# 

Projeto de Graduação em Computação III

IDENTIFICAÇÃO CIVIL DIGITAL

Autor: Kauan Manzato do Nascimento

Orientador: Prof. Dr. Carlos Alberto Kamienski

Santo André – SP

Março de 2022

**ÍNDICE**

RESUMO......................................................................................................................................

1. INTRODUÇÃO........................................................................................................................

1.1 CONTEXTUALIZAÇÃO...........................................................................................

1.2 PROBLEMAS.............................................................................................................

1.3 OBJETIVO GERAL....................................................................................................

1.4 OBJETIVOS ESPECÍFICOS......................................................................................

2. REVISÃO BIBLIOGRÁFICA..................................................................................................

2.1 IDENTIFICAÇÃO......................................................................................................

2.2 CRIPTOGRAFIA DE CHAVE PÚBLICA..................................................................

2.2.1 CRIPTOGRAFIA DE CURVAS ELÍPTICAS.............................................

2.3 CERTIFICADOS DIGITAIS E PKI............................................................................

2.4 IDENTIDADE DIGITAL............................................................................................

3. SOLUÇÃO PROPOSTA...........................................................................................................

3.1 FERRAMENTAS........................................................................................................

3.2 FUNCIONALIDADES...............................................................................................

3.3 EMISSÃO DA CARTEIRA DE IDENTIDADE.........................................................

3.3.1 CÓDIGO DE EMISSÃO DA CARTEIRA DE IDENTIDADE....................

3.4 AUTENTICAÇÃO......................................................................................................

3.4.1 AUTENTICAÇÃO DO CERTIFICADO DO CLIENTE TLS.....................

3.5 CRIPTOGRAFAR E DESCRIPTOGRAFAR.............................................................

3.6 ASSINAR E VALIDAR..............................................................................................

4. TESTES.....................................................................................................................................

4.1 ELEIÇÕES NO BRASIL.............................................................................................

4.2 APLICAÇÃO DO ELEITOR......................................................................................

4.3 APLICAÇÃO DO TSE................................................................................................

5. CONCLUSÃO..........................................................................................................................

6. REFERÊNCIAS BIBLIOGRÁFICAS......................................................................................

**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 na solução implementada na Estônia, porém adaptando à realidade brasileira. Depois de uma extensa revisão do problema, da bibliografia e de soluções parecidas implementadas em outros países, há também uma demonstração da solução, com código disponível online, e aplicação da solução em um cenário hipotético de eleições digitais.

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. Portanto, como é explicado mais tarde, este trabalho não resolve o problema ou garante que a solução é a mais segura, apenas demonstra que é possível utilizá-la na prática para resolver o problema. Por fim, com os testes, é demonstrado que a solução é viável, simples e transparente. Porém, ainda faltarão algumas informações, como o impacto social e político, que este trabalho não trata por estar fora do escopo.

**1 – Introdução**

Este trabalho trata sobre o problema da identificação civil no Brasil e suas consequências e propõe como solução um sistema digital que faz 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;
* **Inclusão social:** a solução deve garantir que haja o maior número possível de pessoas beneficiadas. Os aspectos relacionados a este tópico são: acessibilidade, conhecimento público (conhecimento das pessoas sobre a solução e a facilidade de entender o processo), acesso e exclusão digital, confiança, transparência e conveniência;
* **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 novo coronavírus (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) (BRASIL, 2020). Porém, para receber o benefício, a pessoa precisa cumprir uma série de requisitos, como previsto na 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 (CAIXA, 2021). 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 situações em que sujeitos receberam o benefício sem cumprir os requisitos, e situações em 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 (BRASIL, 1940) (ANDRETTA e ARAÚJO, 2020).

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 (VITORIO, 2021).

O dado pessoal que iremos tratar 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 (BRASIL, 1983). 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.

Além do CPF e do RG, ainda existem outros documentos que podem ser 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.

Como alternativa ao RG, surgiram propostas como

* **Registro Civil Único (RCU)** (BRASIL, 1995)
* **Registro de Identificação Civil (RIC):** surgiu em 1997 (BRASIL, 1997) e regulamentada 13 anos depois, em 2010 (BRASIL, 2010).
* **Registro Civil Nacional (RCN)** (BRASIL, 2015)
* **Identificação Civil Nacional (ICN)** (BRASIL, 2017)
* **Documento Nacional de Identificação (DNI):** usado atualmente como identificação digital. Em outras palavras, outro documento que não resolve o problema (SERPRO, 2018) (BRASIL, 2018).
* **Biometria** como alternativa a documentos físicos (Decreto nº 10.046, de 9 de outubro de 2019).

Surgiram novas propostas por décadas e, mesmo assim, nenhuma realmente resolveu os problemas. Primeiro que 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 temos mais informações sobre o projeto. Segundo que, conforme são criados documentos, adicionamos complexidade no sistema e ainda podemos inserir novas vulnerabilidades nele, que podem permitir ainda mais fraudes.

Com isso, podemos enumerar 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 enumeramos 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 (ROHR, 2021).

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 e data de emissão e registro da data de validade da carteira digital.

Com relação ao mecanismo de identificação e autenticação com a carteira digital consiste em certificado digital e validação para a identificação e 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 construída.

**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 as empresas de prover seus serviços e gerenciar eficientemente os 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 através 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 através do uso de passaportes internos (BYBEE e HOUZE, 2007), 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 (ALEMANHA, 1938).

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 (SMITH, 2015) 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 (RIVEST, 1990). Já o processo de criptografar, de acordo com o dicionário de Oxford, é o processo de converter informações ou dados em código, 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 (GCHQ) britânico. 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 conhecemos como troca de chaves Diffie-Hellman (GCHQ pioneers) (diffie; hellman; 1973). Entretanto, o trabalho do grupo ficou em segredo até 1997, quando o governo britânico liberou as descobertas (REINO UNIDO, 2019).

Texto

Descrição gerada automaticamente

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 (ADLEMAN; RIVEST; SHAMIR, 1978) 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 usaremos 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. Assim, garantimos a confidencialidade da mensagem.

Diagrama

Descrição gerada automaticamente

2.2.1 – CRIPTOGRAFIA DE CURVAS ELÍPTICAS

Dentre os vários tipos de técnicas de criptografia de chave pública, usaremos a criptografia de curvas elípticas, que é usado atualmente no sistema de identidade digital da Estônia (PARSOVS, 2021). Há também outros tipos de criptografia de chave pública, como a criptografia baseada em números primos (RSA).

A criptografia de chave pública de curvas elípticas é baseado em um conceito matemático chamado de curva elíptica, por isso o nome. De forma simplificada, uma curva elíptica é um conjunto de pontos que satisfaz a seguinte equação, com parâmetros :

Os parâmetros e o campo finito usado definem diferentes curvas, com diferentes características e propriedades, como podemos ver abaixo:

Forma

Descrição gerada automaticamente

Os pontos pertencentes às curvas e as operações do respectivo campo finito usado permitem realizar as operações necessárias para criptografar e descriptografar informações.

Como a explicação técnica está fora do escopo, iremos nos limitar ao fato que já há curvas bem conhecidas e usadas, como descrito pela *Internet Assigned Numbers Authority* (IANA, 2022). São alguns exemplos de curvas: secp384r1, brainpoolP512r1 e x25519.

Neste trabalho, usaremos 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 (COOK, 2019).

2.3 ASSINATURAS DIGITAIS

Para garantir autenticidade (e, por consequência, identificação) do emissor, a criptografia de chave pública permite a criação de **assinaturas digitais** através de chaves secretas. Como as chaves são secretas, elas não podem ser forjadas e quem assinou não pode negar a assinatura (RIVEST et al., 1978). Portanto, as assinaturas garantem identificação e autenticação e, por isso, são parte essencial da solução proposta neste trabalho, como veremos mais para frente.

Criar uma assinatura digital é semelhante à operação de criptografia, porém 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 o certificado digital (com a chave pública) e a assinatura, assim o destinatário consegue verificar a autenticidade e a integridade da mensagem e identificar o remetente.

Em poucas palavras, 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 X.

Logotipo, nome da empresa

Descrição gerada automaticamente

2.4 – CERTIFICADOS DIGITAIS E PKI

Em 1988, surge o **certificado digital** com a publicação da primeira versão do padrão X.509 (ITU, 1988). 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. Assim, o certificado digital auxilia a implementação da criptografia de chave pública (IBM, ????), como veremos a seguir.

Interface gráfica do usuário, Diagrama, Texto, Aplicativo

Descrição gerada automaticamente

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, e desenvolvido para garantir segurança das comunicações sobre redes de computadores, 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 (RFC 8446 [x]). O protocolo TLS/SSL usa certificados digitais e criptografia de chave pública: cliente e servidor possuem certificados digitais, que são trocados no começo da comunicação e que permitem a confiança mútua entre cliente e servidor. Essa troca de certificados e chaves é conhecido como *TLS handshake*.

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) (WILSON, 2005). 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.

Diagrama

Descrição gerada automaticamente

Em 2001, foi instituído o órgão público no Brasil responsável pela certificação digital no país, chamado de **ICP-Brasil** (Infraestrutura de Chaves Públicas Brasileira) (BRASIL, 2001 medidaprov). 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.

2.5 – 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 (ESTONIA, E-IDENTITY) e o documento é usado em várias atividades cotidianas dos cidadãos, como internet banking, assistência médica e até eleições.



<https://www.politsei.ee/en/instructions/id-card-sample>

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 (PARSOVS, 2021): 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 (BELGICA, ????)
* Cazaquistão (CAZAQUISTÃO, ????)
* Holanda (HOLANDA, ????)
* Itália (ITÁLIA, ????)
* Espanha (ESPANHA, 2017) etc.

**3 – Solução Proposta**

Conforme escrito anteriormente, a solução proposta é um cartão inteligente baseado no modelo estoniano, adaptando algumas características ao contexto brasileiro, servindo como uma fonte de **autenticação** (chave de autenticação e certificado digital), **identificação** (informações pessoais gravadas digital, 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, usamos 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 aberto[[1]](#footnote-1) 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, usamos o IDLE (*Integrated Development and Learning Environment*), um ambiente de desenvolvimento integrado ao Python que possui interface gráfica e que permite a execução e a criação do código. O IDLE vem junto com o Python, por padrão, e está disponível em diferentes sistemas operacionais, como o Windows, o Linux e o MacOS.

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, 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, escrever novos certificados e reinstalar o applet do smart card.

**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 (ESTÔNIA, 2022).

3.3 – EMISSÃO DA CARTEIRA DE IDENTIDADE

A carteira de identidade, na prática, 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, para fins de demonstração, iremos nos limitar a simular a carteira apenas emitindo as informações digitais da carteira.

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

As chaves privadas armazenadas são protegidas, cada uma protegida por um PIN de 4 dígitos diferente. Uma das chaves, conforme descrito, é usada para autenticação e a outra, para assinatura. Porém, como este trabalho tem a finalidade de demonstrar a solução, iremos emitir apenas uma chave, para manter a simplicidade do projeto e melhorar a didática. A chave privada é uma chave privada de criptografia de curva elíptica (NIST P-384) de 384 bits e criptografada. Seu tamanho é de apenas 379 bytes. Assim, as duas chaves terão um tamanho de 758 bytes. Elas são geradas usando a biblioteca cryptography para Python e são salvas no formato PEM (Privacy Enhanced Mail).

Por fim, os certificados digitais estão no padrão X.509 e são criados a partir do par de 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.

Na prática, 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, iremos pular a cadeia de confiança e gerar certificados auto assinados.

3.3.1 – CÓDIGO DA EMISSÃO DA CARTEIRA DE IDENTIDADE

Primeiro, o usuário é recebido com o cabeçalho (função cabecalho) e com um pedido para inserir 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). As definições das funções utilizadas estão nas figuras abaixo:

Forma

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente



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 definida abaixo. Nesta função, é usado o conceito de expressão regular (regex) para validar a entrada do usuário.

Texto

Descrição gerada automaticamente

Então, geramos a chave privada com a função gen\_key definida abaixo. Conforme dito anteriormente, usamos a biblioteca cryptography para gerar uma chave de criptografia de curvas elípticas, usando a curva NIST P-384.

Texto

Descrição gerada automaticamente 

Depois, a partir da chave privada, extraímos a chave pública:



No próximo passo, geramos o certificado digital com a função gen\_cert, passando como parâmetros o nome do proprietário, nome do emissor e a chave privada. Esta função é definida abaixo:

Texto

Descrição gerada automaticamente

Depois, codificamos a chave privada e o certificado no formato PEM, além de criptografar a chave privada com o PIN escolhido, conforme mostrado abaixo:

Texto

Descrição gerada automaticamente

Então salvamos o certificado e a chave privada junto com as informações pessoais (neste caso, usamos o nome do proprietário para exemplificar as informações pessoais, mas podem ser incluídas outras informações) usando a função save\_file definida abaixo, finalizando assim a simulação da emissão da carteira de identidade.

Tela de celular com letras

Descrição gerada automaticamente com confiança médiaTela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente com confiança média

Analisando o código, é possível ver muitos pontos de melhoria, obviamente. Mas, para os pontos que o trabalho se propôs a demonstrar, o código é suficiente, mostrando que a solução é simples, transparente e segura. Além disso, o código estará disponível de forma atualizada no GitHub[[2]](#footnote-2).

3.3.2 DEMONSTRAÇÃO DA EMISSÃO DA CARTEIRA DIGITAL

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 também tornaria o projeto mais complexo sem contribuir com a proposta do trabalho. Neste caso, vamos usar o terminal para executar o código:

Texto

Descrição gerada automaticamente

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. Como resultado os arquivos são salvos na pasta ./files.

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente com confiança média

Para mostrar o conteúdo do certificado e da chave privada de forma amigável, podemos usar a própria biblioteca OpenSSL. Já as informações pessoais são arquivos codificados em UTF-8 e podemos imprimi-la na tela usando cat.



Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

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 (NIST SP 800-53).

O caso de uso mais popular para a chave de autenticação é para autenticação em serviços Web pela Internet usando o protocolo de autenticação do certificado TLS de cliente. Outros usos menos comuns para autenticação incluem assinatura de e-mails com S/MIME, autenticação SSH e VPN, e login em estações de trabalho (PARSOVS, 2021).

Hoje, há planos em desenvolvimento para introduzir um novo método de autenticação para as carteiras de identidade digital através 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 GitHub[[3]](#footnote-3), 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.

No processo CCA TLS, o cliente envia seu certificado de autenticação para o servidor e prova sua identidade com uma assinatura digital, como definido na RFC 8446 [X].

Abaixo, temos uma figura que ilustra o protocolo de handshake entre cliente e servidor, que permite a autenticação, a integridade dos pacotes e a troca de chaves, que permite a comunicação criptografada entre as duas partes.

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 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 (ÁVILA e MARTÍNEZ, 2011).

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).

No caso da Estônia, a solução também é o sistema híbrido, onde chaves AES de 256 bits são derivadas de um segredo de 48 bytes compartilhado pelo ECDH (Elliptic Curve Diffie-Hellman). E, por fim, as informações são criptografadas com a cifra simétrica AES-256 GCM (Galois/Counter Mode) (PARSOVS, 2021).

Neste trabalho em questão, serão usadas duas operações de criptografia durante o cenário das eleições, por causa do problema explicado acima:

* O voto será criptografado usando uma chave RSA de 4096 bits, previamente gerada. O voto é encriptado com a chave pública, que simula a chave pública do TSE, e é descriptografado com a chave privada e a respectiva senha.
* Os dados necessários que são enviados para o servidor do TSE (voto secreto, assinatura e certificado) serão criptografados usando o algoritmo ECDH (Elliptic Curve Diffie-Hellman). Este algoritmo permite a comunicação segura entre o usuário (eleitor) e o servidor (TSE).

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 (RFC 6979) (MANEL et al., 2013). 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 projetado 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, como visto na seção 4 da solução proposta.

4.1 – ELEIÇÕES NO BRASIL

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** (BRASIL, 1988).

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 (<https://www12.senado.leg.br/noticias/glossario-legislativo/voto-majoritario>). 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 (<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>).

As eleições são divididas em fases, sendo elas (<https://www.elegis.com.br/saiba-quais-sao-as-principais-fases-do-processo-eleitoral/)(https://neritpolitica.com.br/blog/quais-sao-as-principais-fases-do-processo-eleitoral>):

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, consideramos apenas a etapa de votação. As outras etapas estão fora do escopo deste trabalho.

Na eleição digital fictícia construída, o mecanismo de votação é composto de duas aplicações, uma para o eleitor e outra para o TSE (ou TRE). A aplicação do eleitor recebe o certificado público, a assinatura digital e o voto do eleitor, criptografa e salva os dados para que a aplicação do TSE possa recebê-los. A aplicação do TSE coleta os dados, descriptografar os dados, valida a assinatura digital e retorna o voto.

Além disso, a aplicação do TSE tem à disposição o voto do eleitor e seu certificado contendo as informações do eleitor para que estas informações sejam tratadas para as etapas futuras da eleição, como a contagem de votos e a garantia que a pessoa só vote uma vez. Entretanto, como as fases posteriores estão fora do escopo, estas informações não serão tratadas neste momento.

4.2 – APLICAÇÃO DO ELEITOR

A aplicação do eleitor recebe o certificado digital do eleitor, vindo da carteira de identidade proposta, e o voto (um número inteiro). A aplicação então faz a assinatura digital usando o algoritmo ECDSA e criptografa o voto para que apenas o TSE tenha acesso à informação. Os dados que foram recebidos e criados são criptografados com ECDH e salvos, simulando a transmissão dos dados via Internet, ou qualquer outro meio que precise de uma comunicação segura entre as partes. A aplicação do cliente consiste dos seguintes passos:

1. Carregar chaves públicas do TSE
2. Carregar o certificado digital do eleitor no formato PEM
3. Escolher o voto
4. Criptografar o voto
5. Carregar a chave privada do eleitor
6. Gerar assinatura digital
7. Derivar chave compartilhada
8. Criptografar os dados
9. “Enviar” os dados para o TSE

**Passo 1:** carregar chaves públicas do TSE

As chaves públicas do TSE são importantes para que possamos mandar os dados criptografados para o TSE, sem que seja possível ver o conteúdo (confidencialidade). Fazemos isso com a função read\_public\_key, definida conforme figura abaixo:

Texto

Descrição gerada automaticamente

A função read\_public\_key recebe o caminho para o arquivo da chave pública em formato PEM e retorna a chave pública. Dessa forma, carregamos as chaves RSA e EC do TSE conforme mostra a figura abaixo:



**Passo 2:** carregar o certificado digital do eleitor no formato PEM

Aqui não iremos usar uma função própria, já que carregar o certificado é muito simples, bastando abrir o arquivo no modo rb, que lê arquivos em binário, como pode ser visto na figura abaixo:



**Passo 3:** escolher o voto

Este passo também é simples, sendo realizado pela função escolher\_voto, cuja definição é mostrada na figura abaixo:



A função escolher\_voto não tem parâmetros, recebe o voto do eleitor como um inteiro e o transforma em bytes para permitir as operações de criptografia e assinatura depois. A função então retorna esses bytes.

**Passo 4:** criptografar o voto

O voto, em bytes, é criptografado com a chave pública RSA de 4096 bits do TSE por meio da biblioteca cryptography, assim os dados só serão acessíveis com a chave privada do TSE e ilegíveis para possíveis agentes maliciosos. Esta operação é realizada conforme figura abaixo:

Texto

Descrição gerada automaticamente

**Passo 5:** carregar a chave privada do eleitor

A função responsável por esta operação é chamada de load\_private\_key, cuja definição pode ser vista na figura abaixo:

Tela preta com letras brancas

Descrição gerada automaticamente

Essa função recebe o caminho da chave privada a ser carregada e pede ao eleitor a senha da chave privada. Se o eleitor errar a senha três vezes, a aplicação fecha. A senha e o caminho do arquivo são passados para a função get\_private\_key, que é responsável por abrir e recuperar a chave privada, e cuja definição é dada abaixo:

Texto

Descrição gerada automaticamente

A função get\_private\_key recebe o caminho e a senha da chave, abre a chave em modo rb e passa o conteúdo e a senha para a função load\_pem\_private\_key da biblioteca cryptography, que vai efetivamente decifrar a chave e recuperá-la.

**Passo 6:** gerar assinatura digital

Com a biblioteca cryptography, assinar digitalmente é bem simples, basta ter os dados que serão assinados em bytes e a chave privada, conforme figura a seguir:

Texto

Descrição gerada automaticamente

Utilizamos o hash SHA384 por ser do mesmo tamanho das chaves de curvas elípticas.

**Passo 7:** derivar chave compartilhada

Esse passo é um pouco mais complexo porque trabalha com várias informações diferentes. Primeiro, é preciso saber a importância desse passo: ao derivarmos uma chave compartilhada, podemos estabelecer uma conexão segura entre eleitor e TSE, porque criptografaremos com uma chave que só essas duas partes conhecem. O segundo ponto importante é que derivamos a chave usando o algoritmo ECDH, combinando a chave privada de quem está derivando a chave e a chave pública da outra parte envolvida comunicação e o vetor inicial. Por fim, a chave derivada e o vetor inicial são usados na cifra simétrica AES para cifrar e decifrar as informações.

O ECDH foi implementado na função derive\_key, que recebe a chave privada de quem está derivando e a chave pública da outra parte. A função retorna, em bytes, a chave compartilhada que foi derivada.

Texto

Descrição gerada automaticamente

Neste código, a função é usada da seguinte forma:



Essa mesma função será usada na aplicação do TSE para derivar a mesma chave e recuperar as informações cifradas.

Um ponto a ressaltar é que a comunicação segura podia ser feita usando a chave RSA do TSE, a mesma usada por tornar o voto secreto. Entretanto, é mais seguro usar chaves separadas para funções diferentes, o ECDH é muito usado atualmente e, portanto, importante demonstrarmos aqui também, e é interessante mostrar que a criptografia de chave pública permite uma mesma operação de várias formas diferentes, neste caso a comunicação segura entre duas entidades.

**Passo 8:** criptografar os dados

Com a chave compartilhada estabelecida, usaremos ela junto à cifra AES para criptografar os dados e enviar para o TSE de forma segura.

Primeiro, geramos o vetor inicial (IV), que são 16 bytes aleatórios usados pela cifra AES no modo GCM. Esta informação é o ponto de partida para a cifra e não precisa ser secreto, por isso não criptografaremos o IV, simulando o fato que as duas entidades concordaram com o IV. O IV é gerado da seguinte forma:

Texto

Descrição gerada automaticamente

Depois, passamos os dados, a chave compartilhada e o IV para a função aes\_encrypt\_data, responsável por cifrar os dados com a chave, e cuja definição é dada a seguir na figura:

Texto

Descrição gerada automaticamente

A função aes\_encrypt\_data recebe os dados, a chave e o vetor inicial. A função inicia a cifra, realiza o padding dos dados, já que a cifra funciona com blocos, e retorna os dados criptografados em bytes.

Essa função, no código do eleitor, é usada para criptografar os dados a serem enviados para o TSE, conforme mostrado na figura abaixo:

Texto

Descrição gerada automaticamente

**Passo 9:** “enviar” os dados para o TSE

Por fim, salvamos os arquivos localmente como forma de simular o envio deles para o TSE. Para o propósito deste trabalho, o meio por onde esses dados passam é irrelevante. A função responsável por salvar os dados é chamada de save\_file, cuja definição é mostrada a seguir:

Texto

Descrição gerada automaticamente

A função save\_file recebe os dados, em bytes, a serem salvos e o nome do arquivo, e salva os arquivos na pasta de envio para a aplicação do TSE utilizar depois.

Basicamente, essa é a aplicação do eleitor. Aqui mostramos que, com algumas linhas de código, é possível autenticar sua identidade com a assinatura e ainda proteger seus dados com a criptografia de chave pública. O voto, por exemplo, foi criptografado duas vezes, uma com a chave RSA e outra com a chave derivada do ECDH.

Na próxima seção, mostraremos como o TSE pode tratar as informações que chegam e como pode garantir a identidade do proprietário do certificado digital, dada a assinatura, idêntico ao que foi exposto na revisão bibliográfica.

4.3 – APLICAÇÃO DO TSE

A aplicação do TSE recebe as informações enviadas pela aplicação do cliente (eleitor), que inclui a chave pública, o certificado, a assinatura digital e o voto secreto do eleitor e as processa. A criptografia garante a integridade e a confidencialidade das informações, enquanto a assinatura digital garante a autenticidade das informações.

A aplicação do TSE funciona seguindo os passos abaixo:

1. Carregar os arquivos que foram recebidos pelo cliente (ou eleitor)
2. Carregar o certificado digital no formato correto e extrair a chave pública dele
3. Carregar os pares de chaves do TSE (EC e RSA)
4. Derivar a chave compartilhada entre TSE e cliente com ECDH
5. Descriptografar o voto e a assinatura usando a cifra AES em modo GCM
6. Verificar a validade da assinatura, dado o certificado
7. Caso a assinatura seja válida, contar o voto. Caso contrário, descartar o voto.

**Passo 1:** carregar os arquivos que foram recebidos pelo cliente (ou eleitor)

Os arquivos que foram recebidos pelo cliente são carregados através da função load\_file, com a seguinte definição:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente com confiança média

Essa função recebe uma string path como parâmetro, lê o arquivo localizado em path e retorna seu conteúdo em bytes. Essa função é usada para carregar os arquivos “recebidos” pelo cliente, salvos em uma pasta. O bloco de código em que esta função é usada é demonstrado a seguir:

Texto

Descrição gerada automaticamente

Carregamos o voto secreto criptografado, a assinatura criptografada, o certificado digital e o vetor inicial usado na cifra AES no modo GCM.

Note que, na verdade, os arquivos não foram enviados através da Internet, mas apenas salvos localmente para fins de demonstração. Esse ponto não muda a conclusão do trabalho porque o meio em que os arquivos são passados não muda o fato que estão criptografados com a chave pública do TSE e só é possível de visualizá-los com a chave privada do TSE, que é secreta.

**Passo 2:** Carregar o certificado digital no formato correto e extrair a chave pública dele

Esse passo é bem simples porque a biblioteca cryptography já vem com uma função pronta para extrair o certificado digital no padrão X.509 em um arquivo codificado em PEM (Privacy Enhanced Mail), chamada de load\_pem\_x509\_certificate().



Depois de carregarmos o certificado no formato adequado, fica fácil extrair informações dele, como quem emitiu, o proprietário e a chave pública. A chave pública é um atributo do certificado e é extraída da seguinte forma:



Além disso, há também duas funções, criadas para ilustrar, que retornam o emissor e o proprietário do certificado, chamadas de get\_cert\_issuer e get\_cert\_subject, respectivamente, definidas conforme figura abaixo:

Texto

Descrição gerada automaticamente

**Passo 3:** Carregar os pares de chaves do TSE (EC e RSA)

Esse passo é feito com a função read\_private\_key. Essa função recebe dois parâmetros: a string do caminho do arquivo onde a chave privada está armazenada e a senha da chave privada, ambos em bytes. Esta função é definida a seguir:

Texto

Descrição gerada automaticamente

Aqui é importante ressaltar que essa função não é comprovadamente segura. Apesar da biblioteca cryptography ter aplicações reais, o mal uso das funções disponibilizadas por ela pode comprometer sua segurança. O objetivo deste cenário é apenas demonstrar como um certificado digital pode ser usado para autenticar a identidade dos eleitores em um cenário fictício de eleições digitais.

Voltando ao código, a função read\_private\_key é usada da seguinte forma:



Perceba que as senhas estão “hardcoded” no código, ou seja, integradas ao código fonte, o que é, obviamente, uma má prática de programação, além de ser uma vulnerabilidade, mas é irrelevante para o que queremos mostrar neste caso.

**Passo 4:** derivar a chave compartilhada entre TSE e cliente com ECDH

Este passo é realizado através da mesma função derive\_key que foi definida no passo 7 da aplicação do cliente. Esta função é usada da seguinte forma no código do TSE:



A chave compartilhada é derivada da chave privada do TSE e da chave pública do cliente. Esta chave será usada, no lado do TSE, para descriptografar os dados recebidos.

**Passo 5:** descriptografar o voto e a assinatura usando a cifra AES em modo GCM

As funções usadas para implementar a cifra AES no modo GCM são aes\_encrypt\_data e aes\_decrypt\_data, para criptografar e descriptografar, respectivamente, e suas definições estão demonstradas na figura abaixo:

Texto

Descrição gerada automaticamente

As funções recebem os dados a serem cifrados/decifrados, a chave, que no nosso caso é a chave compartilhada, e o vetor inicial, e retorna os dados cifrados/decifrados. Perceba a utilização de *padding*, já que a cifra AES funciona com blocos.

**Passo 6:** verificar a validade da assinatura, dado o certificado

Esse passo é importante, porque é o que queremos mostrar neste trabalho, que é a autenticação da identidade digitalmente. Conforme dito na revisão da bibliografia, uma assinatura digital válida significa a autenticidade da identidade de uma das partes da comunicação. Em outras palavras, se a assinatura digital for válida para um dado certificado digital, então aquela pessoa é quem realmente diz ser. Assim, é garantido que a mensagem não foi violada e só pode ter sido criada pelo proprietário do certificado, o eleitor.

Apesar da importância para o trabalho e da complexidade conceitual, é bem simples de implementar usando a biblioteca cryptography, como podemos ver na figura abaixo:

Texto

Descrição gerada automaticamente

A função verificar\_assinatura recebe a chave pública do eleitor, a assinatura digital e os dados que foram assinados. Se a assinatura for válida, a função retorna True, e False caso contrário.

**Passo 7:** caso a assinatura seja válida, contar o voto. Caso contrário, descartar o voto.

Por fim, depois de verificada a validade da assinatura digital, o voto pode ser considerado válido e contabilizado. Podemos fazer isso descriptografando o voto com a função decrypt\_vote, com a definição mostrada abaixo:

Texto

Descrição gerada automaticamente

A função decrypt\_vote recebe o voto secreto e a chave privada, e retorna o voto como um inteiro. Com isso, temos o voto pronto para ser contabilizado e o fim da aplicação do TSE.

A aplicação do TSE é simples, mas, mesmo com poucas linhas de código, é capaz de gerar dados confidenciais e autenticar a identidade do proprietário do certificado, evitando fraudes. Esse cenário é um bom demonstrativo de como a criptografia de chave pública é poderosa, simples de ser implementada e transparente, no sentido de que é possível tornar o código aberto para auditorias de qualquer cidadão e ainda manter a segurança.

Uma última observação, mas não menos importante, é o fato de que essa aplicação é apenas uma demonstração do conteúdo explicado neste trabalho, que é uma alternativa à autenticação de identidade que temos atualmente no Brasil, e não uma aplicação real. O código está propenso a vulnerabilidades, como, por exemplo, o fato de trabalharmos com uma chave para autenticação e assinatura, e não uma chave para cada função, e, por isso, não é recomendada seu uso em cenários reais.

**5 – Conclusão**

Este trabalho revisou a bibliografia a fim de concentrar os conceitos essenciais 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 mostrou outros países que já implementam essa solução, como a Estônia, e como a solução impacta positivamente a população.

Com este trabalho, foi demonstrado que a criptografia de chave pública tem um grande potencial para mudar a forma como nos identificamos, como nos comunicamos e até como votamos. De fato, as aplicações da criptografia são muitas, mas aqui focamos em apenas uma: autenticação da identidade no contexto brasileiro. Também foi demonstrado que a solução é fácil de ser implementada e segura, além do fato de ser transparente: qualquer cidadão pode verificar os mecanismos de segurança, porque são todos baseados na matemática, e não em segurança através da obscuridade.

Os próximos passos para desenvolver a solução ainda mais 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. ADLEMAN, Leonard; RIVEST, Ron; SHAMIR, Adi. **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**. Communications of the ACM, n. 21, p. 120-126. Disponível em: <https://people.csail.mit.edu/rivest/Rsapaper.pdf>. Acesso em: 10 fev. 2022.
2. 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.
3. ANDRETTA, Filipe; ARAÚJO, Carla. **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.
4. ÁVILA, Carmen Sánchez; MARTÍNEZ, Victor Gayoso. **Analysis of ECIES and other Cryptosystems based on Elliptic Curves**. International Journal of Information Assurance and Security. n. 6. p. 1-9, fev. 2011.
5. BÉLGICA. **What is the eID?** eID software. Disponível em: <https://eid.belgium.be/en/what-eid>. Acesso em: 15 abr. 2022.
6. 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.
7. 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.
8. 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/l7116.htm>. Acesso em: 29 jul. 2021.
9. 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.
10. 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.
11. 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/l9454.htm>. Acesso em: 14 jul. 2021.
12. 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.
13. 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.
14. 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.
15. BRASIL. **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/l13444.htm>. Acesso em: 25 out. 2021.
16. 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.
17. 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.
18. 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.
19. 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/l13982.htm>. Acesso em: 14 jul. 2021.
20. BYBEE, Howard C., HOUZE, Annick. **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.
21. CAIXA ECONÔMICA FEDERAL. **Auxílio Emergencial 2021**. CAIXA. Disponível em: <https://www.caixa.gov.br/auxilio/auxilio2021/Paginas/default.aspx>. Acesso em: 14 jul. 2021.
22. 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.
23. 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.
24. DIFFIE, Whitfield; HELLMAN, Martin. **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.
25. 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.
26. 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.
27. 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.
28. ESTÔNIA. **e-Identity**. e-Estonia. Disponível em: <https://e-estonia.com/solutions/e-identity/id-card/>. Acesso em: 15 abr. 2022.
29. HOLANDA. **DigiD**. Disponível em: <https://www.digid.nl/en/>. Acesso em: 15 abr. 2022.
30. 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.
31. 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.
32. 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.
33. 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.
34. MANEL, Dridi; MTIBAA, Abdellatif; RAMZI, Haddaji, RAOUF, Ouni. **Hash function and Digital Signature based on elliptic curve**. 14th International Conference on Sciences and Techniques of Automatic Control & Computer Engineering, dez. 2013.
35. National Institude 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.
36. 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.
37. 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.
38. 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.
39. **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.
40. **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.
41. 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.
42. 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.
43. SMITH, Richard E. **Elementary Information Security**. Jones & Bartlett Learning, 2016, ed. 2, p. 151.
44. 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.
45. 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.
46. 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.

1. O código-fonte do OpenSSL está disponível em <https://github.com/openssl/openssl>. [↑](#footnote-ref-1)
2. O código-fonte deste trabalho está disponível em: <https://github.com/kauanmn/PGC>. [↑](#footnote-ref-2)
3. O código-fonte do Web eID está disponível em: <https://github.com/web-eid/web-eid-system-architecture-doc>. [↑](#footnote-ref-3)