



Projeto de Graduação em Computação III

IDENTIFICAÇÃO CIVIL DIGITAL

Autor: Kauan Manzato do Nascimento

Orientador: Prof. Dr. Carlos Alberto Kamienski

Santo André – SP

Maio de 2022

Aos meus pais, Vanessa e Dalton, ao meu irmão Yuri e minha amada Melissa, que são minha fonte de inspiração e determinação, que me permitiram chegar tão longe em uma jornada de lutas e sacrifícios e a quem eu prometo trazer orgulhos enquanto me for possível.

ÍNDICE

RESUMO.....	4
1. INTRODUÇÃO.....	5
1.1 CONTEXTUALIZAÇÃO.....	5
1.2 PROBLEMAS.....	6
1.3 OBJETIVO GERAL.....	8
1.4 OBJETIVOS ESPECÍFICOS.....	8
2. REVISÃO BIBLIOGRÁFICA.....	9
2.1 IDENTIFICAÇÃO.....	9
2.2 CRIPTOGRAFIA DE CHAVE PÚBLICA.....	10
2.2.1 CRIPTOGRAFIA DE CURVAS ELÍPTICAS.....	11
2.2.2 SISTEMA CRIPTOGRÁFICO RSA.....	13
2.3 ASSINATURAS DIGITAIS.....	13
2.4 CERTIFICADOS DIGITAIS.....	14
2.5 INFRAESTRUTURA DE CHAVE PÚBLICA (PKI).....	15
2.6 IDENTIDADE DIGITAL.....	16
3. SOLUÇÃO PROPOSTA.....	17
3.1 FERRAMENTAS.....	17
3.2 FUNCIONALIDADES.....	17
3.3 EMISSÃO DA CARTEIRA DE IDENTIDADE.....	18
3.3.1 CÓDIGO DA EMISSÃO DA CARTEIRA DE IDENTIDADE.....	19
3.3.2 DEMONSTRAÇÃO DO CÓDIGO.....	21
3.4 AUTENTICAÇÃO.....	24
3.4.1 AUTENTICAÇÃO DO CERTIFICADO DO CLIENTE TLS.....	24
3.5 CRIPTOGRAFIAR E DESCRIPTOGRAFIAR.....	25
3.5.1 CRIPTOGRAFIA NESTE TRABALHO.....	25
3.6 ASSINAR E VALIDAR.....	26
4. TESTES.....	27
4.1 ELEIÇÕES NO BRASIL.....	27
4.2 ELEIÇÕES DIGITAIS.....	28
4.2.1 FUNÇÕES USADAS.....	29
4.2.2 APLICAÇÃO DO ELEITOR.....	31

4.2.3 APLICAÇÃO DO TSE.....	32
4.2.4 DEMONSTRAÇÃO DAS ELEIÇÕES DIGITAIS.....	32
4.3 OUTRAS APLICAÇÕES.....	36
5. CONCLUSÃO.....	37
6. REFERÊNCIAS BIBLIOGRÁFICAS.....	38

RESUMO

Este trabalho discorre do problema de identificação civil no Brasil, expondo as suas causas e consequências e propondo uma solução baseada em criptografia de chave pública e no documento de identidade digital implementado na Estônia, porém adaptando à realidade brasileira. Depois de uma extensa revisão do problema, da bibliografia e de soluções semelhantes implementadas em outros países, a solução proposta será explicada e, depois, demonstrada por meio da simulação da emissão de uma carteira de identidade digital. Por fim, a solução proposta será aplicada em um cenário fictício de eleições digitais. Ambas as aplicações serão mostradas no trabalho e estarão disponíveis em um repositório no GitHub¹ para que todo e qualquer leitor tenha a possibilidade de testá-las.

O objetivo final deste trabalho, além de propor uma solução a um problema real, é complementar e estender a formação do aluno e avaliar o desempenho do discente tendo em vista os objetivos gerais do curso, conforme a disposição do PGC em 2022. Por este motivo, o escopo do trabalho é definido proporcionalmente ao tempo e os recursos à disposição. E, mesmo com as limitações, o trabalho obteve êxito em demonstrar a viabilidade, a simplicidade e as vantagens da solução proposta, contribuindo para a literatura de identificação civil digital.

¹ O código-fonte deste trabalho está disponível em: <https://github.com/kauanmn/PGC>.

1 – INTRODUÇÃO

Este trabalho trata sobre o problema da identificação civil no Brasil e suas consequências e propõe como solução um cartão inteligente que permite a identificação e a autenticação dos cidadãos brasileiros baseado em infraestrutura de chave pública (PKI) e no sistema atual de identificação digital da Estônia, sendo avaliado pelos seguintes critérios:

- **Eficácia:** se o sistema cumpre os objetivos designados;
- **Eficiência:** quantidade de recursos utilizados para implementar o sistema, mantê-lo e utilizá-lo;
- **Interoperabilidade:** a solução precisa definir um padrão com abrangência nacional e que permita a interação entre os diferentes órgãos públicos;
- **Segurança:** a solução deve garantir a segurança (confidencialidade, integridade e autenticidade) das informações processadas e transmitidas;
- **Limitações:** as limitações e desvantagens conhecidas da solução proposta, em comparação com os benefícios trazidos por ela.

Os impactos políticos e sociais, legislação e regulamentações estão fora do escopo deste trabalho, ficando limitadas a trabalhos futuros. Além disso, uma possível aplicação da solução em um cenário hipotético de eleições digitais também é demonstrada, como forma de exemplificar e dissecar os detalhes da proposta.

1.1 – CONTEXTUALIZAÇÃO

Com o advento da pandemia do Covid-19 em 2020, o Governo Federal brasileiro concedeu um benefício chamado Auxílio Emergencial cujo objetivo é minimizar o impacto da crise do vírus na população de baixa renda, de trabalhadores informais, de microempreendedores individuais e contribuintes individuais do INSS (Instituto Nacional do Seguro Social) [20]. Porém, para receber o benefício, a pessoa precisa cumprir uma série de requisitos, conforme a Lei nº 13.982/2020.

O cadastro dos dados e a liberação dos valores do auxílio à população se dá por meio de um software para smartphones, chamado Caixa Tem: o cidadão instala o aplicativo no dispositivo, informa seus dados pessoais (autodeclaração e identificação) e aguarda a aprovação

do Ministério da Cidadania [22]. Em caso de aprovação, o benefício é liberado para a pessoa na conta do aplicativo, que funciona como uma conta corrente.

Entretanto, desde o início do cadastro, as pessoas têm relatado que sujeitos receberam o benefício sem cumprir os requisitos ou que algum agente malicioso usou os dados de terceiros para receber o benefício indevidamente. Estas situações caracterizam o delito de estelionato, previsto no artigo 171 do Código Penal [4, 7].

1.2 – PROBLEMAS

Os problemas citados na seção anterior acontecem porque dados pessoais (CPF, nome, endereço, gênero, data de nascimento etc.) de muitos brasileiros podem ser encontrados na Internet, disponibilizados para venda e, geralmente, utilizados para fins ilícitos, como fraudes [55].

O dado pessoal que será tratado aqui é o Cadastro de Pessoas Físicas (CPF), registro instituído em 1965 por meio da Lei 4.862, de 29 de novembro de 1965, projetado exclusivamente para a verificação da contribuição do Imposto de Renda de Pessoa Física (IRPF). Atualmente, o CPF é mantido pela Receita Federal do Brasil. Entretanto, na prática, o CPF é usado para a identificação dos cidadãos e suas relações com órgãos públicos em alternativa ao Registro Geral (RG), a exemplo do projeto de Lei 1.422, de 2019. Em outras palavras, o CPF está sendo usado para fins diferentes daqueles previstos no projeto original. Isso acontece porque o Brasil não possui um sistema nacional para a identificação civil e o documento de identificação, o RG, possui problemas.

O Registro Geral (RG), ou carteira de identidade, é um documento utilizado para a identificação de pessoas físicas nascidas no Brasil e tem validade nacional [9]. Contudo, existem alguns problemas associados a este documento:

- Cada unidade federativa é responsável por emitir uma carteira de identidade diferente, sem nenhuma ligação entre si. E, como são 27 unidades federativas, cada cidadão brasileiro pode ter 27 RGs diferentes.
- Os dados que constam no documento variam de acordo com o órgão responsável pela emissão, ou seja, existe uma falta de padrão no documento ao longo do tempo.

Existem outros documentos que são usados para identificar uma pessoa física, como a Certidão de Nascimento, o Título de Eleitor, a Carteira de Habilitação (CNH) e o Registro Nacional de Estrangeiro (RNE) (usado por estrangeiros). Toda essa informação espalhada entre as instituições torna o processo de identificação ainda mais complexo e passível de vulnerabilidades. E, além dos documentos já existentes, surgiram propostas de criação de outro documento usado especificamente para a identificação como:

- **Registro Civil Único (RCU)** [11]
- **Registro de Identificação Civil (RIC):** surgiu em 1997 [12] e regulamentada 13 anos depois, em 2010 [14].
- **Registro Civil Nacional (RCN)** [15].
- **Identificação Civil Nacional (ICN)** [16].
- **Documento Nacional de Identificação (DNI)** [17, 51].
- **Biometria** como alternativa a documentos físicos [18].

Surgiram novas propostas por décadas e, mesmo assim, nenhuma realmente resolveu os problemas. Primeiro que as propostas demoram muito para saírem do papel, como é possível notar no projeto do RIC (Registro de Identificação Civil) que demorou 13 anos para ser regulamentado e ainda não há mais informações sobre o projeto. Segundo que, conforme são criados documentos, adiciona-se complexidade no sistema e, potencialmente, novas vulnerabilidades que podem permitir ainda mais fraudes. Com isso, podem ser enumerados os problemas do sistema de identificação civil no Brasil atualmente:

- **Falta de padrão:** não há documento e informações padronizadas para identificar civis. O que há é muitas informações diferentes dispersas em diferentes instituições públicas, como o Título de Eleitor, CNH, CPF etc.
- **Falta de centralização:** não há uma instituição pública responsável pela centralização dos processos e dos dados para a identificação de civis.
- **Problemas de projeto:** o documento destinado a identificar cidadãos (RG) possui falhas, como foi enumerado acima.
- **Soluções improvisadas e temporárias:** por causa dos problemas na identificação, o CPF acaba sendo uma alternativa para identificar os cidadãos, dado esse que pode ser prejudicial nas mãos de criminosos. Há também muitos projetos para resolver esse problema, mas que nunca saem do papel.
- **Sistema complexo:** a falta de centralização nos dados e processos e de padrões torna a tarefa de identificar pessoas difícil e ineficiente.

- **Burocracia:** as propostas para solucionar problemas de interesse público demoram muito por conta da burocracia envolvida, como exemplificado pela proposta do RIC, que nunca saiu do papel desde 1995.

Todos esses problemas geram consequências sérias como fraudes, inconsistência de dados e vazamentos de dados pessoais [48] como foi exemplificado pelas fraudes envolvendo o Auxílio Emergencial.

1.3 – OBJETIVO GERAL

Este trabalho tem como objetivo geral projetar, desenvolver e implementar um sistema de informações que permita a identificação e a autenticação das pessoas de forma a evitar fraudes, vazamentos de dados e inconsistência dos dados, além de criar um cenário de eleição digital em que o sistema desenvolvido é utilizado, de forma a substituir o CPF dado como identificador e autenticador de cidadãos brasileiros.

1.4 – OBJETIVOS ESPECÍFICOS

O objetivo deste trabalho consiste em emitir carteiras digitais, implementar um mecanismo de identificação e autenticação com a carteira digital e demonstrar como ele funcionaria em um cenário hipotético de eleições digitais.

As carteiras digitais emitidas são compostas de uma chave privada protegida por uma senha de quatro dígitos (PIN), escolhido pelo proprietário da carteira neste caso, e seu respectivo certificado digital, dados pessoais (nome completo, CPF, sexo, foto, filiação e naturalidade), registro do local, data de emissão e data de validade da carteira digital. Por sua vez, o mecanismo de identificação e autenticação com a carteira digital consiste em certificado digital para a identificação e a assinatura digital para autenticação.

Com os objetivos acima concluídos, serão construídas duas aplicações (uma para o eleitor e outra para o TSE) para simular um cenário de eleições digitais, utilizando a carteira digital que foi criada.

2 – REVISÃO BIBLIOGRÁFICA

2.1 – IDENTIFICAÇÃO

A **identificação** é um processo essencial para a sociedade, porque garante a unicidade de um indivíduo e permite a prestação de contas (ou responsabilização), estabelecimento de confiança entre indivíduos e instituições (públicas ou privadas) e o estabelecimento de uma relação entre o indivíduo e as informações relacionadas a ele, e tudo isso sem ambiguidade.

O processo de identificação é usado em vários setores da sociedade, por exemplo: a identificação de pessoas é usada por empresas para garantir que as informações passadas pelos consumidores sejam válidas, para que possam permitir às empresas prover seus serviços e gerenciar eficientemente seus negócios.

A identificação analisada neste trabalho é a **identificação de cidadãos** de uma nação ou território, cujo principal responsável são instituições públicas. A identificação de cidadãos em diversos países é feita por meio dos documentos de identidade, que podem valer para todo o território do país ou não, e podem ser compulsórios ou não compulsórios.

O objetivo da identificação civil é relacionar um indivíduo com informações associadas a ele. Os usos, formatos e políticas, entretanto, variam no espaço e no tempo, por exemplo: no século XIX, a migração de pessoas na França era monitorada pela polícia pelo uso de passaportes internos [21], e no ano de 1938, na Alemanha nazista, os judeus foram obrigados a usar um documento de identidade para fortalecer a opressão do governo sobre eles [3].

Além dos usos citados anteriormente, o **processo de identificação se tornou essencial no meio digital** por causa dos primeiros sistemas computacionais no começo do século XX. Um dos principais mecanismos de controle de acesso, o ACL (*Access-Control List*), por exemplo, foi implementado pela primeira vez em 1965 [53] como parte do sistema de arquivos Multics. Esse e outros mecanismos tiveram influência na identidade digital porque trouxe a estrutura popular nomes de usuários e senhas, que permite uma entidade gerenciar os acessos e permissões dos usuários do sistema.

Outra forma de identificação em meios digitais surgiu na década de 1980, com o conjunto de protocolos TCP/IP. Os protocolos TCP/IP são a base da Internet atualmente e são responsáveis por atribuir endereços aos hosts da rede. Em outras palavras, o TCP/IP é uma forma de identificar os hosts da Internet.

2.2 – CRIPTOGRAFIA DE CHAVE PÚBLICA

É no período da criação dos protocolos TCP/IP (décadas de 1970 e 1980) que a criptografia se populariza como forma de garantir a confidencialidade, integridade e autenticidade das informações que passam pela Internet. A criptografia é o estudo e a prática de técnicas para a comunicação segura na presença de adversários [36]. Já o processo de criptografar, de acordo com o dicionário de Oxford e de Cambridge, é, em resumo, o processo de converter dados em um código secreto, especialmente para prevenir o acesso não autorizado aos dados.

Na década de 1970, dois grupos independentes de cientistas inventaram o conceito de **criptografia de chave pública**. O primeiro grupo a inventar o conceito de criptografia de chave pública era formado pelos cientistas britânicos James H. Ellis, Clifford Cocks e Malcolm J. Williamson, membros do Quartel-General de Comunicações do Governo britânico (GCHQ). Em 1970, Ellis idealizou a possibilidade de um sistema de criptografia não secreta, mas não viu um jeito de implementá-la. Em 1973, Cocks, colega de Ellis, criou um método prático para implementar o “sistema de criptografia não secreta” do amigo. Em 1974, Williamson criou um método de troca de chaves, que hoje é conhecido como troca de chaves Diffie-Hellman [25, 28] (Fig. 1). Entretanto, o trabalho do grupo ficou em segredo até 1997, quando o governo britânico liberou as descobertas [42].

Figura 1 – Troca de Chaves Diffie-Hellman



Fonte: Kauan Manzato do Nascimento, 2022.

A descoberta pública foi feita por cientistas norte-americanos, nos anos 1976 e 1977. Em 1976, Whitfield Diffie e Martin Hellman, influenciados pelo trabalho de Ralph Merkle sobre distribuição de chaves, inventaram um método de troca de chaves usando um conceito matemático chamado campo finito. Em 1977, Ron Rivest, Adi Shamir e Leonard Adleman inventaram o algoritmo RSA de criptografia de chave pública, publicado em 1978 [2] e que foi o estopim para a criação de muitos outros esquemas criptográficos semelhantes. No artigo publicado, também é descrito o conceito de assinatura digital, que será usado mais para frente no trabalho.

De forma simplificada, a criptografia de chave pública funciona da seguinte forma: há dois tipos de chave, uma chave pública e uma chave privada (ou secreta). O emissor da mensagem usa a chave pública do destinatário para criptografar a mensagem, que apenas a chave privada pode descriptografar, sendo esta última em posse do destinatário. Em outras palavras, apenas o destinatário pode descriptografar a mensagem (Fig. 2). Assim, é garantida a confidencialidade da mensagem.

Figura 2 – Funcionamento da Criptografia de Chave Pública



Fonte: Kauan Manzato do Nascimento, 2022

2.2.1 – CRIPTOGRAFIA DE CURVAS ELÍPTICAS (ECC)

Dentre os vários tipos de criptografia de chave pública, o tipo usado neste trabalho é a criptografia de curvas elípticas, que é usada atualmente no sistema de identidade digital da Estônia [40]. Pelo fato de a ECC ser relativamente rápida e não precisar de chaves tão grandes

quanto o sistema RSA, por exemplo, ela foi escolhida para servir de base para a solução deste trabalho. Porém, como será discutido mais à frente, a ECC possui a desvantagem de não possuir um algoritmo próprio para criptografar e descriptografar dados, problema que foi contornado usando uma técnica chamada de ECDH.

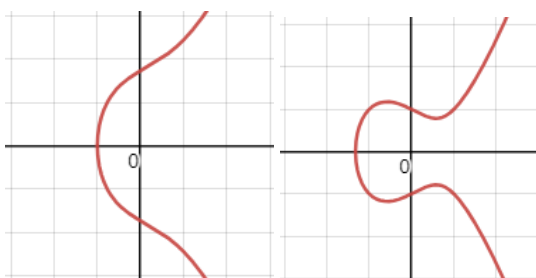
A criptografia de chave pública de curvas elípticas é baseada em um conceito matemático chamado de curva elíptica, por isso o nome. Em síntese, uma curva elíptica é um conjunto de pontos que satisfaz a seguinte equação:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{R}$$

Os parâmetros a, b e o campo finito usado definem diferentes curvas (Fig. 3), com diferentes características e propriedades. Os pontos pertencentes às curvas e certas operações permitem criptografar e descriptografar informações.

Como a explicação técnica está fora do escopo, esta explicação irá se limitar ao fato que já há curvas bem conhecidas e usadas, como descrito pela *Internet Assigned Numbers Authority* [34]. São alguns exemplos de curvas: secp384r1, brainpoolP512r1 e x25519. Neste trabalho, foi usada a curva NIST P-384 (secp384r1), definida no FISP 186-4, padrão usado pelo NIST, Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, que também é a curva usada pela Estônia [24].

Figura 3 – Exemplos de curvas elípticas com diferentes parâmetros a, b



Fonte: Kauan Manzato do Nascimento, 2022

2.2.2 SISTEMA CRIPTOGRÁFICO RSA

Além da já discutida criptografia de curvas elípticas, há também o sistema criptográfico RSA, já citado no trabalho, cuja segurança, diferentemente do ECC, se baseia na dificuldade de calcular os fatores de um número inteiro muito grande. O RSA, por ser o sistema mais simples e ter sido o primeiro a ser estudado, tem a vantagem da popularidade e da facilidade de

implementação. Entretanto, o RSA possui as desvantagens de ter um desempenho pior e chaves maiores. E, apesar de não ser empregado na solução, vale ser mencionado por ser outra opção viável para se trabalhar.

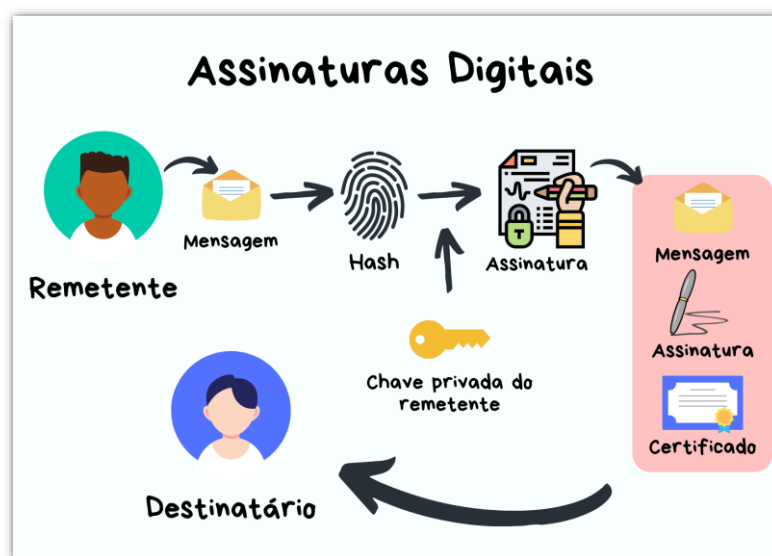
2.3 ASSINATURAS DIGITAIS

Para garantir a autenticação da identidade do emissor, a criptografia de chave pública permite a criação de **assinaturas digitais** por meio de chaves secretas. Como as chaves são secretas, elas não podem ser forjadas e quem assinou não pode negar a assinatura [2]. Portanto, as assinaturas garantem identificação e autenticação e, por isso, são parte essencial da solução proposta neste trabalho.

Criar uma assinatura digital é semelhante à operação de criptografia, mas há diferenças. Em vez de usar a chave pública do destinatário, o remetente usa sua própria chave privada para criar a assinatura. Ao enviar a mensagem, o remetente envia também a chave pública (que está dentro do certificado digital, discutido na próxima seção) e a assinatura, assim o destinatário consegue verificar a autenticidade e a integridade da mensagem e identificar o remetente.

De forma simplificada, a assinatura consiste em calcular o hash da mensagem e criptografar o resultado com a chave privada do remetente. Assim, a assinatura pode ser verificada com a chave pública do remetente. Este mecanismo é mostrado pela Figura 4.

Figura 4 – Assinaturas digitais

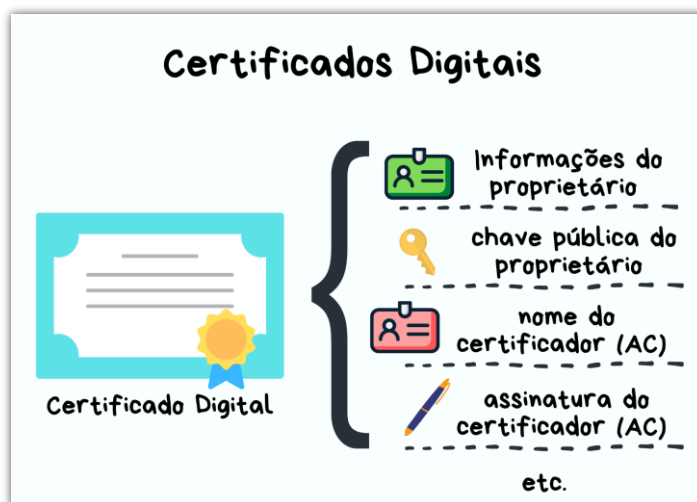


Fonte: Kauan Manzato do Nascimento, 2022

2.4 – CERTIFICADOS DIGITAIS

Em 1988, surge o **certificado digital** com a publicação da primeira versão do padrão X.509 [33]. Os certificados digitais são documentos eletrônicos usados para provar a identidade do proprietário de uma chave pública, e incluem as informações do proprietário, sua assinatura digital e sua chave pública (Fig. 5). Assim, o certificado digital permite a criação da infraestrutura de chave pública e auxilia na implementação da criptografia de chave pública [32], como será discutido mais à frente.

Figura 5 – Certificados digitais



Fonte: Kauan Manzato do Nascimento, 2022

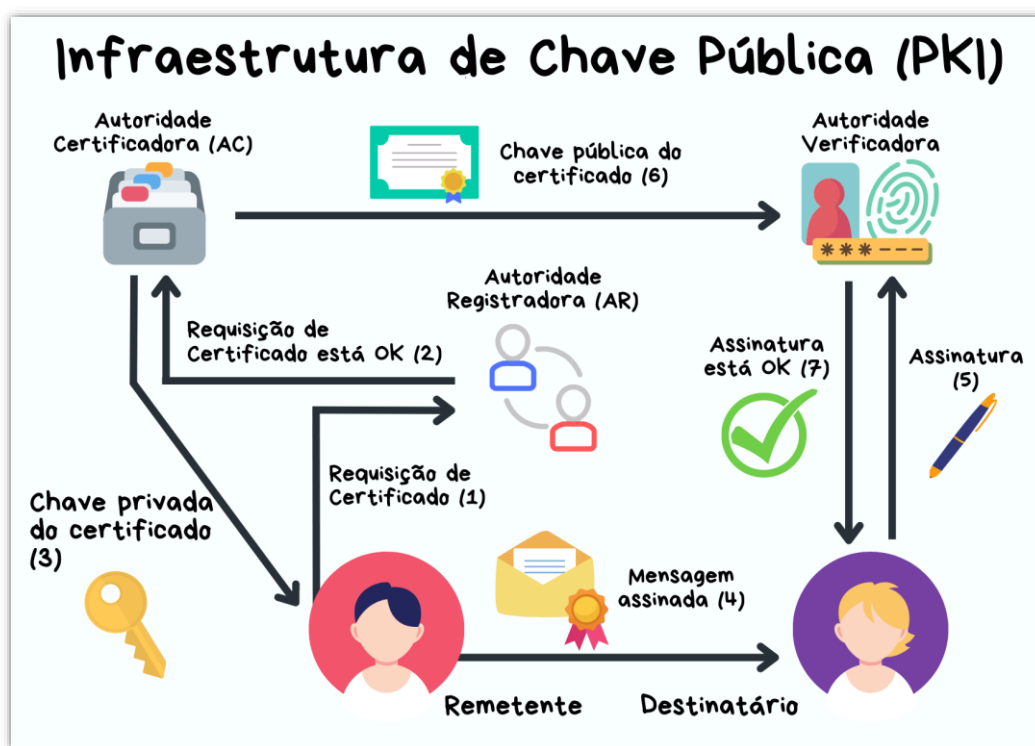
Na década de 1990, a popularização da Internet trouxe a necessidade de comunicações mais seguras, e foi assim que surgiu o protocolo SSL (Secure Sockets Layer). O SSL é um protocolo criptográfico publicado em 1995 na sua versão 2.0 [52], desenvolvido para garantir segurança das comunicações sobre redes de computadores, atuando na camada de aplicação e sendo usado principalmente no protocolo HTTPS, amplamente usado até os dias atuais na Internet.

Atualmente, o sucessor do SSL é o TLS, com sua versão mais recente sendo o TLS 1.3, publicado em 2018 [46]. O protocolo TLS/SSL usa certificados digitais e criptografia de chave pública: cliente e servidor trocam certificados digitais que permitem um cliente confiar em um servidor ou a confiança mútua entre ambos. Essa troca de certificados e chaves e autenticação é conhecido como *TLS handshake* e é o que garante a segurança do protocolo TLS, sendo uma aplicação popular de certificados digitais.

2.5 – INFRAESTRUTURA DE CHAVE PÚBLICA (PKI)

Ainda na década de 1990, com o crescimento do interesse por comunicações seguras pela Internet, surgiu o conceito de **infraestrutura de chave pública** (ou PKI) [56]. Uma infraestrutura de chave pública é um termo usado para se referir a um conjunto de hardware, software, políticas, procedimentos e processos usados para gerenciar certificados digitais e chaves para serem usados no esquema de criptografia de chave pública (Fig. 6).

Figura 6 – Funcionamento básico de uma Infraestrutura de Chave Pública (PKI)



Fonte: Kauan Manzato do Nascimento, 2022

Em 2001, foi instituído o órgão público no Brasil responsável pela certificação digital no país, chamado de **ICP-Brasil** (Infraestrutura de Chaves Públicas Brasileira [13]. O ICP-Brasil é uma estrutura hierárquica composta de várias Autoridades Certificadoras (AC), essas que são as entidades responsáveis por gerenciar e emitir certificados digitais. Uma dessas Autoridades Certificadora é a AC-Raiz (papel realizado pelo Instituto Nacional de Tecnologia da Informação), que credencia e audita as ACs do ICP-Brasil.

2.6 – IDENTIDADE DIGITAL

Em 2002, o governo da Estônia introduziu seu primeiro **documento de identidade digital** que usa criptografia de chave pública e certificados digitais para que os cidadãos estonianos se identifiquem e assinem digitalmente. O documento possui validade jurídica, assim como as assinaturas digitais criadas a partir das chaves do ID-card, como é chamado o documento. E é com base no projeto estoniano e seus resultados que este trabalho é desenvolvido. O documento é considerado um sucesso, já que 99% dos estonianos o possuem [30] e o documento é usado em várias atividades cotidianas dos cidadãos, como internet banking, assistência médica e até eleições (Fig. 7).

Figura 7 – carteira de identidade estoniana de 2021



Fonte: Estonian Police and Border Guard Board

Durante esses quase 20 anos de ID-card, o formato do documento e o chip dentro dele mudaram várias vezes. Entretanto, o funcionamento continuou basicamente o mesmo [40]: o ID-card tem duas chaves privadas com seus respectivos certificados digitais X.509, e chaves simétricas para operações usadas pela fabricante.

Além da Estônia, há outros países que também usam a identificação digital como, por exemplo:

- Bélgica [6]
- Cazaquistão [23]
- Holanda [31]
- Itália [35]
- Espanha [27] etc.

3 – SOLUÇÃO PROPOSTA

Conforme escrito anteriormente, a solução proposta é um cartão inteligente baseado no modelo estoniano, adaptando algumas características ao contexto brasileiro, e que serve como uma fonte de **autenticação** (chave de autenticação e certificado digital), **identificação** (informações pessoais gravadas digital e fisicamente. e certificado digital) e **confidencialidade** (funções criptográficas), a fim de criar uma alternativa às soluções atuais no Brasil.

3.1 – FERRAMENTAS

Para o desenvolvimento da solução deste trabalho, foi usada a biblioteca de funções criptográficas **cryptography** para Python, que inclui interface a diversos algoritmos, cifras simétricas e assimétricas, funções para gerar chaves e *message digests*, como o SHA-3.

A biblioteca **cryptography**, por sua vez, é baseada na biblioteca OpenSSL. O OpenSSL é uma biblioteca de código aberto² escrita em C e que implementa duas bibliotecas: biblioteca de criptografia, que provê funções criptográficas como AES, RSA, SHA-3 etc., e a biblioteca TLS/SSL que implementa o protocolo TLS (SSL, TLS 1.2, TLS 1.3, DTLS etc.). O OpenSSL possui algumas alternativas, como o LibreSSL, BoringSSL e Google Tink, todos de código aberto, baseados no OpenSSL e que têm como objetivo resolver alguns problemas do OpenSSL, mas que são menos populares.

O Python está sendo usado porque permite prototipagem rápida, por ser uma linguagem de programação interpretada e ter uma sintaxe com um nível mais alto que outras linguagens, como por exemplo C ou Java. E, por fim, para criação e execução do código, foi usado o IDLE (*Integrated Development and Learning Environment*), um ambiente de desenvolvimento integrado ao Python e que possui interface gráfica.

3.2 – FUNCIONALIDADES

As funcionalidades inclusas na carteira de identidade digital são duas chaves assimétricas (ECC) com seus respectivos certificados X.509 de chave pública correspondentes,

² O código-fonte do OpenSSL está disponível em <https://github.com/openssl/openssl>.

além da chave simétrica para a realização de operações de manutenção no cartão e informações pessoais.

Chave de autenticação: uma das chaves privadas é a chave de autenticação. Essa chave é usada para se autenticar em serviços on-line ao providenciar uma assinatura digital no processo de autenticação do certificado TLS do cliente. A chave também permite descriptografar arquivos que foram criptografados para o proprietário do cartão, o que não é muito usado, já que estes arquivos ficariam ilegíveis caso o cartão fosse perdido ou destruído.

Chave de assinatura digital: a outra chave privada é a chave de assinatura digital. Essa chave é usada para vincular assinaturas digitais que, no modelo estoniano e sobre a regulamentação europeia eIDAS, são reconhecidas como assinaturas válidas.

Chave simétrica: as chaves de criptografia simétrica são pré-carregadas no cartão para que o fabricante possa realizar algumas operações depois da emissão do cartão, como resetar os códigos PIN, gerar novas chaves e escrever novos certificados.

Informações pessoais: no modelo estoniano, o chip do cartão também contém exatamente as mesmas informações que estão impressas no cartão, incluindo o número de identificação pessoal, chamado PIC, equivalente ao nosso número do RG ou CPF [29].

3.3 – EMISSÃO DA CARTEIRA DE IDENTIDADE

A carteira de identidade, portanto, seria um cartão inteligente com informações pessoais gravadas fisicamente no cartão, como nome e data de nascimento, e digitalmente no chip, além dos pares de chave e certificado. Por ora, por motivos de simplicidade e didática, a emissão da carteira se limitará a emitir as informações digitais da carteira, no caso, o nome do proprietário, e um par de chave privada e certificado digital, sendo este último auto-assinado.

Com relação às informações pessoais, como elas estão visíveis fisicamente no cartão, elas podem ser gravadas sem criptografia no cartão para a leitura fácil. Além disso, como essas informações são basicamente texto, o tamanho total dos arquivos não passa de 1 kB.

As chaves privadas armazenadas são protegidas, cada uma protegida por um PIN de 4 dígitos diferente. A chave privada é uma chave privada de criptografia de curva elíptica (NIST P-384) de 384 bits e criptografada, e seu tamanho é de apenas 379 bytes. Cada chave é gerada usando a biblioteca `cryptography` para Python e salva no formato PEM (*Privacy Enhanced Mail*).

Por fim, os certificados digitais estão no padrão X.509 e são criados a partir do par das chaves pública e privada. Ele contém as informações do emissor, do proprietário e da chave pública do proprietário, data de validade, número de série e outras informações.

Em aplicações reais, os certificados digitais são emitidos por entidades chamadas Autoridades Certificadoras (ACs) e possuem uma cadeia de confiança para serem válidos. Por exemplo: o certificado de um brasileiro é emitido por um cartório que, por sua vez, possui um certificado digital emitido pelo ICP-Brasil. Essa cadeia permite o seguinte: se houver confiança no ICP-Brasil, então é possível confiar no cartório e, por consequência, confiar no certificado digital da pessoa. Para simplificar o projeto, porém, a cadeia de confiança será desconsiderada e serão gerados certificados auto assinados.

3.3.1 – CÓDIGO DA EMISSÃO DA CARTEIRA DE IDENTIDADE

A emissão da carteira digital, neste trabalho, consiste um pequeno programa escrito em Python que recebe algumas informações e emite os dados da carteira, incluindo principalmente a chave privada e o certificado digital, cujo código será analisado a seguir. Em uma aplicação real, este programa poderia ser executado em um cartório, por exemplo, uma instituição oficial que poderia emitir a carteira de identidade.

Primeiramente, é pedido ao usuário o nome do proprietário (função `set_owner_name`) e, depois, o nome da autoridade certificadora que vai emitir a carteira de identidade (função `set_issuer_name`). Segundo, é definido o PIN, que é escolhido pelo proprietário da carteira neste caso, e que protegerá a chave privada, utilizando a função `set_pin` (Fig. 8). Nesta função, é usado o conceito de expressão regular para validar a entrada do usuário.

Figura 8 – Definição da função `set_pin`

```
def set_pin():
    while(True):
        pin = input('\nEscreva um PIN de 4 dígitos para proteger sua chave privada:\n')
        if re.match(r"^\d{4}$", pin):
            return pin.encode()
        else:
            print('\nPIN inválido.')
```

Fonte: Kauan Manzato do Nascimento, 2022.

Então, a chave privada é gerada com a função `gen_key` que usa a função `generate_private_key` da biblioteca `cryptography`, usando a curva NIST P-384 (Fig. 9).

Figura 9 – Definição da função `gen_key`

```
def gen_key():  
    return ec.generate_private_key (  
        ec.SECP384R1()  
    )
```

Fonte: Kauan Manzato do Nascimento, 2022.

Depois, a partir da chave privada, a chave pública é extraída usando o método `public_key` das chaves privadas. Em seguida, o certificado digital é gerado com a função `gen_cert`, tendo como parâmetros o nome do proprietário, nome do emissor e a chave privada. Esta função define os parâmetros do certificado como o nome do proprietário, o nome do emissor, a chave pública, número serial etc. (Fig. 10).

Figura 10 – Definição da função `gen_cert`

```
def gen_cert(owner_name, issuer_name, private_key):  
    name_attribute_owner = x509.Name([x509.NameAttribute(NameOID.COMMON_NAME, owner_name)])  
    name_attribute_issuer = x509.Name([x509.NameAttribute(NameOID.COMMON_NAME, issuer_name)])  
    now = datetime.utcnow()  
  
    cert = (  
        x509.CertificateBuilder()  
        .subject_name(name_attribute_owner)  
        .issuer_name(name_attribute_issuer)  
        .public_key(private_key.public_key())  
        .serial_number(1000)  
        .not_valid_before(now)  
        .not_valid_after (now+timedelta(days=10*365))  
        .add_extension(x509.BasicConstraints(ca=True, path_length=0), False)  
        .sign(private_key, hashes.SHA384(), default_backend())  
    )  
  
    return cert
```

Fonte: Kauan Manzato do Nascimento, 2022.

Depois, aplicação codifica a chave privada e o certificado no formato PEM, além de criptografar a chave privada com o PIN escolhido (Fig. 11). E, por fim, o certificado e a chave privada protegida são salvos junto com as informações pessoais com a função `save_file` (Fig. 12), finalizando a simulação da emissão da carteira de identidade. Vale ressaltar que é usado apenas o nome do proprietário da carteira como informação pessoal digital para simplificar a solução, como dito anteriormente. O código da aplicação pode ser encontrado no repositório do projeto no GitHub.

Figura 11 – Conversão da chave privada e do certificado para o formato PEM

```
cert_pem = cert.public_bytes(encoding=serialization.Encoding.PEM)
private_key_pem = private_key.private_bytes(
    encoding = serialization.Encoding.PEM,
    format = serialization.PrivateFormat.TraditionalOpenSSL,
    encryption_algorithm = serialization.BestAvailableEncryption(pin)
)
```

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 12 – Definição da função `save_file`

```
def save_file(path, data):
    with open(path, 'wb') as file:
        file.write(data)
```

Fonte: Kauan Manzato do Nascimento, 2022.

3.3.2 DEMONSTRAÇÃO DO CÓDIGO

O código escrito para a emissão da carteira digital pode ser executado com qualquer interpretador de Python e consiste em um programa sem interface gráfica que, apesar de deixar o programa mais intuitivo, tornaria o projeto mais complexo sem contribuir com a proposta do trabalho, pois um programa em linha de comando é o suficiente para demonstrar a aplicação de forma satisfatória. Para executar a aplicação será usado o terminal do Windows (Fig. 13).

O programa recebe como entrada as informações pessoais, no caso o nome do proprietário da carteira de identidade, a identidade do emissor da carteira e o PIN que vai proteger a chave privada. Cada etapa do processo é impressa na tela até o fim (Fig. 14). Como resultado os arquivos são salvos na pasta `./files` (Fig. 15).

Figura 13 – Execução do programa de emissão da carteira de identidade

```
PS D:\UFABC\PGC FINAL\Código\carteira digital> python .\emissao.py
*****
*                               *
*  EMISSÃO DA CARTEIRA DE IDENTIDADE DIGITAL  *
*                               *
*****

Qual é o seu nome?
Kauan Manzato do Nascimento

Identificação do emissor da carteira de identidade:
Cartorio de Santo Andre

Escreva um PIN de 4 dígitos para proteger sua chave privada:
3011

Gerando chave privada...
Chave gerada com sucesso!
Gerando certificado...
Certificado gerado com sucesso!
Salvando informações usando a codificação PEM...
Arquivos salvos com sucesso.
```

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 14 – Execução do programa de emissão da carteira de identidade




```
PS D:\UFABC\PGC FINAL\Código\carteira digital> dir .\files\

Diretório: D:\UFABC\PGC FINAL\Código\carteira digital\files

Mode                LastWriteTime         Length Name
----                -
-a----             27/04/2022   12:51           595 certificado.pem
-a----             27/04/2022   12:51           379 chave.pem
-a----             27/04/2022   12:51           27 nome
```

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 15 – Arquivos criados pelo programa

Nome	Data de modificação	Tipo	Tamanho
 certificado.pem	27/04/2022 12:51	Privacy Enhanced Mail	1 KB
 chave.pem	27/04/2022 12:51	Privacy Enhanced Mail	1 KB
 nome	27/04/2022 12:51	Arquivo	1 KB

Fonte: Kauan Manzato do Nascimento, 2022.

Para mostrar o conteúdo do certificado e da chave privada de forma amigável, pode-se usar a própria biblioteca OpenSSL (Fig. 17, 18). Já as informações pessoais são arquivos codificados em UTF-8 e podem ser imprimidas no terminal usando `cat` (Fig. 16).

Figura 16 – Conteúdo do arquivo **nome**

```
PS D:\UFABC\PGC FINAL\Código\carteira digital\files> cat nome
Kauan Manzato do Nascimento
```

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 17 – Conteúdo da chave privada **chave.pem**

```
PS D:\UFABC\PGC FINAL\Código\carteira digital\files> openssl ec -in .\chave.pem
read EC key
Enter PEM pass phrase:
writing EC key
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDC6sEn0T0LWnhMVPjIbUgkVjVpL7zk60oZLAejbidzH3X2Pr8F+V7pj
xt86eb96NIigBwYFK4EEACKhZANiAAT5vcNbD507KYc4TVy1FbROInCmruecFQke
jDkSEpf+gu3Q4yq0tBFfJ2UxcY9Tp8uPCJIE0E98abNHwTsS906Slk/0hLGPuKY
vZX8VN6GK0thR6S3ZzJCPFPDX6A7QI=
-----END EC PRIVATE KEY-----
```

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 18 – Conteúdo do certificado digital

```
PS D:\UFABC\PGC FINAL\Código\carteira digital\files> openssl x509 -in .\certificado.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1000 (0x3e8)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: CN = Cartorio de Santo Andre
        Validity
            Not Before: Apr 27 15:59:39 2022 GMT
            Not After : Apr 24 15:59:39 2032 GMT
        Subject: CN = Kauan Manzato do Nascimento
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (384 bit)
            pub:
                04:f9:bd:c3:5b:0f:9d:3b:29:87:38:4d:5c:b5:15:
                b4:4e:22:70:a6:ae:e7:9c:15:09:1e:8c:39:12:12:
                97:fe:82:ed:d0:e3:2a:b4:3a:d0:45:7c:9d:94:c5:
                c6:3d:4e:9f:2e:3c:22:48:78:e1:3d:f1:a6:cd:1f:
                04:ec:4b:dd:3a:4a:59:3f:d2:12:c6:a5:42:b2:bd:
                95:fc:54:de:86:28:eb:61:47:a4:b7:67:32:42:3c:
                53:d1:0d:7e:80:ed:02
            ASN1 OID: secp384r1
            NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE, pathlen:0
        Signature Algorithm: ecdsa-with-SHA384
            30:66:02:31:00:81:a1:98:82:da:f9:2d:3d:33:be:2f:8c:a0:
            e3:b6:10:24:35:04:02:b0:98:78:95:19:20:79:8c:56:73:16:
            5f:11:0f:76:8a:3e:a8:a4:12:cd:0f:aa:cf:34:c2:3e:b0:02:
            31:00:cc:3f:6e:c2:7a:0b:43:f2:db:ea:69:a3:b0:2b:34:ac:
            c8:e0:02:18:dc:1d:33:1d:e5:d0:06:9a:9d:53:dd:93:f7:1a:
            84:41:a4:ea:0e:8c:5f:31:b6:7a:7d:a4:26:3b
    -----BEGIN CERTIFICATE-----
    MIIBiTCCAQ6gAwIBAgICA+gwCgYIKoZIzj0EAwMwIjEgMB4GA1UEAwwXQ2FydG9y
    aW8gZGUgU2FudG8gQW5kcmUwHhcNMjIwNDI3MTU1OTM5MzIwNDI3MTU1OTM5
    WjAmMSQwIlgYDQDDbTLXVhb1BNYV56YXRvIGRvIE5hc2NpbWVudG8wdjAQBgcq
    hkjOPQIBBgUrgQQAIGNiAAT5vcNbD507KYc4TVy1FbROInCmruecFQkejDkSEpf+
    gu3Q4yq0tBFfJ2UxcY9Tp8uPCJIE0E98abNHwTsS906Slk/0hLGPuKYvZX8VN6G
    K0thR6S3ZzJCPFPDX6A7QKjEzARMA8GA1UDwQIMAYBAf8CAQAwCgYIKoZIzj0E
    AwMDAQAwZgIxAIghmILa+S09M74vJKDjthAKNQCsJh4LRkgeYxWcxZFEQ92ij6o
    pBLND6rPNMI+sAIxAMw/bsJ6C0Py2+ppo7ArNKzI4AIY3B0zHexQBpqdU92T9xQE
    QaTqDoxfMbZ6faQm0w==
    -----END CERTIFICATE-----
```

Fonte: Kauan Manzato do Nascimento, 2022.

3.4 – AUTENTICAÇÃO

De acordo com o *National Institute of Standards and Technology* (NIST, Instituto Nacional de Padrões e Tecnologia dos Estados Unidos), a autenticação é o processo de verificar a identidade de um usuário, processo ou dispositivo, geralmente como pré-requisito para permitir o acesso a diferentes recursos dentro de um sistema de informação.

O caso de uso mais popular para a chave de autenticação da carteira de identidade estoniana, cuja solução proposta neste trabalho é baseada, é a autenticação em serviços Web pela Internet usando o protocolo TLS. Outros usos menos comuns para autenticação da identidade digital incluem assinatura de e-mails com S/MIME, autenticação SSH e VPN, e login em estações de trabalho [40]. O S/MIME (Secure/Multipurpose Internet Mail Extensions) é um padrão que permite criptografar e-mails [47]; a VPN (Virtual Private Network) é uma rede de computadores lógica que usa recursos de uma rede física, geralmente usando criptografia e tunelamento [1]; e o SSH (Secure Shell) é um protocolo que permite operar serviços de uma rede insegura de uma forma segura [44].

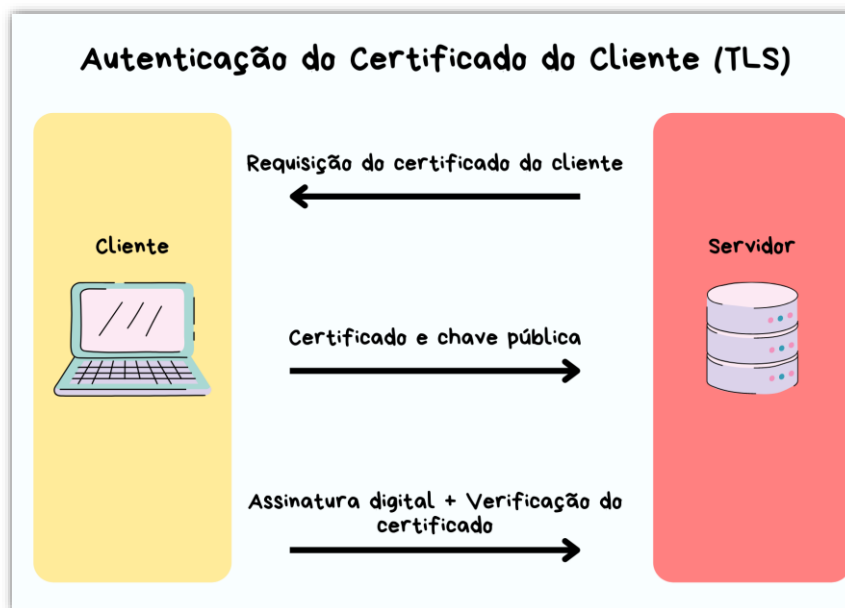
Hoje, há planos em desenvolvimento para introduzir um novo método de autenticação para as carteiras de identidade digital por meio da autenticação a nível de aplicação usando uma extensão no navegador que assina um desafio com a chave de autenticação, de código aberto e disponível no GitHub³, chamado de Web eID.

3.4.1 – AUTENTICAÇÃO DO CERTIFICADO DO CLIENTE TLS

O protocolo TLS inclui autenticação do certificado do cliente (CCA), o que é suportado pela maioria dos navegadores e servidores TLS. Este método pode ser usado pelos provedores de serviços para implementar a autenticação dos usuários com o ID card e garante a autenticação do cliente e a integridade dos dados. Durante o processo CCA, o cliente envia seu certificado de autenticação para o servidor e prova sua identidade com uma assinatura digital, conforme definido pela RFC 8446 [46] (Fig. 19).

³ O código-fonte do Web eID está disponível em: <https://github.com/web-eid/web-eid-system-architecture-doc>.

Figura 19 – Autenticação do Certificado do Cliente (TLS)



Fonte: Kauan Manzato do Nascimento, 2022.

3.5 – CRIPTOGRAFAR E DESCRIPTOGRAFAR

Um dos problemas da criptografia de curvas elípticas (ECC) é que não há formas práticas de criptografar e descriptografar dados como o sistema criptográfico RSA. Foram desenvolvidos três esquemas de ECC, mas cada uma com suas desvantagens, tornando-as impraticáveis. Por isso, a comunidade acadêmica abandonou esses esquemas e abraçou os sistemas híbridos de criptografia, onde curvas elípticas são usadas apenas para trocar chaves simétricas (e.g., troca de chaves com ECDH), sendo essas últimas as responsáveis por criptografar os dados [5]. Dentre os esquemas híbridos usados, o que está disponível em um maior número de padrões (ANSI X9.63, IEEE 1636rd, ISO/IEC 18033-2 e SECG SEC 1) é o ECIES (Elliptic Curve Integrated Encryption Scheme).

3.5.1 CRIPTOGRAFIA NESTE TRABALHO

Assim como na Estônia, a solução proposta neste trabalho faz uso do sistema híbrido de criptografia que combina o ECDH e a cifra simétrica AES-256 no modo GCM (Galois/Counter Mode). Primeiramente, o ECDH recebe a chave privada de quem está usando o algoritmo e a

chave pública para onde as informação irão e retorna a chave compartilhada (a entidade que vai receber as informações, o TSE neste caso, realiza a mesma operação) entre ambas as partes. Esta chave compartilhada derivada pelo ECDH é usada pela cifra AES-256, junto com o vetor inicial IV, um conjunto aleatório de 16 bytes, para criptografar os dados que serão enviados para o TSE, como o voto e a assinatura. O processo de decifrar as informações segue os mesmos passos: derivar a chave com ECDH e depois usá-la com a cifra AES-256 para decifrar as informações.

3.6 – ASSINAR E VALIDAR

Como dito anteriormente, a assinatura digital prova a identidade do proprietário da carteira de identidade digital (autenticação), porque apenas o proprietário da chave privada consegue gerar uma assinatura digital válida. Neste trabalho, a assinatura será criada da seguinte forma: a mensagem é recebida em bytes, seu hash é calculado com SHA-384 e, por fim, a assinatura é feita usando o algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm) com a chave privada do usuário.

Para verificar a assinatura, o ECDSA realiza uma série de cálculos para poder validar a assinatura [37, 45]. Resumidamente, quem está validando a assinatura usa as informações presentes na chave pública para validar. A verificação bem-sucedida da assinatura significa a autenticidade e a integridade da mensagem.

4 – TESTES

Para demonstrar o uso da carteira digital, foi construído um cenário de eleições digitais, onde a confidencialidade do voto deriva da criptografia de chave pública e a autenticidade é resultado da assinatura digital e a sua verificação. Os dados necessários do eleitor, como o certificado digital e a chave privada, foram emitidos previamente usando a aplicação de emissão da carteira de identidade.

4.1 – ELEIÇÕES NO BRASIL

As eleições no Brasil começam com o TSE (Tribunal Superior Eleitoral). O TSE é a autoridade jurídica máxima da Justiça Eleitoral brasileira. As demais instâncias da Justiça Eleitoral é composta pelos juízes e juntas eleitorais e pelos TREs (Tribunal Regional Eleitoral). Junto com os TREs, **o TSE é responsável pela gestão das eleições no Brasil** [10].

As eleições para Presidente da República, governadores, senadores e prefeitos seguem o sistema majoritário de votos: ganha o candidato que tiver a maior quantidade de votos [50]. Para deputados federais, deputados estaduais e vereadores, as eleições seguem o sistema proporcional: os votos não são computados para os candidatos, mas para seus partidos/coligações [49]. As eleições são divididas em fases [26, 39], sendo elas:

1. **Registro de candidatos:** cada partido ou coligação registra um candidato, seguindo alguns pré-requisitos.
2. **Cadastro de eleitores:** assim como os candidatos, os eleitores também precisam se registrar para poderem votar e receber o título de eleitor, um documento que prova a inscrição do eleitor.
3. **Logística eleitoral e preparação das eleições:** nesta fase ocorrem a manutenção e a verificação das peças essenciais da eleição, como transporte e distribuição das urnas, guarda e montagem das seções eleitorais, manutenção e testes das urnas etc.
4. **Votação:** é a etapa mais popular, que consiste na mobilização dos eleitores até as urnas para votarem em seus representantes.
5. **Prestação de contas:** os candidatos e os partidos prestam contas de acordo com a lei nº 9.504 de 1997 para garantir a transparência das eleições. Os candidatos eleitos cujas contas forem rejeitadas podem ser impedidos de tomarem posse de seus cargos.

6. **Totalização e divulgação dos resultados das eleições:** nesta parte, ocorre a contagem dos votos, descartando os votos nulos e brancos. Ela começa quando a votação é finalizada nas seções, então os boletins de urna são assinados e criptografados, para serem levados aos respectivos TREs (TSE no caso da eleição para Presidente da República).
7. **Diplomação dos candidatos eleitos:** por fim, depois dos resultados serem divulgados, a Justiça Eleitoral atesta a aptidão dos candidatos de assumirem seus cargos. O presidente do TSE assina e entrega o diploma, no caso do Presidente da República, e do TRE para os demais cargos.

Neste trabalho, a solução será demonstrada em um cenário de eleições digitais. Portanto, para uma demonstração simples, considera-se apenas a etapa de votação de uma eleição administrada pelo TSE. As outras etapas estão fora do escopo deste trabalho.

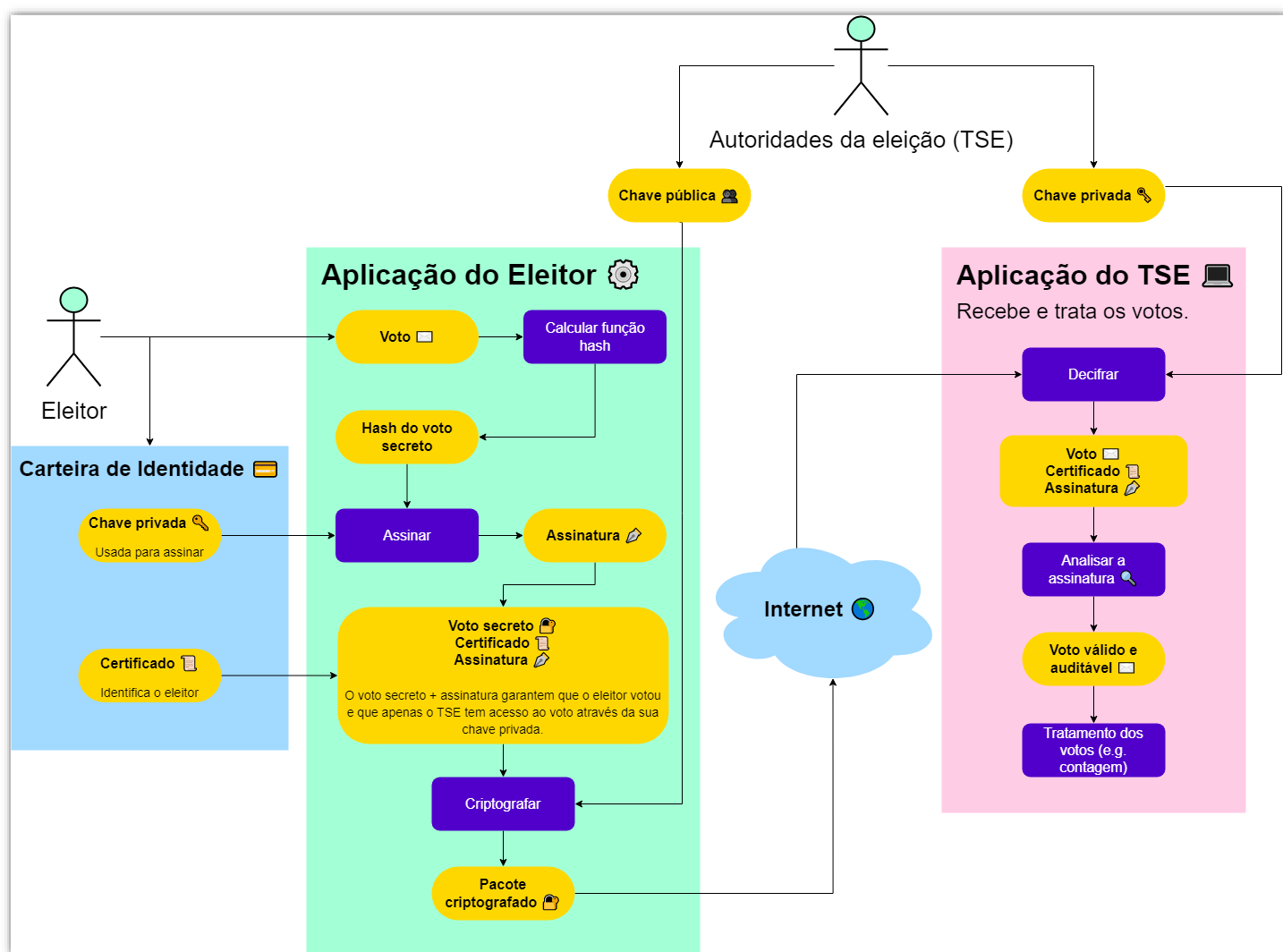
4.2 ELEIÇÕES DIGITAIS

Na eleição digital fictícia construída, o mecanismo de votação é composto de duas aplicações, uma para o eleitor e outra para o TSE. A aplicação do eleitor recebe o certificado digital, a assinatura digital e o voto do eleitor e criptografa e salva os dados para que a aplicação do TSE possa recebê-los. A aplicação do TSE coleta os dados, descriptografa os dados, valida a assinatura digital e retorna o voto. Este sistema é ilustrado pela Figura 20. O tratamento do voto, por estar fora do escopo, foi desconsiderado.

É importante notar que, como o TSE possui a assinatura do eleitor, sua chave pública e seu voto, o TSE pode relacionar cada voto ao seu respectivo eleitor. Em eleições reais, este fato configuraria uma vulnerabilidade, porém, como o cenário tem como objetivo principal a demonstração da aplicação da solução proposta e, como será explicado mais tarde, ainda é possível realizar outros tipos de eleições com o mesmo sistema, como eleições abertas, este ponto também foi desconsiderado.

A criptografia dos dados, logo, não protege os dados de todos (o TSE tem acesso aos dados), mas ainda se faz necessária, porque o voto é transmitido por um meio inseguro, como a Internet, e há a possibilidade de agentes maliciosos interferirem na comunicação. Assim, a criptografia protege os dados de fatores externos.

Figura 20 – Funcionamento das eleições digitais



Fonte: Kauan Manzato do Nascimento, 2022.

4.2.1 FUNÇÕES USADAS

As funções usadas nas aplicações das eleições digitais estão definidas no arquivo `functions.py`. Cada função e seu respectivo papel está listado abaixo de forma resumida.

Funções de certificado digital:

- `read_certificate`: recebe o caminho do arquivo, lê os bites salvos e carrega no formato adequado, que é o padrão X.509 para certificados digitais;
- `get_cert_subject`: recebe um certificado digital e extrai o nome do proprietário
- `get_cert_issuer`: recebe um certificado digital e extrai o nome do emissor

Funções da chave pública:

- `read_public_key`: recebe o caminho da chave pública e retorna o conteúdo no formato adequado.
- `read_public_key_x509`: recebe um certificado X.509 e retorna a sua chave pública.

Funções da chave privada:

- `load_private_key`: recebe o caminho da chave privada e permite três tentativas para inserir o PIN que protege a chave. Ao inserir o PIN, é chamada a função `get_private_key`. Caso o PIN esteja incorreto, a função pede uma nova entrada do PIN. Se o PIN estiver correto, a função retorna a chave privada. Depois de três tentativas, a função fecha a aplicação.
- `get_private_key`: função que auxilia a função `load_private_key` e que recebe o caminho da chave privada e o PIN. Caso o PIN esteja incorreto, retorna uma exceção, ou erro. Caso contrário, retorna a chave privada no formato adequado.

Funções de criptografia simétrica (AES):

- `aes_encrypt`: recebe as informações a serem criptografadas, a chave e o vetor inicial, e retorna as informações criptografadas, usando o algoritmo AES-256 no modo GCM.
- `aes_decrypt`: recebe as informações criptografadas, a chave e o vetor inicial, e retorna as informações decifradas, usando o algoritmo AES-256 no modo GCM.

Funções do algoritmo RSA:

- `rsa_encrypt`: recebe a chave e os dados a serem criptografados, e retorna os dados criptografados, usando o sistema criptográfico RSA.
- `rsa_decrypt`: recebe a chave e os dados criptografados, e retorna os dados decifrados, usando o sistema criptográfico RSA.

Funções de arquivos:

- `load_file`: recebe o caminho do arquivo e retorna o seu conteúdo em bytes, usando o modo binário `'wb'`.
- `save_file`: recebe os dados e o caminho do arquivo, e salva os dados no local indicado, usando o modo binário `'rb'`.

Função do ECDH:

- **derive_key**: recebe a chave privada da entidade que está chamando a função e a chave pública para a outra parte da comunicação, e retorna a chave derivada usando o algoritmo ECDH. A chave derivada pode ser usada para criptografar dados, permitindo a comunicação seguras entre duas entidades, sem que elas precisem trocar suas chaves privadas, assim como o protocolo Diffie-Hellman original.

Funções de assinatura digital:

- **sign**: recebe a chave privada de quem está assinado e os dados a serem assinados, e retorna a assinatura, gerada usando o algoritmo ECDSA e o hash SHA-384.
- **verify_signature**: recebe a assinatura, os dados que foram assinados e a chave pública de quem assinou, e retorna **True**, caso a assinatura seja válida, e **False**, caso contrário, usando o algoritmo ECDSA e o hash SHA-384.

Funções do voto:

- **set_vote**: recebe um inteiro do usuário, o voto, e retorna o voto codificado em bytes.
- **decode_vote**: recebe os bytes do voto e retorna o voto como um número inteiro.

O arquivo que possui as definições das funções compartilhadas está disponível junto às aplicações do eleitor, do TSE e da emissão da carteira de identidade no repositório do GitHub deste trabalho, permitindo que o código possa ser analisado pelo público, caso necessário.

4.2.2 – APLICAÇÃO DO ELEITOR

A aplicação do eleitor recebe e lê o certificado digital do eleitor, vindo da carteira de identidade proposta, com a função **read_certificate**. Depois, a aplicação carrega a chave privada usando a função **load_private_key** e o PIN de 4 dígitos que protege a chave, assim já garantindo a identificação e a autenticação do eleitor. A chave pública é extraída do certificado digital. As chaves públicas do TSE que serão usadas são carregadas com a função **read_public_key**. O eleitor, então, escolhe o voto (um número inteiro), por meio da função **set_vote**. Depois, uma assinatura digital é gerada com a função **sign** e é derivada uma chave compartilhada entre eleitor e TSE que será usada na comunicação segura entre ambas as partes,

usando a função `derive_key`. Os dados são criptografados com a função `aes_encrypt` e salvos localmente com a função `save_file`. Com isso, a identidade do eleitor e o voto estão autenticados e protegidos de entidades externas, prontos para serem processados pela aplicação do TSE, explicada na próxima seção.




4.2.3 – APLICAÇÃO DO TSE

A aplicação do TSE lê as informações da aplicação do eleitor, que inclui o certificado digital, a chave pública, a assinatura digital e o voto do eleitor, todos criptografados, por meio das funções `load_file` e `read_public_key`. Então a aplicação do TSE carrega as chaves privadas que permitem decifrar as informações recebidas usando a função `get_private_key`. Depois é derivada a chave compartilhada entre as duas aplicações usando a função `derive_key`, o que permite decifrar as informações recebidas com a função `aes_decrypt`. Por fim, a assinatura é verificada com a função `verify_signature`. Caso a assinatura seja válida, o voto é decifrado e processado. Caso contrário, o voto pode ser descartado.

4.2.4 DEMONSTRAÇÃO DAS ELEIÇÕES DIGITAIS





Antes de executar as aplicações, algumas informações precisaram ser criadas previamente para poderem ser usadas nas eleições. Dentre as informações criadas antes da execução, tem a carteira de identidade digital (Fig. 21), que foi criada usando o código de emissão de carteira digital e que estão dentro da pasta `./files/carteira`, e tem as chaves do TSE usadas (EC e RSA), que estão na pasta `./files/tse` (Fig. 22).

Figura 21 – Arquivos da carteira de identidade digital

Nome	Tipo	Tamanho
 certificado.pem	CMS (S/MIME) File	1 KB
 chave.pem	CMS (S/MIME) File	1 KB
 nome	Arquivo	1 KB

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 22 – Chaves usadas pelo TSE

Nome	Tipo	Tamanho
 ec_private_key.pem	CMS (S/MIME) File	1 KB
 ec_public_key.pem	CMS (S/MIME) File	1 KB
 rsa_private_key.pem	CMS (S/MIME) File	4 KB
 rsa_public_key.pem	CMS (S/MIME) File	1 KB

Fonte: Kauan Manzato do Nascimento, 2022.

Com tudo configurado, executa-se a aplicação do eleitor com algum interpretador de Python. Neste caso, o código foi executado usando o terminal do Windows, como mostrado na Figura 23.

Figura 23 – Execução da aplicação do eleitor (parte 1)

```
Carregando seu certificado digital...
Certificado carregado.

*****
*                               *
*  ELEIÇÕES 2042               *
*                               *
*****

Seja bem-vindo(a) às eleições digitais de 2042, Sr(a). Kauan Manzato do Nascimento

Para prosseguir com a votação, precisamos validar a sua identidade.
Insira seu PIN de 4 dígitos: 3011
```

Fonte: Kauan Manzato do Nascimento, 2022.

A aplicação lê o certificado digital do eleitor, dá as boas-vindas ao eleitor e pede o PIN para confirmar a identidade do indivíduo (Fig. 23). Com o PIN correto, a chave privada é carregada, junto com as chaves públicas do TSE, e então a aplicação pede para o usuário inserir o voto (Fig. 24).

Figura 24 – Execução da aplicação do eleitor (parte 2)

```
Escolha o seu voto: 123
Seu voto é 123

Criptografando seu voto...
O voto foi criptografado com sucesso.

Assinando seu voto...
Assinatura digital feita com sucesso.






Criando conexão segura com o TSE...
Criptografando os dados...
Enviando os dados...

Pronto. Seu voto foi enviado ao TSE. Agora é só esperar os resultados.
PS D:\UFABC\PGC FINAL\Código\eleições> |
```

Fonte: Kauan Manzato do Nascimento, 2022.

Com o voto escolhido, a aplicação criptografa o voto com RSA, cria a assinatura digital, criptografa tudo com auxílio do ECDH e salva os arquivos na pasta `./files/envio`, simulando o envio dos dados em um meio inseguro de comunicação (Fig. 25). Os dados com o prefixo `enc` são os dados criptografados, composto de bytes ilegíveis, já a `chave_publica_eleitor.pem` e o `iv` estão em texto plano.

Figura 25 – Arquivos criados pela aplicação do eleitor

Nome	Tipo	Tamanho
 chave_publica_eleitor.pem	CMS (S/MIME) File	1 KB
 enc_assinatura	Arquivo	1 KB
 enc_cert	Arquivo	1 KB
 enc_voto_secreto	Arquivo	1 KB
 iv	Arquivo	1 KB

Fonte: Kauan Manzato do Nascimento, 2022.

Agora, com os dados “enviados” ao TSE, executa-se a aplicação do TSE para tratar o voto, também usando o terminal do Windows (Fig. 26). Como não é necessário qualquer entrada de informações por parte do usuário, a aplicação executa sozinha até o final, conforme descrita anteriormente.

Figura 26 – Execução da aplicação do TSE

```
PS D:\UFABC\PGC FINAL\Código\eleições> python.exe .\tse.py
Bem-vindo Kauan Manzato do Nascimento
Sua carteira de identidade foi emitida por Cartorio de Santo Andre
Seu voto é válido e foi contabilizado!
Você votou em 123
PS D:\UFABC\PGC FINAL\Código\eleições> |
```

Fonte: Kauan Manzato do Nascimento, 2022.

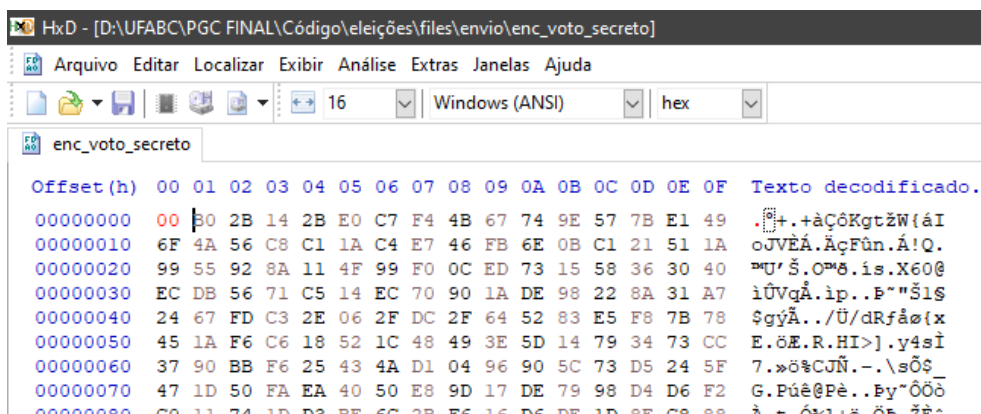
Caso algum byte dos dados enviados seja modificado indevidamente, as operações de decifrar os dados e validação da assinatura podem falhar. Por exemplo, ao modificar um único byte do voto secreto criptografado (*enc_voto_secreto*) (Fig. 27), a verificação da assinatura falha porque os dados assinados estão modificados (Fig. 28). Portanto, para que o voto seja contabilizado, é necessária uma combinação de autenticação, confidencialidade e integridade.

Figura 27 – Falha na verificação do certificado

```
PS D:\UFABC\PGC FINAL\Código\eleições> python.exe .\tse.py
Certificado inválido. Voto descartado.
```

Fonte: Kauan Manzato do Nascimento, 2022.

Figura 28 – Modificação do primeiro byte do voto secreto, usando o programa HxD



Fonte: Kauan Manzato do Nascimento, 2022.

As aplicações das eleições digitais permitem autenticar a identidade do eleitor através da assinatura e do certificado digital e garante a comunicação segura com o TSE por meio da criptografia de chave pública. Como pode ser observado pelas aplicações, trabalhar com assinaturas e certificados digitais e criptografia é relativamente simples porque existem bibliotecas que escondem as complexidades dos algoritmos usados, permitindo a construção de

soluções seguras com pouco esforço. E, como as técnicas usadas pela solução são padronizadas e usadas há décadas no mundo inteiro, a solução se torna mais transparente e confiável.

4.3 OUTRAS APLICAÇÕES

O cenário usado para demonstrar a solução proposta consiste nas eleições políticas administradas pelo TSE, que possuem uma influência indescritível nos rumos da democracia brasileira. Assim, este cenário foi um exemplo extremo de aplicação, inclusive contendo observações e ressalvas. Porém, existem algumas aplicações cuja solução proposta e o sistema de eleições proposto atendem às necessidades.

Para a carteira de identidade digital, as aplicações incluem, mas não são limitadas a: assinatura e criptografia de documentos, autenticação em serviços Web, como Internet Banking, passaporte, transporte público, eleições, saúde (associando a identidade a registros médicos) etc.

Por sua vez, as aplicações das eleições podem não ser ideais para a eleição do presidente de um país com mais de 200 milhões de habitantes, mas pode servir para as eleições de um representante de turma ou de um síndico de condomínio, por exemplo, porque não possuem requisitos muito exigentes de confidencialidade e integridade.

5 – CONCLUSÃO

Este trabalho revisou a bibliografia a fim de discutir os conceitos que são a base para o desenvolvimento da solução proposta, foram dadas as causas do problema de autenticação da identidade no Brasil e as consequências, os quais justificam a criação da solução proposta, e foi criado um cenário fictício de eleições digitais para implementar a solução proposta e demonstrar como ela pode ser aplicada em cenários reais e suas vantagens. Além disso, o trabalho também mostrou outros países que já implementaram soluções semelhantes, como a Estônia, o principal exemplo daquilo que aqui é proposto.

Com este trabalho, foi demonstrado que a criptografia de chave pública tem um grande potencial para mudar a identificação, a comunicação e até mesmo as eleições. De fato, as aplicações da criptografia são muitas, mas, neste trabalho, o foco foi apenas uma: identificação e autenticação da identidade do cidadão no contexto brasileiro. E este trabalho conseguiu, com sucesso, demonstrar que a proposta de uma carteira de identidade baseada em criptografia de chave pública é viável, fácil de ser implementada e aplicada e segura, além do fato de ser transparente, porque os mecanismos de segurança se baseiam em princípios matemáticos bem estudados e não na segurança por meio da obscuridade.

Os próximos passos para amadurecer ainda mais a solução consiste em estudar os pontos negativos da solução, aprofundar o conhecimento sobre os custos de implementação de carteiras físicas de identidade e comparar com a solução atual, demonstrar outras formas de autenticação, como a autenticação TLS, estudar os impactos sociais da solução e emitir um cartão inteligente real para demonstrar a solução em outros cenários práticos.

6 – REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ABRAMS, M. et al. **Guide to Industrial Control Systems (ICS) Security**. National Institute of Standards and Technology, 2015. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>. Acesso em: 28 abr. 2022.
- [2] ADLEMAN, L.; RIVEST, R.; SHAMIR, A. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**. Communications of the ACM, n. 21, p. 120-126, 1978. Disponível em: <https://people.csail.mit.edu/rivest/Rsapaper.pdf>. Acesso em: 10 fev. 2022.
- [3] ALEMANHA. **Erste, Zweite und Dritte Bekanntmachung über den Kennkartenzwang**. Deutsches Reichsgesetzblatt, 23 jul. 1938, vol. 1938, n.115, p. 921-922. Disponível em: https://de.wikisource.org/wiki/Bekanntmachungen_%C3%BCber_den_Kennkartenzwang. Acesso em: 09 mar. 2022.
- [4] ANDRETTA, F.; ARAÚJO, C. **Mentir para receber os R\$ 600 é fraude e pode dar mais de 6 anos de prisão**. UOL Economia, [S. l.], 4 jun. 2020. Disponível em: <https://economia.uol.com.br/noticias/redacao/2020/06/04/auxilio-emergencial-crime-fraude-estelionato-r-600.htm>. Acesso em: 15 jul. 2021.
- [5] ÁVILA, C. S.; MARTÍNEZ, V. G. **Analysis of ECIES and other Cryptosystems based on Elliptic Curves**. International Journal of Information Assurance and Security. n. 6. p. 1-9, fev. 2011.
- [6] BÉLGICA. **What is the eID?** eID software. Disponível em: <https://eid.belgium.be/en/what-eid>. Acesso em: 15 abr. 2022.
- [7] BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Rio de Janeiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 14 jul. 2021.

- [8] BRASIL. **Lei nº 4.862, de 29 de novembro de 1965**. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4862.htm. Acesso em: 15 jul. 2021.
- [9] BRASIL. **Lei nº 7.116, de 29 de agosto de 1983**. Assegura validade nacional às Carteiras de Identidade, regula sua expedição e dá outras providências. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/1980-1988/17116.htm. Acesso em: 29 jul. 2021.
- [10] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 21 abr. 2022.
- [11] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 496, de 1995**. Dispõe sobre o registro civil e o documento único de identificação da pessoa natural em todo o território nacional e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1134522&filename=Dossie+-PL+496/1995. Acesso em 25 out. 2021.
- [12] BRASIL. **Lei nº 9.454, de 7 de abril de 1997**. Institui o número único de Registro de Identidade Civil e dá outras providências. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19454.htm. Acesso em: 14 jul. 2021.
- [13] BRASIL. **Medida provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 15 abr. 2022.
- [14] BRASIL. **Decreto nº 7.166, de 5 de maio de 2010**. Cria o Sistema Nacional de Registro de Identificação Civil, institui seu Comitê Gestor, regulamenta disposições da Lei no 9.454, de 7 de abril de 1997, e dá outras providências. Brasília. Disponível em: http://planalto.gov.br/ccivil_03/_ato2007-2010/2010/Decreto/D7166.htm. Acesso em: 15 jul. 2021.

- [15] BRASIL. Congresso Nacional. **Projeto de lei 1775, de 2015**. Dispõe sobre o Registro Civil Nacional - RCN e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1342951. Acesso em: 25 out. 2021.
- [16] BRASIL. Congresso Nacional. **Lei nº 13.444, de 11 de maio de 2017**. Dispõe sobre a Identificação Civil Nacional (ICN). Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/113444.htm. Acesso em: 25 out. 2021.
- [17] BRASIL. **Decreto nº 9.278, de 5 de fevereiro de 2018**. Regulamenta a Lei nº 7.116, de 29 de agosto de 1983, que assegura validade nacional às Carteiras de Identidade e regula sua expedição. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9278.htm. Acesso em: 25 out. 2021.
- [18] BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 25 out. 2021.
- [19] BRASIL. Congresso Nacional. **Projeto de lei 1.422, de 2019**. Institui o Cadastro de Pessoas Físicas (CPF) como número suficiente para identificação do cidadão nos bancos de dados de serviços públicos, altera dispositivos da Lei nº 13.460, de 26 de junho de 2017, e dá outras providências. Brasília. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0hc634df4zwgpb2a5uedtixl4675198.node0?codteor=1718365&filename=PL+1422/2019. Acesso em: 15 jul. 2021.
- [20] BRASIL. **Lei nº 13.982, de 2 de abril de 2020**. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/113982.htm. Acesso em: 14 jul. 2021.

- [21] BYBEE, H. C.; HOUZE, A. **Nineteenth-Century French Passport Laws and Documents**. The BYU Family Historian, 01 set. 2007, vol. 6. Disponível em: <https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1030&context=byufamilyhistorian>. Acesso em: 09 mar. 2022.
- [22] CAIXA ECONÔMICA FEDERAL. **Auxílio Emergencial 2021**. CAIXA. Disponível em: <https://www.caixa.gov.br/auxilio/auxilio2021/Paginas/default.aspx>. Acesso em: 14 jul. 2021.
- [23] CAZAQUISTÃO. **Passport and Identity Card of the RK**. eGov. Disponível em: <https://web.archive.org/web/20220122201157/http://egov.kz/cms/en/categories/passport>. Acesso em: 15 abr. 2022.
- [24] COOK, J. D. **Elliptic curve P-384**. 11 mai. 2019. Disponível em: <https://www.johndcook.com/blog/2019/05/11/elliptic-curve-p-384/>. Acesso em: 17 fev. 2022.
- [25] DIFFIE, W.; HELLMAN, M. **New directions in cryptography**. IEEE Transactions on Information Theory, vol. IT-22, n. 6, nov. 1976. Disponível em: <https://ieeexplore.ieee.org/document/1055638/>. Acesso em: 05 abr. 2022.
- [26] ELEGIS. **Saiba quais são as principais fases do processo eleitoral**. Disponível em: <https://www.elegis.com.br/saiba-quais-sao-as-principais-fases-do-processo-eleitoral/>. Acesso em: 29 abr. 2022.
- [27] ESPANHA. **Guia de Referencia del DNIE com NFC**. Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre. 27 out. 2017. Disponível em: https://www.dnielectronico.es/PDFs/Guia_de Referencia DNIE con NFC.pdf. Acesso em: 15 abr. 2022.
- [28] ESPINER, Tom. **GCHQ pioneers on birth of public key crypto**. 26 out. 2010. Disponível em: <https://www.zdnet.com/article/gchq-pioneers-on-birth-of-public-key-crypto/>. Acesso em: 05 abr. 2022.

- [29] ESTÔNIA. **How to use your digital ID**. Disponível em: <https://learn.e-resident.gov.ee/hc/en-us/articles/360000624498-How-to-use-your-digital-ID>. Acesso em: 10 fev. 2022.
- [30] ESTÔNIA. **e-Identity**. e-Estonia. Disponível em: <https://e-estonia.com/solutions/e-identity/id-card/>. Acesso em: 15 abr. 2022.
- [31] HOLANDA. **DigiD**. Disponível em: <https://www.digid.nl/en/>. Acesso em: 15 abr. 2022.
- [32] IBM. **Public Key Certificates**. Disponível em: <https://www.ibm.com/docs/en/sdk-java-technology/8?topic=processes-public-key-certificates>. Acesso em: 15 abr. 2022.
- [33] International Telecommunications Union (ITU). **X.509: The Directory - Authentication framework**. 25 nov. 1988. Disponível em: <https://www.itu.int/rec/T-REC-X.509-198811-S>. Acesso em: 14 abr. 2022.
- [34] Internet Assigned Numbers Authority (IANA). **Transport Layer Security (TLS) Parameters**. 31 mar. 2022. Disponível em: <https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>. Acesso em: 14 abr. 2022.
- [35] ITÁLIA. **The Electronic Identity Card (CIE)**. Carta di Identità Elettronica. Disponível em: <https://www.cartaidentita.interno.gov.it/en/home/>. Acesso em: 15 abr. 2022.
- [36] LEEUWEN, J. **Handbook of Theoretical Computer Science**. Elsevier, vol. 1, 1994.
- [37] MANEL, D.; MTIBAA, A.; RAMZI, H; RAOUF, O. **Hash function and Digital Signature based on elliptic curve**. 14th International Conference on Sciences and Techniques of Automatic Control & Computer Engineering, dez. 2013.
- [38] National Institute of Standards and Technology (NIST). **FIPS 186-4**. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>. Acesso em: 17 fev. 2022.
- [39] NeritPolítica. **“Quais são as principais fases do processo eleitoral?”**. 16 jul. 2021. Disponível em: <https://neritpolitica.com.br/blog/quais-sao-as-principais-fases-do-processo-eleitoral>. Acesso em: 29 abr. 2022.

- [40] PARSOVS, Arnis. **Estonian electronic identity card and its security challenges**. Dissertationes Informaticae Universitatis Tartuensis, 3 mar. 2021. Disponível em: <https://dspace.ut.ee/handle/10062/71481>. Acesso em: 25 nov. 2021.
- [41] Receita Federal. **Perguntas e Respostas**. Disponível em: <https://receita.economia.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/assuntos-relacionados/perguntas-e-respostas>. Acesso em: 29 jul. 2021.
- [42] REINO UNIDO. **James Ellis**. Government Communications Headquarters. 11 mar. 2019. Disponível em: <https://www.gchq.gov.uk/person/james-ellis>. Acesso em: 14 abr. 2022.
- [43] **RFC 2764**. A Framework for IP Based Virtual Private Networks. Disponível em: <https://datatracker.ietf.org/doc/html/rfc2764>. Acesso em: 28 abr. 2022.
- [44] **RFC 4251**. The Secure Shell (SSH) Protocol Architecture. Disponível em: <https://datatracker.ietf.org/doc/html/rfc4251>. Acesso em: 28 abr. 2022.
- [45] **RFC 6979**. Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). Disponível em: <https://datatracker.ietf.org/doc/html/rfc6979>. Acesso em: 05 abr. 2022.
- [46] **RFC 8446**. The Transport Layer Security (TLS) Protocol Version 1.3. Disponível em: <https://datatracker.ietf.org/doc/html/rfc8446>. Acesso em: 05 abr. 2022.
- [47] **RFC 8551**. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0. Disponível em: <https://datatracker.ietf.org/doc/html/rfc8551>. Acesso em: 28 abr. 2022.
- [48] ROHR, Altieres. **Megavazamentos de dados expõem informações de 223 milhões de números de CPF: Dezenas de arquivos foram disponibilizados publicamente e colocados à venda por criminosos**. G1 - Economia. 25 jan. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml>. Acesso em: 29 jul. 2021.

- [49] ROSA, Pedro Luiz Barros Palma da. **“Como funciona o sistema proporcional?”**. Escola Judiciária Eleitoral. Revista eletrônica EJE n. 5, ano 3. Disponível em: <https://www.tse.jus.br/o-tse/escola-judiciaria-eleitoral/publicacoes/revistas-da-eje/artigos/revista-eletronica-eje-n.-5-ano-3/como-funciona-o-sistema-proporcional>. Acesso em: 29 abr. 2022.
- [50] SENADO FEDERAL. **Glossário: Voto Majoritário**. Disponível em: <https://www12.senado.leg.br/noticias/glossario-legislativo/voto-majoritario>. Acesso em: 29 abr. 2022.
- [51] SERPRO. **DNI: a identidade unificada e digital do brasileiro**. 05 de junho de 2018. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2018/dni-a-identidade-unificada-e-digital-do-brasileiro>. Acesso em: 25 out. 2021.
- [52] SHOSTACK, Adam. **An Overview of SSL (version 2)**. Mai. 1995. Disponível em: <https://shostack.org/files/essays/ssl/>. Acesso em: 28 abr. 2022.
- [53] SMITH, R. E. **Elementary Information Security**. Jones & Bartlett Learning, 2016, ed. 2, p. 151.
- [54] VINHAS, Ana. **Em um ano, PF abre 931 inquéritos sobre fraude do auxílio: Desde o início do programa, em abril de 2020, foram realizadas 332 operações, 44 prisões e R\$1 milhão de bens apreendidos**. R7, [S. l.], 15 de maio de 2021. Disponível em: <https://noticias.r7.com/economia/em-um-ano-pf-abre-931-inqueritos-sobre-fraude-do-auxilio-15052021>. Acesso em: 14 jul. 2021.
- [55] VITORIO, Tamires. **Site brasileiro expôs 426 milhões de dados pessoais, diz empresa de segurança**. CNN, 22 de setembro de 2021. Disponível em: <https://www.cnnbrasil.com.br/business/site-brasileiro-expos-426-milhoes-de-dados-pessoais-diz-empresa-de-seguranca/>. Acesso em: 25 out. 2021.
- [56] WILSON, Stephen. **The Importance of PKI Today**. 2005. Disponível em: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.753&rep=rep1&type=pdf>. Acesso em: 10 fev. 2022.