Regula

6 March 2025

Understanding Electronic IDs and Digital IDs:

Origins, Types, and Verification Capabilities

Housekeeping

Trouble with audio?
Try dialing in!

Submit your questions live
for our Q&A at the end

REC

We’re recording!
We’ll email you the link

Name/Surname

Kate Volskaya

Business role

Head of Product Marketing

Name/Surname

Dmitry Smolyakov

Business role

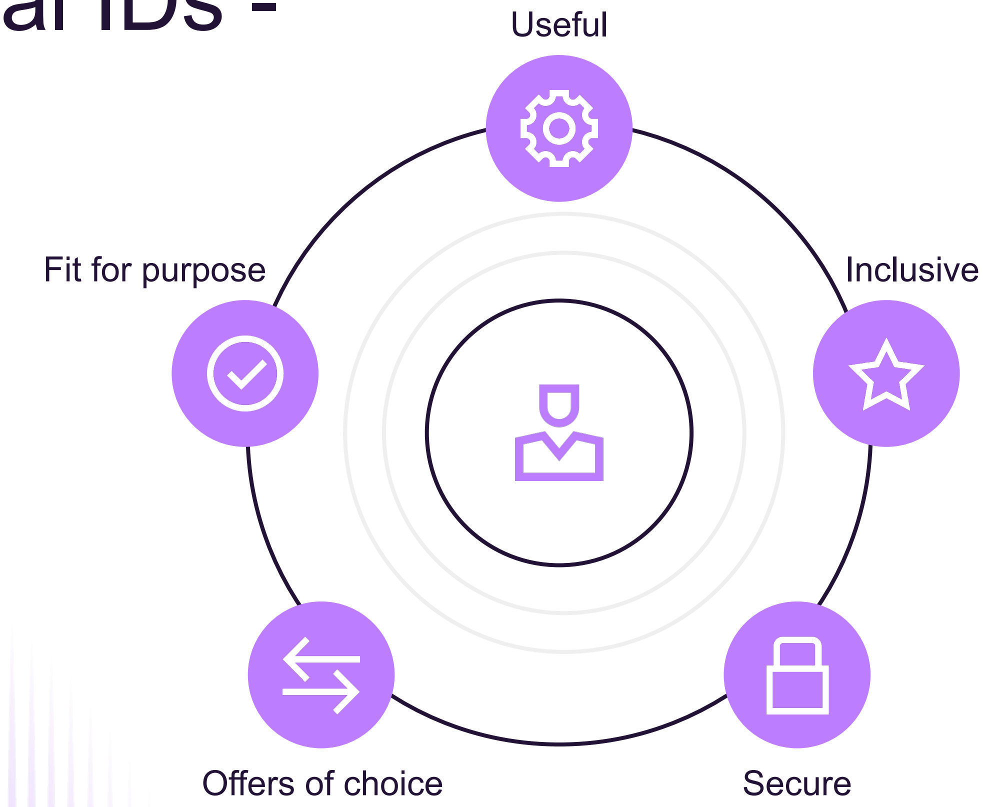
Head of Mobile and Web Development

What and Why: Electronic and Digital IDs

Electronic and Digital IDs - Definition

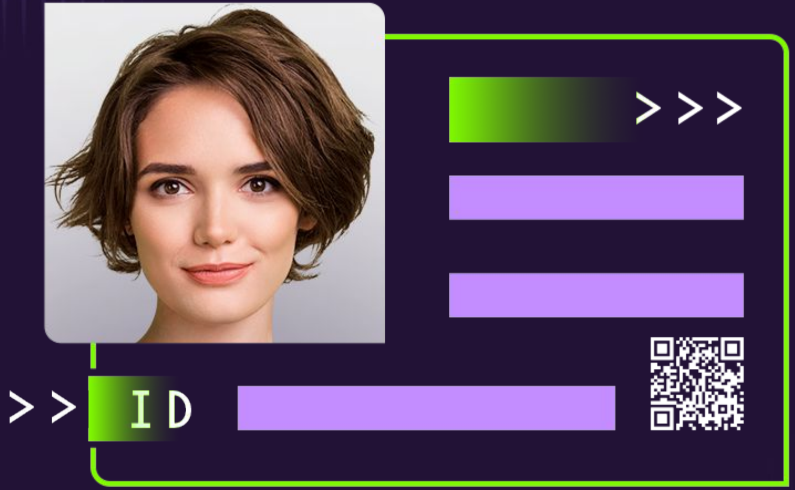
An electronic/biometric ID is a document with a contactless RFID chip that stores personal and biometric data. It can be authenticated remotely or on-site with NFC verification technology.

A digital ID is a digital copy of an individual's identity document that can be authenticated remotely or on-site over digital channels.



Electronic and Digital IDs - Why?

- → More secure
- → A way to prove identity electronically
- → Makes things easier for citizens, businesses and governments
- → Simplifies transactions by enabling access to goods and services remotely
- → Supports the right of every person to have a digital identity that is recognized everywhere



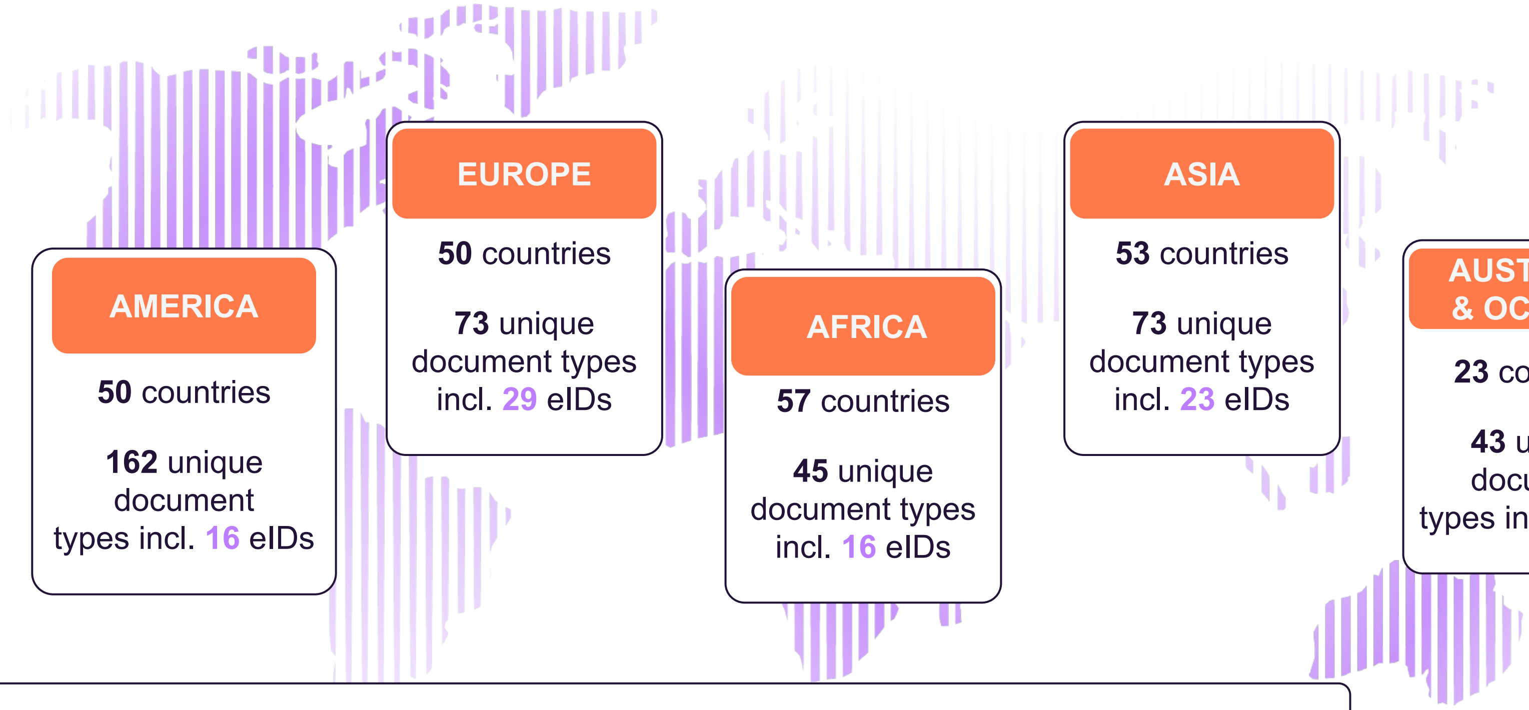
Regula Survey on Electronic IDs: Key Findings

42% of companies are actively integrating electronic and digital IDs into their systems

Online transactions are the most impacted by electronic and digital IDs

77% of respondents believe the adoption of electronic and digital identity will improve security and fraud prevention

Identity Document Coverage



AMERICA

50 countries

162 unique document types incl. 16 eIDs

EUROPE

50 countries

73 unique document types incl. 29 eIDs

AFRICA

57 countries

45 unique document types incl. 16 eIDs

ASIA

53 countries

73 unique document types incl. 23 eIDs

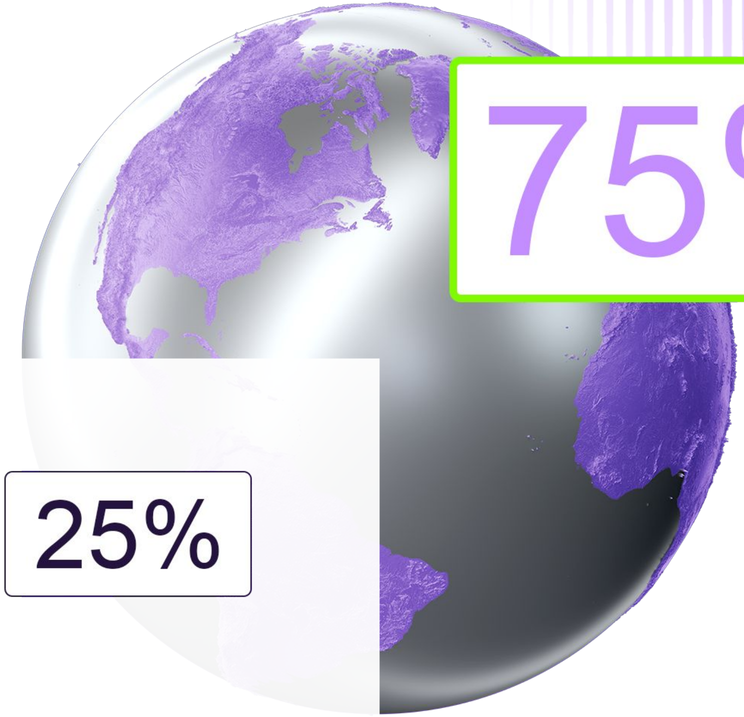
AUSTRALIA & OCEANIA

23 countries

43 unique document types incl. 9 eIDs

Traditional documents still retain a significant share among all documents, especially for use within countries. Our document template database is the most comprehensive and one of the largest, with more than 14,500 items.

Number of Electronic Identity Documents



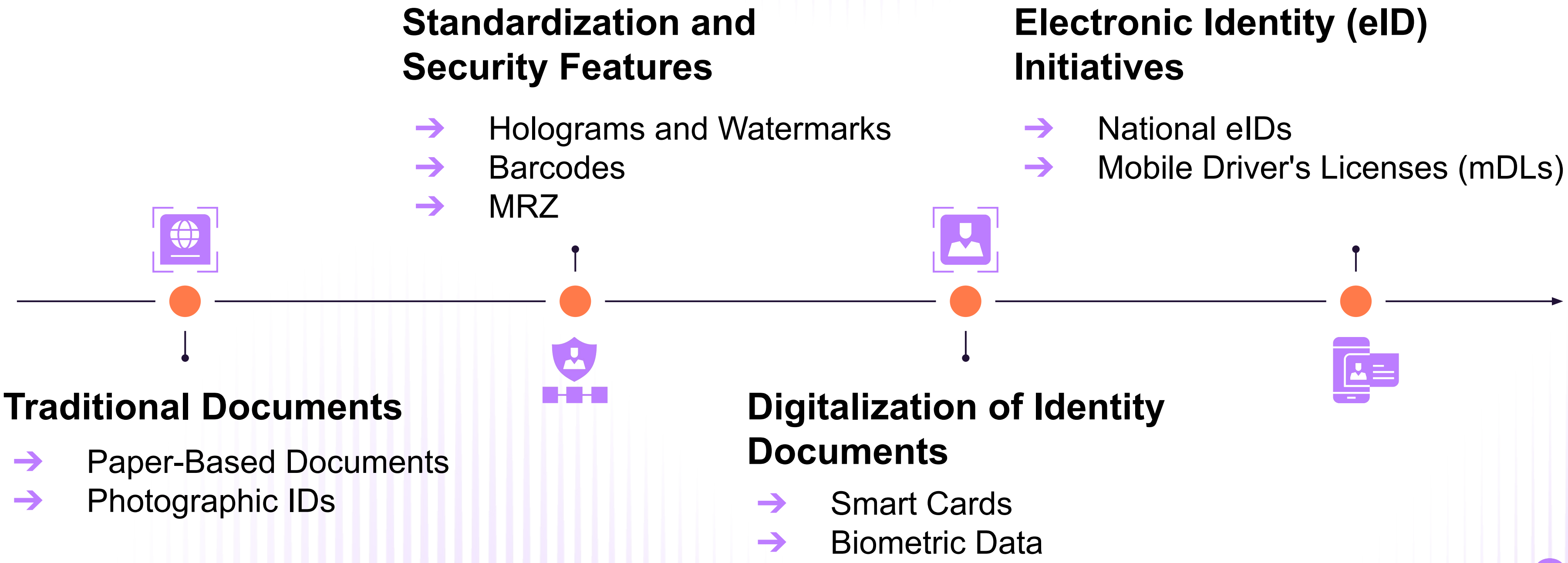
75%

of countries have biometric documents

25%

The Evolution of eIDs and Digital IDs

Historical Context: How eIDs and Digital IDs Came to Be



Traditional Documents

- → Paper-Based Documents
- → Photographic IDs

Standardization and Security Features

- → Holograms and Watermarks
- → Barcodes
- → MRZ

Digitalization of Identity Documents

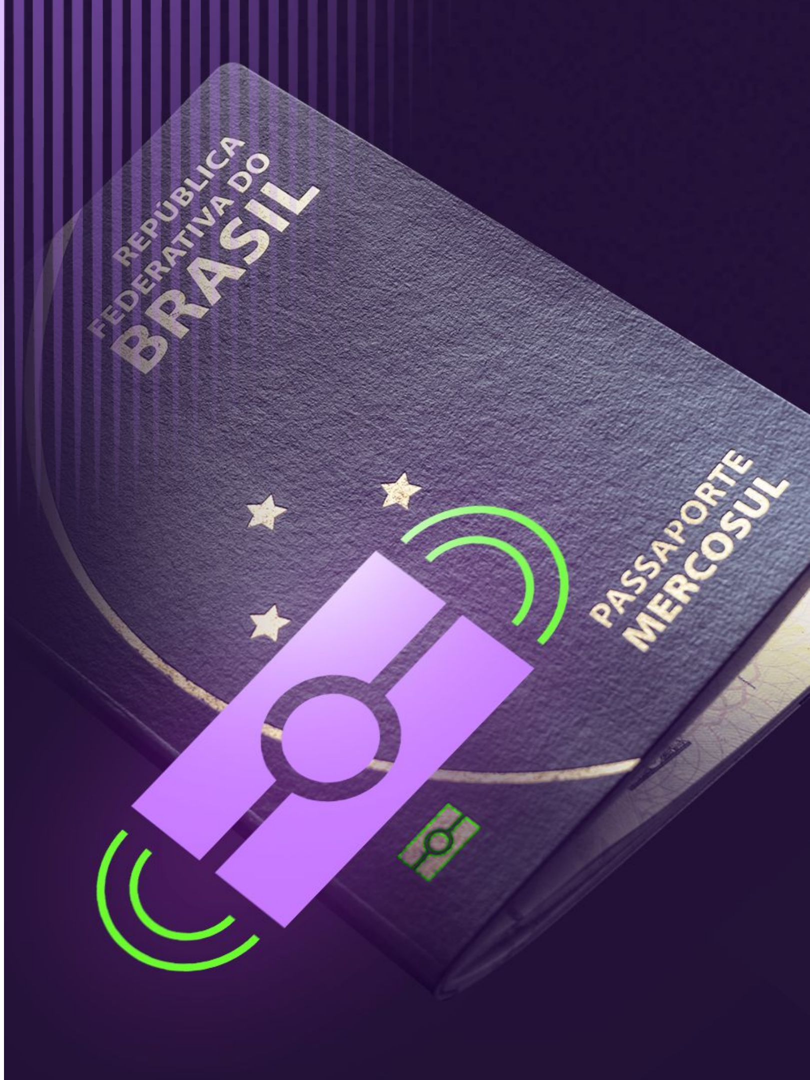
- → Smart Cards
- → Biometric Data

Electronic Identity (eID) Initiatives

- → National eIDs
- → Mobile Driver's Licenses (mDLs)

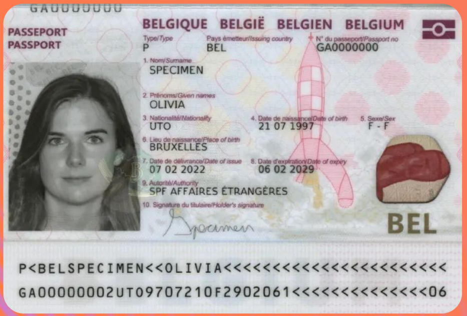
What Are Electronic Identity Documents?

- ➔ ICAO DOC 9303 standard: Documents with an embedded contactless (RFID/NFC) chip including biographical and biometrical data stored in the chip
- ➔ Terminology: Electronic Machine Readable Travel Document (eMRTD) ePassport, biometric passport, electronic identity card (eID) or biometric identity card



Types of Electronic Identity Documents

ePassport



GA0000000

PASSEPORT
PASSPORT

BELGIQUE BELGIË BELGIEN BELGIUM

Type/Type
P

Pays émetteur/Issuing country
BEL

N° du passeport/Passport no
GA0000000

1. Nom/Surname
SPECIMEN

2. Prénoms/Given names
OLIVIA

3. Nationalité/Nationality
UTO

4. Date de naissance/Date of birth
21 07 1997

5. Sexe/Sex
F - F

6. Lieu de naissance/Place of birth
BRUXELLES

7. Date de délivrance/Date of issue
07 02 2022

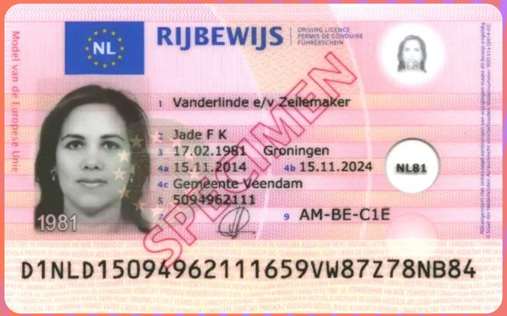
8. Date d'expiration/Date of expiry
06 02 2029

9. Autorité/Authority
SPF AFFAIRES ÉTRANGÈRES

10. Signature du titulaire/Holder's signature
Specimen

BEL

```
P<BELSPECIMEN<<OLIVIA<<<<<<<<<<<<<<<<<<<<<<<<<
GA00000002UT09707210F2902061<<<<<<<<<<<<<<<06
```



Model van de Europese Unie

NL

RIJBEWIJS | DRIVING LICENCE
PERMIS DE CONDUIRE
FÜHRERSCHEIN

SPECIMEN

1 Vanderlinde e/v Zeilemaker

2 Jade F K

3 17.02.1981 Groningen

4a 15.11.2014 4b 15.11.2024

4c Gemeente Veendam

5 5094962111

7

9 AM-BE-C1E

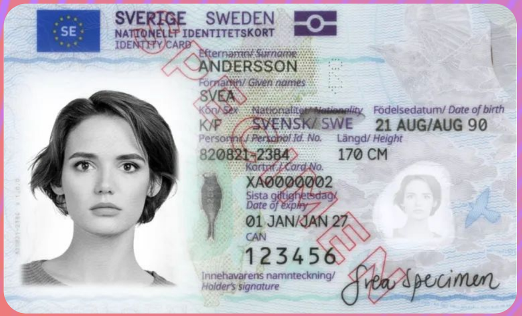
1981

NL81

```
D1NLD15094962111659VW87Z78NB84
```

eDL

eID



SE

SVERIGE SWEDEN
NATIONELLT IDENTITETSKORT
IDENTITY CARD

SPECIMEN

Efternamn/ Surname
ANDERSSON

Förnamn/ Given names
SVEA

Kön/ Sex
K/F

Nationalitet/ Nationality
SVENSK/ SWE

Födelsedatum/ Date of birth
21 AUG/AUG 90

Personnr./ Personal Id. No.
820821-2384

Längd/ Height
170 CM

Kortnr./ Card No.
XA0000002

Sista giltighetsdag/
Date of expiry
01 JAN/JAN 27

CAN
123456

Innehavarens namnteckning/
Holder's signature
Svea Specimen

What an Electronic Document Stores

DG1 Basic personal information: name, date of birth, nationality, sex, etc.

DG2 Holder’s photo

DG3 Fingerprints

DG4 Iris scans

DG5 Additional photo of the holder in higher quality

DG7 Image of the holder’s signature

DG11 Additional details on the holder beyond MRZ data, such as date of issue, full name or the name recorded in a local language, place of birth, etc.

DG12 Information on the issuing body: where, when, and by whom the document was issued

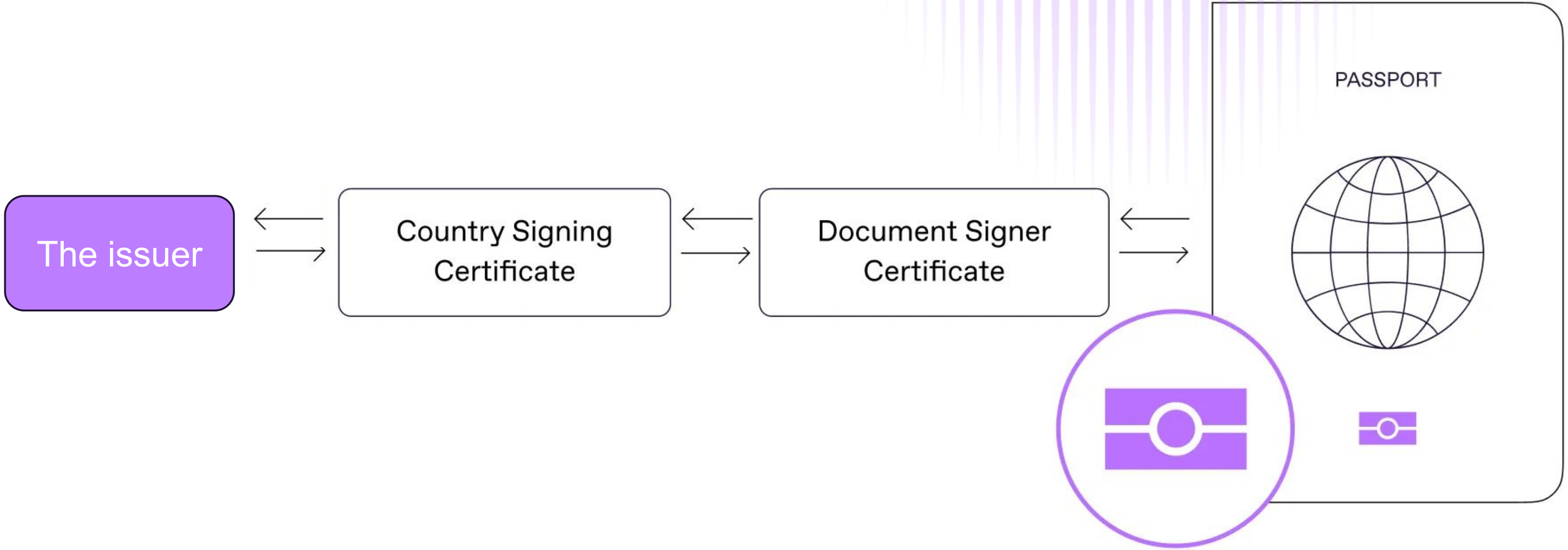
DG13 Additional details reserved for use by the national services of the issuing state

DG14 Information about cryptographic algorithms and a public key used for Chip Authentication (CA)

DG15 Information about cryptographic algorithms and a public key used for Active Authentication (AA)

DG16 Information about persons to notify in case of emergency

The Chain of Trust - Signing Certificates



The CSCA certificates are available in the ICAO PKD, as well as other trusted sources.

How Is an RFID Chip Protected and Verified?

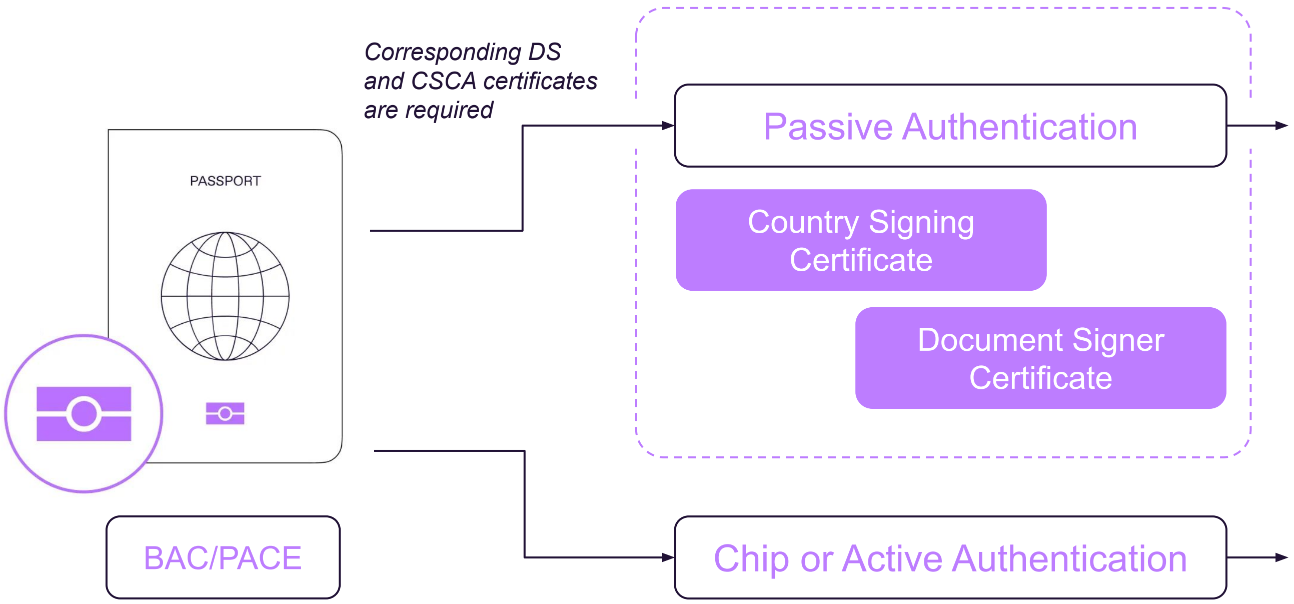
3 forms of access control

- Basic Access Control (BAC)
- Password Authenticated Connection Establishment (PACE)
  - Supplemental Access Control (SAC)
- Extended Access Control (EAC)

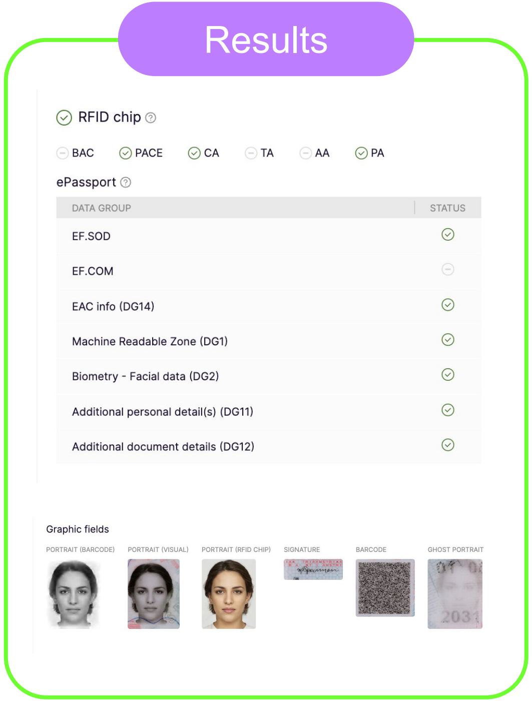
4 types of RFID chip authentication

- Passive Authentication
- Active Authentication
- Chip Authentication
- Terminal Authentication

Electronic Identity Document Verification


PASSPORT
BAC/PACE
Passive Authentication
Country Signing Certificate
Document Signer Certificate
Chip or Active Authentication

Corresponding DS and CSCA certificates are required



✓ RFID chip

– BAC ✓ PACE ✓ CA – TA – AA ✓ PA

ePassport

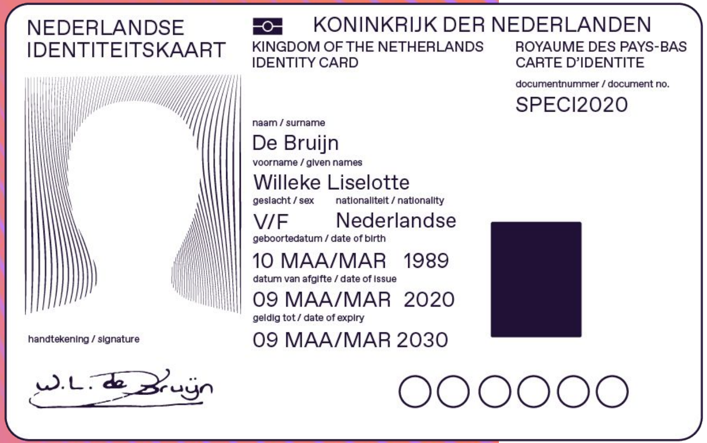
DATA GROUP	STATUS
EF.SOD	✓
EF.COM	–
EAC info (DG14)	✓
Machine Readable Zone (DG1)	✓
Biometry - Facial data (DG2)	✓
Additional personal detail(s) (DG11)	✓
Additional document details (DG12)	✓

Graphic fields

PORTRAIT (BARCODE) PORTRAIT (VISUAL) PORTRAIT (RFID CHIP) SIGNATURE BARCODE GHOST PORTRAIT

The CSCA certificates are available in the ICAO PKD, as well as other trusted sources.

Advantages of Electronic Identity Documents



NEDERLANDSE IDENTITEITSKAART

KONINKRIJK DER NEDERLANDEN

KINGDOM OF THE NETHERLANDS
IDENTITY CARD

ROYAUME DES PAYS-BAS
CARTE D'IDENTITE

documentnummer / document no.
SPECI2020

naam / surname
De Bruijn

voorname / given names
Willeke Liselotte

geslacht / sex
V/F

nationaliteit / nationality
Nederlandse

geboortedatum / date of birth
10 MAA/MAR 1989

datum van afgifte / date of issue
09 MAA/MAR 2020

geldig tot / date of expiry
09 MAA/MAR 2030

handtekening / signature
W.L. de Bruijn

○○○○○○

- → Faster processing with quick NFC scanning and data retrieval
- → More data storage than traditional IDs, including biometric data
- → Stronger fraud prevention with the use of unique identifiers and secure encryption
- → Interoperability that allows working across different systems and countries
- → Improved record keeping for better tracking and management of ID issuance and renewals

Mobile Driver's License (mDL) Overview

- In September 2021, the International Organization for Standardization (ISO) published the Personal Identification – ISO Compliant driving license – Part 5: mobile driving license (mDL) application (ISO/IEC 18013-5) standard.
- The standard details the components of a verified issuer certificate authority list (VICAL).
- AAMVA's DTS is the system that provides the VICAL to issuing authorities and relying parties.

ISO

18013-5

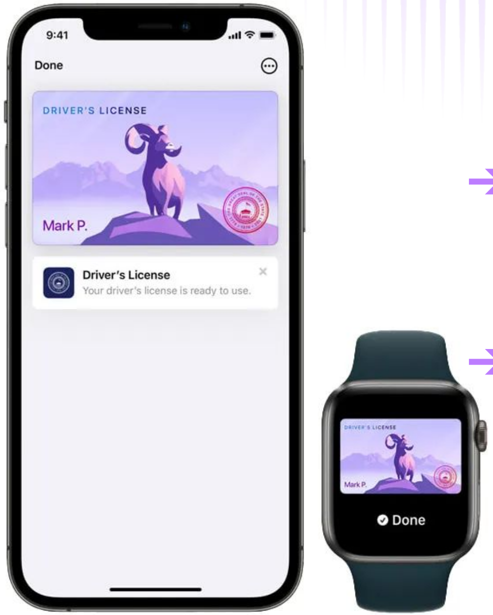
AAMVA

mDL DTS

MOBILE DRIVER'S LICENSE DIGITAL TRUST SERVICE

Advantages of Mobile Driver's License (mDL)

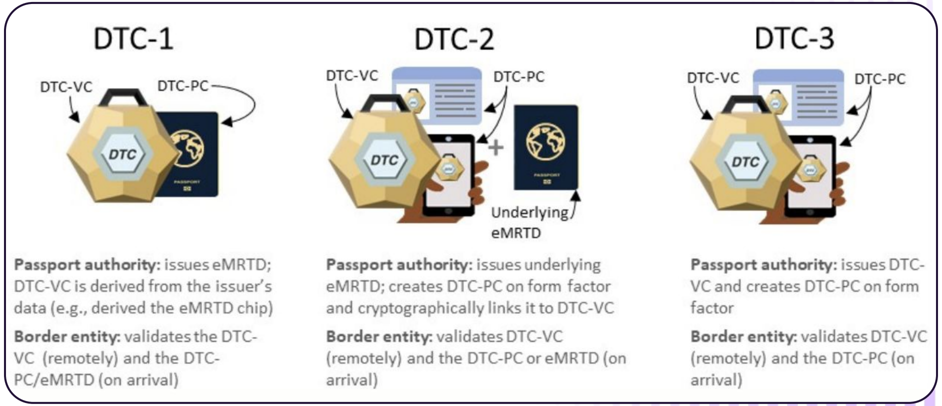
- Digital version of a traditional driver's license
- Allows contactless transactions
- Selective personal data sharing during identity verification
- Reduced risk of identity theft



- High security with cryptography to make sure it can’t be hacked, copied or modified
- Streamlined identity verification and digital onboarding
- Lower costs associated with printing and distributing physical cards

Digital Travel Credential (DTC) Overview

- ICAO Guiding Core Principles for the Development of Digital Travel Credential (DTC)
- The ICAO DTC is a secure and globally interoperable digital companion and/or substitution to a physical eMRTD, designed to support seamless travel.
- The key feature of the ICAO DTC is that authorities can verify a digital representation of the passport data before the traveler's arrival and confirm the data's integrity and authenticity.
- There are three types:



DTC-1

Passport authority: issues eMRTD; DTC-VC is derived from the issuer's data (e.g., derived the eMRTD chip)

Border entity: validates the DTC-VC (remotely) and the DTC-PC/eMRTD (on arrival)

DTC-2

Passport authority: issues underlying eMRTD; creates DTC-PC on form factor and cryptographically links it to DTC-VC

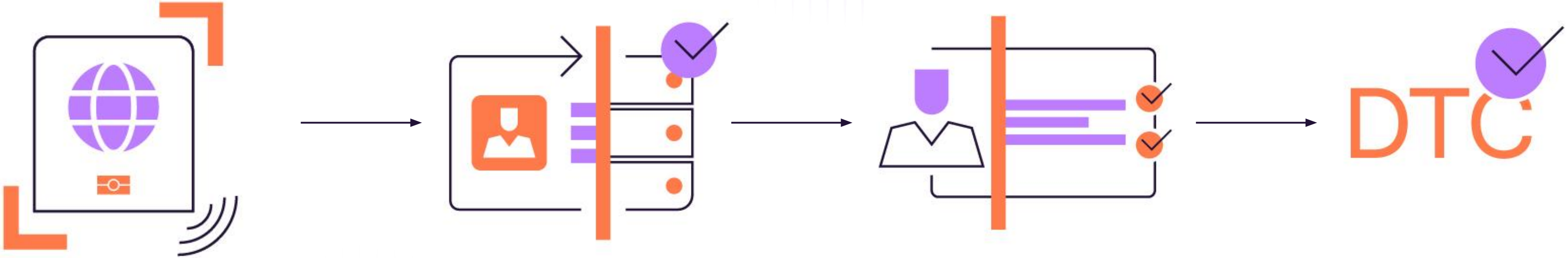
Border entity: validates DTC-VC (remotely) and the DTC-PC or eMRTD (on arrival)

DTC-3

Passport authority: issues DTC-VC and creates DTC-PC on form factor

Border entity: validates DTC-VC (remotely) and the DTC-PC (on arrival)

Regula Just Introduced Support for DTC



NFC Scanning

Secure Server
Side Verification

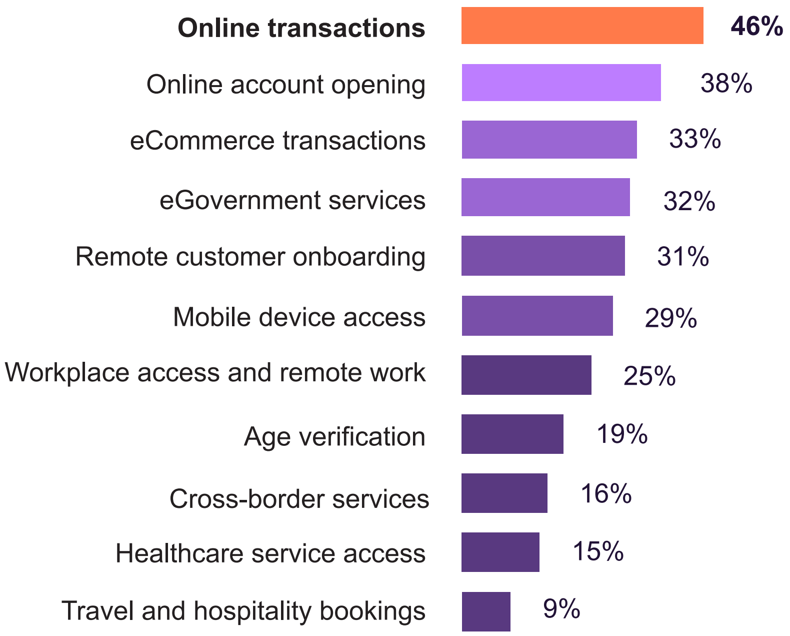
DTC-VC
Creation

DTC-VC
Saving

Standards and Regulations

Use Cases

- ➔ Biometric ID use cases are the same as traditional IDV use cases
- ➔ Online transactions and online account opening are leading at 46% and 38% with digital IDs



New ISO 39794-5 standard

- Support for the new DG2 data format in accordance with the ISO/IEC 39794-5 standard
- Higher interoperability and data integrity across different systems.
- Issuing states and organizations will begin using the new DG2 data formats in identity documents as of January 1, 2026.

Schweizer Sample
Helvetia
Schweiz Suisse Svizzera
01 08 1995
170 cm
Bern BE
26 09 2022
Bern BE
PMCHESCHWEIZER<SAMPLE<<HEL
S0A00B39<5CHE9508015F32092
ISO/IEC 39794 ISO/IEC 39794 ISO/IEC 39794

Digital Identities and Verifiable Credentials W3C – Verifiable Credential Data Model

- → Digital credentials issued by different issuers for different purposes
- → Held securely under control of the wallet holder
- → Wallet holder presents relevant credentials as needed to access services
- → The details are here

ISO/IEC 23220-x Mobile-Based Digital Wallets

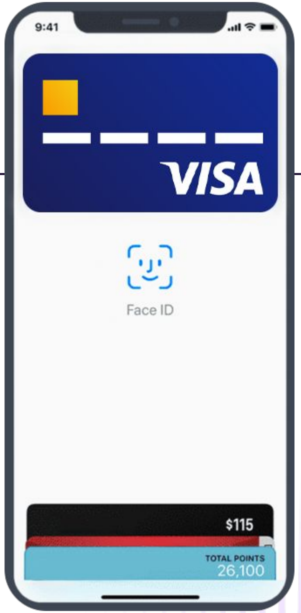
- ➔ Series of standards which specify the use of mobile-based wallets to securely manage and use digital identities and credentials
- ➔ Based on the standard for mobile-based driver’s licenses: ISO/IEC 18013-5
- ➔ Adapted for use with the W3C Credential Model
- ➔ The details are here

European Digital Identity Wallet

- First aim is digital alternative to identity card
  - Also supporting a range of other functions
- High-level security & privacy
  - Sensitive data is held in secure element
  - User-controlled selective disclosure
- Ambitious implementation schedule
  - 4 large-scale EU pilots ongoing
  - EU National implementations by 2026
- The details are here

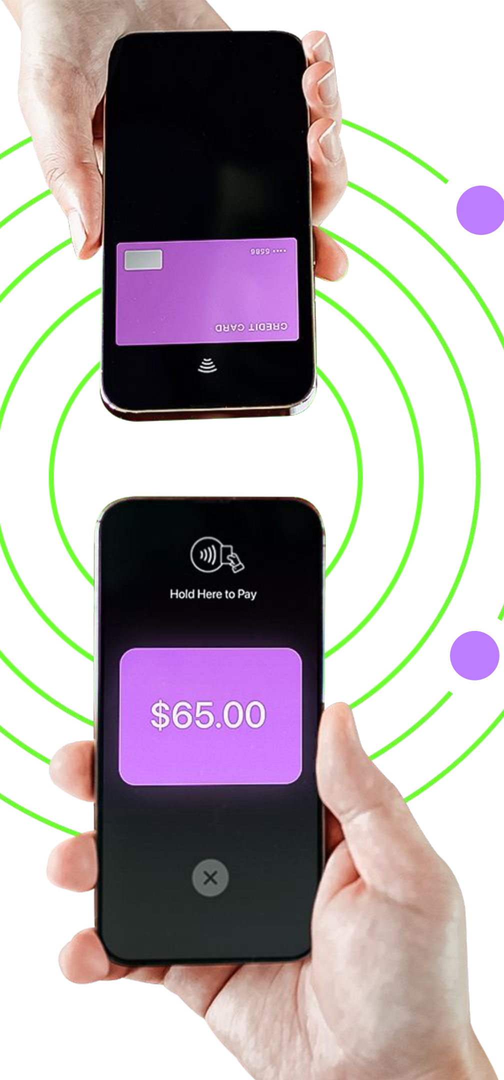
US Digital Identity Guidelines

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



- → The US Department of Commerce’s National Institute of Standards and Technology (NIST) is working on a draft of guidelines
- → NIST Special Publication [SP] 800-63 Revision 4 and its companion publications SPs 800-63A, 800-63B, and 800-63C

Weaknesses of Digital Wallets



Prime target for cyberattacks

Privacy concerns

Lag in adoption, gap between vision and practice

No seamless interaction

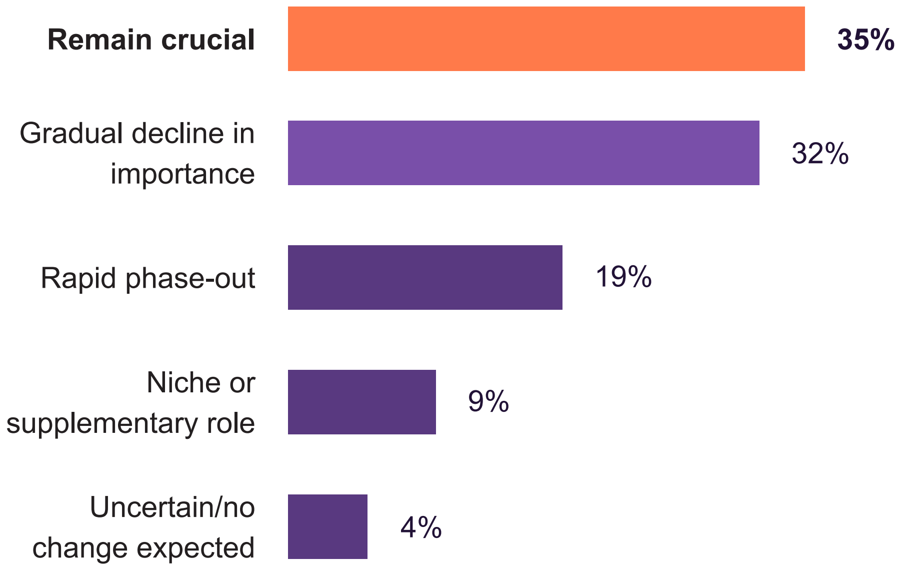
No universal standard for how these wallets and credentials should work together

And so on…

How Quick Will the Transition Be?

Physical Documents Remain Critical

- ➔ Most organizations believe physical docs will remain critical
- ➔ 32% expect a gradual decline in importance
- ➔ Only 19% predict a rapid phase-out, and only 9% believe in the niche role of physical documents



Benefits of Onboarding with Electronic IDs

Enhanced security

Streamlined onboarding process

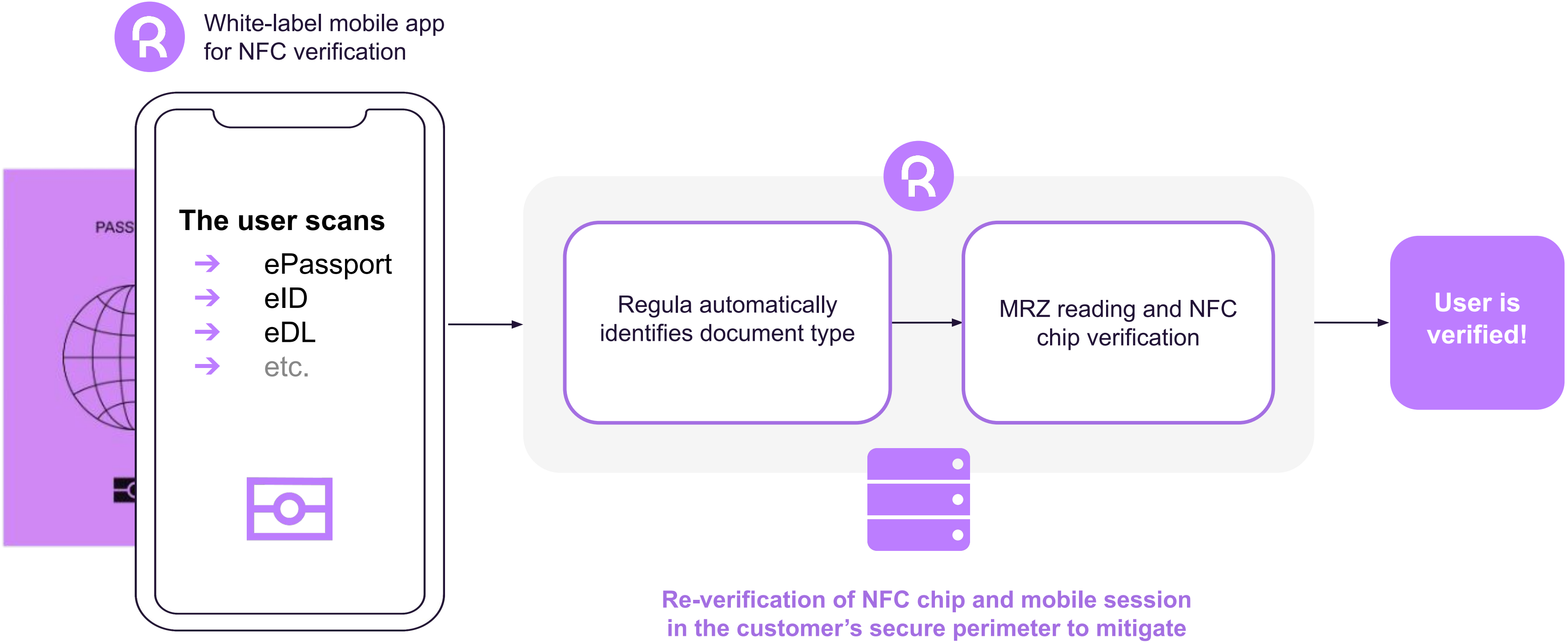
Compliance with regulations

Improved customer experience

Cost savings by avoiding manual checks

User flows

User Flow with Electronic Documents



White-label mobile app
for NFC verification

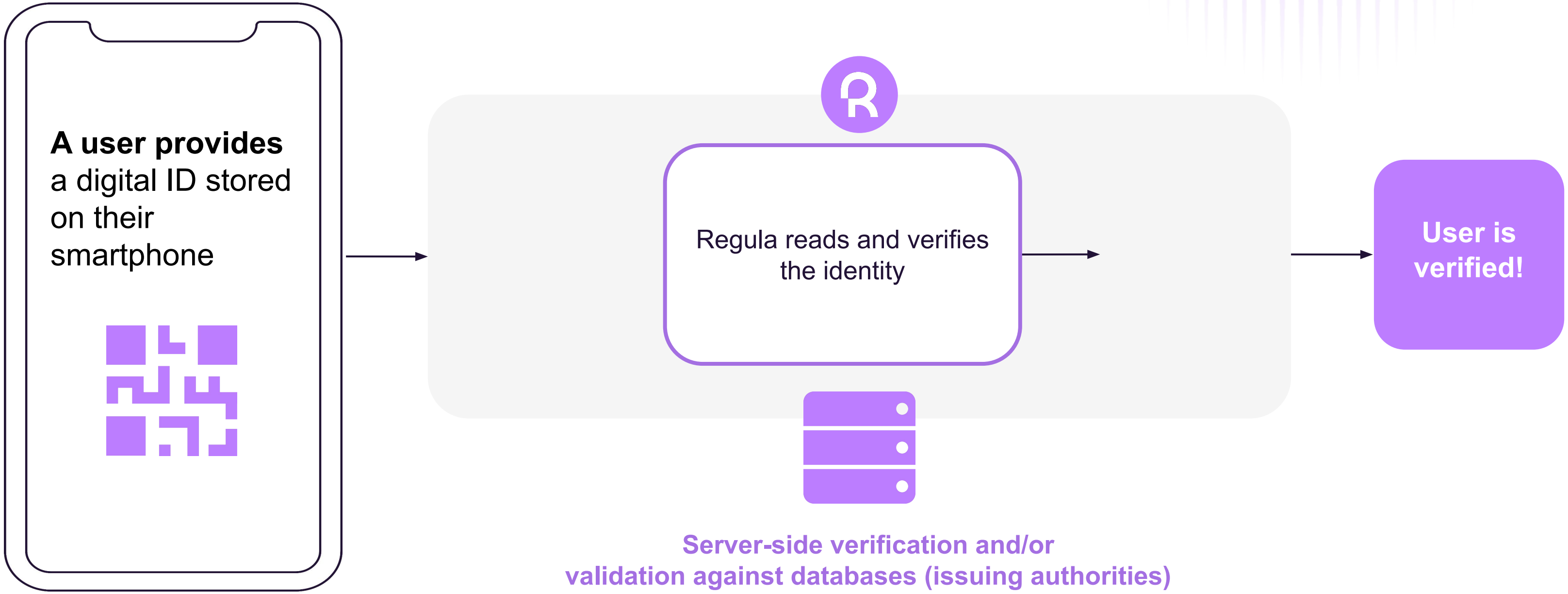
The user scans

- → ePassport
- → eID
- → eDL
- → etc.

Regula automatically identifies document type → MRZ reading and NFC chip verification → **User is verified!**

Re-verification of NFC chip and mobile session in the customer’s secure perimeter to mitigate zero-trust-to-mobile issues

User Flow with Digital IDs



A user provides a digital ID stored on their smartphone

Regula reads and verifies the identity

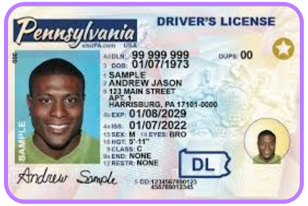
User is verified!

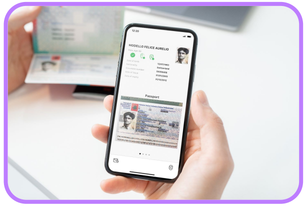
Server-side verification and/or validation against databases (issuing authorities)

Handling IDV Scenarios

Diversity of Scenarios

NATIONAL BANK
DATE
NAME
ADDRESS
PAY TO THE ORDER OF
USD





Regula IDV Platform

Regula Identity Verification (IDV) Platform is a ready-to-integrate and fully customizable on-premises solution that automates identity verification and user authentication through comprehensive document and biometric checks, no matter the document type or device on the user's side.

BUNDESREPUBLIC DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
LO1X00T47
[a] Name/Surname/Nom
[b] Geburtsname/Name at birth/Nom de naissance
[a] MUSTERMANN
[b] GABLER
Vornamen/Given names/Prenoms
ERIKA
Staatsangehorigkeit/Nationality/Nationalite
DEUTSCH
938568
SWEDEN
ENTITETSKORT
ANDERSSON
SVENSK

Regula IDV Platform Highlights

- All-in-one out-of-the-box solution
- Diverse operational scenarios
- Comprehensive database management
- Flexible scalability
- Detailed interaction logging
- Insightful dashboards and reporting
- Seamless data integration
- Customizable solution

Solution Testing

Testing the Solution: Challenges and Considerations

- → Over 170 countries issue biometric identity documents
- → Different designs, surfaces and security features
- → Various races and ethnicities
- → Using genuine identity documents in a development and testing environment is not a good idea, and it does not scale
- → You'll need custom, artificial identity documents for testing purposes
- → You should verify the testing requirements for certifications with the auditor right from the start (e.g., QES, eIDAS)

Recommendations

Add Identity Document Testing Requirements to Your "Must Evaluate" Criteria

Regula NFC TestKit Service

Benefits

- Short time to market
- Flexibility
- Efficient problem identification
- Maximum security assurance

Summary

1

Re-think your onboarding process

2

Create one IDV flow that supports all types of IDs: traditional, biometric, and digital

3

Plan today to include digital IDs

Questions?

Thank you!

Regula

Decades of Forensics for Seamless Identity Verification.

Bringing together 30 years of experience in forensics, border control and business, to create industry standards to trust and follow.