Ecossistemas de credenciais digitais verificáveis

Comparação entre W3C VC e ISO mdoc/mDL

Shirlei Chaves

Comitê Técnico de Gestão de Identidade
15/05/2026

RNP
ORGANIZAÇÃO SOCIAL DO MCTI
Educação, Pesquisa e Inovação em Rede

Agenda

Contextualização
Ecossistema W3C e ISO mdoc/mDL
Considerações Finais

Contextualização

- Alinhando a semântica:
  - **Credencial**: forma de apresentar alegações (*claims*) sobre uma entidade. Podem ser governamentais (carteira de motorista), educacionais (diplomas), de associações (clube, biblioteca), de comprovação de algum atributo (maior de idade), etc.
  - **Credencial digital**: credencial armazenada em formato digital, a fim de substituir ou complementar a credencial física utilizada.
  - **Credencial digital verificável**: credencial digital construída e protegida por técnicas criptográficas que permitem verificar a integridade e a autenticidade da informação contida na credencial.

Contextualização

- Dois ecossistemas dominam o debate sobre credenciais digitais verificáveis:
  - **W3C Verifiable Credentials**
    - Modelo genérico, flexível extensível, mais orientado à descentralização
  - **ISO/IEC mdoc/mDL**
    - Modelo mais prescritivo
    - Forte associação com identidades governamentais
- Ambos buscam:
  - Verificabilidade criptográfica de credenciais digitais, garantindo privacidade, reduzindo fraudes, possibilitando automação e digitalização de serviços, etc.

Contextualização

W3C VC e ISO mdoc/mDL em resumo

- **Modelo de Dados de Credenciais Verificáveis** (*VC Data Model*[1]) - VCDM) da W3C é um padrão aberto que suporta todos os tipos de credenciais:
  - Desde documentos de identidade emitidos pelo governo até certificações acadêmicas e carteiras diversas (de sócio, de clubes de benefícios, etc.)
- **ISO mdoc/mDL**: O formato mdoc (*mobile document* ou documento móvel), detalhado na norma ISO/IEC 18013-5[2], define a estrutura e as especificações para carteiras de habilitação digitais (*mDL, mobile driver license*) e, possivelmente, para outras credenciais digitais.

[1] Versão atual (Maio/2025): Verifiable Credentials Data Model v2.0

[2] ISO/IEC 18013-5:2021 - Personal identification - ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

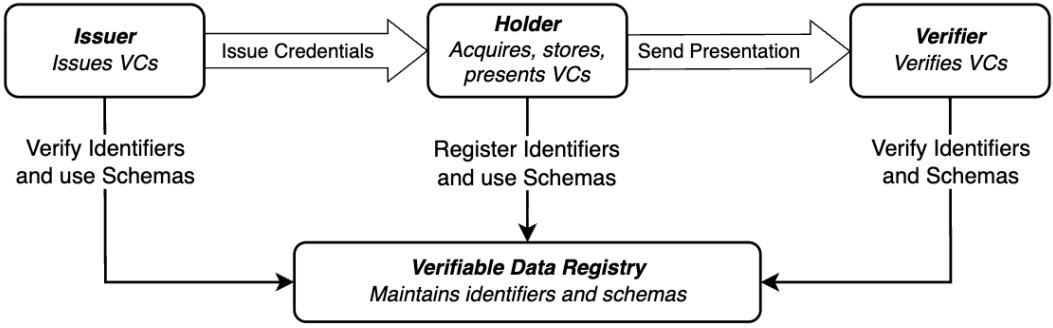
Quem são as organizações padronizadoras?

- **World Wide Web Consortium (W3C)**: principal organização internacional de padronização da Web, responsável por padrões fundamentais como HTTP, HTML, entre outros
  - Os padrões do W3C são abertos, públicos e de acesso gratuito
- **International Organization for Standardization (ISO)**: organização internacional independente e não governamental dedicada ao desenvolvimento de normas técnicas, composta por representantes dos organismos nacionais de padronização de seus países-membros
  - Normas são desenvolvidas por grupos de especialistas, chamados "comitês técnicos", e, em geral, exigem pagamento para acesso

- Tanto W3C VCDM quanto mdoc/mDL operam em um modelo de três partes composto por:
  - **Emissor** (*Issuer*): a entidade que emite a credencial para um usuário, assinando essa credencial criptograficamente de modo que possa ser verificada quando o usuário a apresenta
  - **Portador** (*Holder*): quem detém a credencial, sendo geralmente (mas não sempre) o sujeito de quem a credencial faz afirmações
  - **Verificador** (*Verifier*): entidade a quem a credencial é apresentada e que verifica a autenticidade e integridade da credencial

Ecossistema

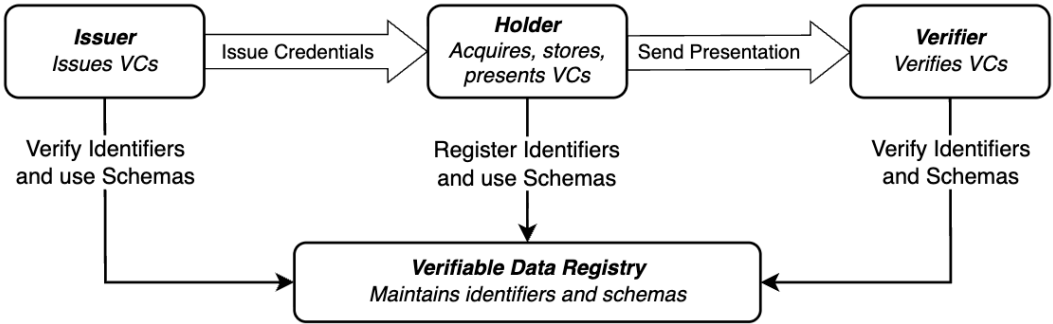
Arquitetura W3C VC



Portador (*Holder*): papel central, o qual recebe a credencial do emissor e a guarda sob seu controle. **Não há restrição quanto ao local de armazenamento da credencial.**

Ecossistema

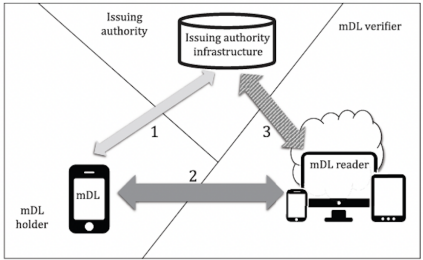
Arquitetura W3C VC



Registro de Dados Verificáveis (VDR, *Verifiable Data Registry*): Sistema confiável para gerenciar identificadores, chaves e esquemas. Dependendo da implementação, pode ser necessário consultá-lo em cada transação.

Ecossistema

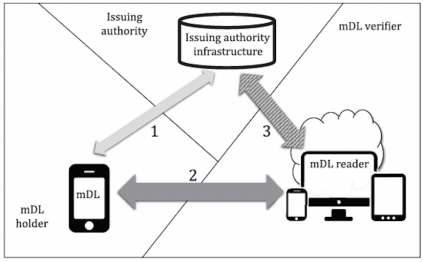
Arquitetura ISO 18013-5 mdoc/mDL



Portador (*Holder*): papel central, o qual recebe a credencial do emissor e a guarda sob seu controle. **Credencial armazenada no dispositivo para o qual foi emitida (*device binding*) ou no servidor da autoridade emissora.**

Ecossistema

Arquitetura ISO 18013-5 mdoc/mDL

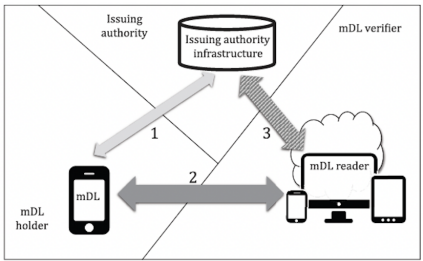


Interface 2

- Estabelecimento da conexão entre dispositivo detentor e o dispositivo leitor: engajamento via QR code ou NFC
- Recuperação de dados da credencial via dispositivo, também chamada recuperação offline

Ecossistema

Arquitetura ISO 18013-5 mdoc/mDL

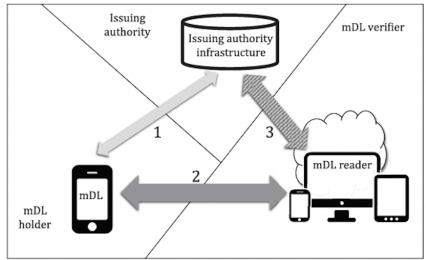


Recuperação de dados via servidor (interface 3):

- Também chamada de recuperação online
- O dispositivo leitor consulta o servidor do emissor utilizando um token fornecido pelo dispositivo com a credencial

Ecossistema

Arquitetura ISO 18013-5 mdoc/mDL



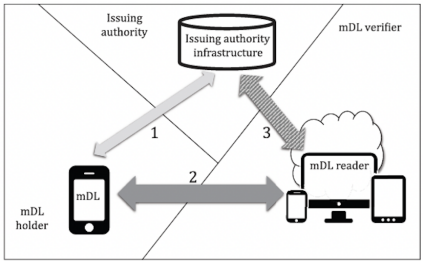
! Importante

Caso primário da ISO 18013-5 - mDL: A apresentação da credencial é presencial (*attended*), devido à proximidade entre o dispositivo detentor e o leitor da credencial. O suporte a NFC e BLE é obrigatório nesses dispositivos.

Antes da recuperação via servidor, o engajamento foi realizado pela interface 2.

Ecossistema

Arquitetura ISO 18013-5 mdoc/mDL



Confiança na autoridade emissora: Uso de Infraestrutura de Chaves Públicas (PKI).

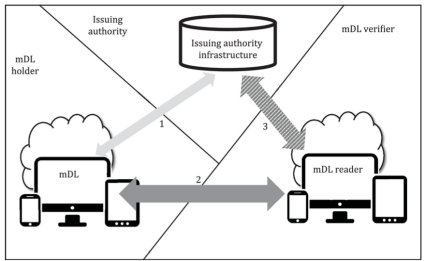
Não há VDR na arquitetura, mas, opcionalmente, a norma prevê o uso de um VICAL (*Verified Issuer Certificate Authority List*) para distribuir os certificados-raiz das autoridades emissoras (IACA) aos verificadores.

Ecossistema mdoc/mDL

- E quando a apresentação não é presencial?

Ecossistema mdoc/mDL

- E quando a apresentação não é presencial?



ISO/IEC 18013-7:2025 Personal identification - ISO-compliant driving licence Part 7: Mobile driving licence (mDL) add-on functions[3]

[3] ISO/IEC TS 18013-7:2025

Ecossistema ISO mdoc/mDL

ISO 18013-7

- Adiciona a funcionalidade de apresentar a mDL a um leitor pela internet (remotamente ou *unattended*)
- Especifica múltiplos fluxos de recuperação dos dados da credencial:
  - OID4VP[4]: para apresentações baseadas em protocolos de identidade abertos
  - Recuperação via Digital Credentials API: Integração nativa com APIs de navegadores e sistemas operacionais (ex: W3C API[5])
  - Consulta ao dispositivo via website

[4] *OpenID for Verifiable Presentations*

[5] Digital Credentials - W3C Working Draft 12 May 2026

Modelo de dados

W3C VC

- **Estrutura de dados genérica e flexível**
  - Não define atributos específicos para tipos de credenciais: apenas alguns campos básicos são padronizados (ex.: `issuer`, `credentialSubject`)
  - Esquemas/templates de credenciais podem ser criados por qualquer entidade
  - Atributos podem ser identificados por URIs globalmente únicos ou por contextos (`context`), que permitem usar nomes mais amigáveis
  - Não exige um formato único de codificação: pode usar JSON, JSON-LD, XML, YAML, CBOR etc.
  - Diferentes implementações podem representar os mesmos atributos de formas distintas
  - Interoperabilidade pode exigir especificações adicionais por caso de uso

Modelo de dados

W3C VC

Propriedade	Requisito	Resumo
`@context`	Obrigatória	Define o vocabulário e mapeia termos para URLs. O primeiro item deve ser o contexto base do W3C.
`type`	Obrigatória	Define o tipo do objeto; deve incluir pelo menos o termo *VerifiableCredential*.
`issuer`	Obrigatória	Identifica a entidade (governo, organização ou indivíduo) que emitiu a credencial.
`credentialSubject`	Obrigatória	Contém um ou mais conjuntos de afirmações (claims) sobre o sujeito da credencial.
`id`	Opcional	Um identific
`name`	Opcional	Nome concis
`description`	Opcional	Descrição te
`validFrom`	Opcional	Data e hora
`validUntil`	Opcional	Data e hora
`credentialStatus`	Opcional	Informações
`credentialSchema`	Opcional	Link para u
`refreshService`	Opcional	Link para u
`termsOfUse`	Opcional	Define as po
`evidence`	Opcional	Informações
`relatedResource`	Opcional	Garante a in

u DID.

tring Status List).

os.

la.

emissão.

s.

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "https://university.example/Credential123",
  "type": ["VerifiableCredential", "ExampleAlumniCredential"],
  "issuer": "did:example:2g55q912ec3476eba2l9812ecbfe",
  "validFrom": "2010-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "https://www.example.org/persons/pat",
    "name": "Pat",
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": "Example University"
    }
  }
}
```

Modelo de dados

W3C VC

Propriedade	Requisito	Re
@context	Obrigatória	De
type	Obrigatória	De
issuer	Obrigatória	Ide
credentialSubject	Obrigatória	Co
id	Opcional	Un
name	Opcional	No
description	Opcional	De
validFrom	Opcional	Da
validUntil	Opcional	Da
credentialStatus	Opcional	Inf
credentialSchema	Opcional	Lin
refreshService	Opcional	Lin
termsOfUse	Opcional	De
evidence	Opcional	Inf
relatedResource	Opcional	Ga

```
{
  ...
"type": ["VerifiableCredential", "ExampleDegreeCredential", "ExamplePersonCredential"],
"issuer": "https://university.example/issuers/14",
"validFrom": "2010-01-01T19:23:24Z",
"credentialSubject": {
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "degree": {
    "type": "ExampleBachelorDegree",
    "name": "Bachelor of Science and Arts"
  },
  "alumniOf": {
    "name": "Example University"
  }
},
"credentialSchema": [{
  "id": "https://example.org/examples/degree.json",
  "type": "JsonSchema"
},
{
  "id": "https://example.org/examples/alumni.json",
  "type": "JsonSchema"
}]
}
```

Modelo de dados

ISO mdoc/mDL

- **mdocs/mDL**: Esquema de dados pré-definido e padronizado.
  - Define exatamente os atributos de uma credencial e como são codificados
  - Formato baseado em CBOR (*Concise Binary Object Representation*), estrutura compacta e eficiente para ambientes com limitações como dispositivos móveis
  - O modelo da ISO 18013-5 permite criar outras credenciais além da mDL:
    - Novas credenciais podem ser definidas por namespaces próprios, os quais definem seus próprios atributos (*data elements*)
  - A mDL usa o namespace padrão `org.iso.18013.5.1` e document type (DocType) `org.iso.18013.5.1.mDL`
    - A norma recomenda namespaces no formato "domínio reverso" para evitar conflitos
  - Novos tipos de credenciais podem reutilizar os mesmos mecanismos de interoperabilidade da norma

Modelo de dados

ISO mdoc/mDL

DocType: `org.iso.18013.5.1.mDL`

namespace: `org.iso.18013.5.1`

Identifier	Name	Definition	Presence	Field format	Encoding
family_name	Family name	Last name, surname, or primary identifier, of the licence holder	M	V36AS	tstr
given_name	Given names	First name(s), other name(s), or secondary	M	V36AS	tstr
birth_date	Date of birth				
issue_date	Date of Issue	Date licence document was issued	M	full-date or date-time	tdate or #6.18013(tstr)
expiry_date	Date of Expiry	Date licence document expires	M	full-date or date-time	tdate or #6.18013(tstr)
issuing_country	Issuing country	country code as alpha 2 code, defined in ISO 3166-1, which issued the mDL or within	M	F2A	tstr
issuing_authority	Issu				
document_number	Lic				
administrative_number	Ad				
driving_privileges	Categories of vehicles/ restrictions/ conditions	Driving privileges the licence holder is authorized to drive. It consists of category issue date, expiry date, restriction/condition sign code, restriction/condition sign and restriction/condition value. See 7.4.4.	M	See 7.4.4	See 7.4.4.
un_distinguishing_sign	UN distinguishing sign	Distinguishing sign of the issuing country according to 18013-1 annex F NOTE this field is added for purposes of the UN conventions on driving licences	R	N/A	tstr
gender	Gender	Licence holder's gender: M for male, F for female, X for not specified	O	F1A	tstr
height	Height (cm) [a]	Licence holder's height in centimetres	O	F3N	uint
weight	Weight (kg) [a]	Licence holder's weight in kilograms	O	F3N	uint
eye_color	Eye colour	Licence holder's eye colour: blue, brown, black, hazel, green, grey, pink, dichromatic	O	V12A	tstr

Ecossistema ISO mdoc/mDL

mdoc/mDL


```
"version": "1.0",
"docType": "iso.org.18013.5.1.mDL",
"nameSpaces": {
    "org.iso.18013.5.1": {
      "family_name": "Doe",
      "given_name": "John",
      "birth_date": "1986-03-22",
      "issue_date": "2019-10-20",
      "expiry_date": "2024-10-20",
      "issuing_country": "AT",
      "issuing_authority": "AT DMV",
      "document_number": "123456789",
      "driving_privileges": [
        {"vehicle_category_code": "A",
          "issue_date": "2018-08-09",
          "expiry_date": "2024-10-20"},
        {"vehicle_category_code": "B",
          "issue_date": "2017-02-23",
          "expiry_date": "2024-10-20"}
      ],
      "un_distinguishing_sign": "USA"
    }
}
```

Protocolos de comunicação

W3C VC

- O VCDM da W3C não define protocolos de comunicação
  - A especificação não assume onde as credenciais serão armazenadas
  - Como o armazenamento é agnóstico, o modelo também não padroniza o transporte ou apresentação
  - Protocolos de interoperabilidade precisam ser definidos separadamente

Protocolos de comunicação

ISO mdoc/mDL

- A ISO 180130-5 define completamente os protocolos entre mDL, leitor e infraestrutura emissora (para *server retrieval*):
  - Toda transação começa com uma fase de engajamento entre os dispositivos (*device engagement*), via QR Code ou NFC: exige proximidade física
  - O protocolo permite solicitar múltiplos documentos e *namespaces* em uma única requisição
  - O leitor deve informar explicitamente cada atributo desejado
  - O holder pode aprovar ou negar o compartilhamento de cada atributo solicitado

- O VC Data Model não define um mecanismo obrigatório de assinatura ou prova
  - Requer prova de integridade e autenticidade, mas não obriga nenhum tipo particular

Segurança

W3C VC

- **Integridade/autenticidade criptográfica dos dados:** Mecanismos de provas incorporadas (*Data Integrity*) ou envelopadas (*JOSE/COSE*)

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  ...
  "credentialSubject": {
    "id": "https://subject.example/subject/3921",
    "degree": {
      "type": "ExampleBachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "DataIntegrityProof",
    "cryptosuite": "eddsa-rdfc-2022",
    "created": "2021-11-13T18:19:39Z",
    "verificationMethod": "https://university.example/issuers/14#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z58DAdFfa9SkqZMVPxAQp...jQCrfFPP2oumHKtz"
  }
}
```

Protected Headers

```
{
  "kid": "ExHkBMW9fmbkvV266mRpuP2sUY_N_EWIN1lapUzO8ro",
  "alg": "ES256"
}
```

application/vc

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
 ...
  "credentialSubject": {
    ...
  },
}
```

application/vc+jwt

eyJraWQiOiJFeEhrQk1XOWZtYmt2VjI2Nm1ScHVQMnNVWV9OX0VXSU4xbGFwVXpPOHJvIiwiYWxnIjoiRVMyNTYifQ
.eyJAY29udGV4dCI6WyJodHRwczovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMvdjIiLCJodHRwczovL3d3dy53My5vcmcvbn
MvY3JlZGVudGlhbHMvZXhhbXBsZXMvdjIiXSwiaWQiOiJodHRwczovL3VuaXZlcnNpdHkuZXhhbXBsZS9DcmVkZW50aWFsMTIzI
iwidHlwZSI6WyJWZXJpZmlhYmxlQ3JlZGVudGlhbCIsIkV4YWlwbGVBbHVtbmlDcmVkZW50aWFsIl0sImlzc3VlciI6ImRpZDpl
eGFtcGxlOjJnNTVxOTEyZWMzNDc2ZWJhMmw5ODEyZmNiZmUiLCJ2YWxpZEZyb20iOiIyMDEwLTAxLTAxVDAwOjAwOjAwWiIsImN
yZWRlbnRpYWxTdWJqZWN0Ijp7ImlkIjoiaHR0cHM6Ly93d3cuZXhhbXBsZS5vcmcvcGVyc2ucy9wYXQiLCJuYW1lIjoiUGF0Ii
wiYWx1bW5pT2YiOnsiaWQiOiJkaWQ6ZXhhbXBsZTpjMjc2ZTEyZWMyMWViZmViMWY3MTJlYmM2ZjEiLCJuYW1lIjoiRXhhbXBsZ
S8Vbml2ZXJzaXR5In19LCJjcmVkZW50aWFsU2NoZW1hIjp7ImlkIjoiaHR0cHM6Ly91bml2ZXJzaXR5LmV4YWlwbGUvQ3JlZGVu
dGlhbDEyMy1zY2hlbWEtY3JlZGVudGlhbCIsInR5cGUiOiJKc29uU2NoZW1hQ3JlZGVudGlhbCJ9fQ .1LXVnn-oj-d-
qYXEGWuwxcRLRaUFHApgcS7YgjNwe5h1Cy_56kgeW5yGooZWmDILm0uj7CIHIfgnrT-jpHCqnA

Segurança

ISO mdoc/mDL

- Recuperação de dados via servidor usa TLS e JWS para garantir confidencialidade e autenticidade dos dados
- Recuperação de dados via dispositivo utiliza criptografia de sessão ponta a ponta
- Todas as mensagens entre mDL e leitor são autenticadas e criptografadas
- O emissor assina digitalmente o *Mobile Security Object* (MSO)
  - O MSO contém hashes de todos os atributos da credencial
  - O verificador valida hashes dos atributos e assinatura do MSO

- Certificados DS (*Document Signer*) e IACA (*Issuing Authority CA*) permitem validação da cadeia de confiança
- mdoc Authentication protege contra clonagem da credencial
  - O dispositivo usa chave privada armazenada localmente e difícil de extrair
  - A chave pública do dispositivo é assinada pelo emissor no MSO
  - O leitor valida prova criptográfica de posse da chave do dispositivo

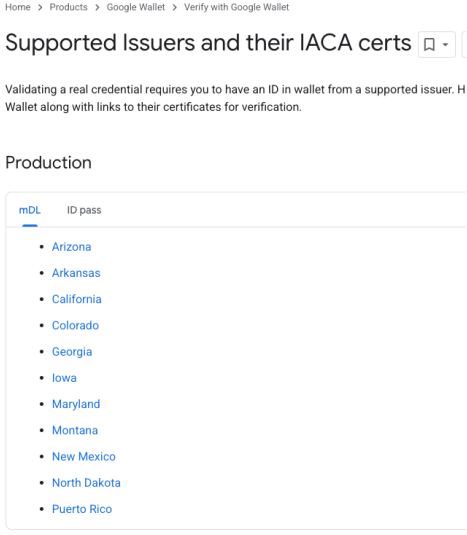
Por que o ecossistema ISO mdoc/mDL tem se destacado?

- Diversas autoridades emissoras (IA, *Issuing Authority*) de carteiras de motorista nos EUA
- Associação Americana de Administradores de Veículos Motorizados (AAMVA, *American Association of Motor Vehicle Administrators*) disponibiliza diretrizes[6] para a implementação prática de um perfil de aplicação da norma internacional ISO/IEC 18013-5
  - Proíbe implementação de recuperação de dados via servidor, prevista na ISO 18013-5 no modo presencial
- Suporte a mdoc/mDL por Google Wallet, Apple Wallet, Samsumg Wallet
- Carteiras Google Wallet, Apple Wallet sendo aceitas pelas autoridades emissoras para armazenar mDL (mais recentemente a Samsumg Wallet, pelo estado da Califórnia)

[6] Mobile Driver's License Implementation Guidelines, v1.5

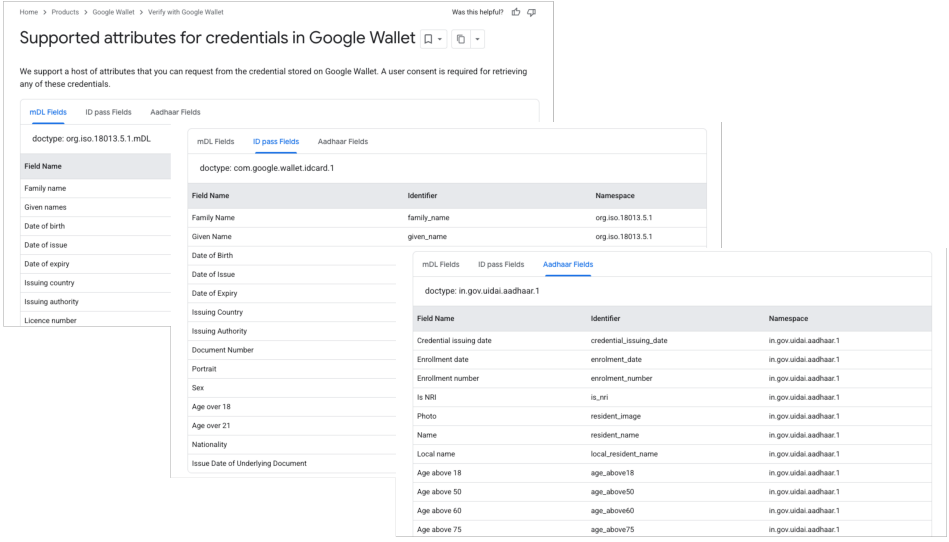
Ecossistema ISO mdoc/mDL

Google Wallet



Ecossistema ISO mdoc/mDL

Google Wallet



Home > Products > Google Wallet > Verify with Google Wallet

Was this helpful?

Supported attributes for credentials in Google Wallet

We support a host of attributes that you can request from the credential stored on Google Wallet. A user consent is required for retrieving any of these credentials.

mDL Fields | ID pass Fields | Aadhaar Fields

doctype: org.iso.18013.5.1.mDL

Field Name
Family name
Given names
Date of birth
Date of issue
Date of expiry
Issuing country
Issuing authority
Licence number

mDL Fields | ID pass Fields | Aadhaar Fields

doctype: com.google.wallet.idcard.1

Field Name	Identifier	Namespace
Family Name	family_name	org.iso.18013.5.1
Given Name	given_name	org.iso.18013.5.1
Date of Birth		
Date of Issue		
Date of Expiry		
Issuing Country		
Issuing Authority		
Document Number		
Portrait		
Sex		
Age over 18		
Age over 21		
Nationality		
Issue Date of Underlying Document		

mDL Fields | ID pass Fields | Aadhaar Fields

doctype: in.gov.uidai.aadhaar.1

Field Name	Identifier	Namespace
Credential issuing date	credential_issuing_date	in.gov.uidai.aadhaar.1
Enrollment date	enrolment_date	in.gov.uidai.aadhaar.1
Enrollment number	enrolment_number	in.gov.uidai.aadhaar.1
Is NRI	is_nri	in.gov.uidai.aadhaar.1
Photo	resident_image	in.gov.uidai.aadhaar.1
Name	resident_name	in.gov.uidai.aadhaar.1
Local name	local_resident_name	in.gov.uidai.aadhaar.1
Age above 18	age_above18	in.gov.uidai.aadhaar.1
Age above 50	age_above50	in.gov.uidai.aadhaar.1
Age above 60	age_above60	in.gov.uidai.aadhaar.1
Age above 75	age_above75	in.gov.uidai.aadhaar.1

Ecossistema ISO mdoc/mDL

NIST NCCoE

- NCCoE (*National Cybersecurity Center of Excellence*) criou um projeto envolvendo diversos participantes para acelerar o uso de mDLs[7]
  - Orientado a casos de uso: serviços financeiros (*onboarding* e KYC), serviços federados governamentais e serviços de saúde/prescrição eletrônica
  - Padrões atualmente em uso na arquitetura de referência em desenvolvimento e testes[8]: OpenID4VP, ISO 18013-5, ISO 18013-7, Digital Credentials API, WebAuthN, OAUTH 2.0, OIDC

[7] Digital Identities - Mobile Driver's License (mDL)

[8] Financial Use Case Reference Architecture

Ecossistema ISO mdoc/mDL

NIST NCCoE

- NIST Special Publication 1800-42A - Digital Identities-Mobile Driver's License (mDL)[9]
  - Guia prático que apresenta uma arquitetura de referência, exemplos de implementação, integrações tecnológicas e os principais resultados e cenários demonstrados do projeto
- Novo perfil para a NIST Special Publication 800-63A[10]: NIST 800-63A Profile for mDL Issuance [11]
  - Padronizar requisitos de emissão de mDL, incluindo validação de identidade, biometria e verificação documental, servindo como referência para aceitação por governos e instituições financeiras

[9] NIST SPECIAL PUBLICATION 1800-42A

[10] Identity Proofing

[11]

Digital Credentials API

- Digital Credentials W3C - **Working Draft**[12]

Nota

A API de Credenciais Digitais permite que sites solicitem credenciais e que usuários consintam em retornar as credenciais que carregam em carteiras digitais [a].

[a] W3C Digital Credentials API publication: the next step to privacy-preserving identities on the web

[12] Digital Credentials W3C Working Draft 12 May

Digital Credentials API

- API prevista pela ISO 18013-7
- Navegador Google Chrome já habilita por padrão desde a versão 141[13]
- Navegador Safari (26+) tem suporte com alguma limitação
- Assunto para outro estudo técnico...

[13] Digital Credentials API: Secure and private identity on the web

Considerações Finais

- **Competitivos ou Complementares?**
  - Não é possível afirmar que um modelo é categoricamente "melhor" que o outro
  - Possuem escopos, origens e maturidades técnicas diferentes
    - Ambos com tecnologias e especificações em evolução/amadurecimento
  - A ISO mdoc/mDL tem ganhado atenção por oferecer uma pilha relativamente completa de protocolos interoperáveis, já definindo modelo de dados, segurança, transporte e apresentação, o que facilita implementações diretas
  - No ecossistema W3C VC normalmente é necessário combinar vários padrões, dificultando a "percepção" de implementação mais direta
  - Coexistência possível a partir de padronização de protocolos de emissão e apresentação, como os da família *OpenID Connect for Verifiable Credentials*

Considerações Finais

- W3C VC Data Model é um framework genérico
  - Define apenas como os dados devem ser estruturados e é agnóstico em relação a protocolos de transporte e formatos de prova criptográfica
  - Oferece flexibilidade total, mas dificulta a interoperabilidade direta
  - Prioriza a soberania e portabilidade do detentor, permitindo que as credenciais sejam armazenadas em qualquer local (nuvem, múltiplos dispositivos, repositórios variados) conforme a escolha do usuário
  - Segue uma filosofia de "mundo aberto": qualquer entidade pode emitir credenciais sobre qualquer assunto
  - Modelo de confiança mais dinâmico e descentralizado

Considerações Finais

- ISO mdoc/mDL é um padrão “pilha completa”, o que traz interoperabilidade ao se seguir a norma
  - Foca forte em evitar a clonagem, não na portabilidade da credencial
  - Baseia-se em uma PKI tradicional com autoridades certificadoras governamentais (IACA) e listas de confiança (VICAL/Master List)
  - Utiliza um mecanismo robusto e já estabelecido de múltiplos hashes no Objeto de Segurança Móvel (MSO).

Muito obrigada!

Shirlei Chaves
Assistente Técnica do CT-GId