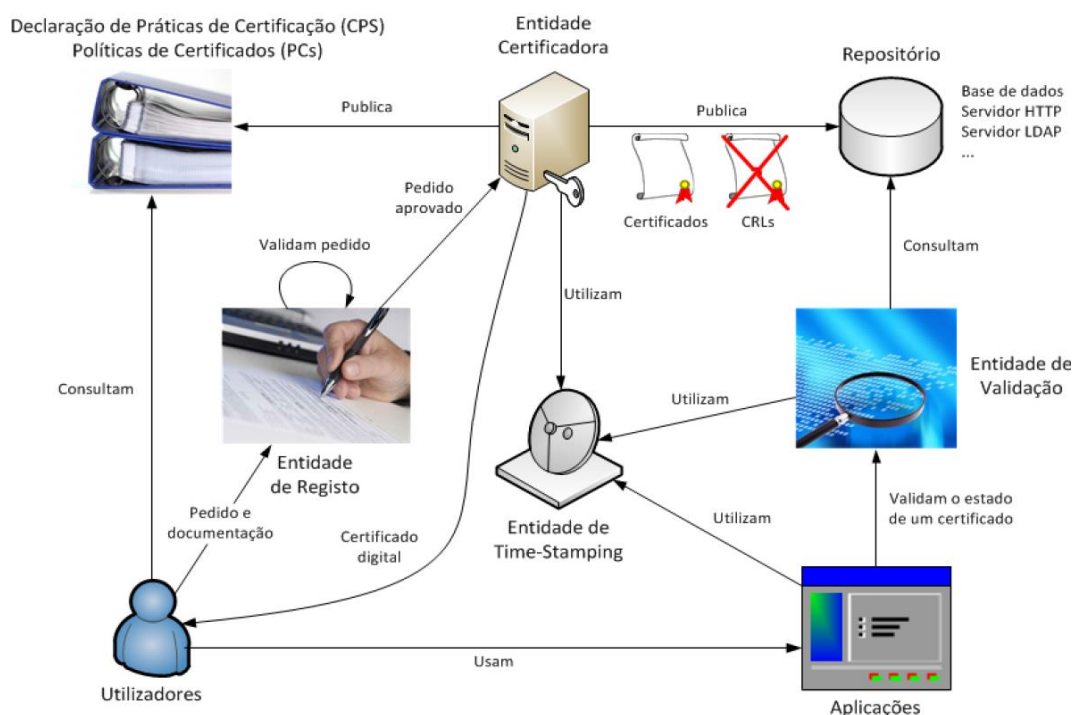
### 2.7.6 Entidade de Time-Stamping (Selos Temporais)

- Disponibilizam um serviço de emissão de *time-stamps*, que associam um valor de *hash* a uma determinada data/hora, provando a existência nesse momento da respetiva informação.
- Utilizam fontes de tempo redundantes e altamente fiáveis, disponível via *Internet* (com sincronização via protocolo *NTP*) ou recorrendo a equipamentos dedicados (por exemplo relógios atómicos)

### 2.7.7 Listas de Revogação (CRLs)

Documentos eletrónicos que identificam todos os certificados revogados por uma determinada CA.

Por exemplo, por omissão a funcionalidade de assinatura digital com o CC não está ativa quando o cartão é entregue ao seu titular. Tal é feito através da publicação de um certificado de revogação, na *CRL* da sua *EC*. Ou ainda em virtude da quebra de confidencialidade da chave privada do utilizador ou da perda do dispositivo onde estava alojada a chave.



**Fig. 21 – Gestão de certificados digitais**

A utilização de certificados como método de identificação dos utilizadores em geral é limitada, pois a gestão e manutenção de milhões de certificados é uma tarefa complexa e difícil de implementar. Na realidade, os certificados são sobretudo utilizados para validar empresas, *sites*, serviços para permitirem estabelecer condições de segurança e de confiança para o acesso dos utilizadores. A identificação e autenticação dos utilizadores são geralmente realizadas através de outros processos como veremos adiante.

## **2.8 Enquadramento Legal**

Em termos de enquadramento legal, considerando a necessidade de qualquer norma respeitar a legislação aplicável a cada organização ou país, entende-se como crucial identificar as leis com relevância aplicável em Portugal, para que seja possível proporcionar a correta e adequada aplicação das normas de segurança às necessidades de segurança da informação identificadas, sem que sejam violadas as leis em vigor.

### **2.8.1 Legislação Nacional**

Embora se verifique que a legislação portuguesa em vigor não contempla a totalidade dos aspetos relacionados com a segurança da informação, frequentemente dispersos em diversa legislação, considera-se pertinente conhecer aqueles que mais diretamente dizem respeito à problemática do Voto eletrónico e à segurança da informação, e como tal, influenciam a utilização do diverso normativo de segurança da informação.

O enquadramento legislativo da segurança da informação é proporcionado por um conjunto de legislação, onde se destaca:

Lei da Criminalidade Informática – Lei nº 109/91, de 17 de Agosto;  
Lei da Proteção Jurídica de Programas de Computador – Lei nº 252/94, de 20

de Outubro;

Lei da Proteção de Dados Pessoais – Lei nº 67/98, de 26 de Outubro;  
Definição dos Documentos eletrónicos e assinatura digital Decreto – Lei nº 116-A/2006, de 16 de Junho;

E uma

Lei Eleitoral do Presidente da Republica.

A legislação referenciada atende a um princípio constitucional constante do seu artigo 35º (Utilização da Informática) e que estabelece que “todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito ...” (ponto 1), que “a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do seu titular, ...” (ponto 3) e ainda que “é proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei” (ponto 4), que permitem um enquadramento daquilo que é permitido acerca da segurança da informação detida pelas

organizações, quer esta diga respeito aos seus clientes, aos seus funcionários ou até aos seus parceiros de negócio.

### **2.8.2 Lei da Criminalidade Informática**

A Lei da Criminalidade Informática (109/91, de 17 de Agosto) proporciona o enquadramento em termos do Código Penal dos crimes no âmbito da Informática, apresentando uma tipificação desses crimes e a respetiva moldura penal [AR 1991].

Perante estes pressupostos, são identificados seis crimes ligados à informática:

- (1) Falsidade informática (artigo 4º);
- (2) Dano relativo a dados ou programas informáticos (artigo 5º);
- (3) Sabotagem informática (artigo 6º);
- (4) Acesso ilegítimo (artigo 7º);
- (5) Interceção ilícita (artigo 8º);
- (6) Reprodução ilegítima de programa protegido (artigo 9º).

### **2.8.3 Proteção Jurídica de Programas de Computador**

Esta Lei (252/94, de 20 de Outubro) transpõe para a ordem jurídica portuguesa a Diretiva nº 91/250/CEE, do Conselho Europeu, de 14 de Maio, relativa à proteção Jurídica de programas de computador.

Esta Lei [AR 1994], de acordo com o estabelecido no seu artigo 1º, atribui proteção, “aos programas de computador que tiverem carácter criativo”, análoga à que é conferida às obras literárias, com equiparação a “programa de computador o material de conceção preliminar daquele programa”.

A Autoria, a Reprodução e Transformação, os Direitos do Utente, a Descompilação, os Direitos, a Apreensão, a Vigência e a Tutela, são algumas das temáticas abrangidas por esta Lei.

### **2.8.4 Lei da Proteção de Dados Pessoais**

A Lei da Proteção de Dados Pessoais (67/98, de 26 de Outubro) transpõe para a ordem Jurídica portuguesa a Diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho Europeu, de 24 de Outubro de 1995, relativa à proteção de Pessoas Singulares em relação ao tratamento de dados pessoais e à livre circulação desses dados.

Esta Lei [AR 1998], de acordo com o estabelecido no seu artigo 4º, “aplica-se ao tratamento de dados pessoais por meios totais ou parcialmente automatizados, bem como ao tratamento

por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados”.

Refira-se ainda a sua aplicação à “videovigilância e outras formas de captação, tratamento e difusão de som e imagens que permitam identificar pessoas”.

### 2.8.5 Documentos eletrónicos e assinatura digital

De acordo com o artigo 6.º, n.º1, da Lei n.º 7/2007, de 5 de Fevereiro, “o cartão de cidadão é um documento de identificação múltipla que inclui uma zona específica destinada à leitura ótica e incorpora um circuito integrado.”

No âmbito da reforma das normas que regem a elaboração do recenseamento eleitoral, será considerada a eliminação do cartão de eleitor passando a ser utilizado apenas o cartão de cidadão. [Nota Informativa].

Nenhuma autoridade ou entidade pública ou privada pode exigir para efeitos de identificação qualquer outro dado pessoal do titular de cartão de cidadão que não seja facultado pelos respectivos meios eletrónicos.

Os **certificados digitais qualificados** contidos no cartão de cidadão, permitem ao seu detentor efetuar a Assinatura Eletrónica Qualificada com o valor probatório instituído pelo Dec-Lei 290-D/99, de 2 de Agosto, e demais legislação complementar. De onde decorre que:

Nenhuma autoridade ou entidade pública ou privada pode recusar o valor probatório da assinatura eletrónica aposta pelo cidadão num documento eletrónico.

### 2.8.6 Lei Eleitoral do Presidente da Republica

Embora não trate de aspetos técnicos a LEI ELEITORAL DO PRESIDENTE DA REPÚBLICA Decreto-Lei n.º 319-A/76, de 3 de Maio, é uma base para qualquer sistema de voto quer seja eletrónico ou tradicional, pois detém o princípio e as regras democráticas a seguir/implementar no SVE (no caso).

Estes elementos são importantes para alinhar o SVE como a lei vigente na Republica Portuguesa. Não é objetivo deste trabalho aprofundar aspetos jurídicos, mas é importante realçar que os fundamentos de segurança foram alicerçados nesta lei eleitoral, com destaque em alguns artigos, tais como os artigos (1º, 70º, 71º, 72º e 73º) (19) (20).

### 3. Modelos de Autenticação

A Autenticação (do grego : *αυθεντικός* = real ou genuíno, de '*authentēs*' = autor) é o ato de estabelecer ou confirmar algo (ou alguém) como autêntico, isto é, que reivindica a autoria ou a veracidade de alguma coisa. A autenticação também remete para a confirmação da proveniência de um objeto ou pessoa, neste caso, frequentemente relacionada com a verificação da sua identidade.

Autenticar, juridicamente, consiste no procedimento legal relativo de tornar *autêntico* - ou verdadeiro - algo que seja cópia ou cuja autoria e veracidade necessitam ser comprovadas.

Para isto, os sistemas legais criam figuras específicas, dentro da estrutura judiciária, com poderes específicos de fé pública e competência legal para atestar, mediante uma declaração que pode ou não ser lavrada em livro próprio, mas que deve ser inserida na peça que se quer autenticar, onde o mesmo apõe o seu sinal público (assinatura).

Em segurança da informação, a autenticação é um processo que busca verificar a **identidade** (credenciais que lhe são associadas) digital do utilizador, de um sistema, programa ou computador.

Para estabelecer a identidade de um sujeito são necessárias as credenciais que lhe são associadas, e um contexto de confiança que permita verificar que estas correspondem a um sujeito existente (*processo de verificação de uma identidade alegada, por meio de comparação das credenciais apresentadas pelo sujeito com outras pré-definidas. Como a combinação username/password por exemplo*). O conjunto destes elementos designa-se **Sistema de Autenticação**.

#### 3.1 Credenciais

Existe hoje em dia uma enorme diversidade de sistemas de autenticação. Porém, devem ser adaptados à realidade de cada organização, pois a complexidade das credenciais e da prova de autenticação dependem do grau de certeza que se pretende obter. Na maioria dos casos, a prova de autenticação é baseada num ou mais segredos e numa relação de confiança entre a entidade que emite as credenciais e a que as verifica.

As credenciais permitem a identificação da entidade ou sujeito geralmente baseadas em vários tipos de informação (algo que o sujeito é, algo que o sujeito possui, algo que o sujeito conhece ou a combinação de vários destes fatores). Estas informações são designadas por fatores de autenticação.

Quantos mais fatores são apresentados para a identificação, mais robusta será a autenticação.

#### 3.2 Autenticação Simples

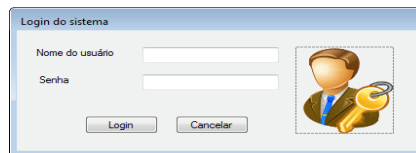
O sistema de autenticação, como já foi referido, vai garantir a prova da identidade da credencial, garantindo o nível de segurança da prova. Na sua forma mais simples é utilizado o *User/ Password* [utilizado na maioria das aplicações correntes (Fig. 22)], geralmente inseguro



pois baseia-se num segredo elementar que o utilizador pode recordar, que é portanto muito fácil de quebrar por força bruta ou dicionário.

Porém, aplicando boas políticas de segurança na organização como por exemplo, *passwords* com mais de 7 caracteres, renovação das mesmas a cada 90 dias, armazená-las encriptadas na BD, pode-se conseguir dar robustez ao sistema.

No entanto, estas medidas podem perder o seu valor quando os utilizadores ou se esquecem da *password* constantemente ou as guardam em ficheiros inseguros (Excel por ex.) ou até debaixo do teclado. Por outro lado a administração de *passwords* em ambientes com muitas aplicações onde os utilizadores têm *passwords* diferentes não é uma tarefa fácil, e cresce a probabilidade de haver proliferação de *passwords* que é uma ameaça de segurança. Quando tal acontece recorre-se muitas vezes a autenticações centralizadas ou federadas.



**Fig. 22 – Login USER/PASSWORD**

### 3.3 Challenge - Response

No desafio – resposta a credencial é usada como base de uma transformação de um valor sugerido pelo sistema de autenticação, o que permite construir sistemas mais seguros.

Requisitos:

- O valor do *challenge* tem de ser aleatório e não reprodutível (*nonce*) para evitar ataques de *replay* em que um intruso captura a credencial e a resposta do sujeito, simulando mais tarde uma autenticação em que responde com o mesmo valor.
- A transformação tem de ser suficientemente complexa para evitar a dedução do segredo (ex. função de *hash* ou criptográfica).

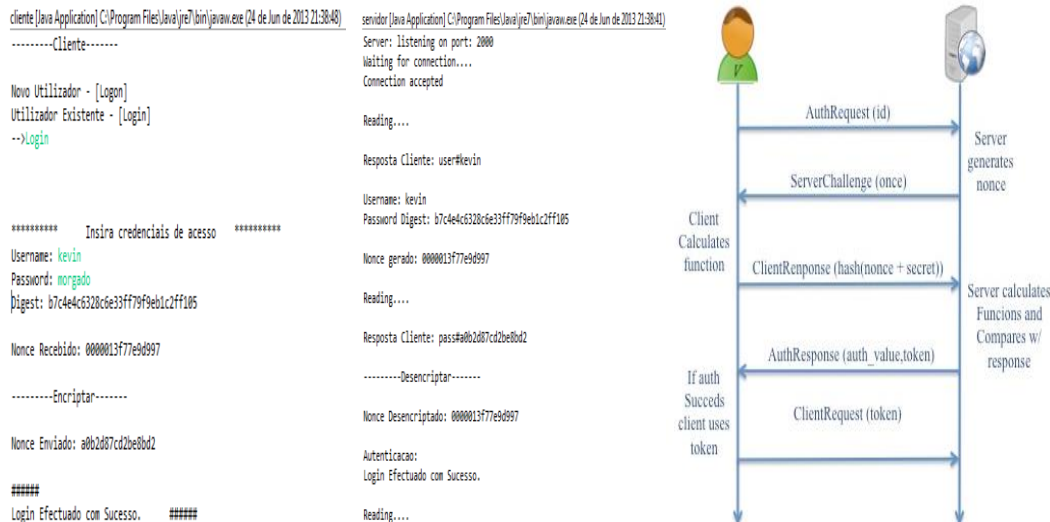
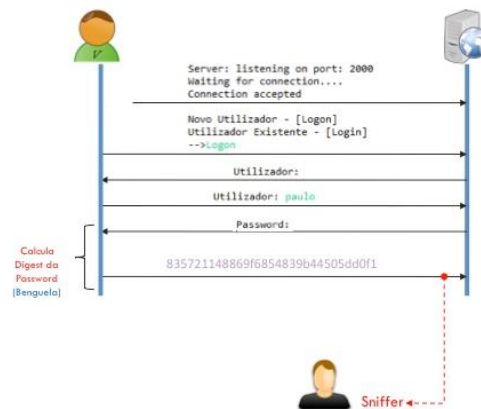


Fig. 23 – Challenge Response

1. A aplicação servidor conhece um conjunto de credenciais de utilizadores (*username* e *password*) que estão armazenadas em ficheiros *txt*, estando as *passwords* sob forma de *digest* (p.ex. MD5).
2. A aplicação cliente começa por pedir ao utilizador o seu *username*.
3. O cliente abre uma conexão para o servidor (utilizando p.ex. a socket API), envia o nome do utilizador em claro e fica à espera de receber uma resposta.
4. O servidor verifica que conhece o nome do utilizador e o *digest* da respetiva *password* armazenada.
5. O servidor envia de volta uma mensagem de *challenge* ao cliente contendo um *nonce* *N* de 64 bits (8 bytes), obtido p.ex. pela concatenação do valor do tempo sistema (32 bits - 4 bytes) com um número inteiro aleatório (32 bits - 4 bytes), e fica à espera da resposta do cliente.
6. O cliente pede ao utilizador a sua *password* *P* e calcula o seu *digest* (p.ex. MD5), obtendo assim  $D_p = MD5(P)$ , com 128 bits (16 bytes).
7. O Cliente utiliza o *digest*  $D_p$  da *password* como uma chave de encriptação *K*, e encripta o *nonce* *N* usando o *Tiny Encryption Algorithm*, obtendo a resposta  $R = TEA(K, N)$ , que envia de volta ao servidor (16 bytes).
8. O servidor descripta o valor recebido usando o mesmo algoritmo TEA, usando o *digest*  $D_p$  da *password* do utilizador armazenada obtendo  $N' = TEA^{-1}(K, N)$ .
9. **if**  $N == N'$ , então o cliente está na posse da *password* certa e está a responder diretamente ao servidor, pois o *nonce* é válido, provando portanto a sua identidade: o servidor envia uma mensagem de sucesso ao cliente
10. **else** não há prova de autenticação. E o servidor envia uma mensagem de erro ao cliente.

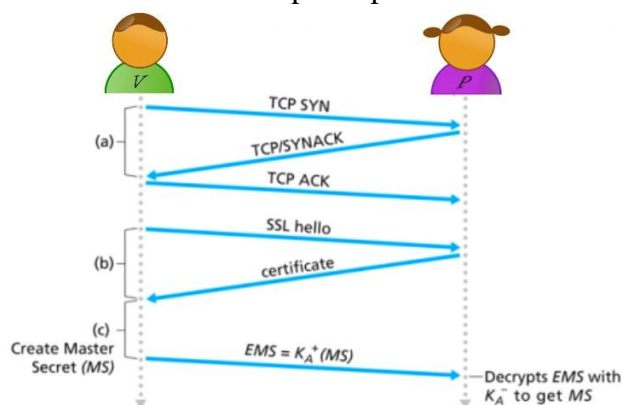
O *Challenge Response* é um sistema forte e seguro de autenticação. Porém deixa algumas “brechas” para invasões, pois a credencial (encriptada) passa pela rede descoberta, o que acarreta o risco de um ataque por *sniffer* ou *replat* (Fig.24).



**Fig. 24 – Sniffer (Challenge – Response)**

### 3.4 Sistemas Híbridos

Para evitar ataques de *replay* ou *sniffer* utilizam-se sistemas híbridos (combinam vários tipos de sistema de prova para garantir níveis de segurança elevados) ou seja: Um canal encriptado com protocolos da família *EAP* (*Extended Authentication Protocol*) utilizados em redes 802.11, para realizar o *challenge response*. Pois na realidade o *challenge-response* não é seguro sobretudo na resposta do sistema em caso de autenticação bem-sucedida. Geralmente envia um *token* (ex.: cookie) que irá permitir ao sujeito identificar todos os seus os acessos posteriores, por isso utiliza-se um canal encriptado para realizar o *challenge-response*.



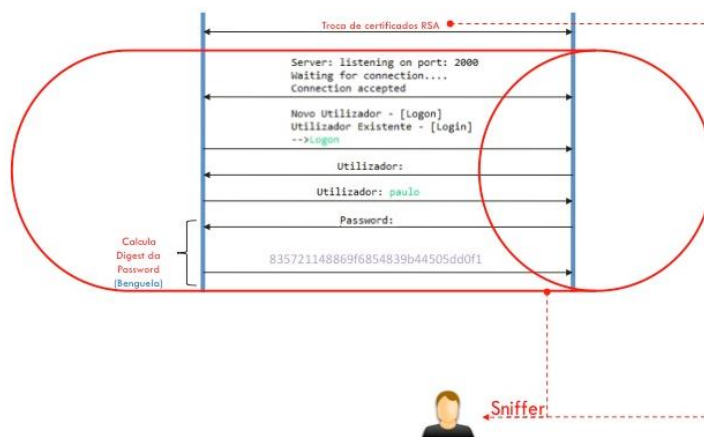
**Fig. 25 – Túnel TLS com certificado da Alice**

- a) Bob e Alice abrem uma ligação *TCP*
- b) Bob envia um *SSL Client Hello* pedindo o estabelecimento da sessão
- Alice envia o seu certificado

c) Bob gera uma chave de sessão (*MS*), encripta-a com a chave pública de Alice extraída do certificado, e envia-a a Alice.

d) Alice e Bob partilham uma chave secreta com a qual criam um canal encriptado para a troca de credenciais

## Riscos em Sistemas Híbridos



**Fig. 26 – Captura do Certificado**

Os sistemas híbridos fornecem mais consistência ao *challenge-response*, porém, não são incontornáveis. Muitas vezes porque não se tem o devido cuidado com o momento da troca dos certificados, eles são capturados e consequentemente usados para passar pelo servidor onde nos queremos ligar e assim roubam-nos a identidade. Por isso deve-se confirmar que o servidor é legítimo e que o cliente é quem diz ser.

## 3.5 Autenticação Mútua

Em muitas circunstâncias, o cliente de um serviço precisa de, ou deve, autenticar o servidor, ou seja, precisa de assegurar de que esta a dialogar com o servidor correto. Tal, é particularmente crítico quando se usa a apresentação explícita de elementos de prova para autenticar o cliente, porque caso esteja a dialogar com um impostor, este terá a possibilidade de se apoderar do elemento de prova e posteriormente personificar o cliente. Mas também é importante quando se usa a apresentação implícita de elementos de prova porque em certos casos as respostas a desafios podem favorecer um atacante.

A autenticação dos servidores tem de ser feita com um elemento de prova que o cliente conheça. Essa prova pode ser um segredo partilhado ou um par de chaves assimétricas. Caso seja um segredo partilhado, será naturalmente o segredo que partilha com o cliente para a autenticação deste último; caso seja um par de chaves assimétricas, o cliente terá de conhecer a sua componente pública (que poderá ser facultada durante a execução do protocolo através de um certificado da mesma).

A autenticação única não precisa ser simétrica, tendo em conta que o método usado no sentido cliente - servidor não precisa ser igual ao que é usado no sentido contrário servidor - cliente.

A tabela 3 resume algumas combinações existentes e possibilita demonstrar a riqueza combinatória existente.

De notar, como é evidente na referida tabela, que não existe qualquer protocolo em que a autenticação do servidor se faça com a chave secreta quando a autenticação do cliente é feita com as chaves assimétricas. Com efeito a autenticação com chaves assimétricas é normalmente mais complexa e requer mais trabalho, logo mais penosa para o cliente, sendo, por isso, reservada para os servidores. Por isso, não faz sentido autenticar os clientes com pares de chaves assimétricas, o que lhe traz mais complexidade mas liberta-os de ter de partilhar um segredo com o servidor, e depois exigir que esse mesmo segredo tenha de existir e ser partilhado para autenticar o servidor.

	Autenticação do servidor	
Autenticação do cliente	Chave secreta	Chaves assimétricas
Chave secreta	MS-CHAPv2[250] Kerberos [158]	SSH [47,200,241]
Chaves assimétricas		PEAP EAP-TTLS SSL/TLS [55] EAP-TLS [208]

**Tabela 3:** Autenticação mútua em diversos protocolos cliente > servidor

Os protocolos de autenticação mútua podem resultar da composição de dois protocolos de autenticação unilateral, mas normalmente estes são misturados de forma a minimizar o número total de mensagens, tal como é explicado nas figuras 27 e 27. Exemplos deste tipo de protocolo, mas usando funções de síntese para a geração das respostas aos desafios, são o protocolo *MS-CHAPv2*, e o protocolo de acordo em quatro passos do *802.1X*.



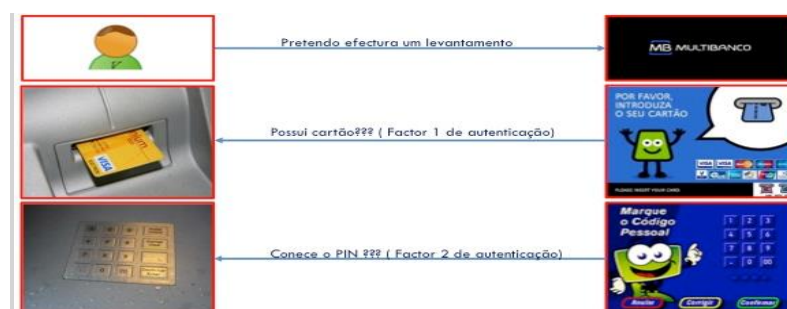
**Fig. 27 – Protocolo genérico de autenticação mútua com desafio-resposta, funções invertíveis  $f$  e  $g$  e elemento de prova  $\epsilon$**



**Fig. 28 – Protocolo genérico de autenticação mútua com desafio-resposta, funções invertíveis  $f$  e  $g$  e elemento de prova  $\epsilon$**

### 3.6 Autenticação com Múltiplos Fatores

Com o advento da Internet, o aumento dos negócios eletrónicos (na forma de produtos e serviços disponibilizados pelas Empresas no mundo virtual) e o desaparecimento lógico das fronteiras empresariais (onde colaboradores têm um papel cada vez mais nómada dentro das organizações) aumentou substancialmente o risco de roubo ou de perda de informação pessoal, potenciando a fraude de identidade. Esta nova forma de fazer negócios em tempo real despoletou a necessidade de informação sempre disponível (a qualquer hora e em qualquer lugar) e aumentou a necessidade e pressão sobre as Organizações para estarem em conformidade com normas e políticas nacionais e internacionais (*PCI - Payment Card Industry Data Security Standard; Basel e Basel II*; ou por exemplo a Diretiva da União Europeia sobre Proteção de Dados).



**Fig. 28 – A identificação utilizada no sistema de autenticação Multibanco utiliza dois factores (Two Factor Authentication). O cartão que o cliente possui e o Pin que conhece.**

Para responder a estas necessidades, a Autenticação Multi-factor (AMF) é um sistema de segurança onde mais do que uma forma de autenticação é implementada, sendo os fatores de autenticação formas independentes de provar a identidade e dar os respetivos privilégios ao utilizador final. Estes fatores, com um papel determinante na ajuda de identificação da identidade real do utilizador, possuem métodos de autenticação que podem envolver até três tipos de fatores:

Algo que o sujeito é. (exemplo: Sistemas biométricos - A credencial).

Algo que o sujeito possui. (exemplo: Cartão de acesso (Viva viagens)).

Algo que o sujeito conhece. (exemplo: Nome de utilizador, PIN de acesso).

Existem hoje à disposição das Organizações vários sistemas de autenticação, facto que ajuda na mitigação do risco de brechas de segurança para níveis próximos do zero. Os sistemas de autenticação mais conhecidos e geralmente utilizados por grandes Corporações são *tokens* físicos com *One Time Password (OTP)*; Cartões com *display*, ou com *event time*; cartões matriz; *tokens* por software incluindo *PKI (Public Key Infrastructure)*; *Smart Cards*; Factores Biométricos e novos métodos, muitos deles sem custo para o utilizador final, como autenticação da máquina que se utiliza (*Desktop*, Portátil ou Telemóvel/PDA), envio de credenciais para meios externos como telemóveis, PDA's ou mesmo telefones físicos e Geo-localização do utilizador final por *IP*.

Como critério de seleção deve-se ter em consideração o custo inicial da solução e o custo operacional da mesma, calculando assim o *TCO (Total Cost Of Ownership)* da solução durante um determinado período de tempo. Quanto à “usabilidade” da solução, os utilizadores não deverão ter impacto no modo como estão habituados a interagir com os sistemas sendo este um dos pontos-chave para o sucesso deste tipo de soluções. Uma escolha sábia dos fatores de autenticação, cujo impacto na vida quotidiana do utilizador seja praticamente nulo, tem mais hipóteses de ter sucesso e aceite pelos mesmos. A plataforma deve ajustar-se ao perfil de risco dos utilizadores, e ser flexível para que possa mudar e acrescentar métodos de autenticação durante a vida útil da mesma, e finalmente, a integração com terceiras partes.

Neste âmbito, têm surgido inúmeras soluções de autenticação muito flexíveis, disponibilizando um conjunto de métodos de autenticação com custos reduzidos e, considerando que muitas das opções de autenticação não necessitam da compra de hardware, a plataforma corre em praticamente qualquer servidor e o utilizador não tem uma significativa alteração no modo como interage com as aplicações.

Face ao papel cada vez mais preponderante da Internet na forma como as empresas fazem negócio e contactam com os seus públicos, não há dúvida que a resposta do mercado tem vindo a aguçar a necessidade da utilização deste tipo de soluções disponibilizando uma plataforma aberta, versátil e que permite às Organizações incrementarem de forma dramática a segurança, mitigando o risco de ocorrerem potenciais ataques.

Com o elevado conjunto de sistemas de autenticação existentes, escolher os apropriados pode ser uma tarefa *herculana*. No entanto, soluções com a administração e gestão centralizada de múltiplos fatores de autenticação fornecem uma forma simples, flexível e ajustável, ao perfil de risco dos utilizadores alvo.

### 3.7 Autorização e Controlo de Acessos

Depois de responder a questão “**quem** é o utilizador?” (autenticação), vamos agora perceber “**o que** o utilizador (Já autenticado) tem autorização para fazer no sistema?” (autorização), e posteriormente poder auditar e responsabilizar (se necessário) **o que o utilizador fez** (auditoria).

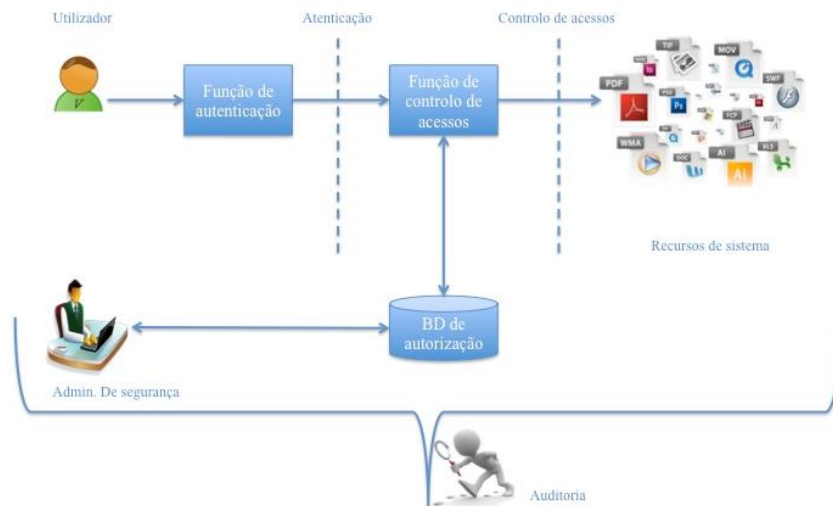
Mas para que os processos de diferenciação entre os utilizadores possam ser inicializados, é necessário primeiramente *validar* a identidade apresentada. E, para entender como isso acontece, é fundamental conhecer as terminologias a seguir:

**Autorização:** processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao sujeito autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos numa base de dados centralizada. (Cada sujeito herda as características do grupo a que pertence...)

**A auditoria (*accounting*):** é uma referência à recolha da informação relativa à utilização, pelos utilizadores, dos recursos de um sistema. Esta informação pode ser utilizada para gestão, planeamento, cobrança etc. As informações que são tipicamente relacionadas com este processo são a identidade do utilizador, a natureza do serviço entregue, o momento em que o serviço se inicia e o momento do seu término.



O controlo de acesso, na segurança da informação, é composto pelos processos de autenticação, autorização e auditoria (*accounting*) Fig. 29. Neste contexto o controlo de acesso pode ser entendido como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo).



**Fig. 29 – Controlo de acessos (relação entre autenticação, autorização e auditoria)**

O controlo de acessos é realizado com base num conjunto de políticas que definem os direitos ou autorizações que os sujeitos ou entidades têm sobre os recursos.

### 3.8 Políticas de Controlo de Acessos

Uma política de controlo de acessos, pode ser incorporada num bando de dados de autorização, e dita quais os tipos de acesso permitidos, sob quais circunstâncias e por quem. Em geral, políticas de controlo de acessos são agrupadas nas seguintes categorias:

**Discretionary Access Control (DAC)** Controla acessos com base na identidade do requisitante e em regras de acesso (autorizações) que declaram o que os requisitantes têm ou não permissão para fazer. Esta política é denominada discricionária porque uma entidade pode ter direitos de acesso que lhe permitem por sua própria vontade, habilitar outra entidade a aceder algum recurso. Exemplo: Modelo de CA do *Unix*

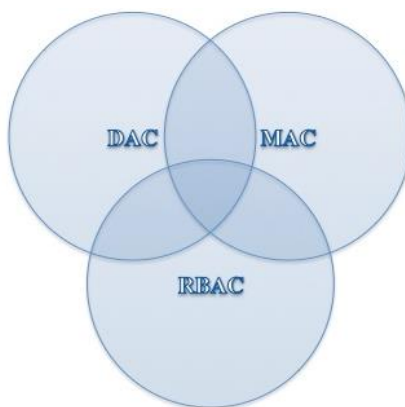
**Mandatory Access Control (MAC)** Controlo de acessos baseado na comparação de rótulos de segurança (que quão sensível ou críticos são os recursos do sistema) com autorizações de segurança (que indicam quais entidades do sistema têm direito de aceder certos recursos). Esta política é denominada obrigatória porque uma entidade que está autorizada a aceder um recurso não pode, apenas por sua própria vontade, habilitar outra entidade a aceder aquele recurso. Exemplo: *Mandatory Integrity Control da Microsoft*

**Role Based Access Control (RBAC)** Controla os acessos com base nos papéis que os utilizadores desempenham dentro do sistema e em regras que definem quais os acessos são



permitidos aos utilizadores em determinados papéis. O *RBAC* é cada vez mais popular, e aprofundamos este tema na secção 5.1.1.

Estas três políticas, não são mutuamente exclusivas (Fig. 30). Um sistema mecanismo de controlo de acessos pode empregar duas destas políticas ou até todas para abranger diferentes classes de recursos do sistema.



**Fig. 30 – Políticas de controlo de acesso (DAC, MAC e RBAC) não são mutuamente exclusivas.**

### 3.8.1 Role Based Access Control (RBAC)

Com a dependência das organizações nas *TCI's* para suportar as suas atividades, o número de utilizadores e de recursos torna-se cada vez mais difícil de ser gerido através de relações diretas entre o sujeito e o objeto (usando *ACL's* por exemplo).

Como acima mencionado o *RBAC* é um mecanismo de autorização (controlo de acesso) que define um conjunto de papéis (*roles*) e atribui a cada papel um conjunto de permissões. Cada utilizador é então associado a um ou mais papéis e herda todas as permissões desses papéis.

A grande vantagem associada ao uso do *RBAC* é a simplificação do processo de gestão de permissões. Olhando para o E-VOTO com CC por exemplo, verificamos que milhões de cidadãos serão utilizadores. Entretanto, pode-se observar que muitos destes possuem exatamente os mesmos privilégios (votar por ex.), pois desempenham o mesmo papel (ou função) dentro do sistema. A ideia é então agrupar os cidadãos em papéis, que representam sua função junto do sistema e atribuir aos papéis e não aos utilizadores individuais o seu conjunto de permissões.

As características do controle de acesso são administradas de forma centralizada em termos de *roles* e relações entre *roles*, nos quais são mapeados os perfis dos utilizadores, dos grupos e dos recursos [Relações *one-to-many*: ( *role* ) => { *users* }] Deste modo reduz-se a complexidade das relações entre sujeitos e objetos, permitindo uma visão global de conjunto.

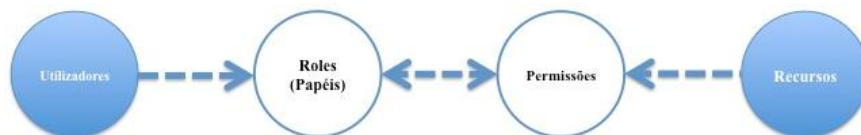
O *RBAC* assenta em 3 regras fundamentais:

**Role Assignment:** todos os sujeitos de um sistema tem obrigatoriamente um *role* atribuído.

**Role Authorization:** um sujeito só integra um *role* se tiver *autorização para o efeito*.

**Action Authorization:** um sujeito só pode executar uma ação se estiver autenticado para um dado *role* e essa ação for autorizada nesse *role*.

Ou seja, as autorizações não são atribuídas individualmente aos sujeitos mas aos respetivos *roles* (Fig. 31).



**Fig. 31 – RBAC (permissões para determinadas ações)**

### *Roles* vs Grupos

Existem algumas semelhanças entre grupos e *roles*, mas os conceitos são muito diferentes.

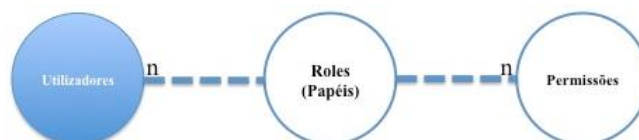
#### **Roles:**

Privilégios atribuídos a papéis são derivados a partir das responsabilidades pertencentes aos trabalhos associados a eles.

Papéis e privilégios são atribuídos e geridos por administradores.

Podemos atribuir mais de um papel a um mesmo utilizador. A um papel, estão associados vários utilizadores.

Uma permissão pode ser atribuída a um ou mais papéis. A um papel, podem estar associadas uma ou mais permissões.



**Fig. 32 - Um Role é uma coleção de utilizadores associada a uma coleção de permissões.**

### **Grupos**

Um grupo é geralmente um conjunto de utilizadores e não um conjunto de direitos de acesso

As autorizações são associadas ao grupo e aos utilizadores, o que implica que se um grupo deixa de ter acesso a um conjunto de recursos, os utilizadores ainda possam ter acesso individualmente

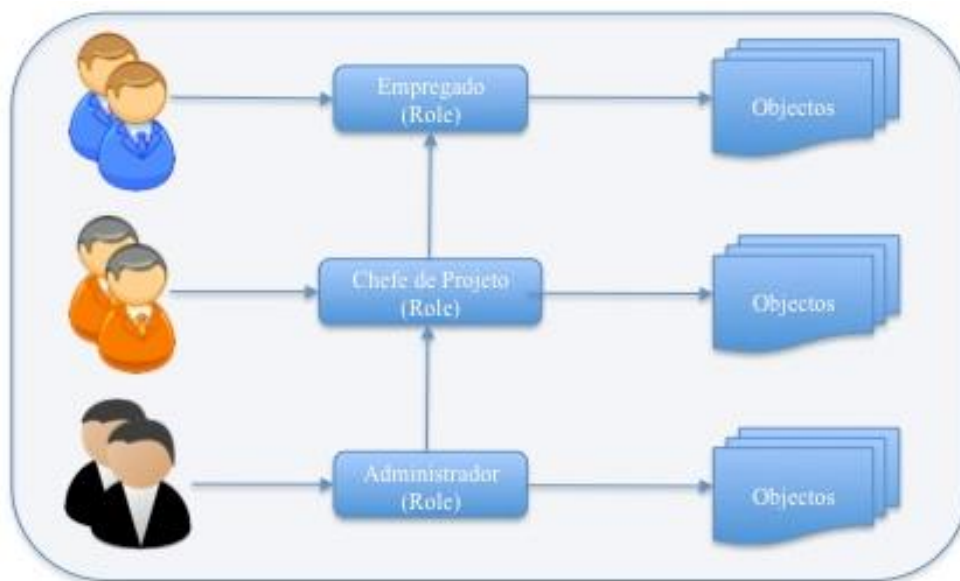
Portanto a gestão de autorização tem de ser feita por grupo e por utilizador, o que não reduz a complexidade e pode criar falhas de segurança.



**Fig. 33 - Groups são tratados como uma coleção de utilizadores (e não uma coleção de permissões).**

## Hierarquias de Roles

O modelo do *RBAC* suporta hierarquias de *roles* possibilitando herança de direitos de acesso. Esta aproximação permite uma implementação das políticas de autorização de forma adequada à natureza hierárquica das organizações.



**Fig. 34 – (Hierarquias de roles) O role Administrador inclui todos os direitos dos roles Chefe de Projeto e Empregado, o role Chefe de projeto inclui os privilégios do role Empregado mas não partilha os direitos do role Administrador e role Empregado não partilha direitos com nenhum dos outros dois.**

Para garantir a implementação correta dos princípios do *RBAC*, são adicionados os dois princípios seguintes.

## Privilégios Mínimos

O princípio do menor privilégio é basicamente para minimizar o **impacto** de qualquer falha, acidente ou vulnerabilidade do sistema, reduzindo os **privilégios das contas de utilizador** ao mínimo necessário para desempenhar as suas funções autorizadas. Pois, a atribuição de privilégios desnecessários facilita a introdução de falhas de segurança

Algumas precauções quanto aos privilégios concedidos aos utilizadores são:

- Proteger o dicionário de dados

- Revogar os privilégios desnecessários de *PUBLIC*, pois nem sempre todos os utilizadores têm acesso aos mesmos objetos.

- Restringir os diretórios que os utilizadores podem aceder, evitando o acesso a dados externos que não lhe foram concedidos.

- Limitar os utilizadores com privilégios de administrador.

- Restringir a autenticação remota a *BD*.

A utilização de *RBAC* facilita a implementação deste princípio.

## Segregação de Funções

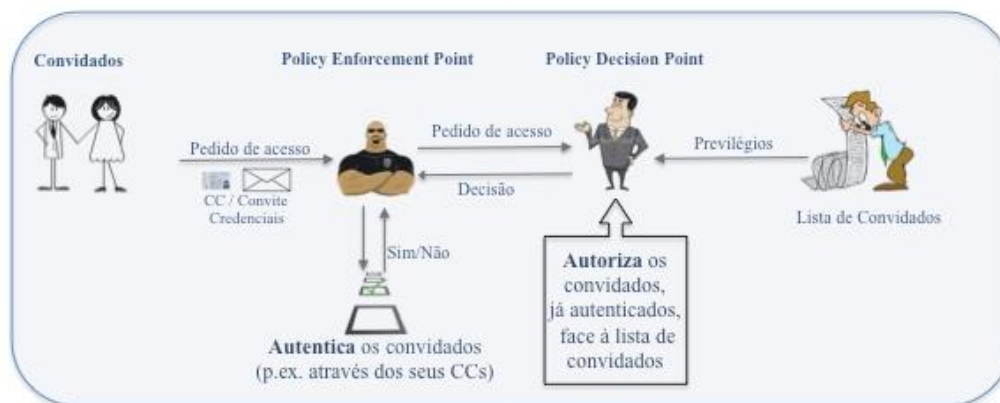
De acordo com (30) o *SoD* (*Separation of Duties* - Segregação de Funções) ou a segregação de funções é um primeiro passo para a criação de uma estrutura que permite a monitorização constante da atividade e desempenho de funções, particularmente em ambientes complexos. Este método permite identificar conflitos de privilégios de vários utilizadores sobre o desempenho de funções.

De uma maneira geral, o sistema de controlo interno, deve prever segregação entre as funções de aprovação de operações, execução e controlo das mesmas, de modo que nenhuma pessoa possa ter completa autoridade sobre uma parcela significativa de qualquer transação.

Este tipo de constrangimento pode ser extremamente difícil de implementar em sistemas com muitos sujeitos e objetos. O recurso ao *RBAC* facilita a implementação, pois permite criar *roles* complementares para uma dada transação.

## 4. Sistemas de Gestão de Identidade

Um Sistema de Gestão de Identidade é uma solução que integra políticas, processos, pessoas e tecnologias e que permite administrar, autenticar, autorizar, auditar e gerir identidades (Fig. 35).



**Fig. 35 – Gestão de Identidades (31)**

Contudo, se pensarmos que podemos definir “Identidade”, como sendo um conjunto de características essenciais e distintivas de alguém ou de alguma coisa, começamos a pensar que então esta solução irá controlar, quem somos, o que nos caracteriza, os nossos direitos de acessos, o nosso perfil, quem autoriza o quê e acima de tudo quem verifica a validação das nossas características, acessos e autorizações.

Com a multiplicação de tipos distintos de identidades cresce a necessidade de acomodar uma grande diversidade de identidades, o que impõe uma enorme pressão nos modelos de gestão, que têm vindo a sofrer grandes modificações.

Facilmente pode-se verificar que cada aplicação/sistema que existe nas nossas organizações tem a sua própria definição de identidade, multiplicando o número de vezes que a nossa Identidade existe bem como as características da mesma.

O mesmo acontece no nosso dia-a-dia como cidadãos, vejamos, eu sou um “Adilson Morgado” para o Ministério das Finanças, outro para a Segurança Social, outro para a Direcção-Geral de Viação, outro para o Centro de Saúde onde me encontro inscrito, outro para a instituição bancária A e outro para a instituição bancária B, isto só para mencionar alguns exemplos. Tudo isto leva a que, a definição de um único “Adilson Morgado” ao nível dos sistemas de informação seja, de alguma forma, complexo.

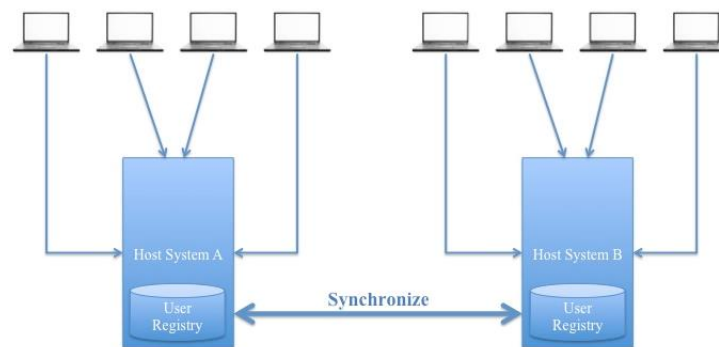
A Gestão de Identidades é um desafio inevitável para qualquer organização, os modelos mais comuns são portanto:

- Modelo Local/Centralizado.
- Modelo Distribuído.
- Modelo Federado.
- Modelo Web Global.

## 4.1 Modelo local / centralizado

Este modelo evoluiu da gestão de utilizadores dos grandes sistemas informáticos (*Mainframes*, sistemas de *time-sharing*, sistemas multi-utilizadores, etc.), e desde então tem vindo a sofrer grandes transformações quer do ponto de vista dos identificadores quer do sistema de controlo associado.

Num cenário de autenticação não centralizada, todos os utilizadores realizam o processo de autenticação com base em credenciais que podem ser armazenadas em vários repositórios, e que podem ser distintas de uma aplicação para outra se não existir sincronismo entre elas.



**Fig. 36 – Modelo Centralizado**

### Vantagens:

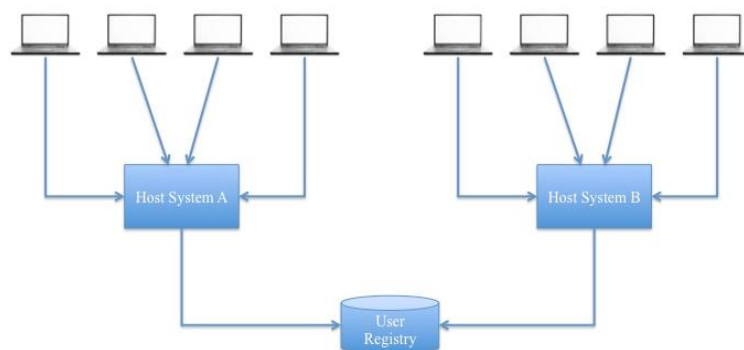
Esta solução permite um espaço de nomeação linear e tem uma implementação simples, pois tem poucos pontos de falha o que acelera a resolução de problemas técnicos como a gestão de certificados *SSL* por exemplo.

### Desvantagens:

O modelo centralizado tem uma arquitetura rígida na presença de políticas de segurança distintas, pelo que há necessidade de sincronismo ou alteração de políticas de segurança quando temos vários repositórios de atributos. E ainda salientar que um utilizador pode ter um *id* em cada sistema o que dificulta a relação entre eles.

Existem soluções para estes constrangimentos (desvantagens), tais como a centralização ou o *Single Sign-On (SSO)*.

#### 4.1.1 Centralização



**Fig. 37 – Centralização**

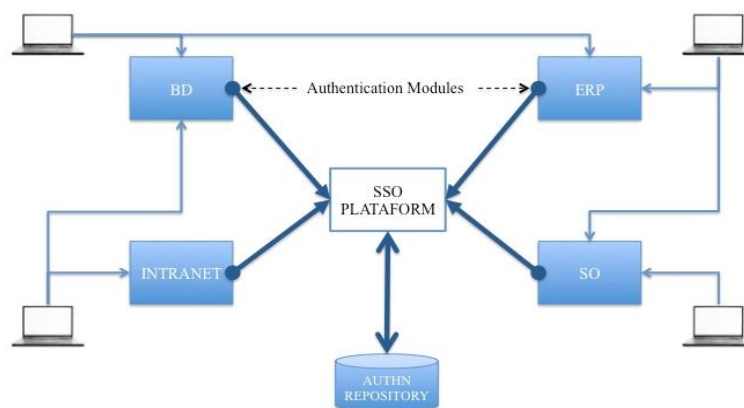
De forma a evitar a disparidade de credenciais, os repositórios podem tornar-se centralizados, havendo um único ponto de acesso à informação dos utilizadores para todas as unidades orgânicas da instituição. Todavia, com esta abordagem, os utilizadores terão de se autenticar explicitamente em todas as aplicações.

1.O *Host System A* e B (fig.37) respetivamente nesta abordagem são sistemas autónomos (independentes) e centralizados.

2. Embora o repositório de identidade seja partilhado, os utilizadores devem-se autenticar em todos os sistemas que queiram aceder pois estes têm controlos de acessos separados.

#### Single Sign-On

O *SSO* é um mecanismo pelo qual uma única ação de autenticação e autorização do utilizador concede acesso a vários computadores e sistemas aos quais ele tem acesso, sem a necessidade de fornecer múltiplas senhas (32). Por ser um método muito interessante por representar um bom *trade-off* entre segurança e usabilidade, surgiram assim muitos sistemas de autenticação *SSO*.



**Fig. 38 – SSO Centralizado**

O *Single Sign-On (SSO)*, é muito utilizado pois tenta resolver um dos maiores problemas relacionados à autenticação (o mau uso das senhas) por outro lado este modelo é bastante criticado por introduzir o risco do Ponto Único de Falha (PUF) no identificador central, podendo assim comprometer todo o sistema em caso de falha desse provedor. Um outro risco associado a esse modelo é o poder informacional concentrado no identificador, que conhece tudo sobre os utilizadores e pode utilizar essas informações como quiser (possível razão para a falha do *Microsoft Passport Network*).

## 4.2 Modelo Federado

Para evitar que os utilizadores tenham várias credenciais de acesso (dado o numero de serviços que usam, que leva a terem senhas “fracas” ou a guarda-las em local inseguro) nasceu o conceito de Federação.

Uma Federação consiste num grupo de organizações que partilham um conjunto de políticas e regras, estabelecendo-se desta forma uma confiança com o objetivo de se atingir uma autenticação e autorização transversal entre os vários domínios existentes. No âmbito do projeto da Plataforma de Interoperabilidade da Administração Pública - *Framework* de Serviços Comuns, é disponibilizado um modelo de autenticação federado. Este modelo de autenticação, prevê a existência de Fornecedores de Autenticação (FA), que são peças de *software* que permitem a autenticação de uma forma standard e independente das tecnologias de credenciais utilizadas.

A utilização do FA do CC, em alternativa a uma implementação específica de autenticação tal como é descrito neste documento, tem como vantagens para além de evitar que se repitam as implementações específicas de autenticação com o cartão, a possibilidade de *garantir Single Sign On* entre todas as aplicações que o utilizem.

### 4.2.1 Fornecedor de Identidade e Fornecedor de Serviço

No seio de uma federação assente numa infraestrutura de autenticação e autorização existem dois componentes essenciais (fig.39):



**Fig. 39 – Service Provider (1) e Identity Provider (2)**

1) O componente de autenticação *IdP* (designado **Fornecedor de Identidade** ou “*Identity Provider*”) consiste num conjunto de *software* que autentica os utilizadores perante pedidos



efetuados a recursos protegidos (**Fornecedor de Serviço ou "Service Provider"**), e fornece atributos com base em políticas para que possa ser efetuada uma autorização no acesso ao serviço inicialmente requisitado.

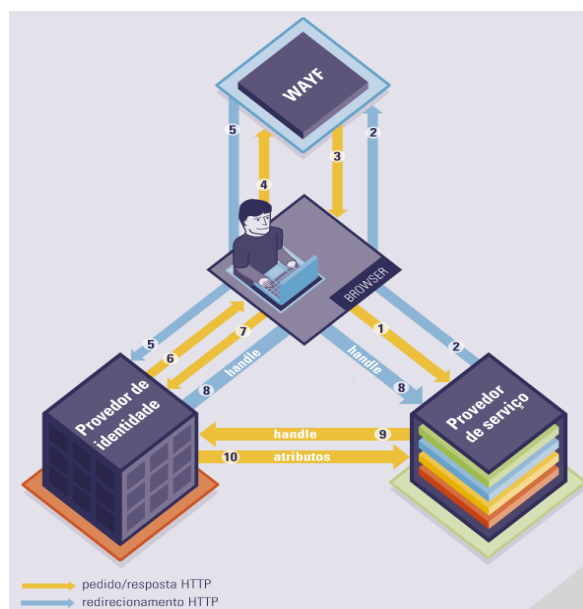
2) O componente *SP* (**Fornecedor de Serviço ou "Service Provider"**) consiste numa camada de *software* que protege e autoriza o acesso a um determinado recurso *Web*. A Autorização é realizada com base nos atributos necessários enviados pelo fornecedor de identidade.

O formato de dados trocados entre o *FA* e o *FS* é baseado em *SAML v2.0* (*Security Assertion Markup Language*), de forma a assegurar a autenticidade e integridade de todas as transações. A utilização do *SAML HTTP Post Binding* associado ao *SAML Web Browser SSO Profile* permite que a autenticação seja transitada através do *browser* do Utilizador, sem necessidade de ligação física entre as Entidades e o *FA*.

As comunicações entre o Fornecedor de Autenticação e Entidades, que podem ser realizadas pela Internet, devem sempre ser efetuadas sobre *HTTP* em canal cifrado – *SSL* ou *TLS*. A utilização de canais cifrados, associado ao formato específico *SAML* que permite a cifra e assinatura de partes específicas das mensagens, garante a privacidade e integridade dos dados trocados.

#### 4.2.2 Fluxo de Informação

A figura 40 ilustra as interações realizadas durante um acesso típico, via navegador, a um serviço federado. O fluxo apresentado assume que nenhuma informação sobre o utilizador é conhecida pelo provedor do serviço, e que este é o primeiro acesso do utilizador a um serviço federado.



**Fig. 40 – Funcionamento de uma Federação (33)**

1. O utilizador direciona o seu navegador para a página do serviço desejado.
2. O servidor redireciona o navegador para o serviço de descoberta da federação (*WAYF*).
3. O serviço de descoberta apresenta ao utilizador as instituições que oferecem provedores de identidade para a federação.
4. O utilizador seleciona uma instituição, e seu navegador envia ao serviço de descoberta os dados dessa seleção.
5. O serviço de descoberta redireciona o navegador para a instituição selecionada.
6. O provedor de identidade da instituição envia ao navegador a página de autenticação do utilizador.
7. O utilizador fornece as suas credenciais e o navegador envia-as ao provedor de identidade.
8. O provedor de identidade gera um *handle* e envia-o ao navegador, que o encaminha ao provedor de serviço, que assim obtém a prova de autenticação do utilizador. Para algumas aplicações, isso é suficiente para autorizar o acesso do utilizador ao serviço.
9. Opcionalmente, o provedor de serviço pode enviar um pedido de atributos ao provedor de identidade/atributos, utilizando o *handle* para especificar o utilizador em questão.
10. O provedor de identidade/atributos retorna os valores dos atributos requisitados.

## **5. E-voto com recurso ao CC**

Através do chamado governo eletrónico é possível construir a ideia de um cidadão mais presente. A construção deste tipo de governo envolve razões dos mais diversos tipos, tais como económico, político e cultural. Características importantes deste processo de construção são as infraestruturas tecnológicas, os conteúdos disponíveis, a capacitação e participação das pessoas envolvidas. Existem fragilidades, riscos e inseguranças, mas os benefícios são imensos. Nisto, realça-se a relevância da Internet para reduzir as distâncias físicas e o desaparecimento das fronteiras territoriais.

Neste contexto, foi desenvolvido o Cartão de Cidadão Português (CC) para identificar e autenticar o cidadão nas instituições do estado (34). O CC é uma ferramenta poderosa do ponto de vista da segurança eletrónica (ver a secção 2.4 deste documento). É com base nesta ferramenta que se desenvolveu o sistema de voto eletrónico com recurso ao cartão de cidadão, denominado por E-voto, que numa perspetiva por excelência otimista, poderá permitir a participação de uma grande maioria permanentemente excluída das eleições, quer por se encontrar no estrangeiro ou por ser portadores de necessidades especiais. Em síntese o E-voto com recurso ao cartão de cidadão é um sistema de voto eletrónico com recurso a autenticação baseada no cartão de cidadão.

### **5.1 Arquitetura da Solução**

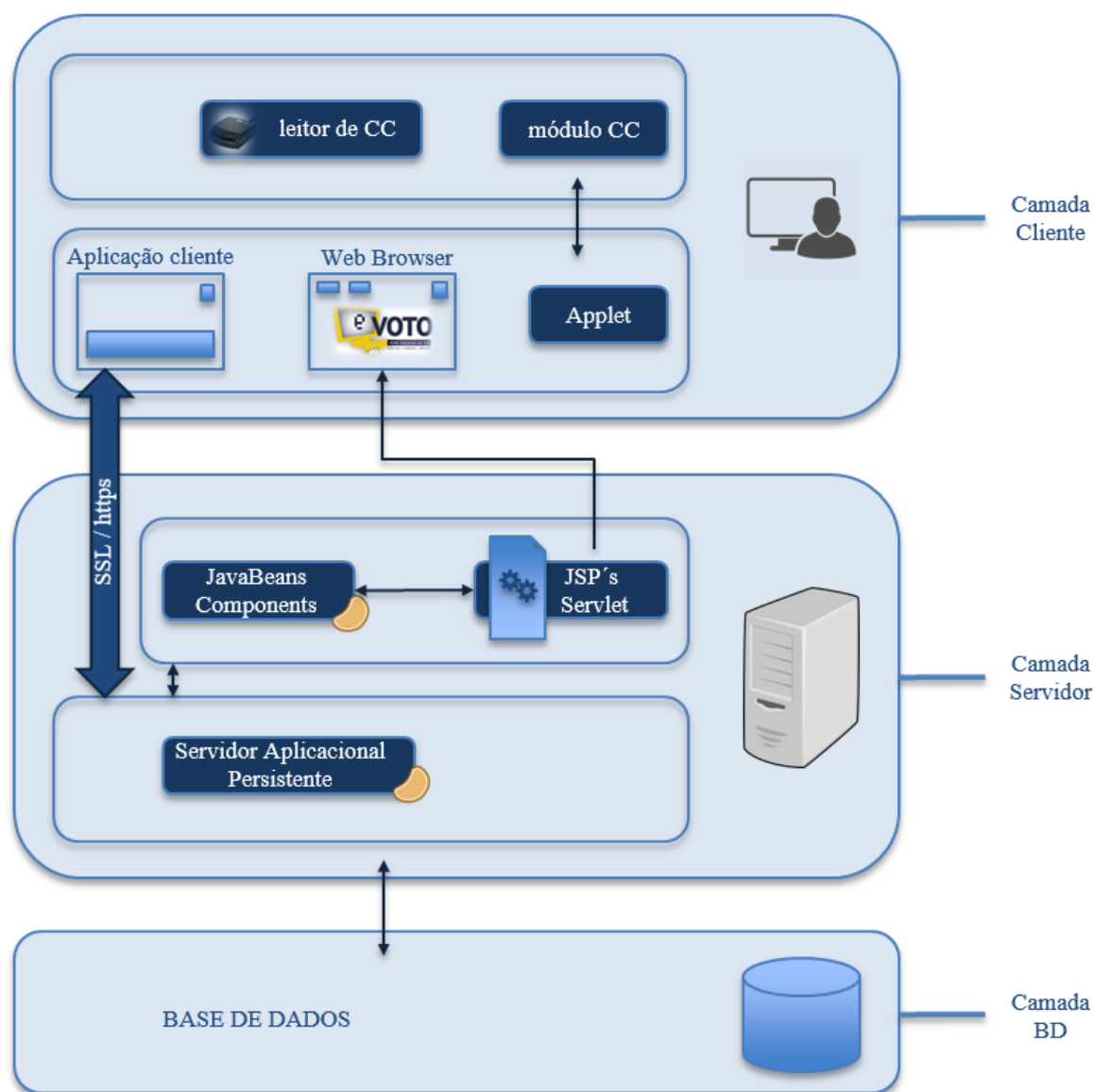
Porque o grande objetivo do E-voto com recurso ao CC é “chegar” a todos os cidadãos e dar-lhes a possibilidade de votarem em qualquer lugar, a solução foi concebida como uma aplicação Web que não se instala no computador (cliente), mas que corre em Browser, dando acesso a um Portal de Voto.

Tendo em conta as necessidades de segurança já referidas, a segurança da aplicação tem de garantir a identificação e autenticação forte dos cidadãos. Para tal, é utilizado o Cartão de Cidadão, que implementa uma autenticação baseada em fatores múltiplos. Nesse sentido, a aplicação necessita de interagir localmente (na máquina cliente) com o módulo do Cartão de Cidadão do eleitor. Esta interação é realizada utilizando uma Applet assinada, descarregada a partir do Portal de Voto, que corre no contexto do browser do utilizador. Esta interage localmente com a aplicação genérica do Cartão de Cidadão [Referência], que deve estar previamente instalada na máquina do cliente.

Obtém-se assim uma arquitetura genérica baseada em 3 (três) módulos (interface web, Applet e bibliotecas locais de acesso ao cartão de cidadão) no lado cliente. Contudo para realizar a ligação local entre a Applet de voto e as bibliotecas locais do Cartão de Cidadão, foi necessário desenvolver um pequeno módulo adicional (“mini applet”) para encapsular a API do cartão de cidadão e adaptá-la às características do sistema de voto eletrónico. Esta camada trata igualmente da autenticação dos cidadãos eleitores e do seu redirecionamento para o portal de voto, caso sejam autenticados com sucesso.

Quando um utilizador é autenticado na Applet, é criado um cookie para gerir uma conexão persistente ao servidor, para que o cidadão exerça o seu direito de voto dentro de uma janela temporal limitada. A transação de voto é acompanhado do número do CC (identificador

único), que é guardado na base de dados para garantia da unicidade, mas sendo impossível relacionar o voto ao identificador do eleitor para garantir do seu anonimato.



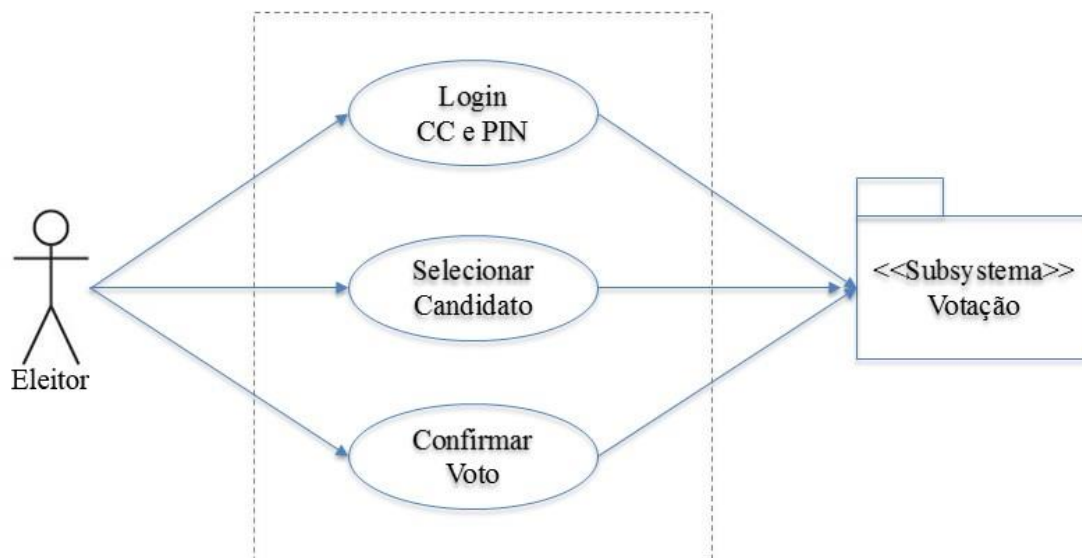
**Figura 41 – Arquitetura do Sistema**

## 5.2 Diagramas de Sistema

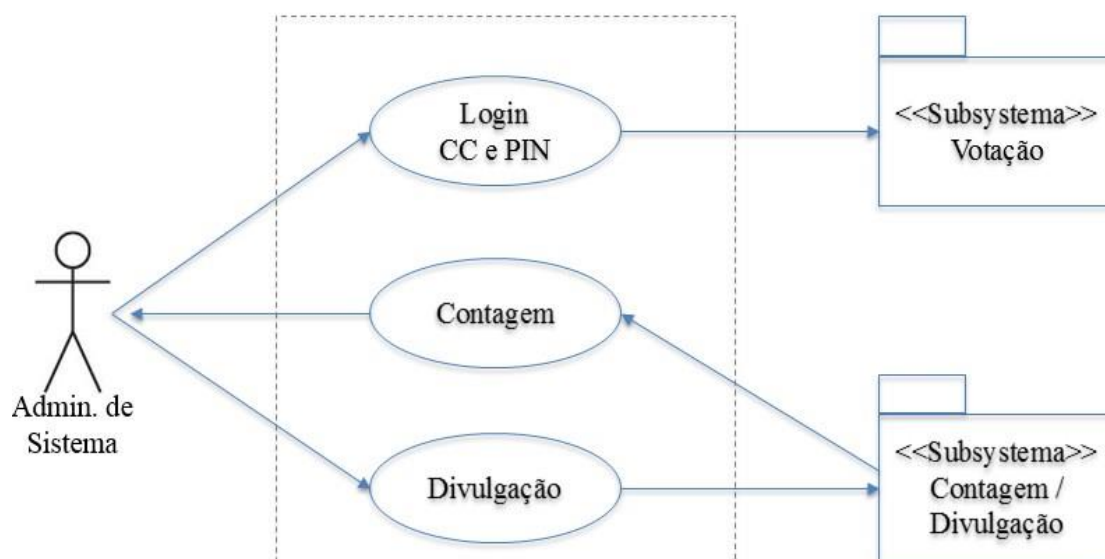
Para visualizar a arquitetura e a comunicação entre os módulos do E-voto, foram realizados alguns dos diagramas mais significativos utilizando a Linguagem de Modelagem Unificada (UML).

### 5.2.1 Diagrama de Caso de Uso

Este diagrama descreve a sequência de eventos de um ator que usa o E-voto para completar um processo".



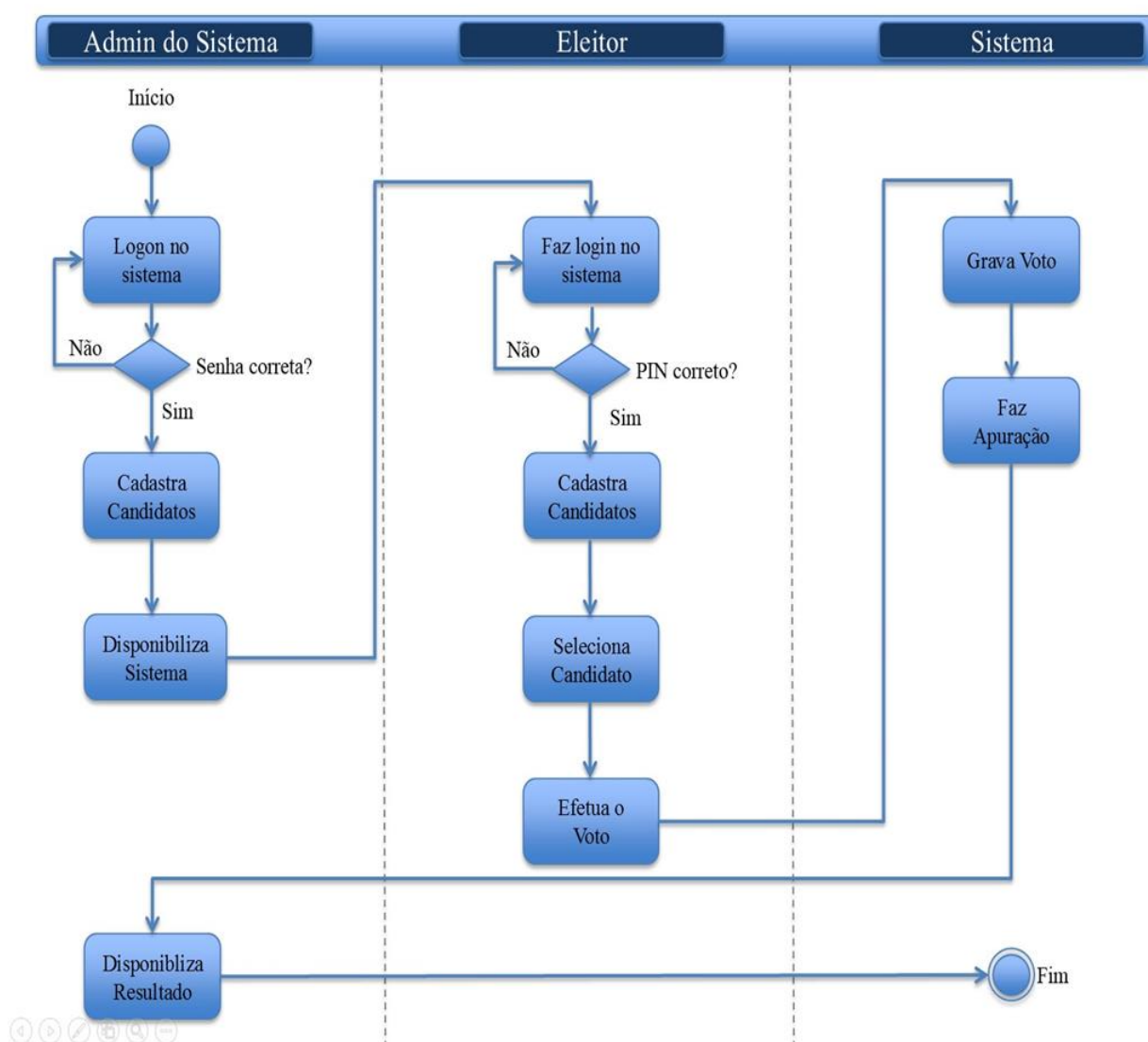
**Fig. 42 – Diagrama de Caso de Uso (Votação)**



**Fig. 43 – Diagrama de Caso de Uso (Votação)**

### 5.2.2 Diagrama de Atividades

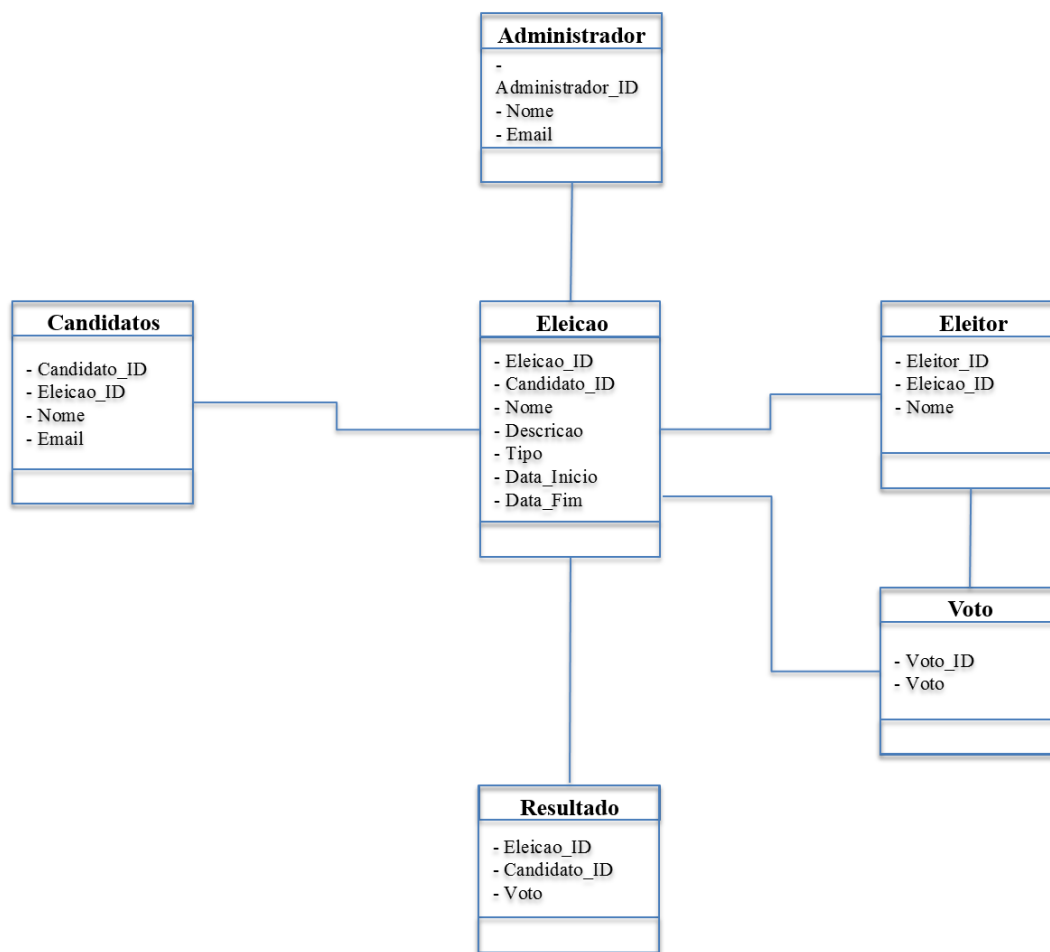
O Diagrama de Atividades, tal como é definido pelo UML, mostra o fluxo sequencial das atividades realizadas no E-Voto.



**Fig. 44 – Diagrama de Atividades**

### 5.2.3 Diagrama de Classes

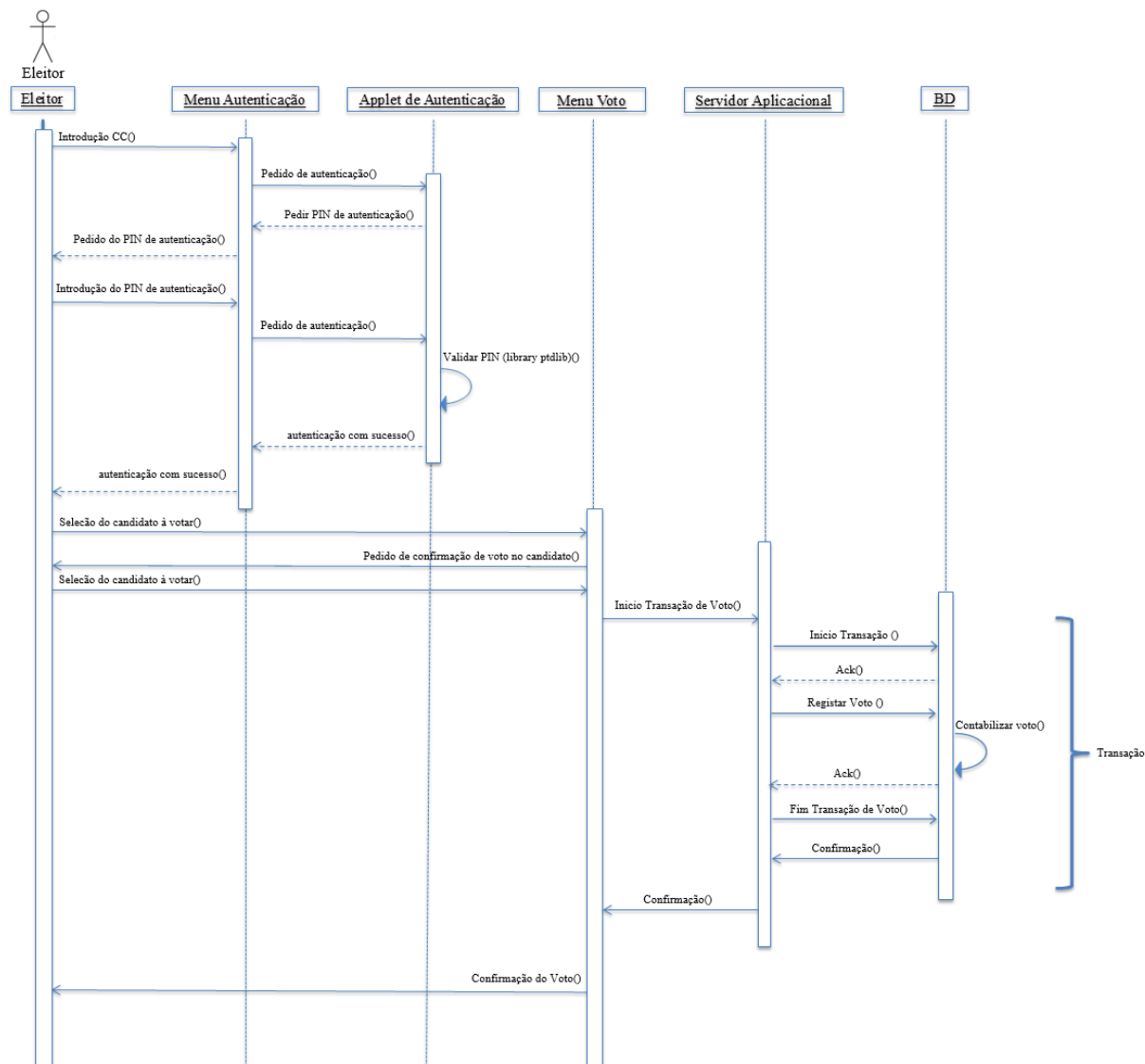
Esta vista define as classes que o sistema necessita para armazenamento da informação (dados e metadados), sendo a base para a construção dos diagramas de comunicação, sequência e estados.



**Fig. 45 – Diagrama de Classes**

### 5.2.4 Diagrama de sequência

Este Diagrama de Sequência representa o conjunto de interações entre os objetos do E-voto, realizados através de operações/métodos (procedimentos/funções) da interface utilizador e o servidor aplicacional.



**Fig. 46 – Diagrama de Sequência**



## 5.3 Protótipo

Tendo em conta a arquitetura e as interações referidas, foi desenvolvida uma aplicação, utilizando a linguagem de programação JAVA, que implementa os conceitos básicos do sistema de votação eletrónica acima descrito. A aplicação recolhe os votos dos eleitores e apura o resultado das eleições, sendo todo processo realizado de acordo com os requisitos de segurança que um SVE deve ter, tais como: Integridade, Confidencialidade, Disponibilidade, Unicidade, Privacidade, Anonimato Autenticidade, Transacionalidade (descritos na secção 2.2).

Este sistema é utiliza um servidor Apache Tomcat 7.0, uma base de dados MySQL Workbench 6.3, e é composto por um módulo denominado User-E-voto (Interface Utilizador e gestão da interface local com o CC) e outro denominado Serv-E-voto (servidor), que assegura a interação com a BD e a coerência do sistema.

### 5.3.1 Servidor

Foi utilizado o servidor Apache Tomcat 7.0 por ser um servidor livre e uma ferramenta de referência das especificações das tecnologias de servlets e Java Server Pages (JSP). Foi instalado e configurado com as especificidades exigidas neste sistema para executar a aplicação web, mais especificamente as JSP do projeto.

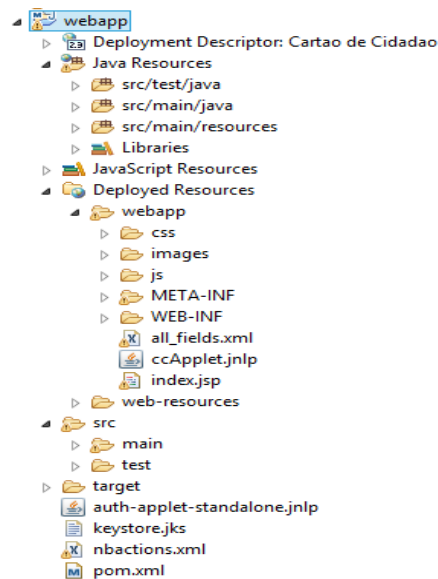
### 5.3.2 Base de Dados

Com a necessidade de gerir um universo grande de eleitores, foi necessário dispor de uma BD relacional e escalável para gerir todo o processo de voto e suportar o sistema de segurança do E-voto. Para isto foi utilizado o **MySQL Workbench** o que permitiu criar, executar e otimizar consultas SQL. Foi criado um sistema de back-up paralelo para o caso de failback e/ou inspeção e auditoria do sistema.

A BD é um elemento crítico neste trabalho pois agrega (guarda) os elementos vitais do sistema, tais como: Os partidos **candidatos** ao pleito eleitoral dados, que são guardados em claro, a hash do **voto** do cidadão, o número do CC (identificador único do cidadão) este que “nunca” poderá ser associado ao seu voto. Por outro lado, a relação voto/candidato permite-nos apurar o resultado das eleições em near real time, o que não deixa de ser um feito importante num universo grande de cidadãos

### 5.3.3 User\_E-Voto

A aplicação de nominada User:E-voto é a aplicação que interage com o cartão, lê os dados e valida o pin de autenticação do CC e redireciona o utilizador a pagina de voto (Serv-E-voto), este projeto está organizado em pastas como mostra a figura 41.



**Fig. 47 – Estrutura simplificada do User:E-voto**

## Resumo do conteúdo das pastas

**Src** – Código fonte Java (CardManagerApplet.java). Lê o cartão e valida o pin

**Build** – Onde o Eclipse compila as classes (.classe)

**User:E-voto** – content directory (applet, css etc. foram aqui)

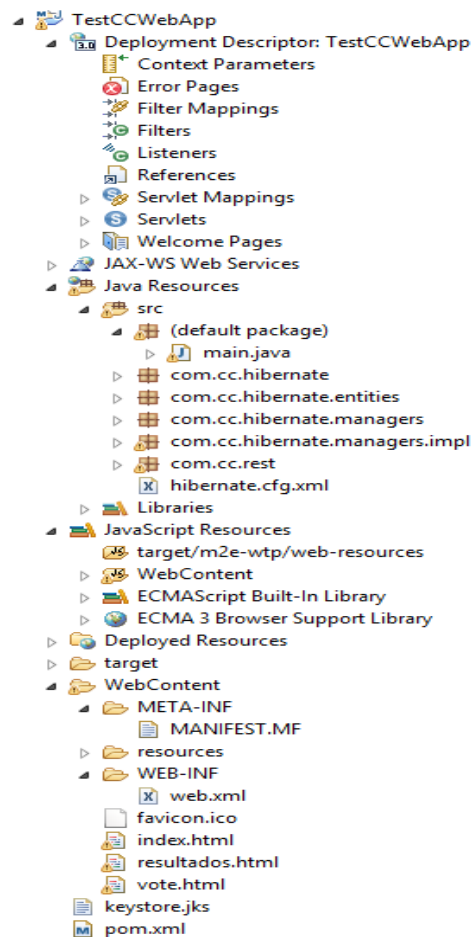
**User:E-voto /WEB-INF/** – Pasta oculta com configurações e recursos do projeto

**User:E-voto /WEB-INF/lib/** – Biblioteca que a applet usa para “falar” com o cartão. Esta pasta é muito importante e contém recursos vitais para o funcionamento do projeto. Esta pasta não deve ser acessada pelos utilizadores “cidadãos”, pois contém bibliotecas potencialmente sigilosas, arquivos de configuração interna do cartão, etc.

**User:E-voto /WEB-INF/classes/** – Arquivos compilados são compilados para cá.

### 5.3.4 Serv-E-voto

A aplicação de nominada Serv-E-voto é a aplicação que somos redirecionados depois de autenticados, é onde podemos votar e apurar o resultado das votações. Esta aplicação foi criada totalmente de raiz com os pré-requisitos de um SVE.



**Fig. 48 – Estrutura simplificada do Serv-E-voto**

#### Resumo do conteúdo das pastas

**Src** – Código fonte Java (main.java).

**Build** – Onde o Eclipse compila as classes (.classe)

**Serv-E-voto** – content directory (paginas, css etc. foram aqui)

**Serv-E-voto /WebNontent/META-INF/** – É onde se vota através da camada rest”/vote” e mostra os resultados através da chamada rest “/getcount”

**Serv-E-voto /WEB-INF/** – Responsável por mostrar a pagina Inicial, pagina de voto e pagina resultados.

## 6. Análise de Risco

O termo “Risco” é utilizado para designar o resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento, aleatório, futuro e independente da vontade humana, e o impacto resultante caso ele ocorra (35).

O dicionário eletrónico *Houaiss* da Língua Portuguesa define “risco” Como a probabilidade de insucesso de determinado empreendimento, em função de um acontecimento eventual, incerto, cuja ocorrência não depende exclusivamente da vontade dos interessados.

A preocupação com os riscos não é uma novidade: desde os raios que fizeram com que os homens procurassem abrigo aos modernos sistemas de segurança e defesa nacionais, o desejo de proteção ou tentar diminuir as consequências da incerteza sempre fez parte da natureza humana.

Esta preocupação, atualmente, ganha evidência devido aos acontecimentos recentes na história. Como o “onze de setembro”, por exemplo, o processo de globalização, questões ecológicas e climáticas que afetam a própria possibilidade de sobrevivência da nossa espécie; e, não menos importante, a afluência da sociedade do conhecimento. Acontecimentos que colaboram para que cada vez mais haja uma maior preocupação com a questão do tratamento de riscos.

Nesse estado de “coisas”, as organizações têm estabelecido diretivas e políticas que salvaguardam os seus interesses, e procuram alternativas para melhorar cada vez mais a gestão de risco sem oferecer detrimento às suas missões, seja busca do lucro, para as entidades privadas ou atendimento aos cidadãos ou outros fins ligados ao bem público, para as organizações públicas. De qualquer forma, todas estão cada vez mais preocupadas em atender às exigências de seus *stakeholders*.

### 6.1 Identificação e Análise de Riscos

Para atender aos requisitos da Política de Segurança, é necessário a identificação de ameaças, a avaliação da probabilidade de ocorrência e o impacto causado caso esta ameaça venha a ocorrer. Tem-se, então, um mecanismo para identificar claramente quais os maiores riscos que afetam o processo eleitoral.

Para o dimensionamento dos riscos foi utilizado um método sugerido na norma ISO27000 (36), classificando as ameaças por impacto e probabilidade, atribuindo-se a cada fator um valor crescente de 0 a 5. O valor do risco é obtido a partir do resultado da multiplicação dos valores dos fatores de cada ameaça.

AMEAÇAS	Impacto (0 – 5)	Probabilidade (0 – 5)	Risco
Identificação e Autenticação - Ameaça programada que mascara a identificação (CC)	4	1	4
Disponibilidade - Ataques de negação de serviço distribuído (DDoS)	5	3	15
Integridade - Dano deliberado ao conteúdo de arquivos ou sistemas confidenciais	4	2	8
Colaboradores Internos (acidental, propositado) - Utilizadores internos praticarem atos ilegais.	5	3	15

Tabela 4: Análise de risco

## 6.2 Tratamento dos Riscos

**Identificação e Autenticação** (Ameaça programada que mascara a identificação (CC) do cidadão) ao acontecer teria um impacto muito elevado na continuidade e reputação do e-voto, porém, acredita-se que os controlos do cartão de cidadão são suficientemente efetivos para prevenir que a agressão se concretize. O que pela escala de risco que tem (4) nos permite aceitá-lo.

**Integridade** (Dano deliberado ao conteúdo de arquivos ou sistemas confidenciais) apesar da grande motivação de violar as eleições por alguns grupos (*hakers*), no e-voto existem controlos de acessos efetivos para a *DMZ* mitigar estes riscos.

**Colaboradores Internos** Estes ainda são tidos como o elo mais fraco das organizações e no e-voto não é diferente. Se por um lado mitigamos os riscos associados aos nossos colaboradores com controlos e políticas de segurança com (segregação de funções e privilégios mínimos) por outro lado não existe tecnologia para evitar o ataque de um engenheiro social [MITNICK, 2003]. Porém, planos de treinamento contra o engenheiro social bem como campanha de *awareness* são tidas como medidas de mitigação desta ameaça tão perigosa e que representa tanto risco. Afinal é difícil ou quase impossível detetar se fomos alvo de um ataque desta natureza até ser tarde demais.

**Disponibilidade** (Ataques de negação de serviço distribuído *DDoS*) No e-voto a disponibilidade é um dos principais pilares e fatores críticos de sucesso, daí existir uma grande preocupação com os ataques *DDoS*. Esta é das principais ameaças pois já prejudicaram sites conhecidos, tais como os da *Amazon*, *Yahoo*, *Microsoft* e *eBay*.

Para mitigá-lo são tomadas as seguintes medidas:

Implementar um *PROXY* Reverso. Ou seja, tudo que não for utilizador autenticado vai ficar barrado na *firewall*.

Monitorizar o tráfego (para aferir se tem mais tráfego que o normal)

Utilizar *softwares* de *IDS* (*Intrusion Detection System* - Sistema de Identificação de Intrusos).

Verificar as atualizações de segurança dos sistemas operacionais e softwares utilizados pelos computadores.

Embora tomadas estas medidas de mitigação do risco, deverá ser feito um plano de **recuperação de desastre (RD)** (envolve um conjunto de políticas e procedimentos para permitir a recuperação ou continuação da infraestrutura tecnológica e sistemas vitais) (37) da infraestrutura *IT* que suporta as funções críticas do negócio (38) de forma a manter o sistema de votação disponível apesar de eventos disruptivos significantes. Sendo este um subconjunto da continuidade do negócio (39) (tema não aprofundado nesta tese). Esta infraestrutura deverá ser de alta disponibilidade (abordado na seção 8.2.1) e replicada em pontos distantes com balanceamento automático.

### 6.2.1 Infraestrutura de Alta Disponibilidade

Um **sistema de alta disponibilidade** (HA: *High-Availability*) é um sistema informático resistente a falhas de *hardware*, *software* e energia, cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível (37). Ou seja, para garantir a alta disponibilidade do E-voto, precisamos garantir que os seus serviços em diferentes situações de operação (falhas, carga, desastres e etc.), com níveis de qualidade pré-estabelecidos. Tais como: Tolerância a falhas, suporte a picos de carga e alta procura, recuperação de desastre, cenários de redundância de dados do *site* e funcionalidades.

No e-voto a disponibilidade é um fator crítico onde 99% de disponibilidade pode ser pouco dado o **objetivo de tempo de recuperação** (RTO) que se pretende não superior a 2 segundos para que não haja votos perdidos pois o **objetivo de ponto de recuperação** (RPO) deve ser igual ao ponto de falha (*Rollback*). Lembrando que:

O E-voto é um sistema transacional projetado para manter a integridade do sistema (base de dados) num estado conhecido e consistente, garantindo que as operações interdependentes no sistema ou estão todas concluídas com êxito ou todas canceladas com sucesso. Ou seja, o cidadão ou votou ou não votou (0-1), não existe meio termo para este binómio.

Para que isto aconteça o sistema deve ter 99,999% (*Uptime*) de disponibilidade segundo a tabela abaixo.

Disponibilidade (%)	Downtime/ano	Downtime/mês
96%	14 dias 14:24:00	1 dias 4:48:00
97%	10 dias 22:48:00	0 dias 21:36:00
98%	7 dias 7:12:00	0 dias 14:24:00
99%	3 dias 15:36:00	0 dias 7:12:00
99,9%	0 dias 8:45:35.99	0 dias 0:43:11.99
99,99%	0 dias 0:52:33.60	0 dias 0:04:19.20
99,999%	0 dias 0:05:15.36	0 dias 0:00:25.92

**Tabela 5: Níveis de alta disponibilidade**

Contudo, para garantir este nível de disponibilidade exigido pelos requisitos do negócio, exige-se igualmente um investimento alto quer financeiro quer nas definições de *hardware*, *software* e redes que suportam adequadamente os níveis exigidos.

### 6.3 (Riscos inerentes ao CC, Java e Applet)

Além dos riscos de infraestrutura, intrusões, catástrofes naturais e etc. que acabam por ser de alguma forma genéricos, com os quais até certo ponto “sabemos” como lidar, pois existem vários *standards* e boas práticas para os mitigar, deparamo-nos também com outros riscos, que à partida tínhamos previsto, ligados à tecnologia, suporte e evolução da solução adotada (autenticação com o CC baseada numa *Applet*).

#### Tecnologia:

Existe o risco já identificado que as implementações com CC têm problemas que não são fáceis de resolver. Isto verifica-se mesmo nas suas implementações mais oficiais, tais como o erro de autenticação no portal de cidadão e a complexidade associada ao uso desta ferramenta, o que consideramos ser um entrave na adesão por parte dos cidadãos na sua adoção. Este facto traduz-se num risco na implementação de um sistema de voto com recurso a esta tecnologia, uma vez que o E-Voto com recurso ao CC visa promover a facilidade, transparência e disponibilidade do pleito eleitoral. Sendo assim este sistema poderá não ter o impacto esperado em virtude da má experiência do cidadão eleitor no uso de soluções tecnológicas associadas às atuais versões do cartão de cidadão.

#### Suporte:

Esta tecnologia não tem o suporte necessário a nível de quem o desenvolveu/implementou e mesmo a nível do governo para a tornar mais robusta e transparente, é uma autêntica “caixa preta”, o que dificulta o desenvolvimento de soluções suficientemente maduras para trabalhar em contexto nacional.

Ao longo do desenvolvimento desta arquitetura, várias foram as tentativas de contacto à empresa como a Caixa Mágica, Zetes Burótica e até ao Portal de Cidadão para obter algum tipo de suporte e material, todas sem sucesso.

O *kit* de desenvolvimento está há mais de um ano indisponível, o que inviabiliza o desenvolvimento a cidadãos estrangeiros (como é o meu caso) e mesmo para nacionais, uma vez que os testes de erros não são aprofundados com o receio de bloquear o CC. Arriscaria dizer que estamos perante um caso de segurança por obscuridade, pois, o que sabemos sobre o cartão de cidadão é apenas o que aparece nos *media* ou pouco mais além disso. O que de certa forma dificulta o entendimento e desenvolvimento das bibliotecas associadas ao CC.

#### Evolução:

Esta tecnologia é baseada em muitos casos em *Applets*. E este é o maior risco identificado, pois ao longo do trabalho foram saindo atualizações da *Applet*, o que se traduzia em erros incompreensíveis e difíceis de identificar.

Percebo que as mensagens apresentadas dependem de fatores de risco, tais como usar versões antigas do *Java* ou executar o código *Applet* que não foi assinado por uma Autoridade de Certificação confiável. Mas devo realçar que a atualização das *applets* podem pedir algum privilégio de acesso aos computadores dos utilizadores, o para os comuns dos mortais não é encarado da melhor forma, muitas vezes visto como intrusivo, porém, do ponto de vista de segurança, o facto de os utilizadores autorizarem este acesso às *applets* é um fator de risco pois, as *applets* não são consideradas seguras

Ainda realçar que esta tecnologia (*Applet*) deixou de ser suportada em alguns *browsers* como *Google Chrome* e *Microsoft Edge* por exemplo, pois está a ser descontinuada, o que levanta muitas dúvidas sobre o futuro da autenticação com recurso ao CC, este que é o maior risco associado ao uso desta tecnologia.



## 7. Conclusão e Perspetivas

No sistema de voto eletrónico (E-voto) como em qualquer outro sistema desta natureza a informação é crítica, os requisitos são exigentes, a construção das políticas de segurança devem ser feitas de forma criteriosa de acordo com os requisitos do sistema. A definição de um método de construção de políticas de segurança é fundamental.

A metodologia seguida, para além de permitir a definição de políticas de segurança, permitiu-nos obter uma visão global do sistema, identificando as principais ameaças, vulnerabilidades, papéis desempenhados, acessos à informação assim como o suporte da tecnologia de segurança associada ao sistema. Para tal, foram utilizadas as propriedades de segurança do CC baseadas em tecnologia criptográfica.

Um dos maiores entraves no que toca a adesão a um sistema de e-voto, é a confiança (40) dos cidadãos, pois existe ainda uma grande incerteza relativamente à viabilidade dos sistemas de votação *on-line*. Os eleitores têm de confiar no sistema que utilizam, os partidos têm de confiar nos resultados e legitimar os mesmos. Para tal, é necessário construir a confiança, essencialmente baseada na segurança oferecida pela solução, de modo a suportar os requisitos de um sistema de voto eletrónico (41).

Em síntese, depois da investigação feita e do trabalho realizado nesta dissertação, acredito que o CC preenche os requisitos necessários para a identificação eletrónica/digital de um sujeito, e o E-voto constitui um primeiro protótipo nesse sentido. Adicionalmente, as políticas e mecanismos de segurança adotados serão vitais para o sucesso de uma implementação em escala real.

É igualmente importante realçar que os testes feitos na plataforma desenvolvida (Protótipo) revelam que esta abordagem permite evitar os votos nulos, uma vez que não foi dada essa opção no E-voto com recurso ao CC. Visto que, os votos nulos não contam para eleger ou para impedir a eleição de nenhum Candidato (42). Este é um assunto delicado, que sai um pouco fora do âmbito tecnológico do trabalho, e entra em considerações político-constitucionais...

A plataforma é interativa e fácil de usar, pelo que irá certamente permitir efetivas reduções no tempo do processo de voto e da apuração dos resultados. Porém, muitos desafios ainda persistem, de entre os quais salientamos a própria capacidade de fiscalização do processo eleitoral e a possibilidade de realização de auditoria ao sistema.

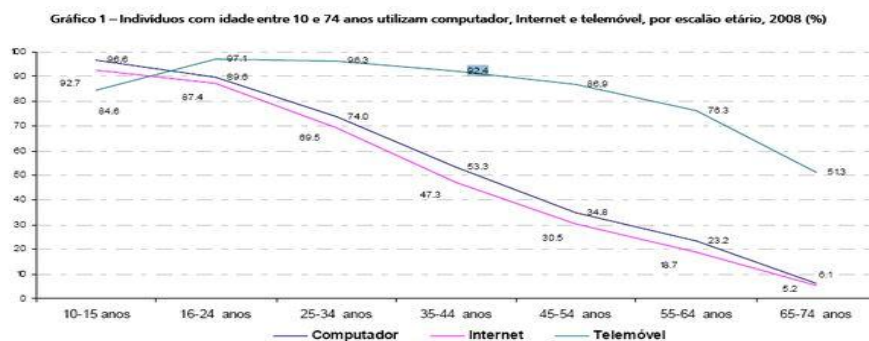
Parece razoável concluir que o E-voto com recurso ao CC pode ser usado como base para uma implementação viável de um sistema de voto eletrónico com segurança idêntica ou superior à de outras atividades já realizadas na *Internet* tais como o *Home banking*, o *e-Comerce* ou as declarações de IRS. Nesse sentido o estudo realizado neste trabalho constitui uma base credível para a implementação de soluções reais para a automação do processo eleitoral, apresentando propostas viáveis para os vários aspetos de um sistema de voto, sobretudo no que respeita à segurança da informação.

Ironicamente, o próprio uso do termo "viável" pode ser aqui utilizado com todo o seu significado, dado que a votação *on-line* é uma realidade cuja tendência é irreversível, sendo

talvez o e-Voto uma das melhores formas do governo eletrónico (*e-Government*) se colocar realmente ao serviço do cidadão.

## 7.1 Trabalhos Futuros

Desde 2005 o telemóvel é das ferramentas que mais revela crescimento segundo o INE (43), com isto, o E-voto visa implementar o voto online a partir do telemóvel e levar aos cidadãos maior agilidade e mobilidade sem abrir mão da segurança na hora de votar. Para isto penso implementar a opção de autenticação forte usando a Chave *Móvel* Digital (CMD).



**Fig. 49 – Indivíduos dos 10 aos 74 anos que usam telemóvel (26)**

A Portaria n.º 189/2014 que regulamenta a CMD foi publicada a 23 de setembro no Diário da República. A CMD é um meio de autenticação eletrónica, complementar ao CC, que pretende contribuir para o aumento do número de utilizadores dos serviços públicos disponíveis online. Entrará em vigor a 1 de janeiro de 2015 (44).

### A Chave Móvel Digital

A Chave Móvel Digital não é mais do que o conjunto de duas palavras-passe que vão permitir a autenticação. Uma é permanente, embora passível de alteração por parte do utilizador, e a outra temporária. Mas só funcionam quando associadas a um número de telemóvel ou a um endereço de *e-mail*.

Sempre que aceder a um site (que tenha este sistema de autenticação), o cidadão identifica-se com o número do cartão e a palavra-passe permanente. Mas a autenticação só fica completa se solicitar o envio de um *mail* ou *SMS* com o código numérico temporário. Trata-se de um sistema semelhante ao que algumas instituições bancárias já utilizam com os seus clientes de *homebanking*.

Como pedir a Chave Móvel Digital

Forma de autenticação voluntária, impõe-se a questão: como solicitar a Chave Móvel Digital? Pode optar por um dos seguintes meios:

**Online** - através do portal autenticação pode associar a sua identificação civil a um número de telemóvel ou endereço de correio eletrónico e é gerada automaticamente a palavra-chave permanente;

**Presencial** – numa Loja do Cidadão ou Conservatória do Registo Civil, onde lhe será atribuída a palavra-chave.

Esta solução não visa descontinuar o CC, muito pelo contrário esta medida visa apenas desmaterializar o CC, e criar meios alternativos de autenticação, alias como já aconteceu noutros dispositivos como o multibanco e o *MB WAY* por exemplo.

Resumindo, autenticamo-nos com o cartão de cidadão em certa entidade (AMA), e geramos dois fatores de autenticação novos (1 – número permanente e 2 – código temporário associado a este número), o que nos garante aqui múltiplos fatores de autenticação. Esta desmaterialização tem ainda associada a vantagem de que não precisamos do *hardware* que acompanha a autenticação com o CC (Leitor de cartões).

Embora muito segura, a CMD está neste momento a suscitar algumas reservas no que toca a privacidade. Pois ao que tudo indica a AMA terá assim acesso a “todas as interações dos cidadãos que utilizam a CMD” na sua relação com a AP. Tendo esses dados, a AMA pode realizar o “total rastreamento das operações efetuadas pelo cidadão utilizador, sabendo, em concreto, que serviços utilizou e que operações efetuou” (45). A CNPD propunha que a AMA ficasse apenas com os dados de registo para a ativação da chave, devendo os restantes dados permanecerem nos respetivos serviços, numa proposta de descentralização dos dados pessoais.

## 8. Bibliografia

1. Wikipédia. *Wikipedia.org*. [Online] 2015 йил 10-Novembro. [Cited: 2015 йил 17-Novembro.] [https://pt.wikipedia.org/wiki/Democracia#cite\\_note-1](https://pt.wikipedia.org/wiki/Democracia#cite_note-1).
2. **Smartmatic.** *smartmatic.com*. [Online] 2015 йил. <http://www.smartmatic.com/pt/votacao/voto-eletronico/>.
3. **segurança, Departamento de.** *euskadi. euskadi.net*. [Online] [http://www.euskadi.net/botoelek/otros\\_paises/ve\\_mundo\\_impl\\_c.htm](http://www.euskadi.net/botoelek/otros_paises/ve_mundo_impl_c.htm).
4. UMIC. *UMIC.pt*. [Online] 2011 йил 24-Outubro. [Cited: 2015 йил 17-Novembro.] [http://www.unic.pt/index.php?option=com\\_content&task=view&id=44&Itemid=112](http://www.unic.pt/index.php?option=com_content&task=view&id=44&Itemid=112).
5. **PE.** Portal do Eleitor. *portaldoeleitor.pt*. [Online] [Citação: 15 de 02 de 2016.] <http://www.portaldoeleitor.pt/Paginas/PossoVotarNaInternet.aspx>.
6. Tribunal Superior Eleitoral. *tse.jus.br*. [Online] 2014 йил. <http://www.tse.jus.br/imprensa/noticias-tse/2014/Junho/conheca-a-historia-da-urna-eletronica-brasileira-que-completa-18-anos>.
7. **Eleitoral, Tribunal Superior.** *tes. tes.jus.br*. [Online] <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/seguranca>.
8. **Marcelo Karam, Felipe Scarel, Diego Aranha.** *(in)segurança do voto eletronico no brasil*. 2010.
9. *Urna electronica pode ser fraudada?* **Borges, Bruna.** Segurança, Brasília : UOL, 2014 йил.
10. brunazo. *www.brunazo.eng.br*. [Online] 2012 йил 10-Dezembro. [Cited: 2015 йил 17-Novembro.] <http://www.brunazo.eng.br/votoe/textos/RelatorioCMind.pdf>.
11. pcworld.uol. *www.pcworld.uol.com.br*. [Online] 2011 йил 13-Agosto. [Cited: 2014 йил 20-Setembro.] <http://pcworld.uol.com.br/noticias/2008/05/19/falta-de-seguranca-leva-holanda-a-proibir-o-uso-de-urnaseletronicas/?0.820055808629>.
12. Globo. *Globo.org*. [Online] 2014 йил 5-Setembro. [Cited: 2015 йил 21-Junho.] <http://g1.globo.com/Noticias/Mundo/0,,MUL418621-5602,00-ELEICOES+NO+PARAGUAI+NAO+TERAO+URNAS+ELETRONICAS.html>.
13. idgnow. *idgnow.uol*. [Online] 2013 йил 6-Setembro. [Cited: 2014 йил 28-Março.] <http://idgnow.uol.com.br/seguranca/2009/03/03/corte-mais-alta-daalemanha-proibe-utilizacao-de-urnas-eletronicas/>.
14. **ISACA.** Glossary of terms, 2008. [Online] 2008 йил. <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>.

15. Manual da teoria da comunicação. [book auth.] Paulo J. Serra. s.l. : Labcom, 2007.
16. **Cerveira**. *Teoria da Computação*. São Paulo : s.n., 1967.
17. A ciência da comunicação. [book auth.] LE CODIAC. s.l. : Briquet, 1996.
18. ISO\_27001. *NP\_ISO\_IEC\_27001\_213*. 2013 йил. Segurança da Informação.
19. LEI ELEITORAL DO PRESIDENTE DA REPÚBLICA. [Online] 2006 йил. [Cited: 2015 йил 17-Novembro.] [Http://www.portaldoeleitor.pt/Documents/DecretosLei/presidente-republica-2006-lei.pdf](http://www.portaldoeleitor.pt/Documents/DecretosLei/presidente-republica-2006-lei.pdf) Artigo 72.º.
20. Lei da privacidade de dados. *cndp.pt*. [Online] [Cited: 2015 йил 17-Novembro.] <http://www.cnpd.pt/bin/legis/nacional/LPD.pdf>.
21. LEI ELEITORAL DO PRESIDENTE DA REPÚBLICA. *Http://www.portaldoeleitor.pt*. [Online] [Cited: 2015 йил 17-Novembro.] [Http://www.portaldoeleitor.pt/Documents/DecretosLei/presidente-republica-2006-lei.pdf](http://www.portaldoeleitor.pt/Documents/DecretosLei/presidente-republica-2006-lei.pdf) Artigo 73.º.
22. melhorseguranca . *melhorseguranca.blogspot.pt*. [Online] [Cited: 2015 йил 17-Novembro.] <http://melhorseguranca.blogspot.pt/2013/10/sistemas-de-intrusao-normas-en50131.html> .
23. **WIKIVERSIDADE**. *wikiversidade.org*. [Online] 2015 йил Outubro. [https://pt.wikiversity.org/wiki/Seguran%C3%A7a\\_em\\_Redes\\_de\\_Dados/Seguran%C3%A7a\\_da\\_Informa%C3%A7%C3%A3o](https://pt.wikiversity.org/wiki/Seguran%C3%A7a_em_Redes_de_Dados/Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o).
24. NetLab. *Netlab.ulusofona.pt*. [Online] [Cited: 2015 йил 17-Novembro.] <http://netlab.ulusofona.pt/im/teoricas/IM-02-IdMgmt.pdf>.
25. Decreto-lei de criação do cartão de cidadão. *http://dre.pt*. [Online] 2007 йил 5-Fevereiro. [Cited: 2015 йил 17-Novembro.] <http://dre.pt/pdf1s/2007/02/02500/09400948.pdf>.
26. taskblog. *www.taskblog.com.br*. [Online] [Cited: 2015 йил 17-Novembro.] <http://www.taskblog.com.br/05/certificacao-digital-parte-iv-criptografia-simetrica-modelos-diffie-hellman-e-rsa/> .
27. wikipedia. *wikipedia.org*. [Online] 2015 йил 1-Setembro. [Cited: 2015 йил 17-Novembro.] [https://pt.wikipedia.org/wiki/Ataque\\_man-in-the-middle](https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle).
28. itu. *itu.int*. [Online] [Cited: 2015 йил 17-Novembro.] <http://www.itu.int/rec/T-REC-X.509-200508-I/en>.
29. bsi. *www.bsi.bund.de*. [Online] [Cited: 2015 йил 17-Novembro.] 20-<https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html>.
30. **Gehrke, Wolr &**. *A Maturity Model for Segregation of Duties*. 2009.

31. **NetLab.** NetLab. *netlab.ulusofona.pt*. [Online] <http://netlab.ulusofona.pt/im/>.
32. **searchsecurity.** *http://searchsecurity.techtarget.com*. [Online] 2008 йил. <http://searchsecurity.techtarget.com/definition/single-sign-on>.
33. **RPN.** *Rede Nacional de Ensino e Pesquisa*. [Online] [Cited: 2015 йил 17-Novembro.] <https://portal.rnp.br/web/servicos/como-funciona>.
34. **Notariado, Instituto dos Registos do.** *portaldocidadao*. [Online] [Citação: 9 de Setembro de 2015.] [www.portaldocidadao.pt](http://www.portaldocidadao.pt).
35. **Dorow, Emerson.** Governança de TI. *http://www.governancadeti.com*. [Online] 2007 йил Novembro. <http://www.governancadeti.com/2010/11/governanca-e-a-gestao-de-riscos-em-ti/>.
36. **Ferrer, Rogerio.** SISTESEG. [Online] 2008 йил. [http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwiHueizvczJAhWJuRoKHcGBCNYQFgg6MAQ&url=http%3A%2F%2Fwww.sisteseg.com%2Ffile%2FMicrosoft\\_Word\\_-\\_METODOLOGIA\\_DE\\_ANALISIS\\_DE\\_RIESGO.pdf&usg=AFQjCNGKPoM1CK8btSUJrTnETBS6sPqWyQ](http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwiHueizvczJAhWJuRoKHcGBCNYQFgg6MAQ&url=http%3A%2F%2Fwww.sisteseg.com%2Ffile%2FMicrosoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf&usg=AFQjCNGKPoM1CK8btSUJrTnETBS6sPqWyQ).
37. **Cluster, HA storage.** *open-e.com*. [Online] [http://www.open-e.com/site\\_media/download/documents/ha-storage-cluster.pdf](http://www.open-e.com/site_media/download/documents/ha-storage-cluster.pdf).
38. **Business, Computer.** Disaster Recovery. [Online] 2012 йил. <http://www.computerbusinessresearch.com/Home/enterprise-architecture/disaster-recovery>.
39. **IBM.** Disaster Recovery and Business Continuity. [Online] 2011 йил Agosto.
40. **Bannet, J. e. a.** *"Hack-a-Vote: Demonstrating Security Issues with"*. 2003.
41. **Rivest, R. L.** *Electronic Voting. Financial Cryptography*. 2001.
42. **Tornado, Jornal.** *www.jornaltornado.pt*. [Online] 01 de 2016. [Citação: 22 de 02 de 2016.] <http://www.jornaltornado.pt/o-que-diz-o-direito-sobre-abstencao-votos-nulos-e-em-branco/>.
43. **INE.** *sapo.pt*. [Online] 2012 йил. [http://tek.sapo.pt/noticias/telecomunicacoes/artigo/85\\_dos\\_jovens\\_usa\\_telemovel-911480tek.html](http://tek.sapo.pt/noticias/telecomunicacoes/artigo/85_dos_jovens_usa_telemovel-911480tek.html).
44. **administrativa, Agencia para a modernização.** *ama. ama.pt*. [Online] [http://www.ama.pt/index.php\\_option=com\\_content&task=view&id=1586&Itemid=44.html](http://www.ama.pt/index.php_option=com_content&task=view&id=1586&Itemid=44.html).
45. **Fonseca, Pedro.** *computerworld*. *http://www.computerworld.com.pt*. [Online] 2015 йил. <http://www.computerworld.com.pt/2014/05/16/cartao-do-cidadao-perde-para-chave-movel-digital/>.

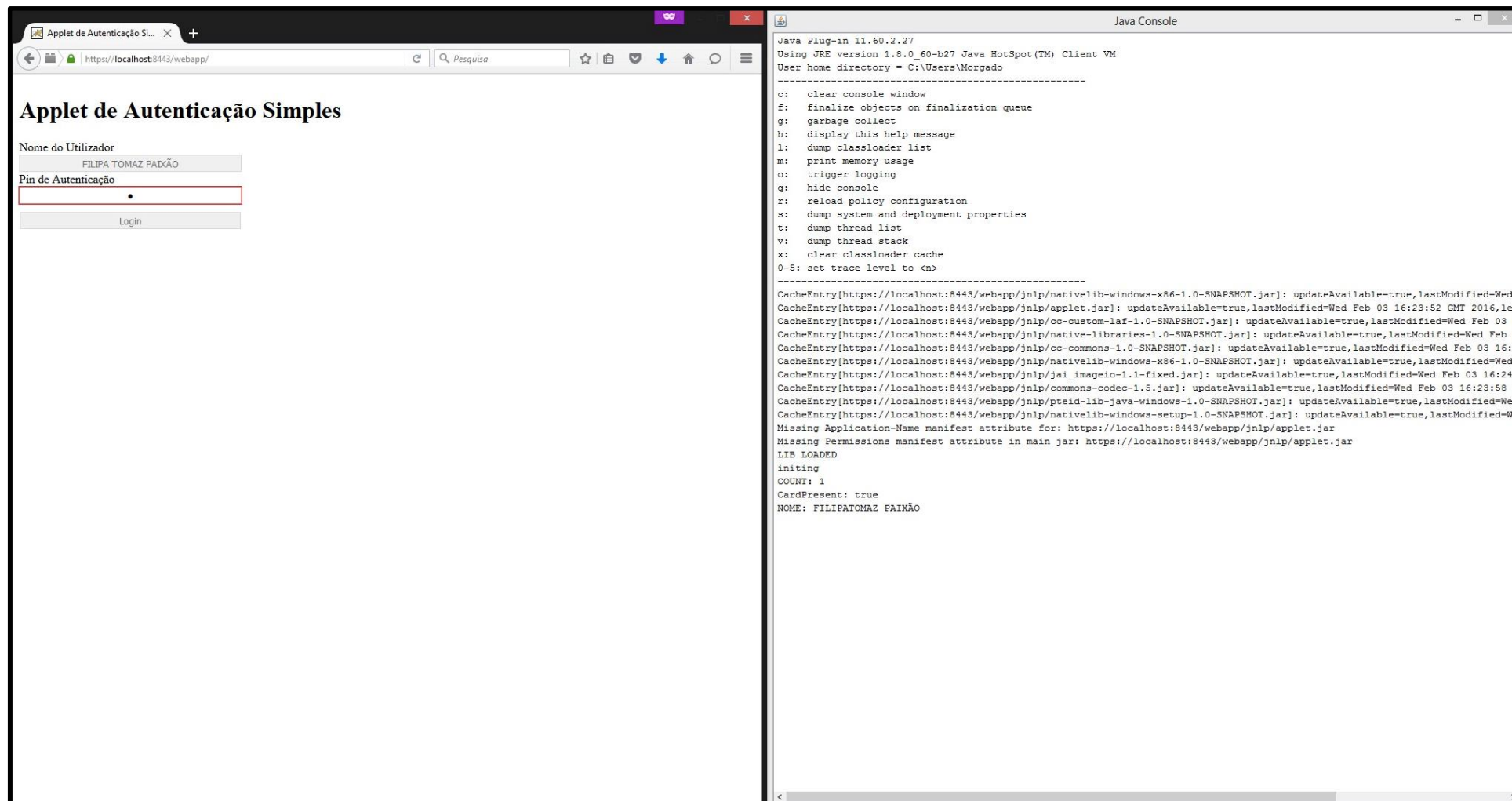
46. [egov. \*egov.ufsc.br\*](http://www.egov.ufsc.br). [Online]  
[http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwiO8bfIttnJAhXBaxQKHQLoD70QFggqMAM&url=http%3A%2F%2Fwww.egov.ufsc.br%2Fportal%2Fsites%2Fdefault%2Ffiles%2Fa\\_importancia\\_do\\_voto\\_eletronico\\_em\\_estonia\\_para\\_o\\_avance\\_da\\_democracia.pdf&u](http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwiO8bfIttnJAhXBaxQKHQLoD70QFggqMAM&url=http%3A%2F%2Fwww.egov.ufsc.br%2Fportal%2Fsites%2Fdefault%2Ffiles%2Fa_importancia_do_voto_eletronico_em_estonia_para_o_avance_da_democracia.pdf&u).

# ANEXOS

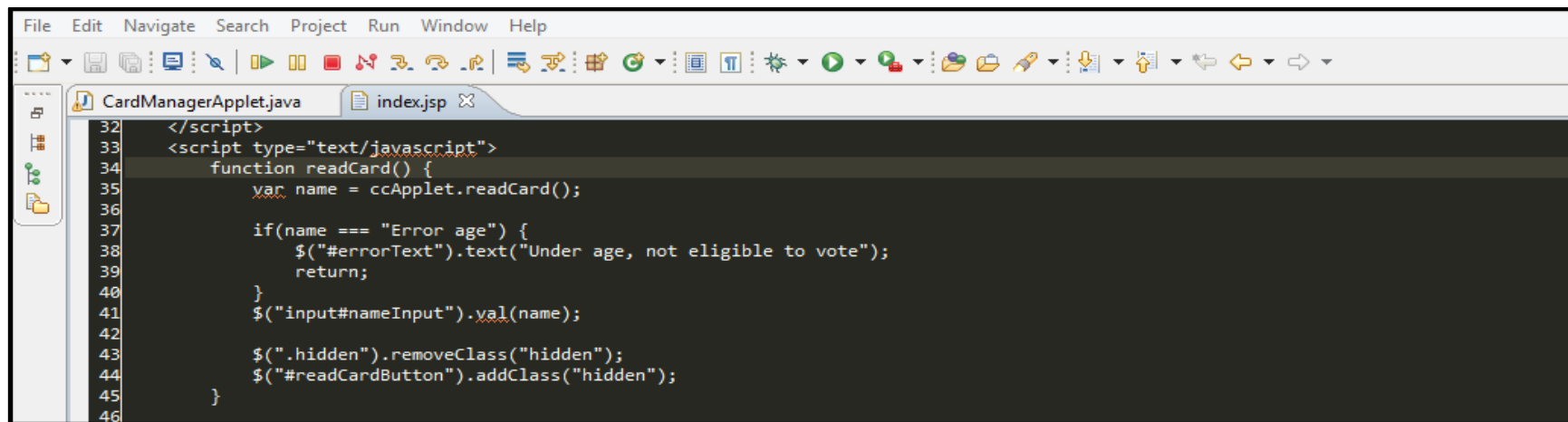




Logotipo E-voto



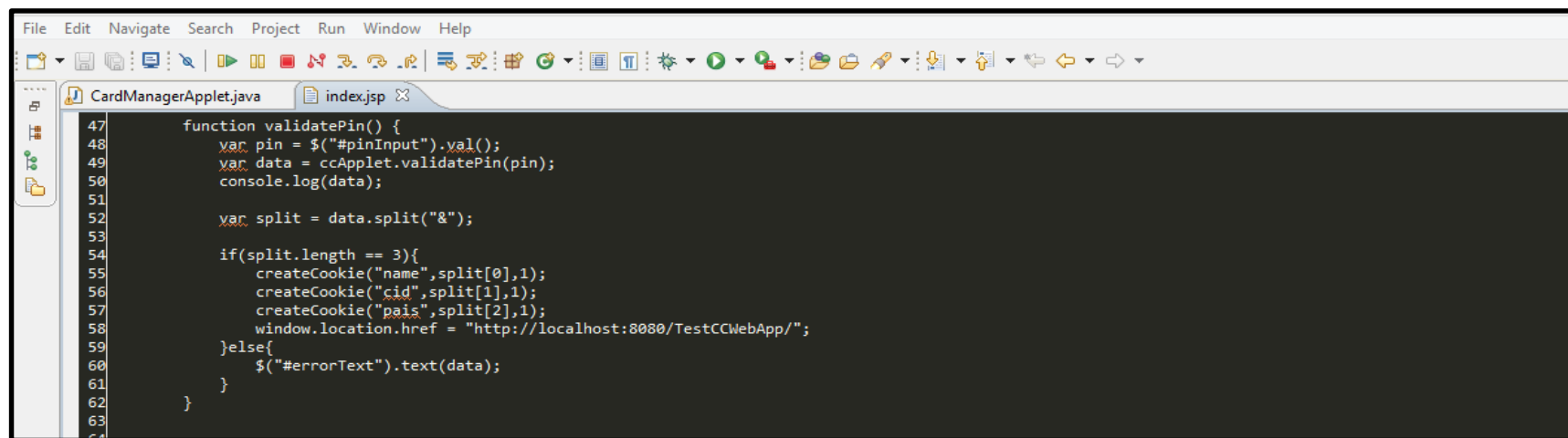
### Menu login



The screenshot shows an IDE window with two tabs: 'CardManagerApplet.java' and 'index.jsp'. The 'index.jsp' tab is active, displaying a JavaScript function 'readCard()' starting at line 33. The function reads a card value, checks for an 'Error age' condition, and updates the UI by removing a 'hidden' class from an input field and adding it to a button.

```
32 </script>
33 <script type="text/javascript">
34   function readCard() {
35     var name = ccApplet.readCard();
36
37     if(name === "Error age") {
38       $("#errorText").text("Under age, not eligible to vote");
39       return;
40     }
41     $("input#nameInput").val(name);
42
43     $(".hidden").removeClass("hidden");
44     $("#readCardButton").addClass("hidden");
45   }
46
```

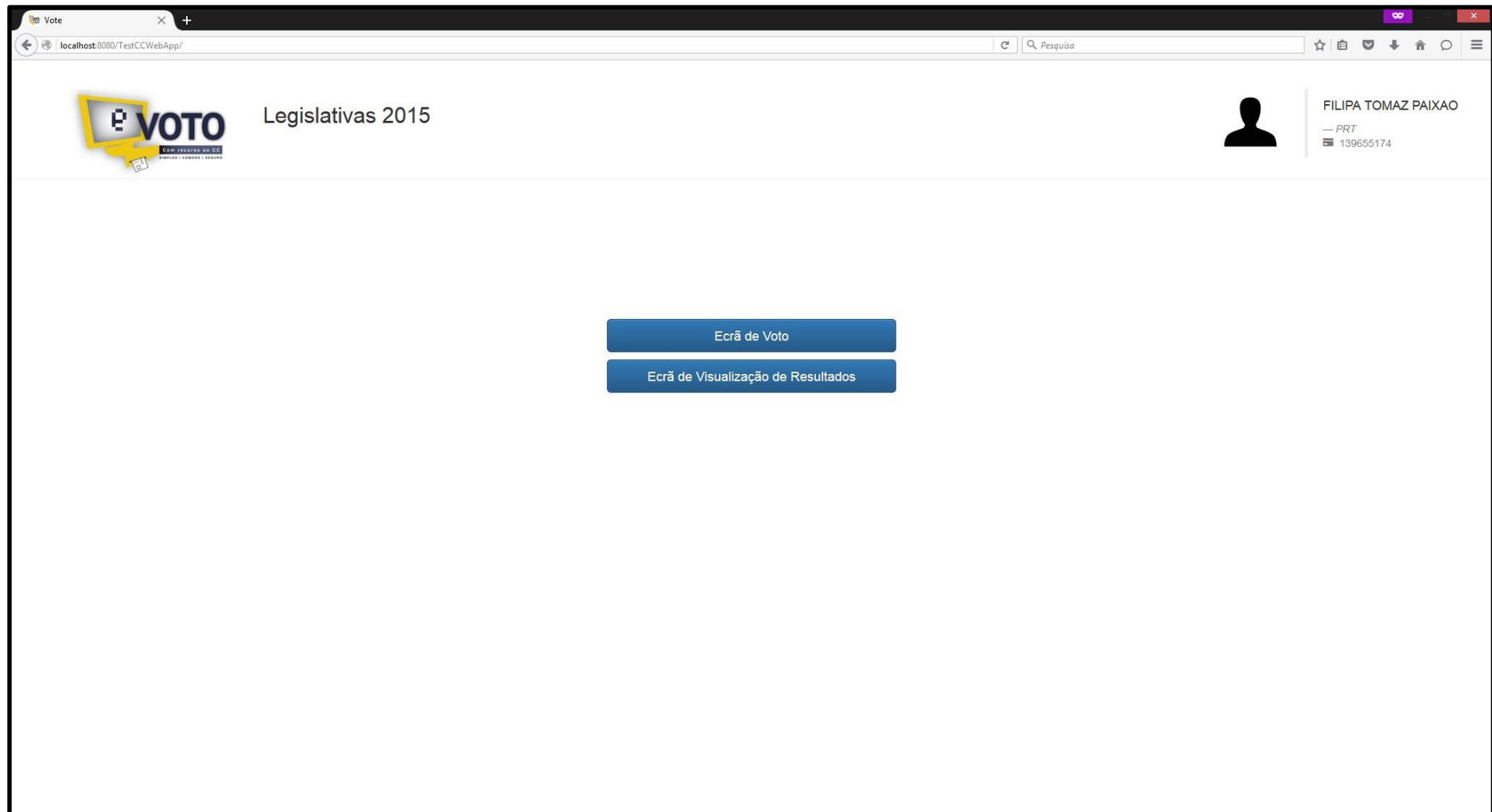
### Uma parte significativa do código de leitura do CC



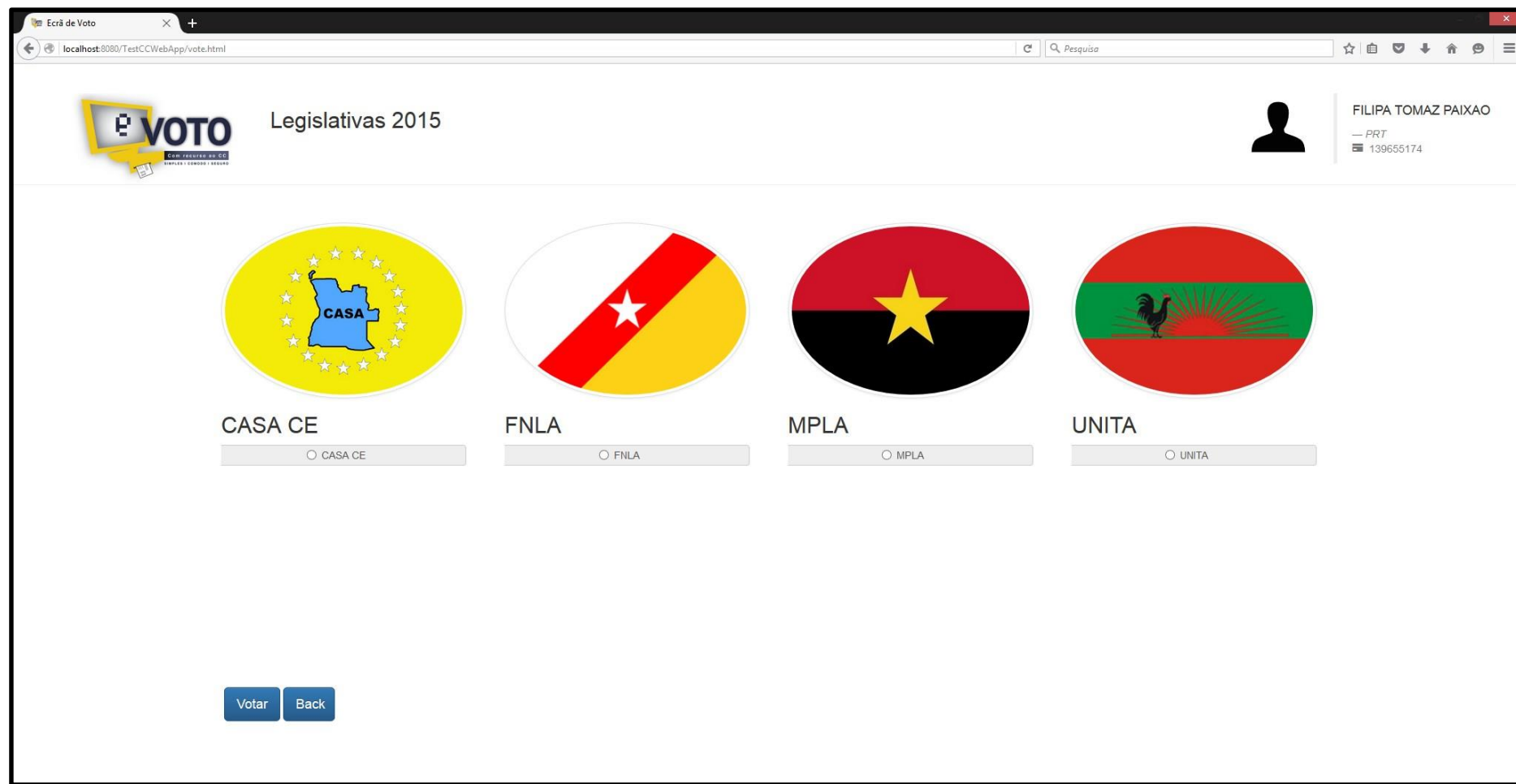
The screenshot shows the same IDE window with the 'index.jsp' tab active, displaying a JavaScript function 'validatePin()' starting at line 47. The function validates a PIN, splits the resulting data into cookies for 'name', 'cid', and 'pais', and sets the window location to the test application URL. It also includes an error handling path for the errorText field.

```
47   function validatePin() {
48     var pin = $("pinInput").val();
49     var data = ccApplet.validatePin(pin);
50     console.log(data);
51
52     var split = data.split("&");
53
54     if(split.length == 3){
55       createCookie("name",split[0],1);
56       createCookie("cid",split[1],1);
57       createCookie("pais",split[2],1);
58       window.location.href = "http://localhost:8080/TestCCWebApp/";
59     }else{
60       $("#errorText").text(data);
61     }
62   }
63
```

### Uma parte significativa do código de autenticação



**Menu seleção (Voto / Resultado) visível depois de autenticado com sucesso**




### Menu Voto (selecção de candidatos)

Ecrã de Voto


localhost:8080/TestCCWebApp/vote.html

Pesquisa

☆ 📁 🔽 🏠 🗨️ ☰




Legislativas 2015




FILIPA TOMAZ PAIXAO  
— PRT  
139655174

Voto com sucesso! - Artigo 70.º 73




CASA CE

☐ CASA CE



FNLA


☐ FNLA



MPLA

Movimento Popular de Libertação de Angola (MPLA) é um partido político de Angola, que governa o país desde sua independência de Portugal em 1975. Foi, inicialmente, um movimento de luta pela independência de Angola, transformando-se num partido político após a Guerra de Independência de 1961-74. Conquistou o poder em 1974/75, durante o processo de descolonização e saiu vencedor da Guerra Civil Angolana de 1975-2002, contra dois partidos rivais, a UNITA e a FNLA.

☒ MPLA



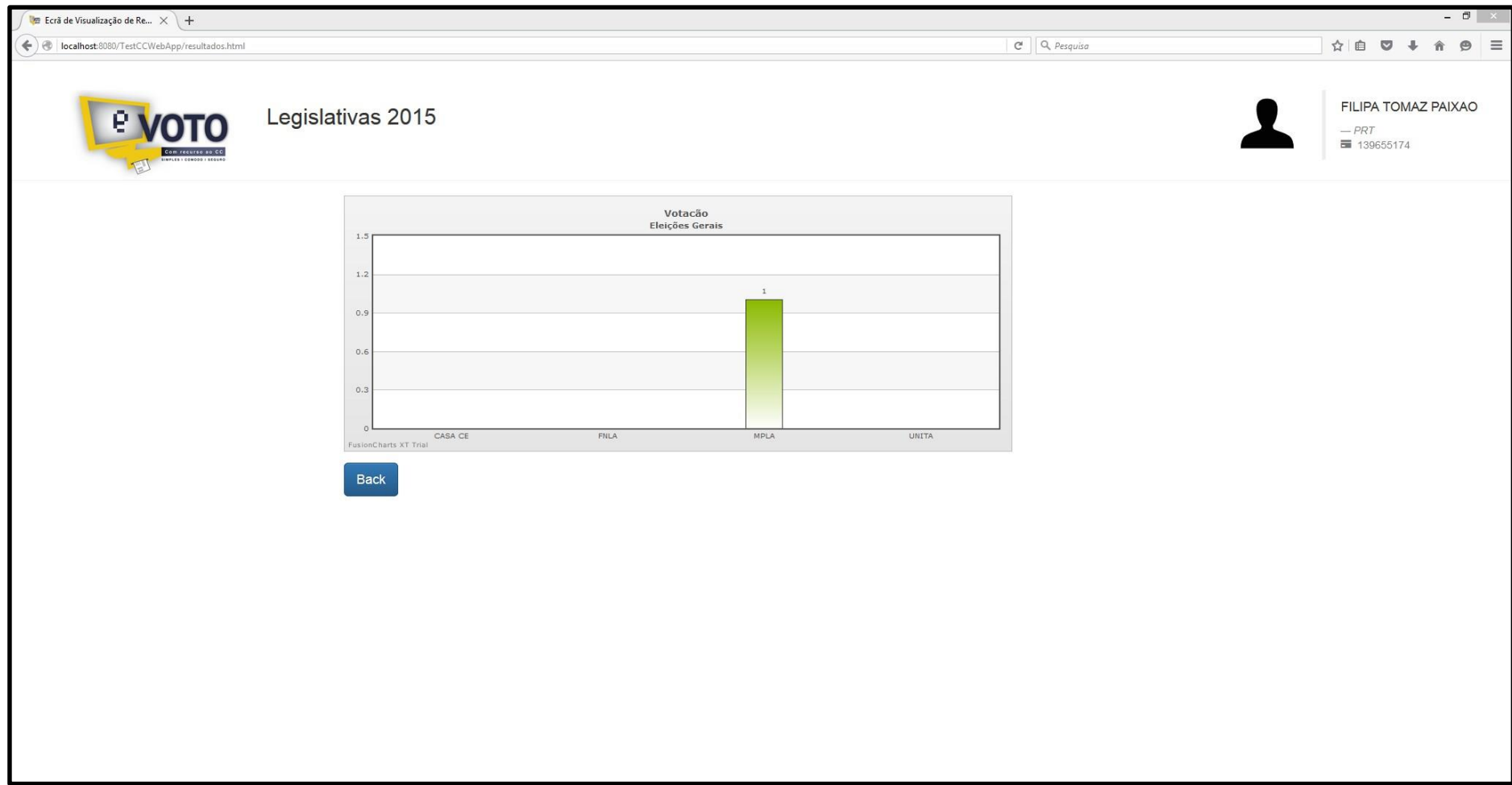
UNITA

☐ UNITA

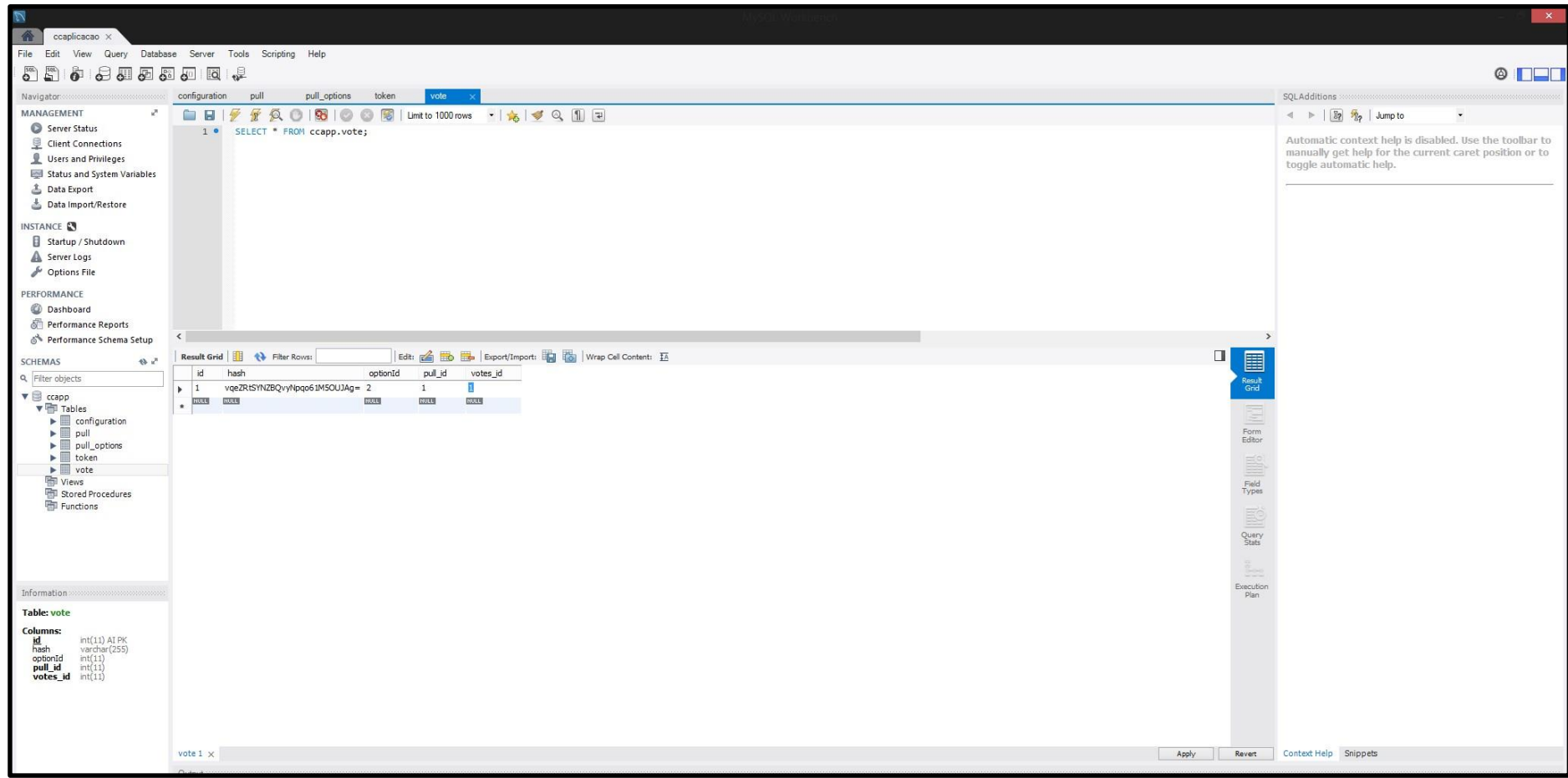
Votar

Back

### Confirmação do voto (Artigo 70.º)



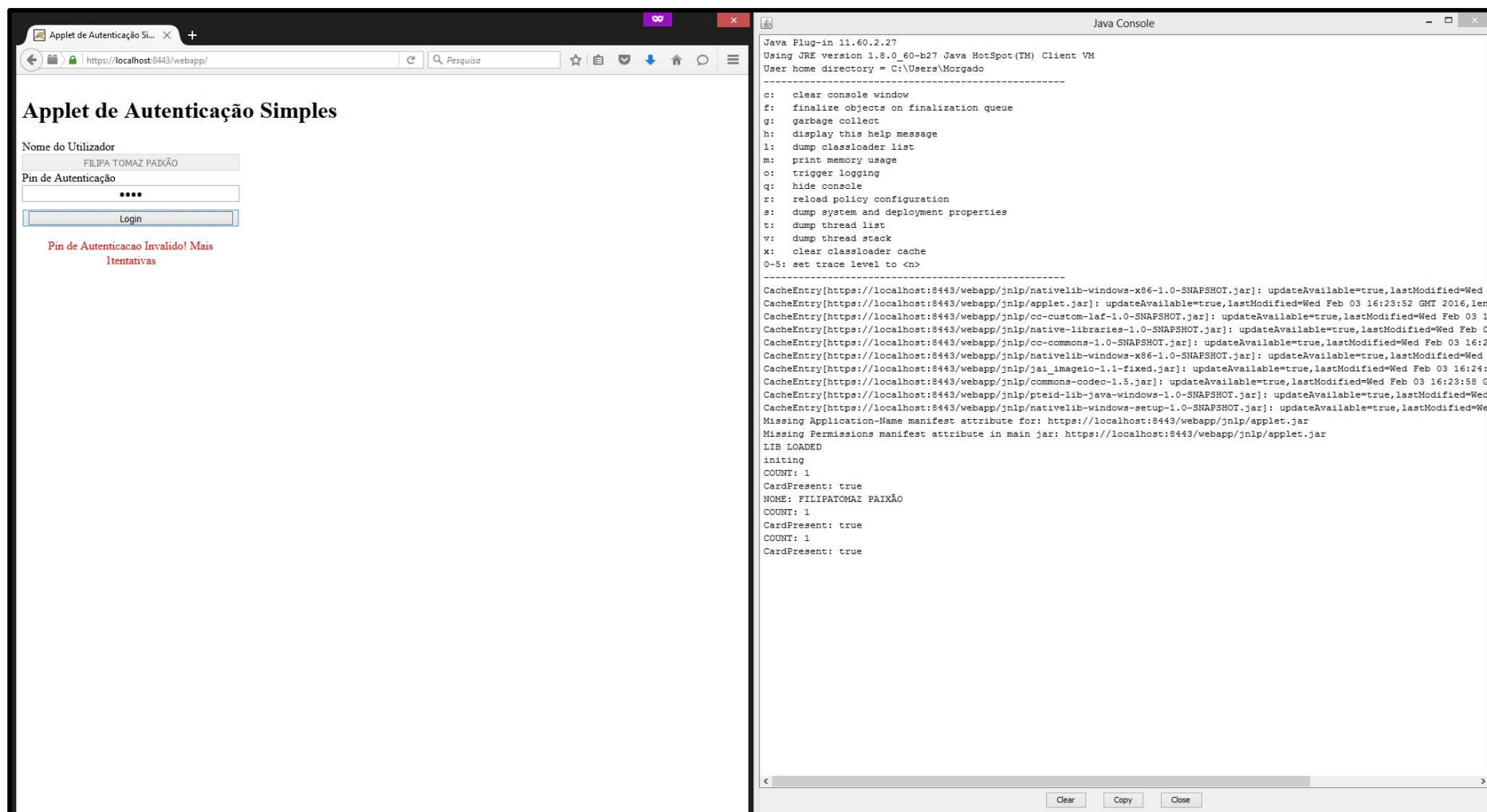
**Menu resultado (voto contabilizado)**



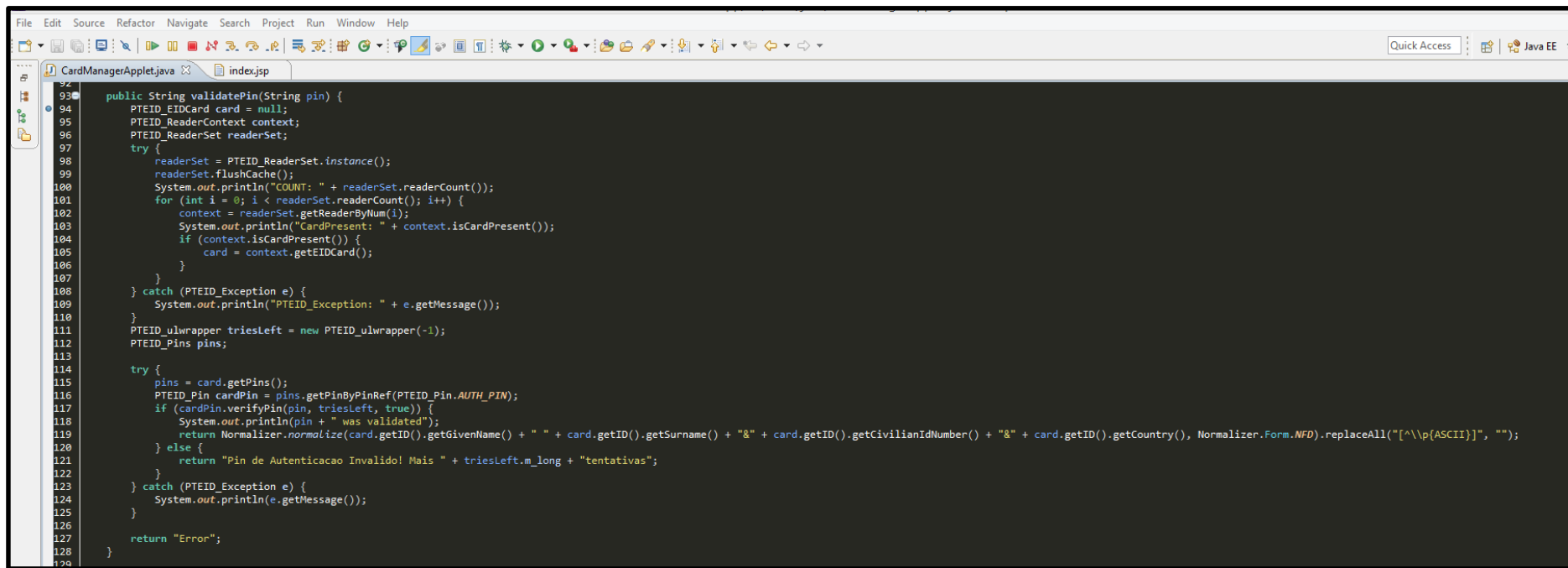
**Voto na Base de Dados (hash do número do cartão + nome para garantia de privacidade)**



# MENSAGENS DE ERRO

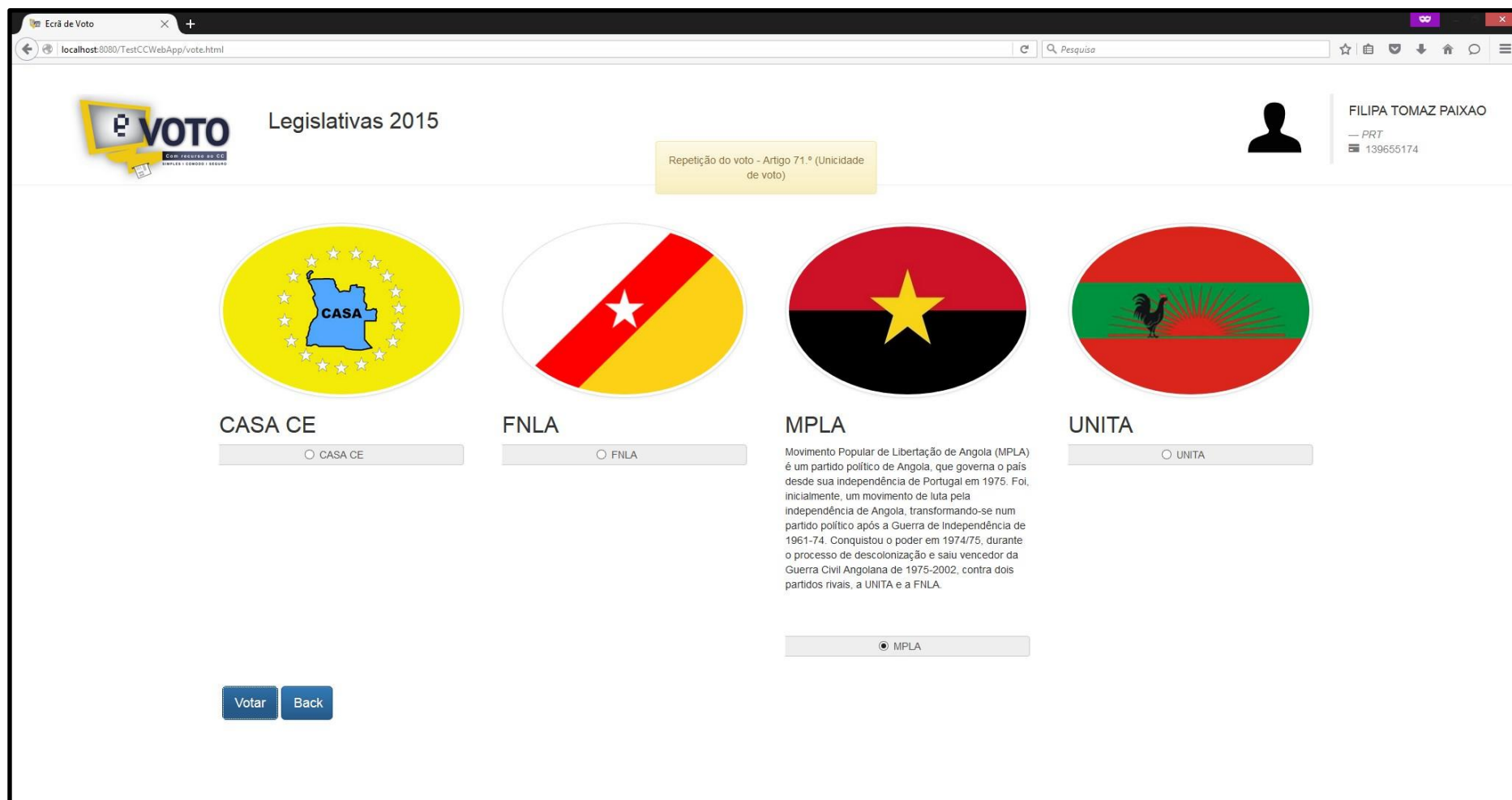


### Tentativa de autenticação sem sucesso (PIN errado)

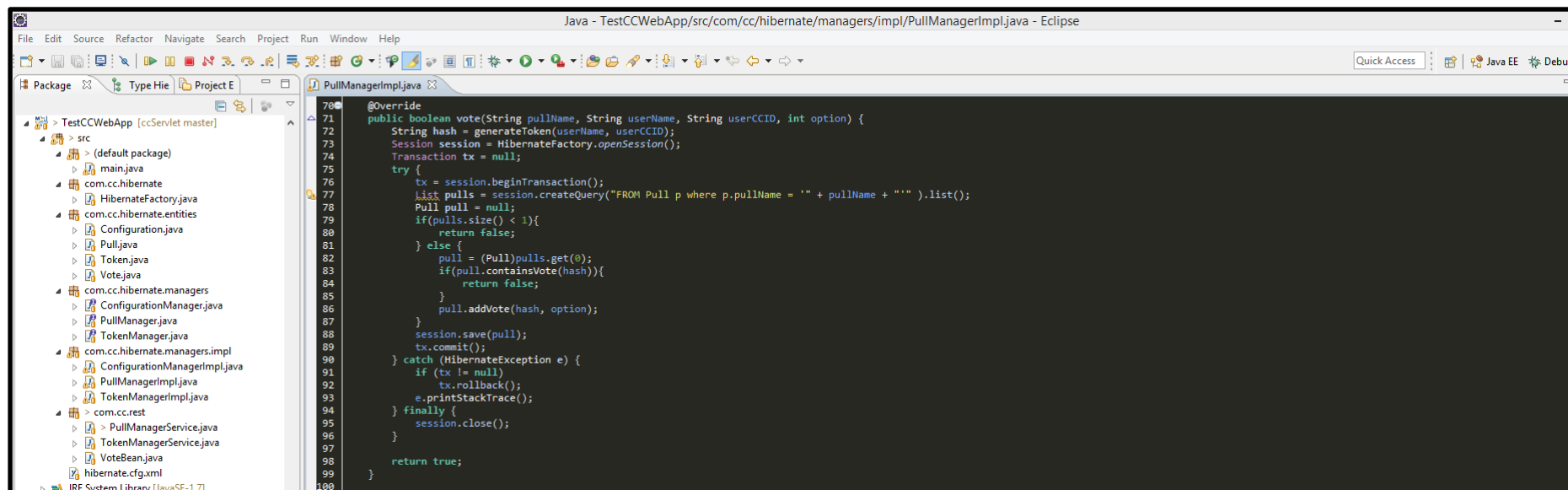


```
92  
93 public String validatePin(String pin) {  
94     PTEID_EIDCard card = null;  
95     PTEID_ReaderContext context;  
96     PTEID_ReaderSet readerSet;  
97     try {  
98         readerSet = PTEID_ReaderSet.instance();  
99         readerSet.flushCache();  
100         System.out.println("COUNT: " + readerSet.readerCount());  
101         for (int i = 0; i < readerSet.readerCount(); i++) {  
102             context = readerSet.getReaderByNum(i);  
103             System.out.println("CardPresent: " + context.isCardPresent());  
104             if (context.isCardPresent()) {  
105                 card = context.getEIDCard();  
106             }  
107         }  
108     } catch (PTEID_Exception e) {  
109         System.out.println("PTEID_Exception: " + e.getMessage());  
110     }  
111     PTEID_ulwrapper triesLeft = new PTEID_ulwrapper(-1);  
112     PTEID_Pins pins;  
113  
114     try {  
115         pins = card.getPins();  
116         PTEID_Pin cardPin = pins.getPinByPinRef(PTEID_Pin.AUTH_PIN);  
117         if (cardPin.verifyPin(pin, triesLeft, true)) {  
118             System.out.println(pin + " was validated");  
119             return Normalizer.normalize(card.getID().getGivenName() + " " + card.getID().getSurname() + "&" + card.getID().getCivilianIdNumber() + "&" + card.getID().getCountry(), Normalizer.Form.NFD).replaceAll("[^\\p{ASCII}]", "");  
120         } else {  
121             return "Pin de Autenticacao Invalido! Mais " + triesLeft.m_long + "tentativas";  
122         }  
123     } catch (PTEID_Exception e) {  
124         System.out.println(e.getMessage());  
125     }  
126  
127     return "Error";  
128 }  
129 }
```

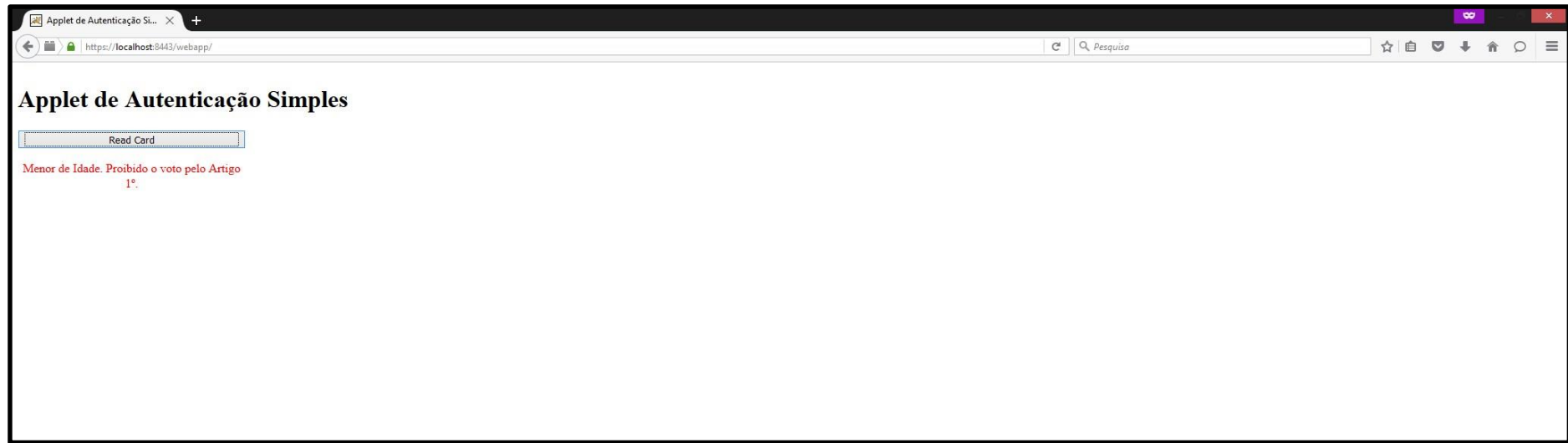
**Uma parte significativa validação do PIN e alerta das tentativas em falta em caso de ERRO**



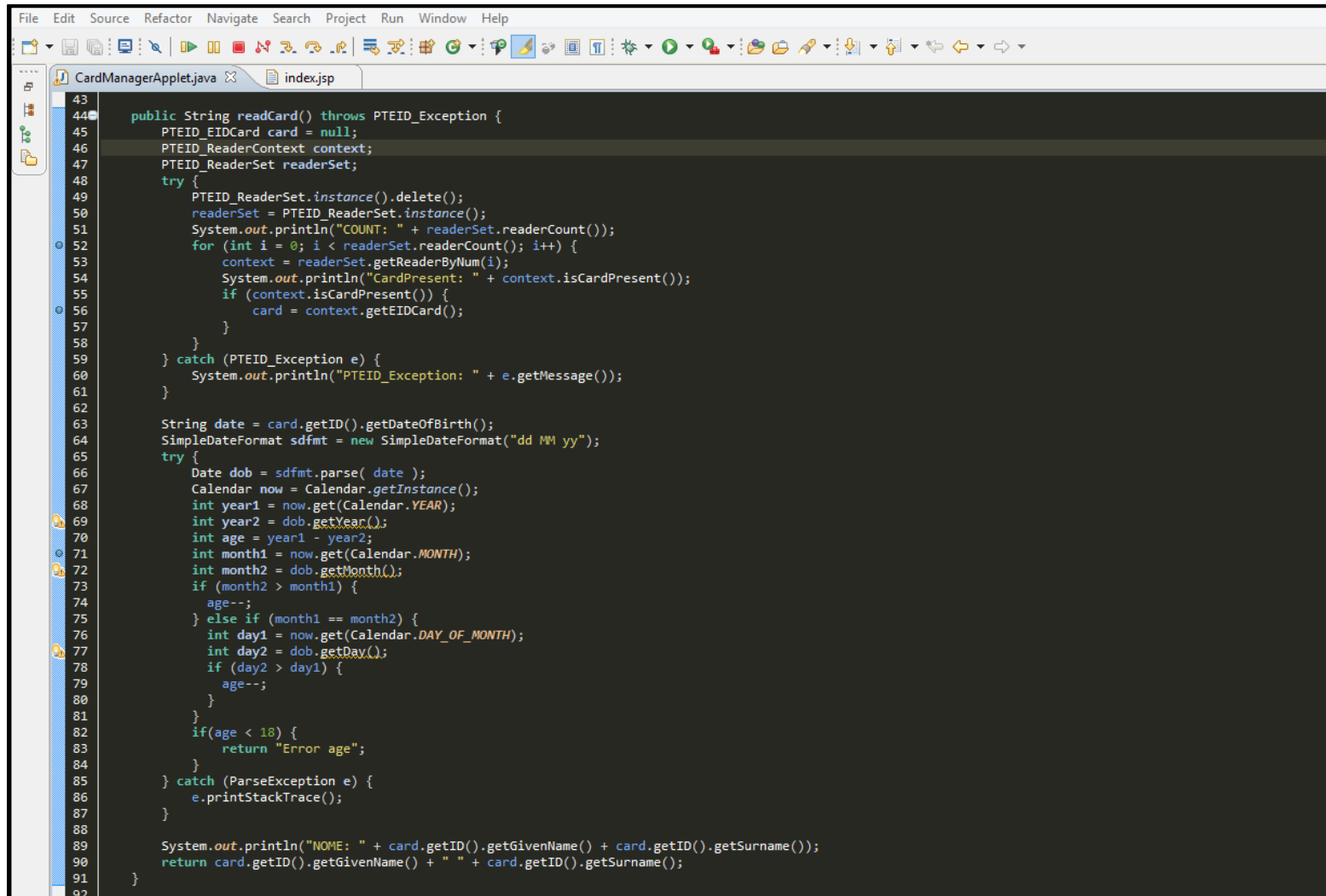
**ERRO: Tentativa de votar pela 2ª vez, baseado no artigo 71º (Unicidade)**



### Comparação da hash do novo requerente com as existentes na BD para garantia da Unicidade



**ERRO: Tentativa de Login de menor de idade, baseado no artigo 1º**



```
43
44 public String readCard() throws PTEID_Exception {
45     PTEID_EIDCard card = null;
46     PTEID_ReaderContext context;
47     PTEID_ReaderSet readerSet;
48     try {
49         PTEID_ReaderSet.instance().delete();
50         readerSet = PTEID_ReaderSet.instance();
51         System.out.println("COUNT: " + readerSet.readerCount());
52         for (int i = 0; i < readerSet.readerCount(); i++) {
53             context = readerSet.getReaderByNum(i);
54             System.out.println("CardPresent: " + context.isCardPresent());
55             if (context.isCardPresent()) {
56                 card = context.getEIDCard();
57             }
58         }
59     } catch (PTEID_Exception e) {
60         System.out.println("PTEID_Exception: " + e.getMessage());
61     }
62
63     String date = card.getID().getDateOfBirth();
64     SimpleDateFormat sdfmt = new SimpleDateFormat("dd MM yy");
65     try {
66         Date dob = sdfmt.parse( date );
67         Calendar now = Calendar.getInstance();
68         int year1 = now.get(Calendar.YEAR);
69         int year2 = dob.getYear();
70         int age = year1 - year2;
71         int month1 = now.get(Calendar.MONTH);
72         int month2 = dob.getMonth();
73         if (month2 > month1) {
74             age--;
75         } else if (month1 == month2) {
76             int day1 = now.get(Calendar.DAY_OF_MONTH);
77             int day2 = dob.getDay();
78             if (day2 > day1) {
79                 age--;
80             }
81         }
82         if (age < 18) {
83             return "Error age";
84         }
85     } catch (ParseException e) {
86         e.printStackTrace();
87     }
88
89     System.out.println("NOME: " + card.getID().getGivenName() + card.getID().getSurname());
90     return card.getID().getGivenName() + " " + card.getID().getSurname();
91 }
92
```

### Uma parte significativa validação da Idade