

Regula

| Identity week America · 2026

Physical proof, digital trust

Making hybrid identity work today

SPEAKER

Arif A Mamedov, PhD
CEO, Regula



Name / Surname

Arif A Mamedov

Business role

CEO, Regula · PhD



- Works with government and border-control authorities on large-scale identity programs.
- Connects operational requirements with Regula's R&D and product strategy.
- Focuses on identity verification across physical and digital channels.

One person



Multiple ways to present
identity evidence

PHYSICAL ID ■



■ ePASSPORT

■ MOBILE CREDENTIAL



Government-backed digital credentials are entering everyday use



21 U.S. states + Puerto Rico

had live mDL programs by January 2026.



By the end of 2026

every EU Member State must provide at least one European Digital Identity Wallet.



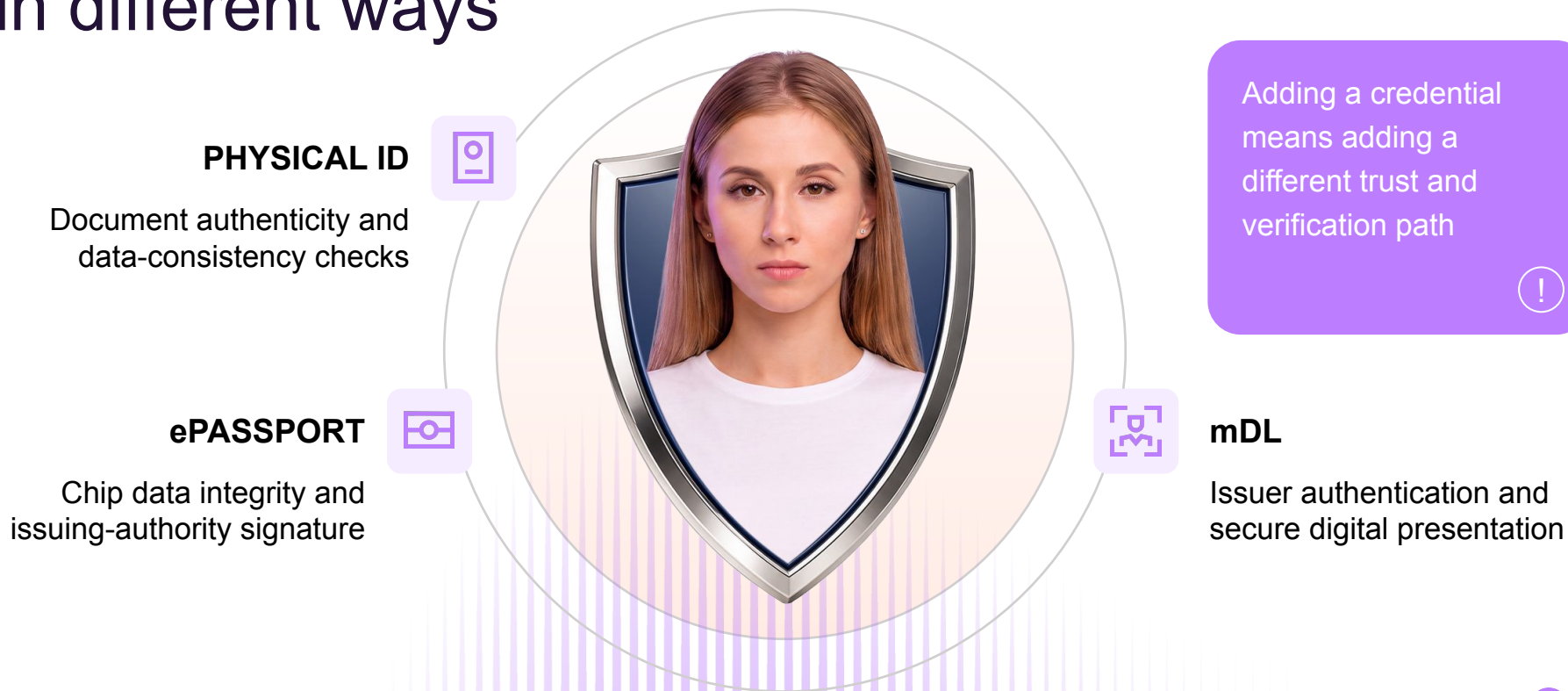
By 2030

at least 80% of EU citizens should be able to use a digital identity solution for key public services.



Digital credentials are entering existing identity journeys, not waiting for physical documents to disappear.

Different credentials establish trust in different ways



The complexity lands on the verifier

CREDENTIAL TYPES



PHYSICAL ID



ePASSPORT



mDL



WALLET credentials

OPERATIONAL COMPLEXITY

- Formats and protocols
- Trust sources
- Channels and exceptions

**POINT OF
ACCEPTANCE**

verifier +
relying party

Credential diversity becomes operational complexity at the point of acceptance



The strain is already measurable

44%

say automated orchestration is essential for managing diverse user scenarios.

43%

face challenges automating and orchestrating IDV processes.

”

“Much of the complexity falls on the verifier, or RP, to correctly handle different credential formats and associated trust models.”

NIST, Digital Identities: Getting to Know the Verifiable Digital Credential Ecosystem, 2026

The core distinction

VERIFIED  SUFFICIENT

Verification checks the evidence. Policy decides whether it is enough for the transaction.

Same credential. Different requirements.



Age 21+ check

What must be established?

The person is over 21

An issuer-signed age-over-21 attribute may be sufficient

Verified

- Issuer signature valid
- Credential current
- Presentation integrity passed



High-risk account recovery

What must be established?

The presenter is the legitimate account holder

Additional authentication may be required

Before trusting a signal, ask three questions

Origin

Where did it come from?

Capture

How was it captured?

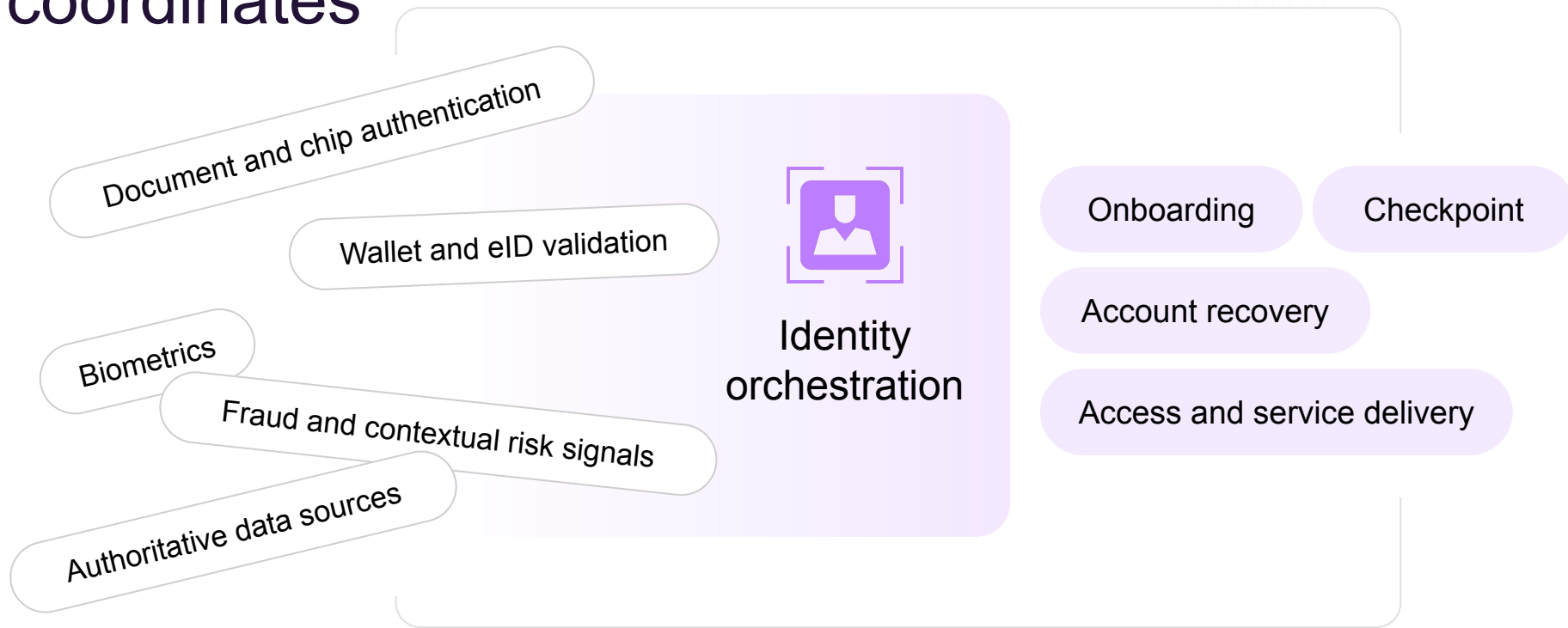
Consistency

Does it agree with the other evidence?



Hybrid identity needs
multi-credential
orchestration

What multi-credential orchestration coordinates



Orchestration assembles the right capabilities for each identity journey



Four principles for multi-credential orchestration

Composable capabilities

Combine document, chip, wallet, biometric and risk checks as needed

Preserved context

Pass structured results, provenance and confidence with defined data controls

Separated verification and acceptance

Let technical verification evolve independently from business policy

Journey-centered orchestration

Select verification capabilities according to the use case and its risk

Separate technical verification from business acceptance

Technical verification

- Credential authenticity and status
- Issuer and holder binding
- Checks performed and confidence signals

Output: structured verification result
Owner: verification and technical services

Business/policy acceptance

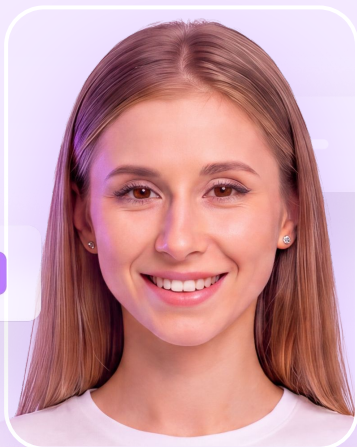
- Transaction risk
- Regulatory and service requirements
- Required evidence and exception rules

Output: accept, request more evidence, review or reject
Owner: the relying party, risk and compliance functions

- **Verification** establishes what the evidence shows.
- **Policy** determines what the organization will accept.

Orchestration routes to the missing proof

Verified mDL



What does the transaction require?

- Issuer authenticated
- Credential current
- Secure presentation verified



Age-restricted transaction

Age over 21 established

→ **Proceed**

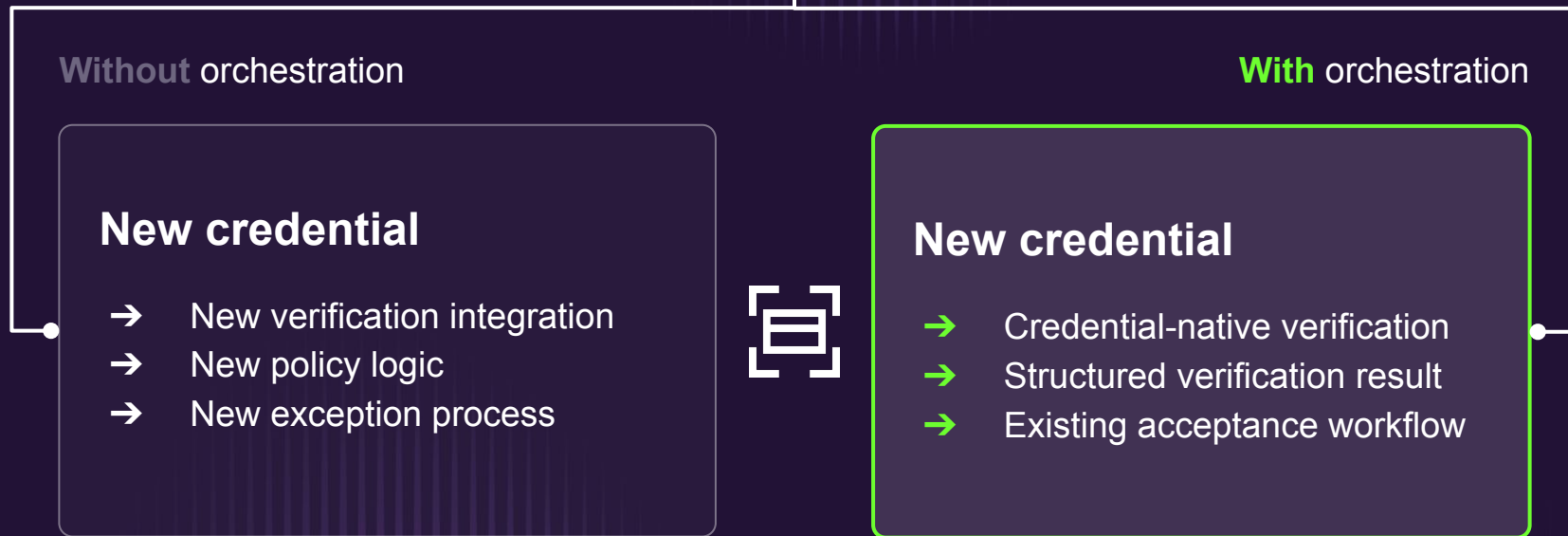


High-risk account recovery

The mDL verifies the person, but not their connection to this account

→ **Use an approved account recovery method**

Adding a new credential path



The credential path changes. The entire operating process does not have to be rebuilt.

How to apply this to an existing workflow

1

Choose an existing transaction

Select a workflow that already accepts identity evidence.

2

Set the acceptance criteria

State what must be established and who owns the final decision.

3

Connect native verification results

Pass credential-specific checks, confidence and provenance into the workflow.

4

Configure additional checks and exceptions

Define when to proceed, request more evidence or send the case for review.

Making hybrid identity work today

Accept different credentials
without building a different
process for each one.





Identity Verification for the AI Era

Forensic Science Inside

Regula