Relatório

Kauan Manzato do Nascimento

RA: 11201721592

Universidade Federal do ABC

Santo André, SP

1. Introdução e Justificativa

1.1 Introdução ao trabalho

Este trabalho trata sobre o problema da identificação civil no Brasil, 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 (identificação e autenticação);
- **Eficiência e custo:** quantidade de recursos usados para implementar e manter o sistema;
- **Interoperabilidade:** a solução precisa definir um padrão com abrangência nacional e que permita a interação entre os diferentes órgãos públicos;
- **Segurança:** nível de segurança garantido pela solução proposta, suas vulnerabilidades, se existentes;
- **Inclusão social** (acessibilidade, conhecimento público, acesso e exclusão digital, confiança, transparência, conveniência): a solução deve garantir que haja o maior número possível de beneficiados por ela;
- **Limitações:** limitações e desvantagens presentes e conhecidas na solução proposta, em comparação com os benefícios trazidos pela mesma.
- Impactos políticos e sociais, legislação e regulamentações estão fora do escopo deste trabalho, ficando limitadas a trabalhos futuros.

Uma possível aplicação da proposta em uma eleição digital também é discutida, como forma de exemplificar e dissecar os detalhes da proposta.

1.2 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 faz o download do 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) (ARAÚJO; ANDRETTA, 2020).

1.3 Problemas

Estas situações 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 (BRASIL, 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 novos 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 padrão 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).

2. Objetivos

2.1 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.

2.2 Objetivos Específicos

São objetivos específicos:

1. Emitir carteiras de identidade digitais:
    a. Criação de 2 conjuntos de Chave Privada e Certificado Digital (X.509) protegidas por um PIN (4 dígitos), baseando-se no modelo estoniano.
        i. As chaves ECC P-384, usadas pela Estônia (PARSOVS, 2021), serão geradas usando o software XCA.
        ii. O certificado (arquivo `.pfx`) vai ser criado com o software XCA.
        iii. Vamos extrair a chave privada (criptografada) usando o OpenSSL.
    b. Registro de dados pessoais: Nome completo, CPF, Sexo, Foto, Filiação e Naturalidade.
    c. Registro do local e data de emissão.
    d. Registro da data de validade.
2. Implementar um mecanismo de identificação e autenticação com a carteira digital
    a. A carteira de identidade deve permitir que o seu portador assine digitalmente
    b. O receptor dos dados pode validar a assinatura, confirmando a identidade e autenticando a outra parte.
    c. O processo de autenticação consiste no processo de autenticação TLS do certificado do cliente
        i. aqui teremos que implementar um servidor TLS para demonstrar

3. Implementar uma demonstração de um sistema de eleições simples que usa a carteira digital para identificar e autenticar votos.
    a. Talvez alguma tentativa de ataque ou agente malicioso, para demonstrar a segurança?

3. Revisão Bibliográfica

3.1 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.

Esse processo é usado em vários setores da sociedade. Por exemplo: a identificação de pessoas também é usada por empresas para garantir que as informações passadas pelos consumidores sejam válidos, 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 (WHITLEY & HOSEIN, 2010 `Global Challenges for Identity Policies`), 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 (https://de.wikisource.org/wiki/Bekanntmachungen_über_den_Kennkartenzwang).

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 `Richard E. Smith - Elementary Information Security, p. 150`) como parte do sistema de arquivos Multics. Esse e outros mecanismos tiveram influência na identidade digital porque trouxe a estrutura popular de nomes de usuários e senhas, que permitem uma entidade gerenciar os acessos e permissões dos usuários do sistema.

Em 1982, o conjunto de protocolos TCP/IP foi implementado e a sua primeira especificação foi publicada em 1983 (IETF RFC 882, https://tools.ietf.org/html/rfc882). O TCP/IP, que é a base da Internet atualmente, atribui endereços aos hosts, que é basicamente uma forma de identificar os hosts.

3.2 Criptografia de chave pública

É neste período (décadas de 1970 e 1980) que a criptografia entra como forma de revolucionar a segurança e a autenticação de identidade. Na década de 70, dois grupos independentes de cientistas inventaram o conceito de **criptografia de chave pública**.

O primeiro grupo a inventar o conceito 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 do primeiro, criou um método prático para implementar o "sistema de criptografia não secreta" de Ellis. Em 1974, Williamson criou um método de troca de chaves, que hoje conhecemos como troca de chaves Diffie-Hellman

(https://www.zdnet.com/article/gchq-pioneers-on-birth-of-public-key-crypto/). Entretanto, o trabalho do grupo ficou em segredo até 1997, quando o governo britânico liberou as descobertas (https://www.gchq.gov.uk/person/james-ellis).

A descoberta pública foi feita por cientistas americanos, nos anos de 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 campos finitos. Em 1977, Ron Rivest, Adi Shamir e Leonard Adleman inventaram o algoritmo RSA de criptografia de chave pública, publicado em 1978 (https://people.csail.mit.edu/rivest/Rsapaper.pdf) e que foi o estopim para a criação de muitos outros esquemas criptográficos semelhantes. No paper 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, esta última que está em posse do destinatário. Em outras palavras, apenas o destinatário pode descriptografar a mensagem. Assim, garantimos a confidencialidade da mensagem.

Para garantir autenticidade (e por consequência, identificação) do emissor, a criptografia de chave pública permite a criação de **assinaturas** através das 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 a identificação e a autenticação. Por isso, as assinaturas digitais são essenciais para este trabalho.

3.2.1 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 identificação digital da Estônia (PARSOVS, 2021).

A criptografia de chave pública é baseada em estruturas algébricas sobre campos finitos, chamadas de curvas elípticas. De forma simplificada, uma curva elíptica é um conjunto de pontos que satisfaz a seguinte equação, com parâmetros $a, b \in \mathbb{R}$, e se parece com a figura 32:

$$y^2 = x^3 + ax + b$$

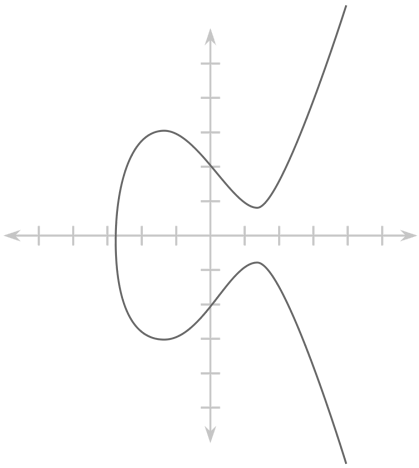


Figura 32

Os parâmetros a, b e o campo finito usado definem diferentes curvas, com diferentes características, como podemos ver na figura 453:

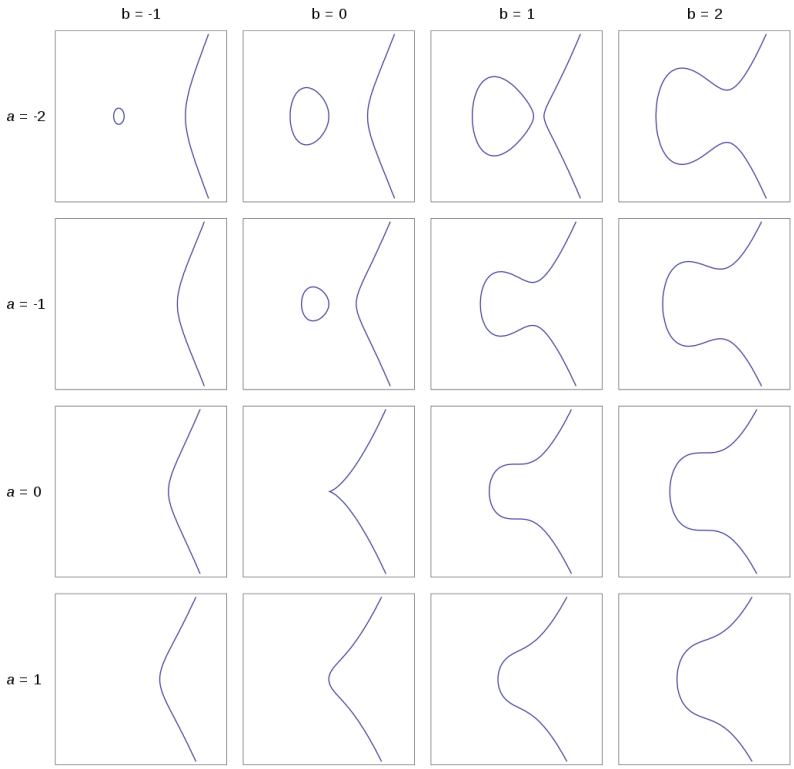


Figura 453

Os pontos pertencentes às curvas e as operações do respectivo campo finito utilizado 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 na página dos parâmetros do TLS no website da IANA (Internet Assigned Numbers Authority) (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8). São alguns exemplos de curvas: secp384r1, brainpoolP512r1 e x25519.

Usaremos a curva NIST P-384, definido em https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (NIST), que é a curva atualmente usada pela Estônia. (https://www.johndcook.com/blog/2019/05/11/elliptic-curve-p-384/).

3.3 Certificados digitais e PKI

Em 1988, surge o **certificado digital** com a publicação da primeira versão do padrão X.509 (https://www.itu.int/rec/T-REC-X.509-198811-S). Os certificados digitais são documentos eletrônicos usados para provar a identidade do proprietário de uma chave pública, e incluem as informações do proprietário e sua assinatura digital. Assim, o certificado digital auxilia a implementação da criptografia de chave pública (https://www.ibm.com/docs/en/sdk-java-technology/8?topic=processes-public-key-certificates), como veremos a seguir.

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, https://datatracker.ietf.org/doc/html/rfc8446). 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** (PKI) (WILSON, 2005 https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.753&rep=rep1&type=pdf).

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.

Em 2001, foi instituido o órgão público no Brasil responsável pela certificação digital no país, chamado de **ICP-Brasil** (Infraestrutura de Chaves Públicas Brasileira) (http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm). 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.

3.4 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 98% dos estonianos o possuem (https://e-estonia.com/solutions/e-identity/id-card/) e o documento é usado em várias atividades cotidianas dos cidadãos, como internet banking, assistência médica e até eleições.

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 (https://dspace.ut.ee/handle/10062/71481): o ID-card tem duas chaves privadas com seus respectivos certificados digitais X.509, e chaves simétricas para operações usadas pela fabricante.

Uma das chaves privadas é a chave de autenticação. Essa chave é usada para fazer login 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.

A outra chave privada é a chave de assinatura digital. Essa chave é usada para vincular assinaturas digitais que, sobre a regulamentação europeia eIDAS, são reconhecidas como assinaturas válidas.

As chaves de criptografia simétrica são pré-carregadas no cartão para que o fabricantes 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.

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 (https://learn.e-resident.gov.ee/hc/en-us/articles/360000624498-How-to-use-your-digital-ID).

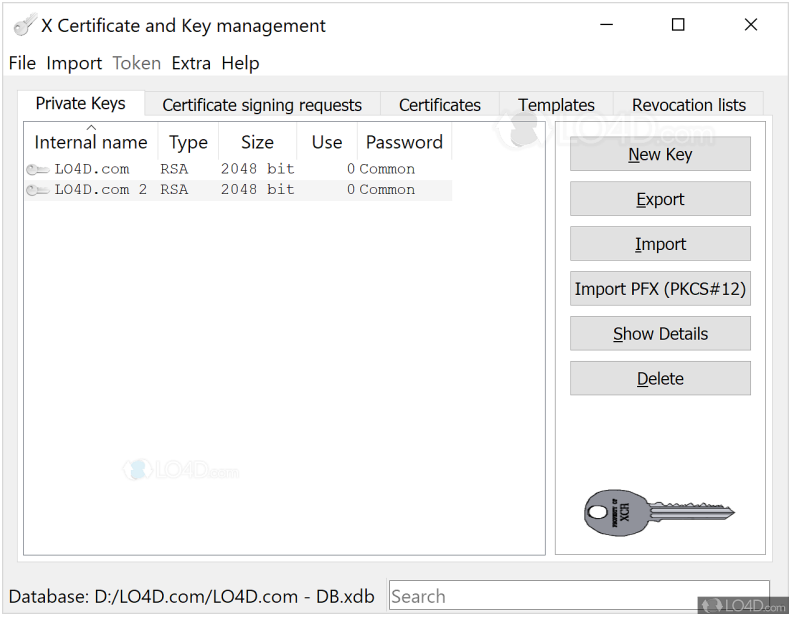
Outros países também usam a identificação digital, sendo eles:

- Bélgica (https://eid.belgium.be/en/what-eid)
- Cazaquistão (https://egov.kz/cms/en/categories/passport)
- Holanda (https://www.digid.nl/en/)
- Itália (https://www.cartaidentita.interno.gov.it/, em italiano)
- Espanha (https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf, em espanhol), etc.

4. Solução proposta

Para o desenvolvimento da solução deste trabalho, pretende-se usar o XCA e o OpenSSL para simular a geração de chaves e certificados, e a infraestrutura de chave pública (PKI).

O XCA (X-Certificate and Key Management) é uma aplicação open-source (https://github.com/chris2511/xca/) cujo objetivo é gerenciar certificados X.509, requisições de certificados, chaves assimétricas (RSA, DSA e EC), smartcards e CRLs (Listas de Revogação de Certificados). O XCA armazena as informações criptográficas em um banco de dados relacional SQL, o que permite a integração com outras aplicações facilmente.



O OpenSSL é uma biblioteca open-source (https://github.com/openssl/openssl) escrita em C e que implementa duas bibliotecas: biblioteca de criptografia, que provê funções criptográficas como AES, RSA, SHA3 etc., e a biblioteca TLS/SSL que implementa protocolos TLS/SSL (SSL, TLS 1.2, TLS 1.3, DTLS etc.). O OpenSSL possui algumas alternativas, como o LibreSSL, BoringSSL e Google Tink, todos open-source, fork do OpenSSL e que têm como objetivo resolver alguns problemas do OpenSSL, mas que são menos populares.

OpenSSL
Cryptography and SSL/TLS Toolkit

```
┌──(kousekip㉿ako-kaede-mirai)-(04:53pm)-(07/22)─┐
└─(Documents)─$ openssl x509 -in lets-encrypt-r3.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Validity
            Not Before: Sep  4 00:00:00 2020 GMT
            Not After : Sep 15 16:00:00 2025 GMT
        Subject: C = US, O = Let's Encrypt, CN = R3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
                    92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
                    2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
                    94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
                    a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
                    e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
                    37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
                    45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
                    60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
                    d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
                    30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
                    c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
                    e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
                    a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
                    09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
                    63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
                    a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
                    db:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
            X509v3 Authority Key Identifier:
                keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E

            Authority Information Access:
                CA Issuers - URI:http://x1.i.lencr.org/
```

<citar figuras>

Como a proposta é avaliada, não só pela eficiência e eficácia, mas pela acessibilidade de quem é beneficiado, é importante o fato que as ferramentas usadas são open-source e gratuitas. O XCA é uma solução por si só e de fácil uso, enquanto que o OpenSSL é a biblioteca mais usada por servidores HTTPS e possui muitos exemplos e casos de uso para referência, além da integração com muitas aplicações diferentes.

4.1 Preparação do PKI

4.1.1 Configuração do certificado raiz

4.2 Emissão da carteira de identidade

4.2.1 Geração das chaves

As chaves serão geradas usando o software XCA e serão chaves ECC P-384, o que significa que utilizaremos criptografia de curvas elípticas, considerando a curva P-384.

4.2.2 Criação do certificado

4.2.3 Inserção dos dados pessoais

5. Testes

6. Conclusão e discussão

7. Trabalhos futuros

8. Referências Bibliográficas

ARAÚJO, Carla; ANDRETTA, Filipe. **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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

CAIXA ECONÔMICA FEDERAL. **Auxílio Emergencial 2021**. CAIXA. Disponível em: https://www.caixa.gov.br/auxilio/auxilio2021/Paginas/default.aspx. Acesso em: 14 jul. 2021.

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.

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.

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 de janeiro de

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.

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.

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.

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.