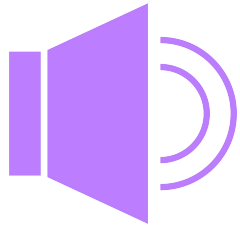




October 15, 2025

Building Trusted Journeys in the Digital Identity Era

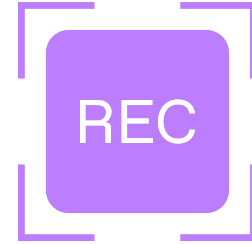
Housekeeping



Trouble with audio?
Try dialing in!



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



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



Name/Surname

Henry Patishman

Business role

**Executive VP of Identity
Verification Solutions
at Regula**

Regula Key Facts

30+

years in the industry

100%

in-house R&D

15,000+

the most comprehensive library
of identity documents from
254 countries and territories

170+

countries covered by Regula
solutions

80+

border controls globally equipped
with Regula solutions

1,000+

clients



Name/Surname

Ken Ebert

Business role

Chief Technology Officer
Indicio



Everything you need to build astonishingly efficient, powerful, and simple, decentralized solutions for a new era of digital trust.

Travel & hospitality

Seamless, secure border crossings, travel document verification

Financial Services

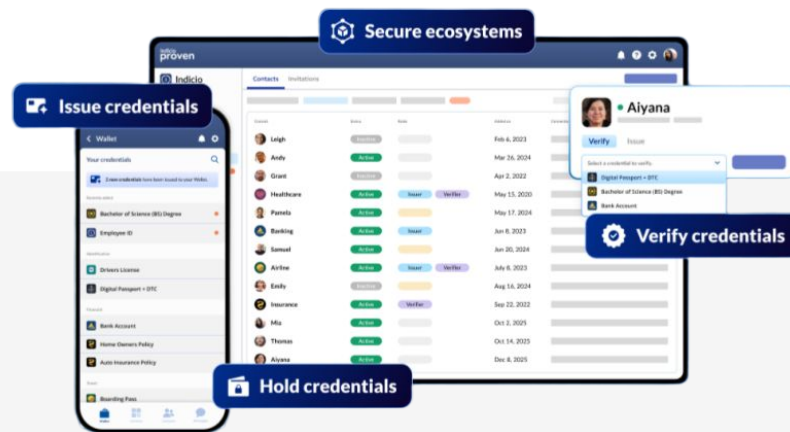
Reusable KYC, secure payments, regulatory compliance

Enterprise

Fast employee access and onboarding, and secure invoicing

Education

Supporting career mobility with digital certificates and diplomas



- Decentralized identity
- Verifiable Credentials
- Digital Wallets
- Passwordless login
- Document authentication
- Portable biometrics
- Modular architecture
- AI verification

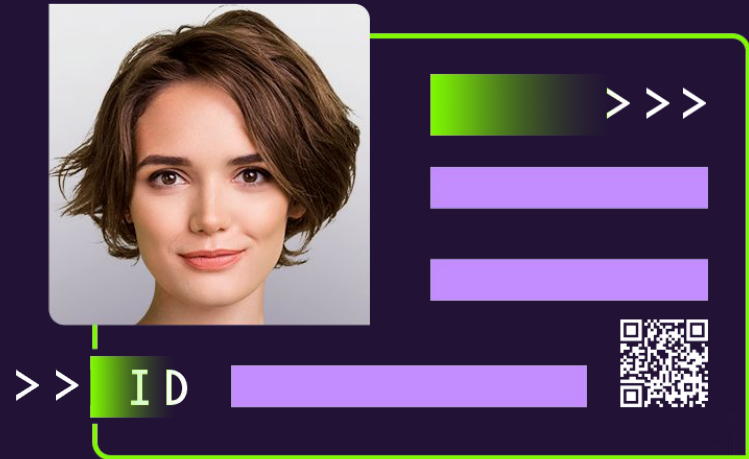


Aligned with global standards for interoperability W3C | ICAO | ISO | eIDAS | EUDI | 1EdTech

Let's get started!

Digital Identity: Why It Matters

- A way to prove identity electronically
- Makes things easier for citizens, businesses and governments
- Enables economic value by fostering access to goods and services
- The right of every person to have a digital identity that is recognised everywhere



Market direction

“By 2026, at least 500 million smartphone users will be regularly making verifiable claims using a digital identity wallet built on distributed ledger technology.”

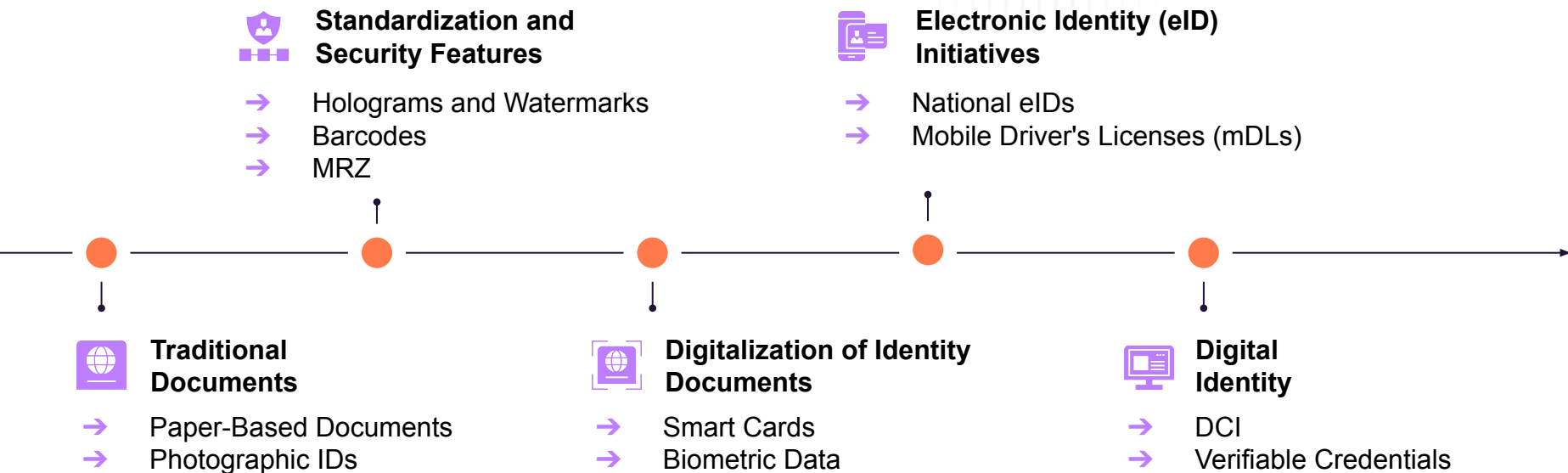
Benefits

“For identity verification, account takeovers, fraud, privacy and security... [decentralized identity] represents magnitudes of improvement in terms of efficiency, cost and assurance.”

The evolution of Digital Identity

Historical Context:

How Digital IDs Came to Be



Standardizing how digital trust is built

Regulatory Landscape

Europe and the UK

European Union - GDPR, EUDI

United Kingdom - UK GDPR

North America

United States - CCPA, BIPA, HIPAA

Canada - PIPEDA

Mexico - LFPDPPP

Latin America & South America

Brazil - LGPD

Colombia - Law 1581

Chile - LPPD

Uruguay - LPPD 2008 data protection framework

Middle East

UAE - Federal Decree Law No. 45 of 2021

Saudi Arabia - PDPL

Jordan - JPDPA

Qatar - PDPL

APAC

India - DPDA

Japan - APPI

South Korea - PIPA

Singapore - PDPA

China - PIPL

Australia - Privacy Act of 1988

Africa

South Africa - POPIA

Nigeria - NDPA

African Union - Convention on Cyber Security
And Personal Data Protection

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

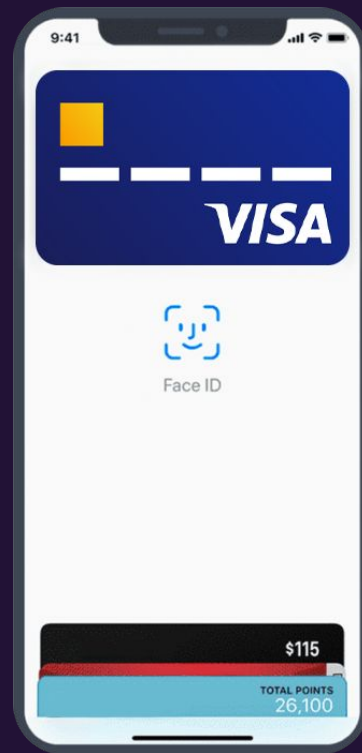


- First aim is digital alternative to identity card
 - ◆ Also supporting a range of other functions
- High-level security & privacy
 - ◆ Sensitive data is held in secure element
 - ◆ User-controlled selective disclosure
- Ambitious implementation schedule
 - ◆ 4 large-scale EU pilots ongoing
 - ◆ EU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



US Digital Identity Guidelines

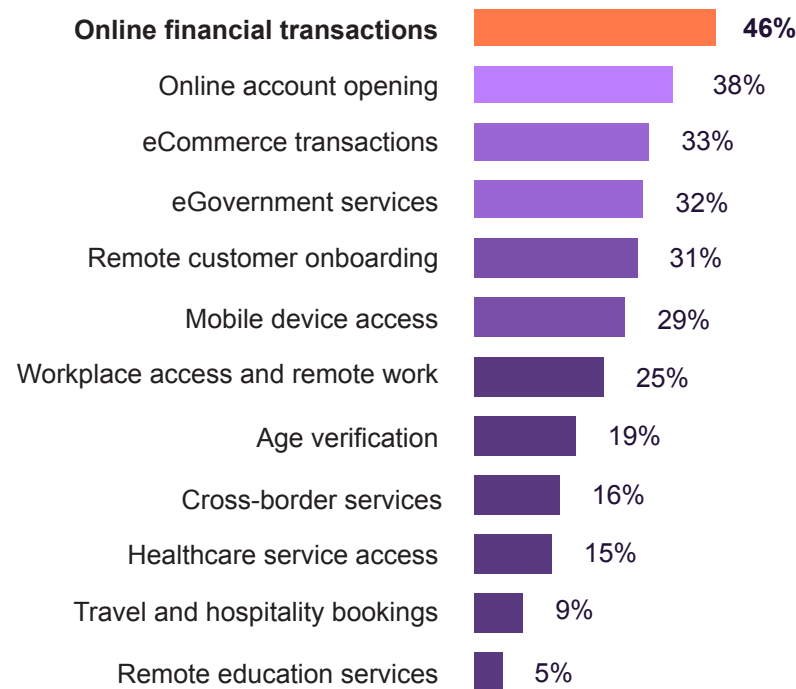
- The US Department of Commerce's National Institute of Standards and Technology (NIST) is working on a draft of guidelines
- NIST Special Publication [SP] 800-63 Revision 4 and its companion publications SPs 800-63A, 800-63B, and 800-63C



What drives adoption

- Digital ID use cases are the same with traditional IDV use cases
- The financial sector is leading with online transactions and online account opening at 46% and 38%
- 50% in UK consider eGovernment services will benefit most of all

Diverse Use Cases



Q12. In which of the following use cases the benefits from digital ID implementation will be noticeable and bring fastest results?



Digital Identity Augments Processes



Financial Services

Perform identity authentication, fraud prevention in KYC for digital-first financial transactions, seamless account access. Eliminate time-consuming paper document KYC.



Hotels

Pre-validate guests, enable automated check-in, and prevent fraud, especially chargeback fraud.



Airlines

Mitigate identity fraud, reduce manual data entry error and create seamless processes that streamline passenger experiences.



Borders

Ensure pre authorized travel and seamless border crossing.

Interoperability and trusted frameworks

Identity Fraud is Overwhelming Legacy Technology

- Identity fraud is surging — traditional tech can't keep up.
- Manual verification, siloed databases, and static credentials create vulnerabilities.
- Digital ecosystems demand a new foundation of trust and interoperability.



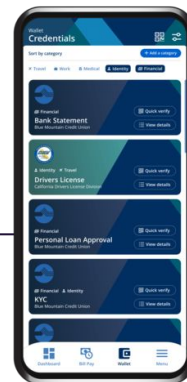
A leap forward in functionality, speed, security

The difference between a digital credential and a Verifiable Credential is like the difference between...



Legacy identity verification and data sharing

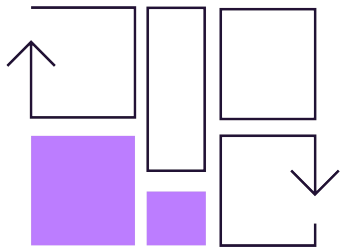
Create a direct connection and phone home to verify data.



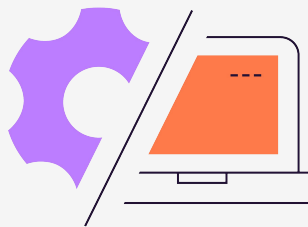
Verifiable Credentials in a digital wallet

Hold cryptographically verifiable, tamper-proof data, share from anywhere, online or offline, authenticate everywhere.

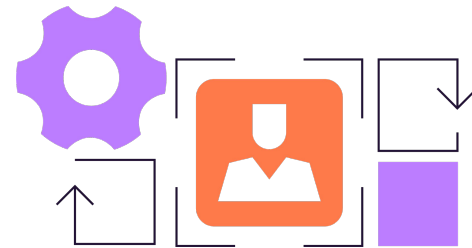
The Must-Have Capabilities Include



Verifiable credentials, DTCs



DIDs, which establish and maintain the relationship between a wallet holder and service provider



An identity wallet

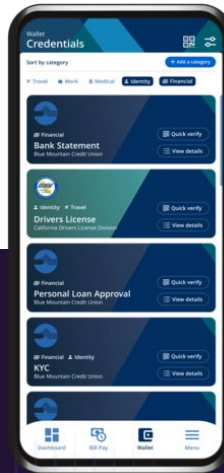
Verifiable Credentials **transform the way we authenticate** and share data by providing portable and secure seamless authentication at low cost.

As with a container, a Verifiable Credential can seal any kind of digital information.

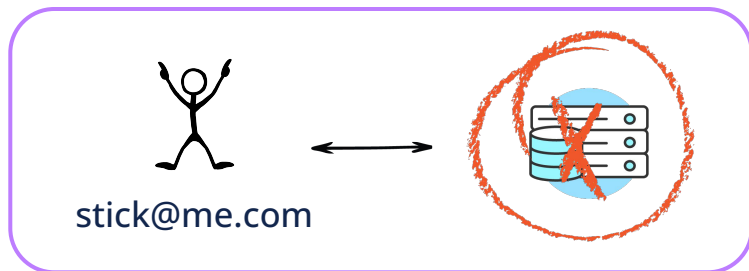
You can't alter the contents of the credential without breaking the seal.

You can be certain who issued the credential. If you trust the source, you can trust the contents.

Select information can be shared from the container in privacy-preserving ways.

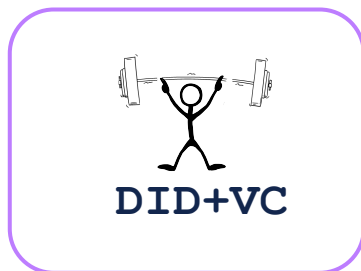
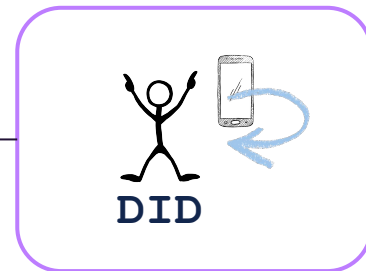


Background on Mutual Authentication



Instead of relying on a third party to give you a digital identifier in exchange for personal data...

...you use software in a digital wallet to create your own identifier—a decentralized identifier or “DID.”



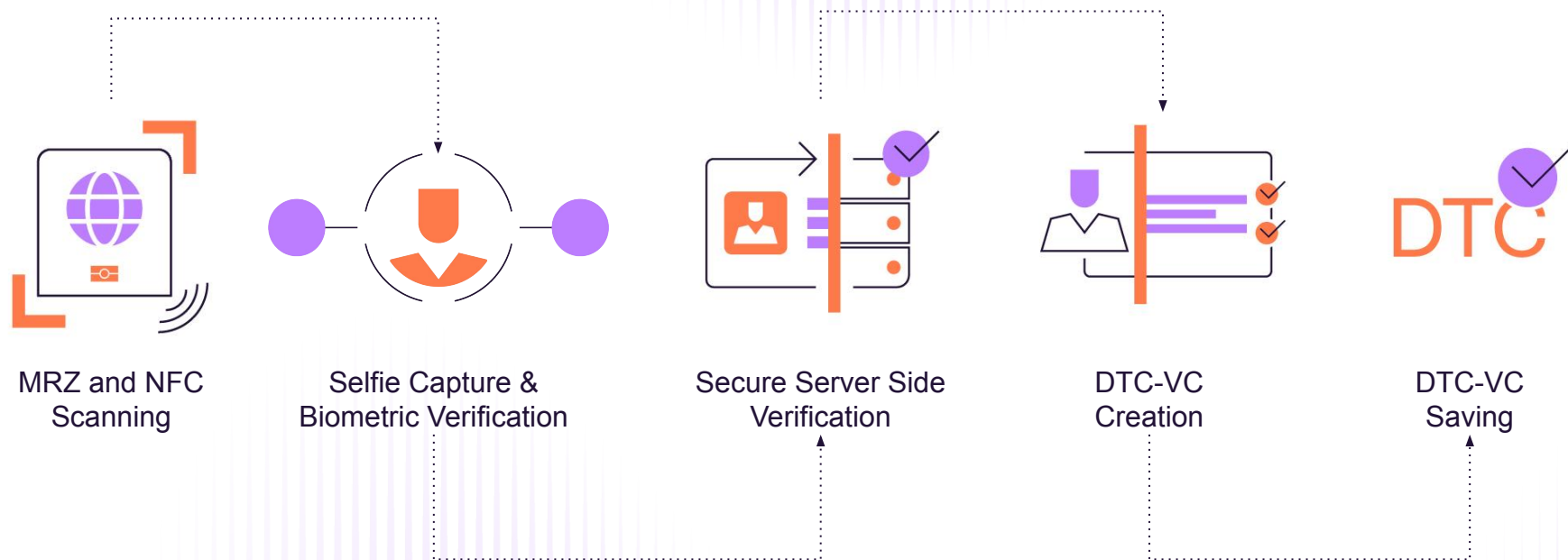
DIDs are a new and very powerful way to manage digital identity.

Digital Travel Credential (DTC)

- 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:



Digital Travel Credential (DTC) in Minutes



Decentralized Ecosystem Governance



Decentralized Ecosystem Governance (DEGov)

A simple way to establish who is a trusted issuer of credentials.

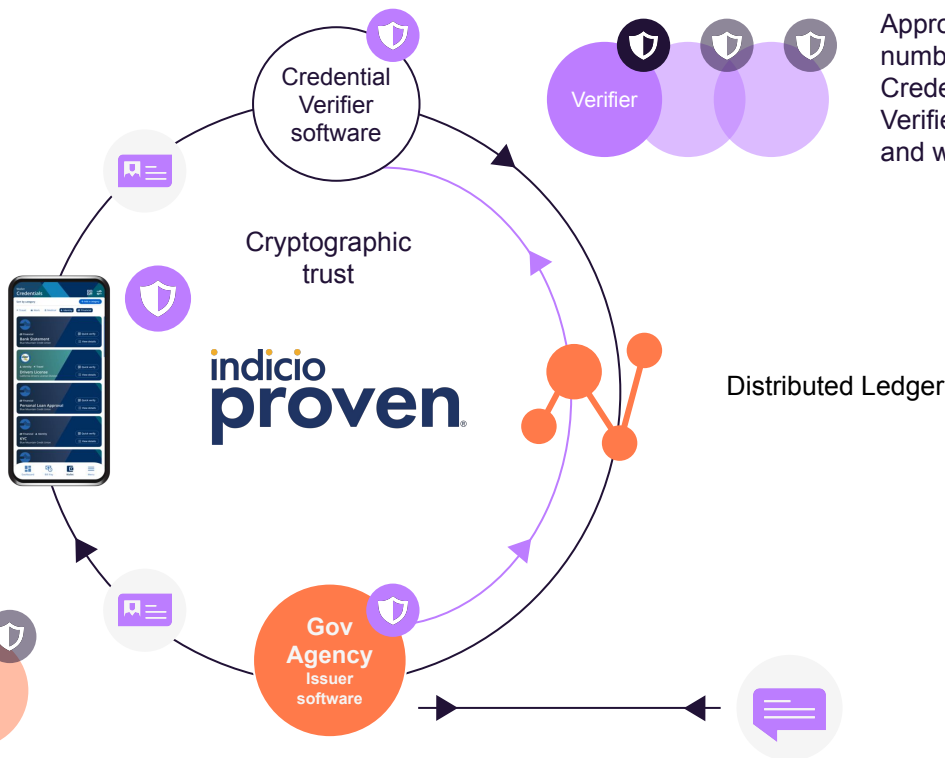
A machine-readable file published by governing authority for the overall network. This lists approved credential issuers, verifiers, workflows.

Easily updated by the governance authority.

As rules are cached in the software of each participant, facilitating offline verification.

Based on Decentralized Identity Foundation's Credential Trust Establishment specification.

Approve any number of Credential Issuers



Approve any number of Credential Verifiers, mobile and web based

Mutual Authentication Before Data Sharing

You really do know your customer — and they know it's you too

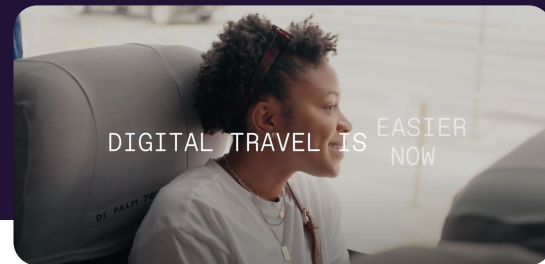
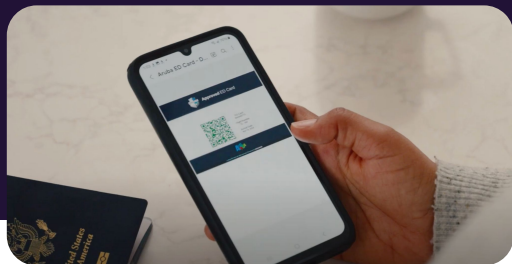
Authentication + Fraud Protection



- With Verifiable Credentials, you get a **secure** communications channel for interaction.
- **A way to prove** that each party is in control of their end of the “phone line.”
- **A way to bind** that control to verifiable proof of who they are.
- **No more phishing** attacks or bot impersonations. No more MFA.
- Just **seamless**, cryptographic authentication that's AI resistant.
- People and organizations now have **full control** over their identities.

Interoperable International Travel

Aruba, Delta Air Lines, and SITA



Still images from a [recent video](#) by Delta Air lines and SITA using Indicio
Proven technology for seamless digital travel from the U.S. to Aruba.

The trial was the first to demonstrate interoperability between EU travel and DTC-1 credentials for international travel.

Joint value proposition

End-to-End Digital Trust

Regula

Trusted identity verification and lifecycle management.

+

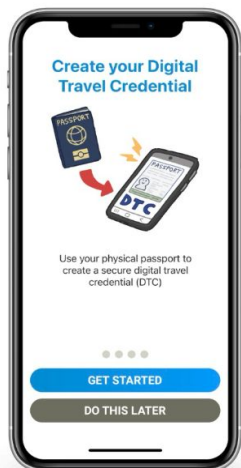
indicio

Decentralized infrastructure for verifiable credentials.

=

Together = Government-grade, privacy-preserving digital identity.

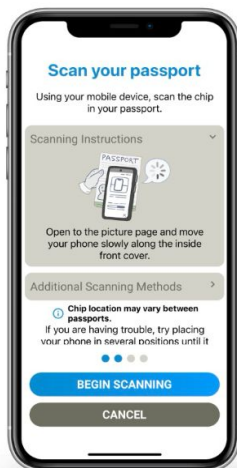
From Passport Chip to VC with Indicio & Regula



Get started



MRZ and OCR
scan



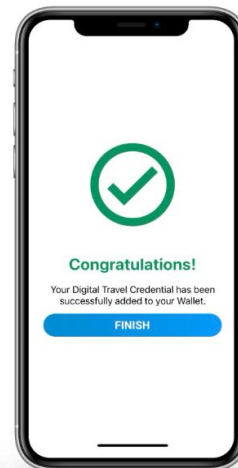
NFC chip
capture



Liveness & face
match

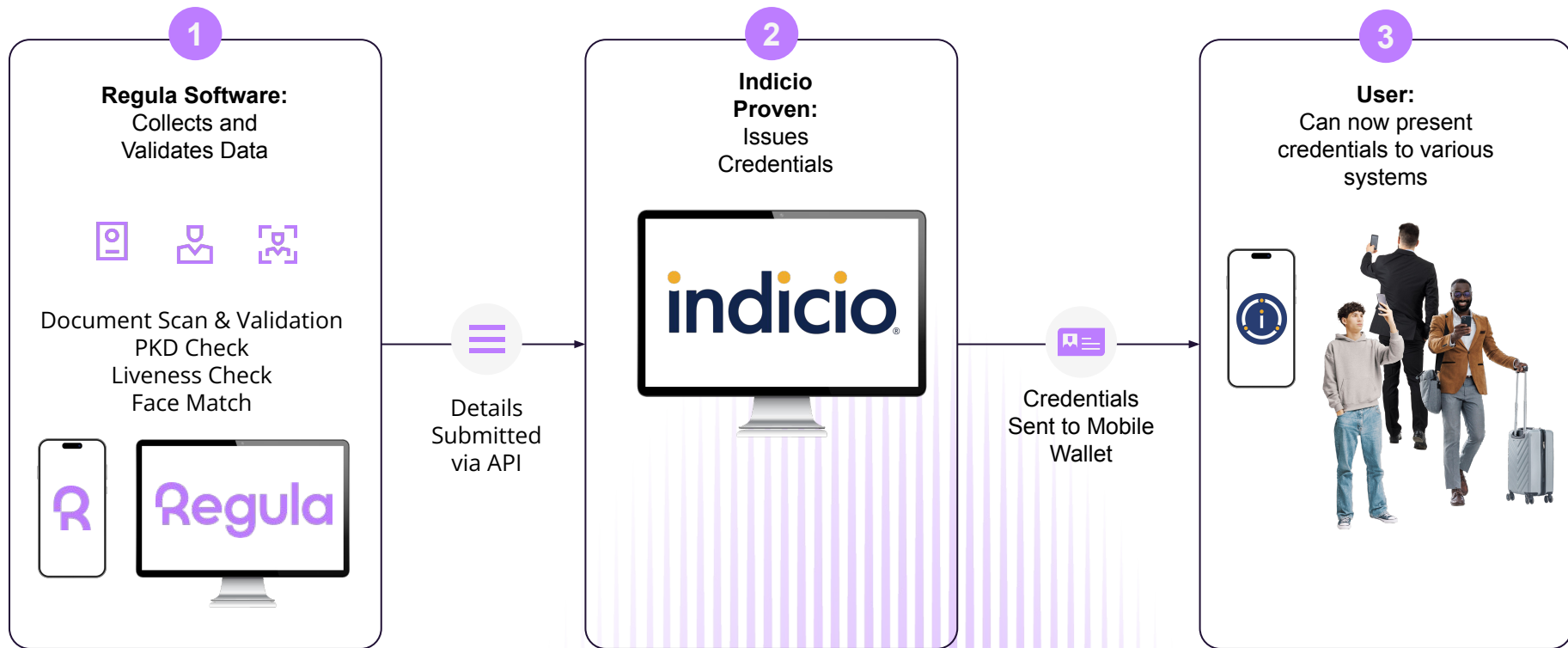


Request DTC

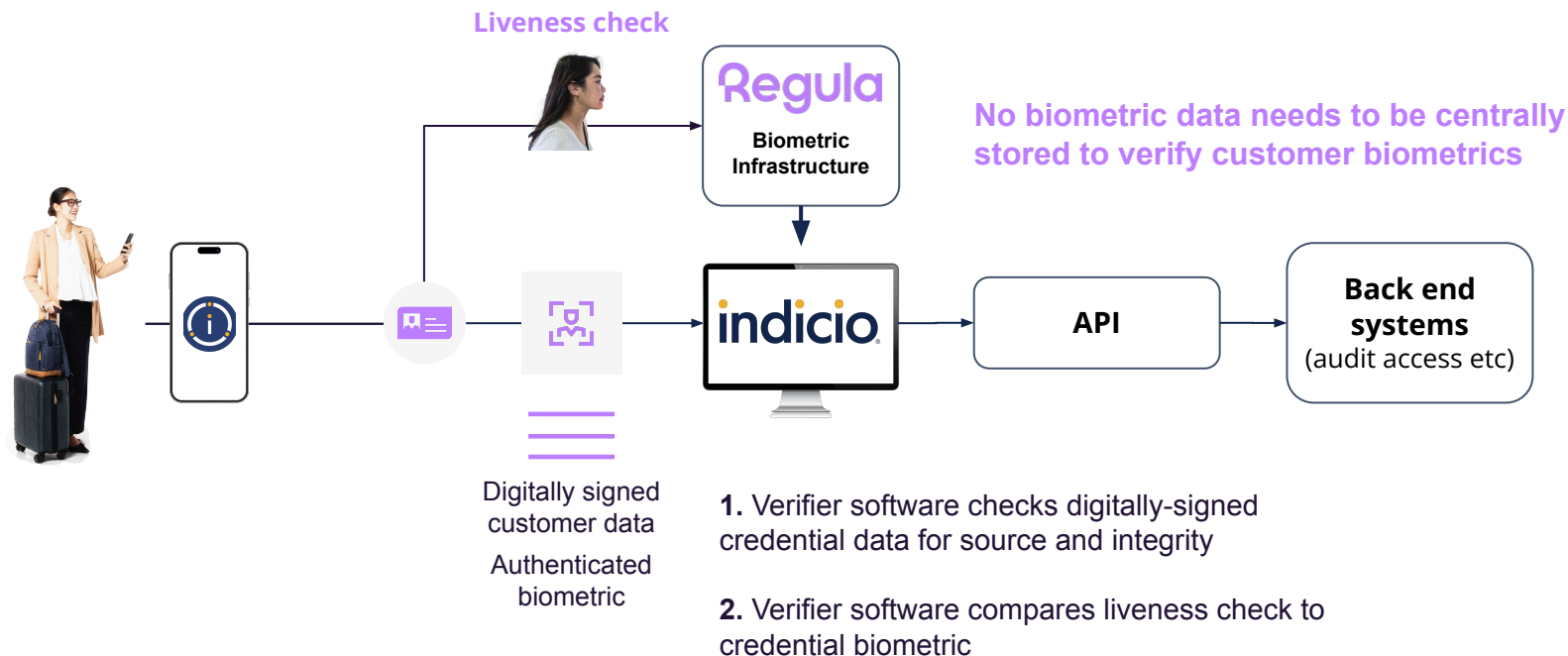


Receive DTC

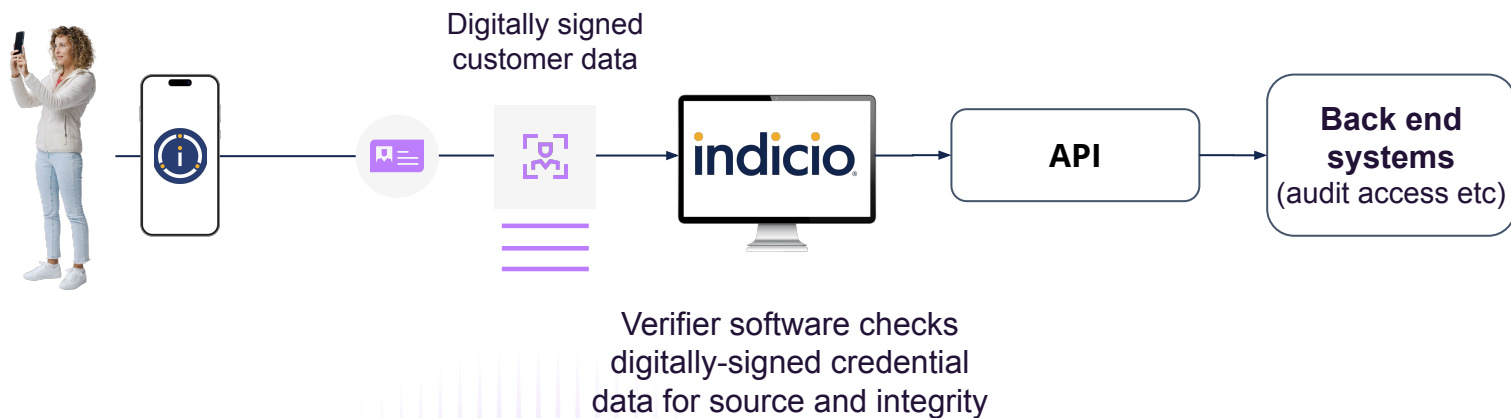
Regula Credential Issuance



Using authenticated biometric credentials with biometric infrastructure



Presenting Regula-Issued Credentials

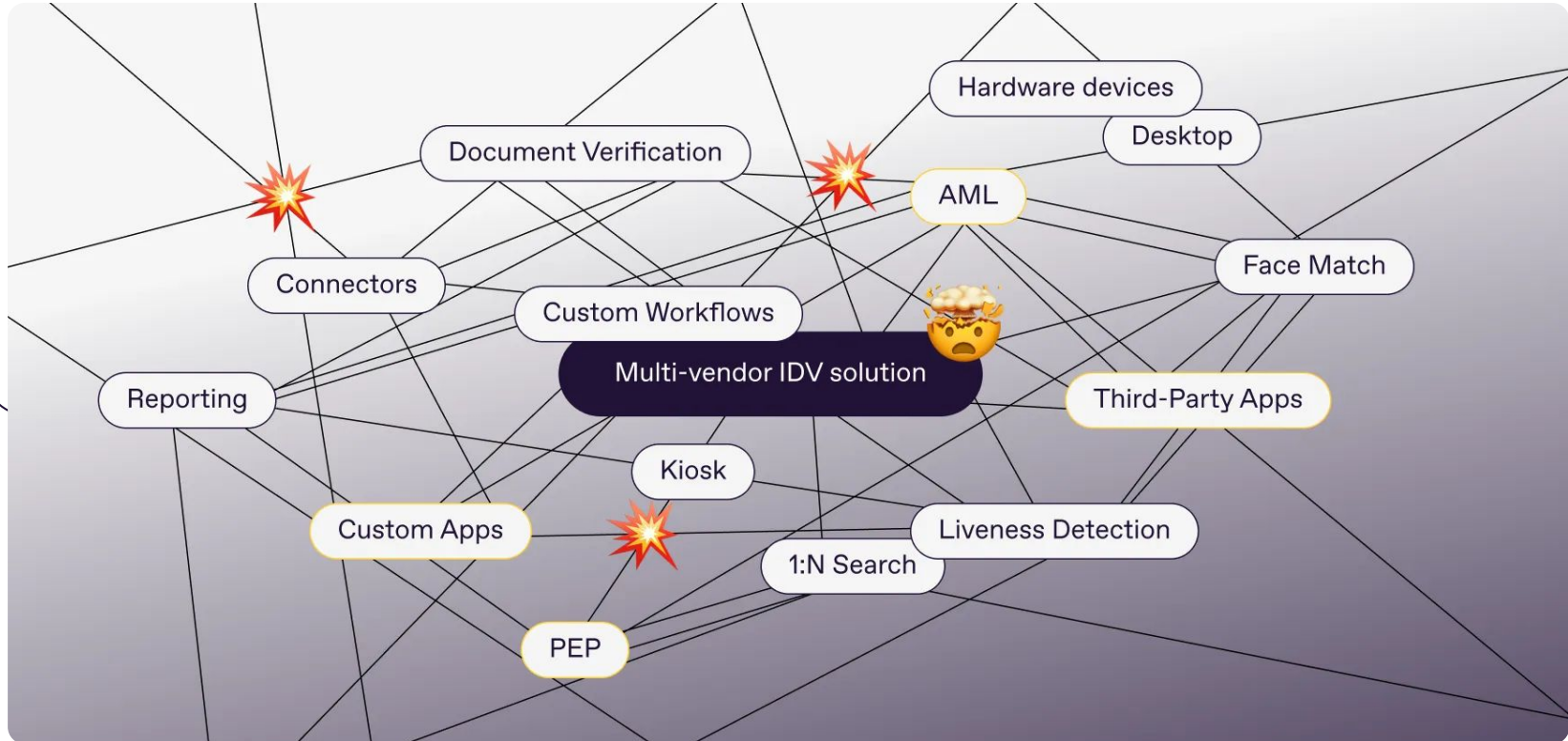




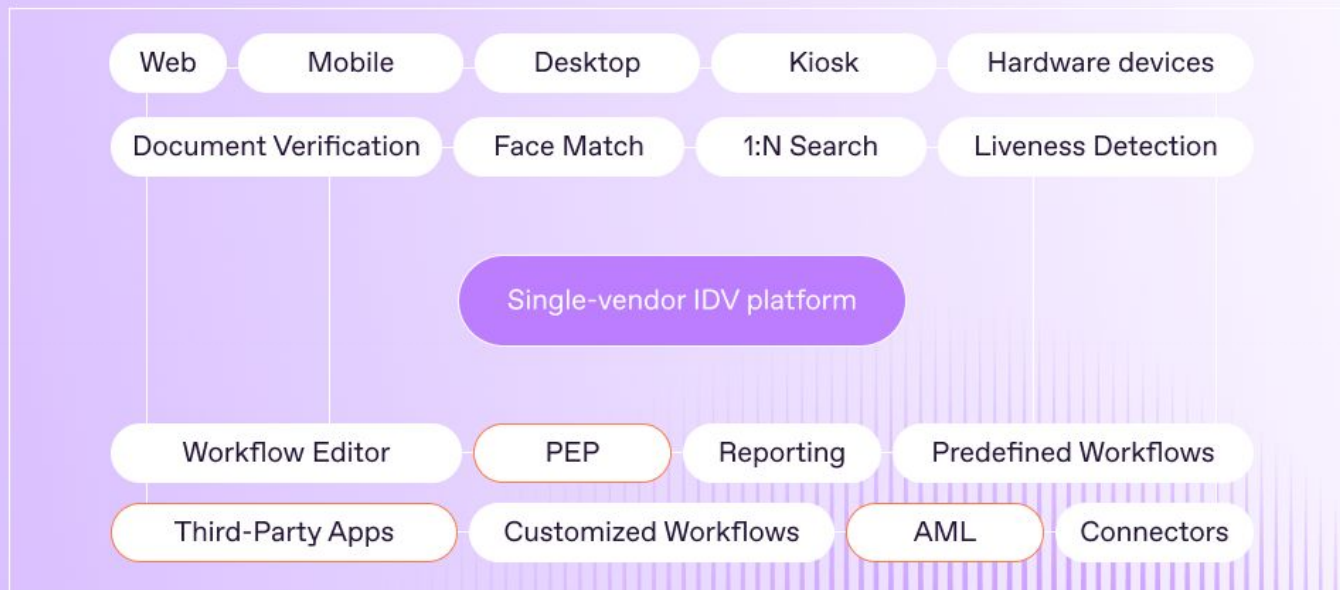
Prepare for a chaotic period of vendor consolidation in the DCI market by **choosing a vendor with a track record of early success in supporting diverse use cases**

Orchestrating identity lifecycle

Chaos vs.



Control in Customer Verification



Regula's All in One IDV Platform

Customer onboarding

Complete document and biometric verification in seconds for a seamless user experience.

Workflow orchestration

Create and automate tailored workflows across every stage of the user journey with maximum/ultimate flexibility.



Identity management

Maintain full control over every user's identity while protecting personal data.

Regulatory compliance

Effortlessly adhere to regulations across multiple jurisdictions with robust, built-in compliance capabilities.



Any Source, One Platform

Mutual support of all required components to perform the required tasks in all relevant processes

Remote User onboarding/verification

Web app 

Mobile app 

Tablet app 

Self-service

Gate 

Kiosk 

Web cam 

RFID reader 

Regula IDV
Platform



Manager's desk

Document reader 

Web cam 

RFID reader 

Fingerprint scanner 

...

...

...

...

Custom setup

Takeaways

- **Digital ID is not about replacing physical documents** but enhancing them.
- **Unified global standards implementation is essential.** This rallying cry lays the cornerstone for a truly integrated global digital framework, fostering trust and collaboration across borders.
- **Biometric checks** are an important part of IDV systems and must be done on the business side.
- **Widespread adoption and positive perception** discovered by the Regula's research with Forrester show that businesses are mostly ready to implement Digital ID.



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.

