

# Notas sobre Verificação de Identidade Digital

Ermogenes Palacio

Março de 2022

## Abstract

Notas sobre o processo de verificação de identidade digital, com foco na prestação de serviços públicos por entidades governamentais. O problema é apresentado, acompanhado de técnicas para o tratamento do problema e considerações úteis para aquisição de serviços de terceiros.

## Sumário

<b>1</b>	<b>O problema</b>	<b>2</b>
<b>2</b>	<b>Técnicas</b>	<b>3</b>
2.1	Verificação de identidade do mundo real com foco em documentos	3
2.2	Afirmação de identidade do mundo real com foco em dados . . .	4
2.3	Afirmação de identidade com foco em dispositivos . . . . .	5
2.4	Afirmação de identidade com foco em atributos digitais . . . . .	6
2.5	Afirmação de identidade com foco em análise de comportamento	7
2.6	Afirmação de identidade com foco em número de telefone . . . .	7
<b>3</b>	<b>BYOI - <i>Bring Your Own Identity</i></b>	<b>8</b>
3.1	Redes Sociais . . . . .	8
3.2	Governo . . . . .	9
3.3	Instituições Financeiras . . . . .	11
3.4	Operadoras de Telefonia . . . . .	12
3.5	Uso Corporativo e Provedores de BYOI . . . . .	13
<b>4</b>	<b>Considerações para aquisição</b>	<b>14</b>
4.1	Viés demográfico . . . . .	14
4.2	Corroboração de identidade . . . . .	15
4.3	Orquestração . . . . .	16
<b>5</b>	<b><i>Features</i> de provedores de identidade</b>	<b>16</b>
5.1	Integração . . . . .	16
5.2	Captura de imagens de documentos . . . . .	17
5.3	Cobertura de formatos . . . . .	17
5.4	<i>Selfie</i> e <i>liveness detection</i> . . . . .	17
5.5	NFC, códigos de barras e QR Codes . . . . .	17
5.6	Automação . . . . .	17
5.7	Acurácia . . . . .	17
5.8	Gestão do viés demográfico . . . . .	17

5.9	Armazenamento de dados de identidade . . . . .	17
5.10	Conexões com terceiros . . . . .	17
5.11	Deduplicação . . . . .	17
5.12	Autenticação . . . . .	17
5.13	Aumento de dados de perfil . . . . .	18
5.14	<i>Dashboards</i> e relatórios . . . . .	18
<b>6</b>	<b>Fornecedores</b>	<b>18</b>
<b>7</b>	<b>Referências</b>	<b>18</b>

## 1 O problema

O clamor pela transformação digital e a pressão por serviços remotos nos períodos pandêmico e pós-pandêmico são motores de inovação e exigem criteriosos requisitos de segurança e privacidade.

Qualquer serviço digital que permita o registro ou criação de contas (*onboarding*) está passível de fraude por parte do usuário solicitante, variando de contas *fake* (onde o usuário não corresponde a uma pessoa legítima) a impersonificação (onde um agente malicioso se passa por uma pessoa legítima).

Devido à dificuldade e ao alto custo muitos serviços abrem mão da verificação, assumindo os riscos de negócio e de imagem. Porém, a alternativa nem sempre pode ir à mesa devido à regulações, *compliance* ou necessidades de verificação rígidas associadas a custo, requisitos de negócio e privacidade. Redes sociais são exemplos de indústrias com baixo foco em verificação (e alta poluição com perfis *fakes*), em oposição às *fintechs* (com seus processos de *onboarding* 100% remotos).

Projetos governamentais frequentemente fazem esse tipo de análise de *trade-off*. Isso parece estar mudando, evidências dadas pelas iniciativas federal (gov.br<sup>1</sup>), estadual (LoginSP<sup>2</sup>) e municipal (Login Único<sup>3</sup>) (entre tantas outras) de centralização de identidade do cidadão.

No Brasil esse processo é reconhecidamente complexo devido à inexistência de cadastros compreensivos unificados com um nível de completude capaz de atender a diferentes casos de uso, e à miríade de documentos de identificação em suas múltiplas versões.

Nesse cenário, serão discutidas alternativas para a implantação da verificação de identidade em um cenário plausível de uma aplicação governamental para prestação de serviços ao cidadão, onde ao se registrar é requerida a genuína verificação da identidade do próprio usuário, bem como sua presença física junto ao dispositivo no ato do cadastro.

*Verificação de identidade*, neste texto, se refere a combinação de diversas atividades realizadas durante o evento de interação onde o usuário alega possuir

<sup>1</sup><https://acesso.gov.br/>

<sup>2</sup><https://login.sp.gov.br/>

<sup>3</sup><https://legislacao.prefeitura.sp.gov.br/leis/decreto-60663-de-25-de-outubro-de-2021/detalhe>

uma identidade no mundo real, geralmente em sua primeira interação (registro, cadastro, *onboarding* e afins). Em diversos níveis de tolerância, busca-se verificar se a alegação procede, confirmando se a identidade real existe, se o usuário alegando posse da identidade é o seu verdadeiro possuidor, e se sua presença durante o processo é genuína.

Além da verificação, outros métodos podem ser utilizados, com menor nível de confiabilidade, para adicionar evidências de suporte à verificação. Vamos chamá-los de métodos de *afirmação de identidade*. Seu uso como única fonte de verificação é desencorajado.

Buscaremos alternativas à tradicional (e altamente confiável) verificação presencial de identidade realizada por agentes públicos em balcões de atendimento físicos, como no caso do serviço de identidade paulistano Senha Web<sup>4</sup>, em prol de soluções nativamente remotas em canais digitais.

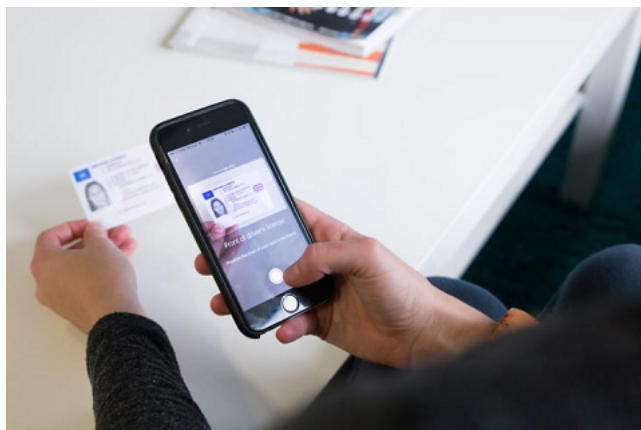
## 2 Técnicas

Várias alternativas são disponibilizadas pelo mercado. As soluções mais robustas devem utilizar a combinação de diversas técnicas para alcançar um nível de confiabilidade adequado ao problema.

Abaixo, algumas das alternativas.

### 2.1 Verificação de identidade do mundo real com foco em documentos

Consiste no uso de dispositivos de captura de imagem (*webcams* ou câmeras de *smartphones*) em canais digitais remotos (tipicamente aplicações baseadas em *browser* ou aplicativos *mobile*) para obtenção de imagens ou vídeos de documentos físicos.



Captura de documento em aplicação *mobile* (Imagem: biometricupdate.com)<sup>5</sup>

A partir da captura podemos:

<sup>4</sup><https://www.prefeitura.sp.gov.br/cidade/secretarias/fazenda/servicos/senhaweb/>

<sup>5</sup><https://www.biometricupdate.com/201905/digital-identity-and-document-verification-market-to-generate-15-billion-by-2024>

- identificar o documento (é um documento conhecido? é um RG<sup>6</sup> ou uma CNH?);
- buscar por sinais de adulteração e falsificação;
- realizar OCR dos textos;
- obter a foto de identificação.

Normalmente esse processo está associado a um mecanismo de detecção de presença “ao vivo” (*Liveness Detection*, ou *Presentation Attack Detection*). Nesse caso, a foto do documento é comparada com uma *selfie* do usuário (imagem ou vídeo) tirada no durante o processo. Caso haja uma base prévia de imagens confiável, também é possível realizar o reconhecimento facial.



Reconhecimento facial de *selfie* (Imagem: computerid.com.br)<sup>7</sup>

Este método entrega um nível aceitável de confiança, dadas as verificações de “algo que *somente você possui*” (seu documento) e de “algo que *somente você é*” (sua face).

A técnica também é conhecida como “ID+*selfie*” ou “eKYC” (*electronic- Know Your Consumer*).

## 2.2 Afirmação de identidade do mundo real com foco em dados

Consiste na comparação dos dados fornecidos pelo usuário (nome, data de nascimento, endereço, ...) com bases de dados confiáveis (registros governamentais, dados censitários, dados financeiros, ...).

Pode se manifestar como uma verificação passiva (os dados são fornecidos pelo usuário e verificados pela aplicação) ou por algum método de desafio-resposta (onde o usuário é desafiado a responder corretamente a alguma pergunta criada com base em seus dados conhecidos previamente pela aplicação).

<sup>6</sup><https://www.terra.com.br/noticias/infograficos/nova-carteira-de-identidade/index.htm>

<sup>7</sup>[https://computerid.com.br/solucoes/solucoes\\_view.php?c=10&s=16&p=9](https://computerid.com.br/solucoes/solucoes_view.php?c=10&s=16&p=9)

Vamos criar sua conta gov.br confirmando alguns de seus dados pessoais?

1. Qual é o seu ano de nascimento ?

1982 1979 1983 1985 1981 1980 1984

2. Qual é o primeiro nome da sua mãe?

ARIADNE CORINA PETA CICALISA WILLOW TOMASA MAMAE

3. Qual é o seu dia de nascimento ?

25 30 23 01 02 24 05

Voltar ao início

Continuar

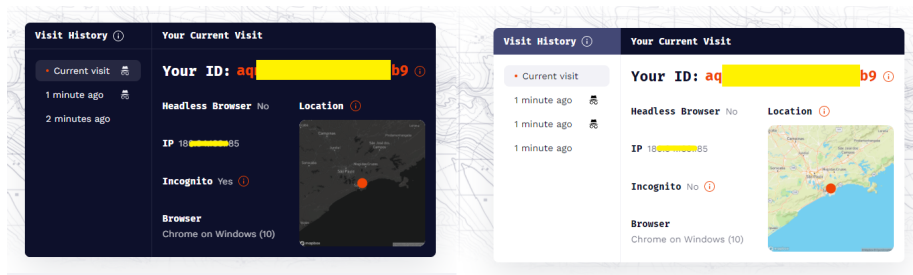
Questionário de confirmação de identidade em gov.br<sup>8</sup>

Esta técnica foi a mais utilizada pelo mercado durante muito tempo. Porém, entrega um nível baixo de confiança dada a verificação única de “algo que *não somente você sabe*” (seus dados pessoais).

Considerando o crescimento de vazamentos de dados, engenharia social e *mal-wares*, não é recomendado seu uso como verificação de identidade, mas somente como método de afirmação.

## 2.3 Afirmação de identidade com foco em dispositivos

Consiste na geração de um identificador único do usuário baseado em informações combinadas de hardware e software do dispositivo do usuário, chamado de *device fingerprint*.



Identificação do usuário mesmo em abas anônimas (fingerprintjs.com)<sup>9</sup>

Pode ser utilizado para inferir risco em alguns casos de usos, quando utilizado em acessos subsequentes. Por exemplo, várias contas sendo criadas pelo mesmo dispositivo podem ser consideradas indício de fraude, assim como o acesso pelo mesmo dispositivo onde o cadastro foi criado pode indicar um sinal de confiança.

<sup>8</sup>[http://faq-login-unico.servicos.gov.br/en/latest/\\_perguntasdafaq/contaacesso.html#cadastro-com-as-informacoes-basicas-do-cidadao](http://faq-login-unico.servicos.gov.br/en/latest/_perguntasdafaq/contaacesso.html#cadastro-com-as-informacoes-basicas-do-cidadao)

<sup>9</sup><https://fingerprintjs.com/>

## 2.4 Afirmção de identidade com foco em atributos digitais

Consiste no uso de atributos digitais (como e-mail, endereços IP e perfis em redes sociais) para afirmação de identidade, preferencialmente em correlação com identidades do mundo real.

Segundo o Gartner, o e-mail tem se provado um atributo de identidade particularmente persistente tendendo a permanecer por grandes períodos sem alteração.

Apesar de não poderem ser utilizados como identificação única e inequívoca, dados de geolocalização por IP podem ajudar a identificar fraudes caso divirjam consideravelmente do histórico do usuário ou de endereços previamente conhecidos.



The screenshot shows a web browser displaying the IP2Location website. The address bar shows the URL <https://www.ip2location.com/demo/187.15.15.85>. The page title is "IP Lookup Result". There is a "Share The Result" link. The main content is a table with the following data:

Permalink	<a href="https://www.ip2location.com/187.15.15.85">https://www.ip2location.com/187.15.15.85</a>
<input checked="" type="checkbox"/> IP Address	187.15.15.85
<input checked="" type="checkbox"/> Country	 Brazil [BR] ⓘ
<input type="checkbox"/> Region	Sao Paulo
<input type="checkbox"/> City	Santos
<input type="checkbox"/> Coordinates of City	-23.960830, -46.333610 (23°57'39"S 46°20'1"W)
<input type="checkbox"/> ISP	Claro S.A.
<input type="checkbox"/> Local Time	15 Mar, 2022 04:12 PM (UTC -03:00)
<input type="checkbox"/> Domain	claro.com.br
<input type="checkbox"/> Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
<input type="checkbox"/> IDD & Area Code	(55) 013
<input type="checkbox"/> ZIP Code	11400-000

Exemplo de dados obtidos via serviço de geolocalização por IP<sup>10</sup>

Também é comum considerar e-mails ou perfis recém-criados ou não encontrados em nenhuma base de dados como potencialmente arriscados.

<sup>10</sup><https://www.ip2location.com/demo/>

## 2.5 Afirmação de identidade com foco em análise de comportamento

Consiste na criação de perfil de usuário com base em seu comportamento (cadência de digitação, padrão de movimento de ponteiro do mouse, padrão de toque/arrasto), geralmente no primeiro uso de uma aplicação (ou de outra aplicação que compartilhe o perfil).

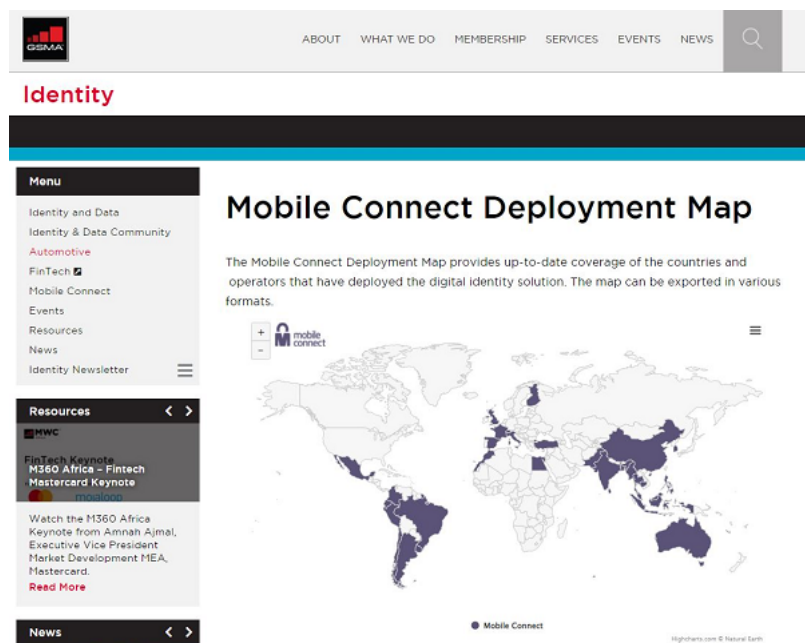
Pode ser usado para obter indícios de confiança na identidade ou de fraude. Por exemplo, usuários podem ter dificuldades no preenchimento de um formulário que um agente malicioso não apresentaria (por repetir muitas vezes, ou por ser um *bot* pré-programado).

## 2.6 Afirmação de identidade com foco em número de telefone

Consiste no uso de dados obtidos pela rede telefônica para correlacionar o usuário com uma identidade do mundo real.

Entre as possibilidades de uso estão:

- Ligação feita pelo dispositivo a uma central que identifica a chamada;
- Análise de sinal para detecção de possíveis grampos;
- Correlação de número telefônico com cadastro de proprietário;
- Idade do *SIM card* (se muito recente pode indicar risco de fraude);
- Criação de perfil de voz;
- Identificação por voz (em acessos subsequentes);
- *Login* baseado em verificação do dispositivo (por exemplo, via GSMA Mobile Connect).

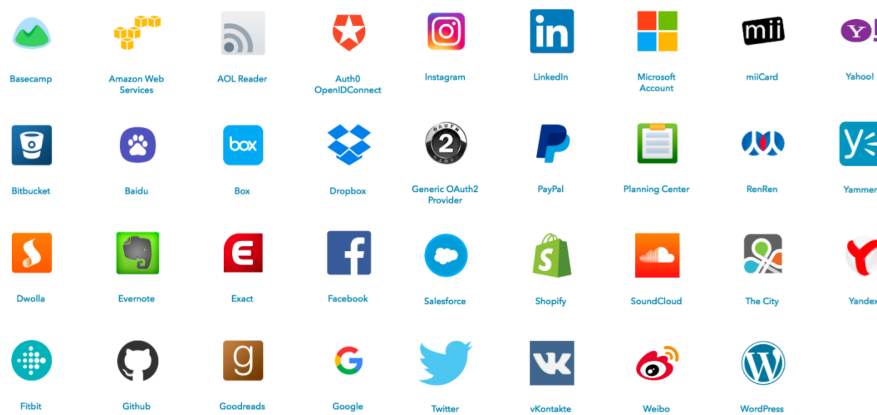


Brasil listado entre os países que suportam *GSMA Mobile Connect*<sup>11</sup>

### 3 BYOI - *Bring Your Own Identity*

Em busca de reduzir a quantidade de identidades digitais que uma pessoa gerencia, o conceito de BYOI traz a ideia de reutilização das suas identidades reconhecidas em uma fonte confiável em outros pontos de acesso.

A maioria das implementações usam *Single Sign-On* (SSO) via OAuth<sup>12</sup> e OpenID Connect<sup>13</sup>. O nível de confiabilidade esta diretamente correlacionada com a confiança no emissor.



Exemplos de serviços online que permitem login social no Auth0<sup>14</sup>

Em termos de UX, a escolha de alguns poucos provedores é preferida. A disponibilidade de muitas opções prejudica a experiência do usuário tanto visualmente (“NASCAR problem”<sup>15</sup>) quanto funcionalmente (“paradoxo da escolha”<sup>16</sup>).

#### 3.1 Redes Sociais

Identidades gerenciadas por serviços *online*, como redes sociais e e-mails (Facebook, Google, Microsoft, Apple, ...).

<sup>11</sup><https://www.gsma.com/identity/mobile-connect-deployment-map>

<sup>12</sup><https://oauth.net/>

<sup>13</sup><https://openid.net/>

<sup>14</sup><https://auth0.com/blog/social-login-on-the-rise/>

<sup>15</sup>[https://indieweb.org/NASCAR\\_problem](https://indieweb.org/NASCAR_problem)


<sup>16</sup>[https://en.wikipedia.org/wiki/The\\_Paradox\\_of\\_Choice](https://en.wikipedia.org/wiki/The_Paradox_of_Choice)






# Entrar no Slack

Recomendamos usar o endereço de e-mail que você usa no trabalho.

 Entrar com Google

 Entrar com Apple

OU

Entrar com e-mail

✧ Enviaremos um código mágico por e-mail para entrar sem senha. Você também pode [entrar manualmente](#).

Tela de *login* do Slack com opções de *login* social<sup>17</sup>

Podem garantir a diferenciação entre um usuário e outro, mas quase nada podem fazer para garantir que o usuário é quem ele diz ser (por exemplo, o possuidor de um CPF específico). O grande número de contas *fake* torna desencorajador o seu uso como único método de identificação de uma pessoa real (apesar de frequentemente ser suficiente para o comércio de produtos e serviços, por exemplo, onde a realização segura do pagamento - que independe da identidade - é o objetivo final).

Comumente são utilizadas somente para autenticação, em forma de vínculos adicionais a uma conta já verificada anteriormente.

## 3.2 Governo

Identidades digitais atestadas por uma entidade governamental responsável, geralmente carregando o peso das verificações físicas associadas.

O gov.br<sup>18</sup> e o LoginSP<sup>19</sup> são iniciativas com esse fim, e permitem a integração das identidades entre diversos sistemas governamentais com alta confiabilidade e suporte a SSO com OAuth/OpenID. Em São Paulo, o Senha Web<sup>20</sup> possui

<sup>17</sup><https://slack.com/signin#/signin>

<sup>18</sup><https://acesso.gov.br/>

<sup>19</sup><https://login.sp.gov.br/>

<sup>20</sup><https://www.prefeitura.sp.gov.br/cidade/secretarias/fazenda/servicos/senhaweb/>

verificação física de identidade em balcões de atendimento.

Senha Web permite autenticação com certificado digital<sup>21</sup>

Um exemplo híbrido é o e-CPF<sup>22</sup> (digital ou digital+físico, como nos tokens A3) que inclui as entidades certificadoras no processo, permitindo adicionalmente serviços como assinatura digital de documentos.



e-CPF físico (A3) emitido pela Prodesp<sup>23</sup>

É utilizado, por exemplo, para afirmação de identidade no gov.br<sup>24</sup>, e como método de autenticação no Senha Web<sup>25</sup>.

<sup>21</sup><https://senhawebsite.prefeitura.sp.gov.br/>

<sup>22</sup><https://certificadodigital.imprensaoficial.com.br/certificados-digitais/e-cpf>

<sup>23</sup><https://certificadodigital.imprensaoficial.com.br/certificados-digitais/e-cpf>

<sup>24</sup>[http://faq-login-unico.servicos.gov.br/en/latest/\\_perguntasfaq/comoadquirircertificadodigitalpessoa fisica.html](http://faq-login-unico.servicos.gov.br/en/latest/_perguntasfaq/comoadquirircertificadodigitalpessoa fisica.html)

<sup>25</sup><https://www.prefeitura.sp.gov.br/cidade/secretarias/fazenda/servicos/senhawebsite/>

## Obter Confiabilidade por Certificado Digital

O certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

[Saiba Mais](#) | [Como obter](#)

CPF

[Voltar](#)

[Ler Certificado Digital](#)

Afirmação de identidade com certificado digital no gov.br<sup>26</sup>

O uso de documentos legíveis por máquina através de QRCode e NFC apresenta um notável potencial de expansão, pois já é suportado por alguns documentos como a CNH, passaportes e o novo RG brasileiro.

### 3.3 Instituições Financeiras

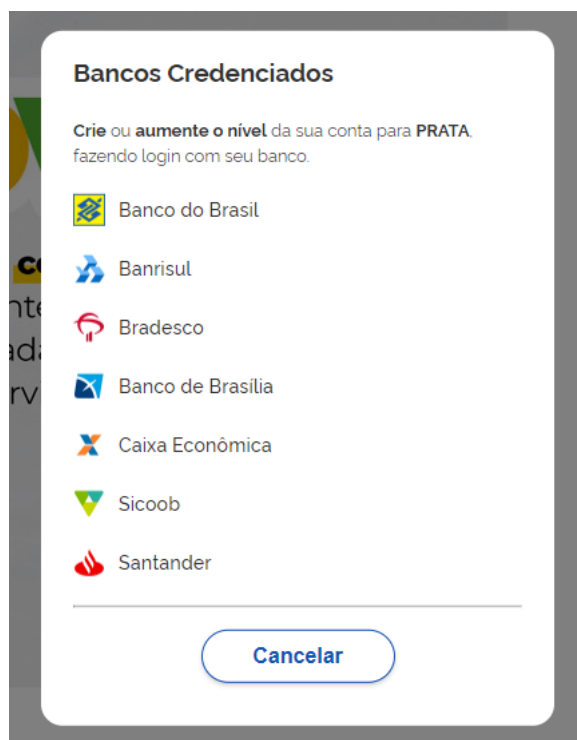
Bancos possuem uma grande base de usuários verificados (inclusive por razões de *compliance*) e podem prestar o serviço de verificação de identidade.

Com o crescimento do padrão Open Banking<sup>27</sup> isso se torna uma realidade factível e de simples implementação, tornando os bancos em potenciais provedores de identidade para SSO.

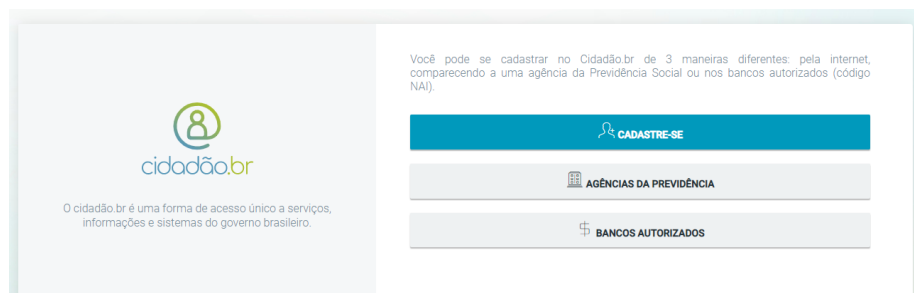
No processo de registro do gov.br dois métodos são disponibilizados em parceria com instituições bancárias. Em um deles usa-se SSO, e no outro gera-se um código de verificação (código NAI do *cidadão.br*/DataPrev) no *internet banking* que é validado no processo de registro.

<sup>26</sup>[http://faq-login-unico.servicos.gov.br/en/latest/\\_perguntasfaq/comoadquirircertificadodigitalpessoaafisica.html#como-atribuir-o-selo-certificado-digital-de-pessoa-fisica](http://faq-login-unico.servicos.gov.br/en/latest/_perguntasfaq/comoadquirircertificadodigitalpessoaafisica.html#como-atribuir-o-selo-certificado-digital-de-pessoa-fisica)

<sup>27</sup><https://openbankingbrasil.org.br/>



SSO com instituições bancárias no gov.br<sup>28</sup>



Uso do NAI no registro do cidadão.br<sup>29</sup>

### 3.4 Operadoras de Telefonia

O padrão GSMA Mobile Connect<sup>30</sup> permite que operadoras de telefonia disponibilizem serviços de identidade com alta portabilidade, vinculados aos *SIM cards* dos dispositivos.

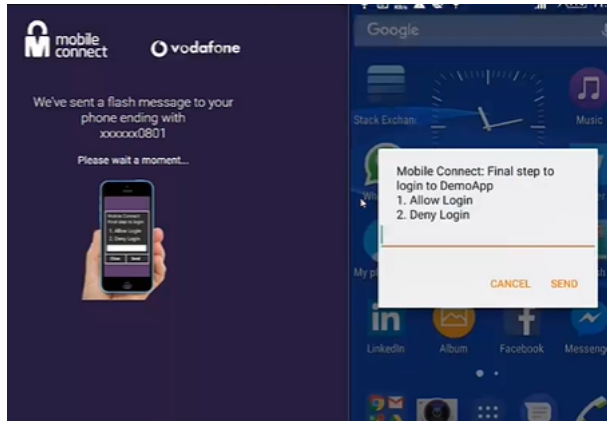
A autenticação e a afirmação são aplicações práticas, porém a confiabilidade da verificação varia de acordo com os requisitos nacionais de identificação no registro de compra de *SIM cards*, além de possuir cobertura limitada a poucos países (o Brasil é um deles).

<sup>28</sup><https://acesso.gov.br/>

<sup>29</sup>[https://mte.api.dataprev.gov.br/auth/login?pat\\_first\\_access=true](https://mte.api.dataprev.gov.br/auth/login?pat_first_access=true)

<sup>30</sup><https://www.gsma.com/identity/mobile-connect>

Sua operação permite o SSO aprovado automaticamente quando solicitado pelo próprio dispositivo, ou então a confirmação via SMS caso em outro dispositivo.

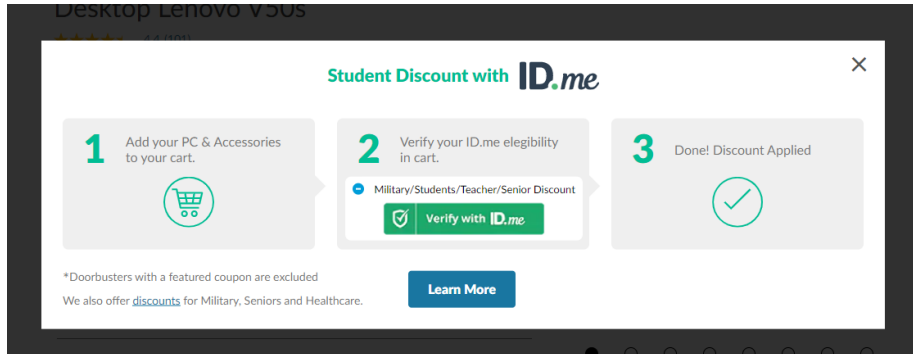


Exemplo de implementação de Mobile Connect com WSO2<sup>31</sup>

No futuro deve incluir biometria nos cadastros, o que pode simplificar o processo e melhorar a confiabilidade.

### 3.5 Uso Corporativo e Provedores de BYOI

O mercado corporativo de verificação de identidade é bastante variado, incluindo provedores de identidade com as mais diversas fontes de verificação.



O provedor ID.me possui *compliance* para diversos serviços governamentais americanos. Imagem: Lenovo.com<sup>32</sup>

Além disso, organizações costumam integrar seus próprios diretórios de colaboradores como fontes de identidade, normalmente usando LDAP e Active Directory.

<sup>31</sup><https://wso2.com/library/webinars/2016/11/securing-access-to-saas-apps-with-gsma-mobile-connect/>

<sup>32</sup><https://www.id.me/business>



Acesso usando conta Azure AD integrada para alunos das Escolas Técnicas Estaduais<sup>33</sup>

## 4 Considerações para aquisição

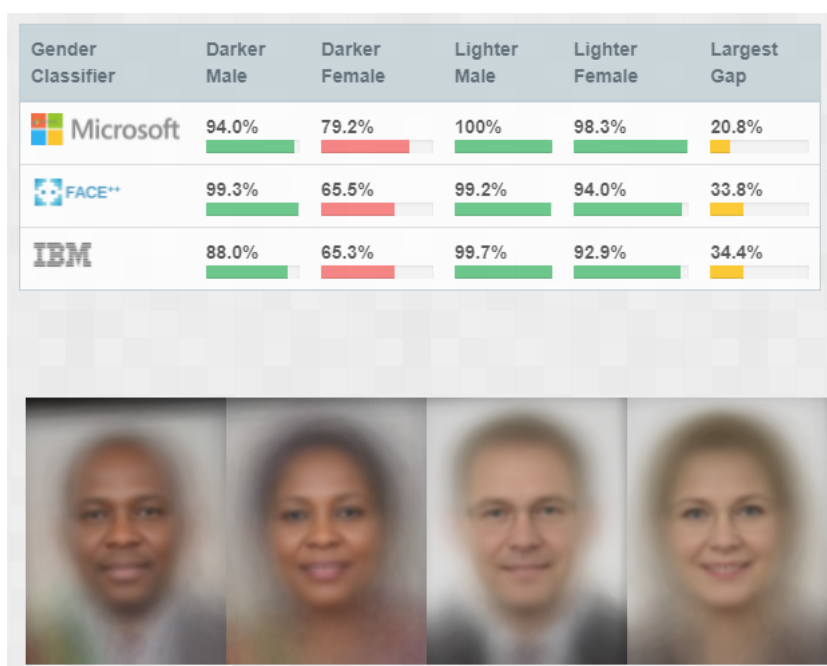
### 4.1 Viés demográfico

As soluções de detecção facial são probabilísticas e dependem dos seus algoritmos e dos seus dados de treinamento. Há diversos<sup>34</sup> estudos<sup>35</sup> que mostram diferença significativa nos resultados de acordo com características demográficas como sexo, idade e etnia.

<sup>33</sup><http://etec.sp.gov.br/>

<sup>34</sup><https://arxiv.org/pdf/2103.01592.pdf>

<sup>35</sup><http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>



Algoritmos possuem menor precisão ao avaliar mulheres negras, segundo o estudo do GenderShades<sup>36</sup>

Dois tipos de erros são mais comuns:

- Falso positivo: duas imagens de pessoas diferentes são avaliadas como a mesma pessoa;
- Falso negativo: duas imagens da mesma pessoa são avaliadas como pessoas diferentes.

Segundo o Gartner, o número de falsos positivos entre pessoas asiáticas pode chegar a ser 100 vezes maior do que entre caucasianos. Esse número é reduzido em algoritmos desenvolvidos na Ásia. Falsos negativos são mais comuns em mulheres e pessoas jovens.

É importante avaliar os resultados e medir os riscos de negócio, legais e de imagem.

## 4.2 Corroboração de identidade

A afirmação baseada em dados normalmente se baseia em dados de fontes autoritativas convencionais, como fontes governamentais, financeiras, postais ou eleitorais.

O uso de fontes não convencionais, como verificação em entidades parceiras, pode melhorar os resultados. Por exemplo, diferentes *e-commerces* em uma mesma rede de confiança poderiam verificar se um usuário consta em uma base compartilhada, reduzindo a possibilidade de fraude.

<sup>36</sup><http://gendershades.org/>

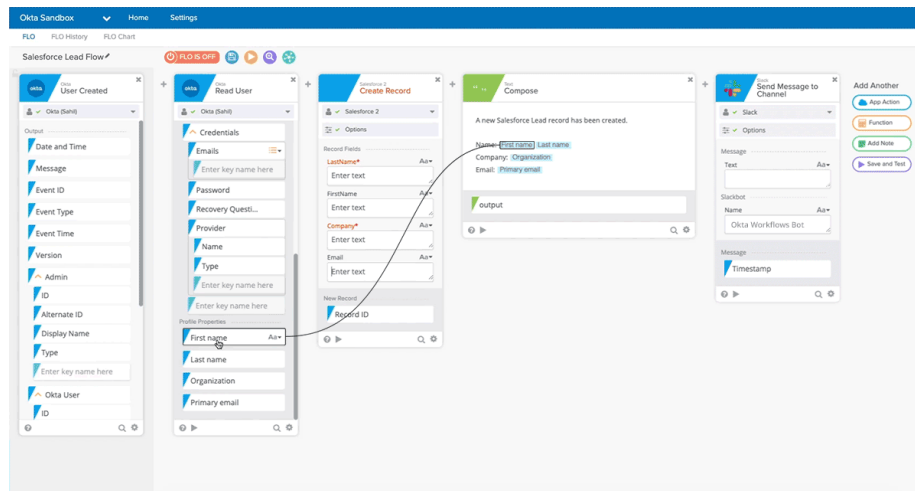
Dados de registro também podem ser comparados em bases de dados de vazamentos, que poderiam indicar um possível uso indevido.

### 4.3 Orquestração

Quanto maior o rol de funcionalidades que o caso de uso exija, menor será a chance de encontrar um fornecedor que as ofereça em um único produto. O grande desafio que se apresenta é realizar a orquestração dos diversos provedores em um *workflow* robusto que não degrade a experiência do usuário, aumente a complexidade da solução, ou os custos. Um único ponto de integração é o ideal.

São características de um orquestrador:

- Configuração de *workflows* (registro, autenticação, recuperação, ...), preferencialmente em estilo *no-code*;
- Integração entre diversos fornecedores de verificação e afirmação;
- Normalização dos diferentes formatos de dados obtidos;
- Gestão de políticas de *workflow*, de forma a controlar a UX (*go/no-go*);
- Ferramentas de análise e monitoramento;
- Flexibilidade para execução de testes A/B, facilitando a mudança de políticas;
- Redundância de *workflows* entre diferentes fornecedores.



Interface de configuração de *workflow* de identidade do Okta<sup>37</sup>

## 5 *Features* de provedores de identidade

### 5.1 Integração

Suporte a aplicações web e *mobile*, disponibilização de SDKs e APIs, *deploys on premises* ou *cloud*.

<sup>37</sup><https://www.okta.com/platform/workflows/workflows-for-lifecycle-management/>



## **5.2 Captura de imagens de documentos**

Disponibilização de interface amigável de captura.

## **5.3 Cobertura de formatos**

Identificação e OCR de diferentes documentos de diversas geografias, e seu processo de manutenção contínua.

## **5.4 *Selfie e liveness detection***

Interface para captura ao vivo de *selfie*, permitindo verificação da presença do usuário.

## **5.5 NFC, códigos de barras e QRCodes**

Suporte à extração de dados previamente armazenados em diferentes mídias.

## **5.6 Automação**

Uso de processos automatizados na maioria dos casos, usando validação por analistas somente em casos extremos.

## **5.7 Acurácia**

Baixa presença de falsos positivos/negativos e alta detecção de fraudes.

## **5.8 Gestão do viés demográfico**

Existência de métricas e clareza no trato da questão.

## **5.9 Armazenamento de dados de identidade**

Clareza e controle do cliente sobre os métodos e locais de armazenamento dos dados que identificam um usuário.

## **5.10 Conexões com terceiros**

Disponibilidade de integrações para verificação e afirmação pré-construídas, e facilidade na configuração/construção de novas.

## **5.11 Deduplicação**

Detecção e tratamento de duplicação de identidades.

## **5.12 Autenticação**

Configuração de diferentes fluxos para registro, autenticação e recuperação de contas de acordo com os requisitos do negócio.

### 5.13 Aumento de dados de perfil

Dados que o provedor é capaz de adicionar a um perfil criado, por exemplo usando dados públicos ou parcerias de integração.

### 5.14 *Dashboards* e relatórios

Ferramentas de gestão do processo.

## 6 Fornecedores

Abaixo, uma lista **não extensiva** de fornecedores de serviços de verificação identidade. Foram listados somente *players* em que foi possível encontrar alguma referência de atendimento ao Brasil.

- Acuant<sup>38</sup> \*
- Daon<sup>39</sup> \*
- Serasa Experian<sup>40</sup> \*
- Idemia<sup>41</sup> \*
- Idwall<sup>42</sup>
- Jumio<sup>43</sup> \*
- Trulioo<sup>44</sup> \*
- Unico<sup>45</sup>
- 4stop<sup>46</sup> \*

\* constantes em listagens do Gartner

## 7 Referências

- KHAN, Akif; CARE, Jonathan. Market Guide for Identity Proofing and Affirmation. Gartner, 2020.
- KHAN, Akif; CARE, Jonathan. Buyer's Guide for Identity Proofing. Gartner, 2021.
- TERHORST, Philipp; KOLF, Jan N; *et al.* A Comprehensive Study on Face Recognition Biases Beyond Demographics<sup>47</sup>. Journal of Latex class files, vol. 14, no. 8, 2015.
- BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification<sup>48</sup>. Proceedings of Machine Learning Research 81:1–15, 2018.

---

<sup>38</sup><https://www.acuant.com/>

<sup>39</sup><https://www.daon.com/>

<sup>40</sup><https://www.serasaexperian.com.br/solucoes/crosscore/>

<sup>41</sup><https://www.idemia.com/>

<sup>42</sup><https://idwall.co/>

<sup>43</sup><https://www.jumio.com/>

<sup>44</sup><https://www.trulioo.com/>

<sup>45</sup><https://unico.io/unico-check/>

<sup>46</sup><https://4stop.com/>

<sup>47</sup><https://arxiv.org/pdf/2103.01592.pdf>

<sup>48</sup><http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>



© *Prodam/SP - Núcleo de Inovação*, Março de 2022.