IOTA

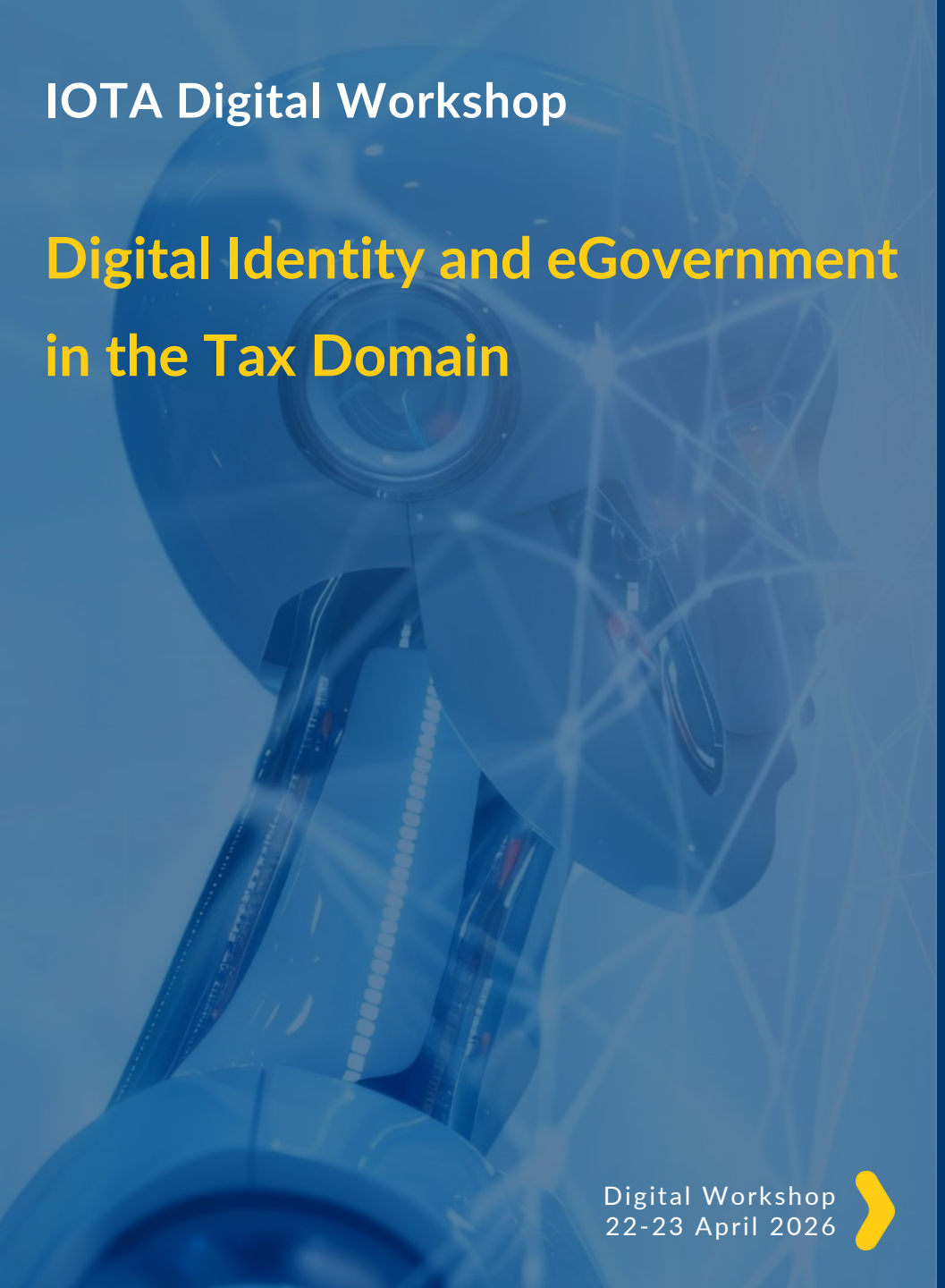
IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

FEEDBACK
Group Discussion Session 1
Interactive Case Study

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain



Digital Workshop
22-23 April 2026

Executive Snapshot

Domestic digital identity systems are relatively mature
Participants described national digital identity solutions as functioning and often multi-channel, especially for domestic users.

Cross-border SME access is the main gap
The harder problem is proving that a person is authorised to act for a company across borders (proof of representation), as currently various documents are requested to be submitted by the legal representative.

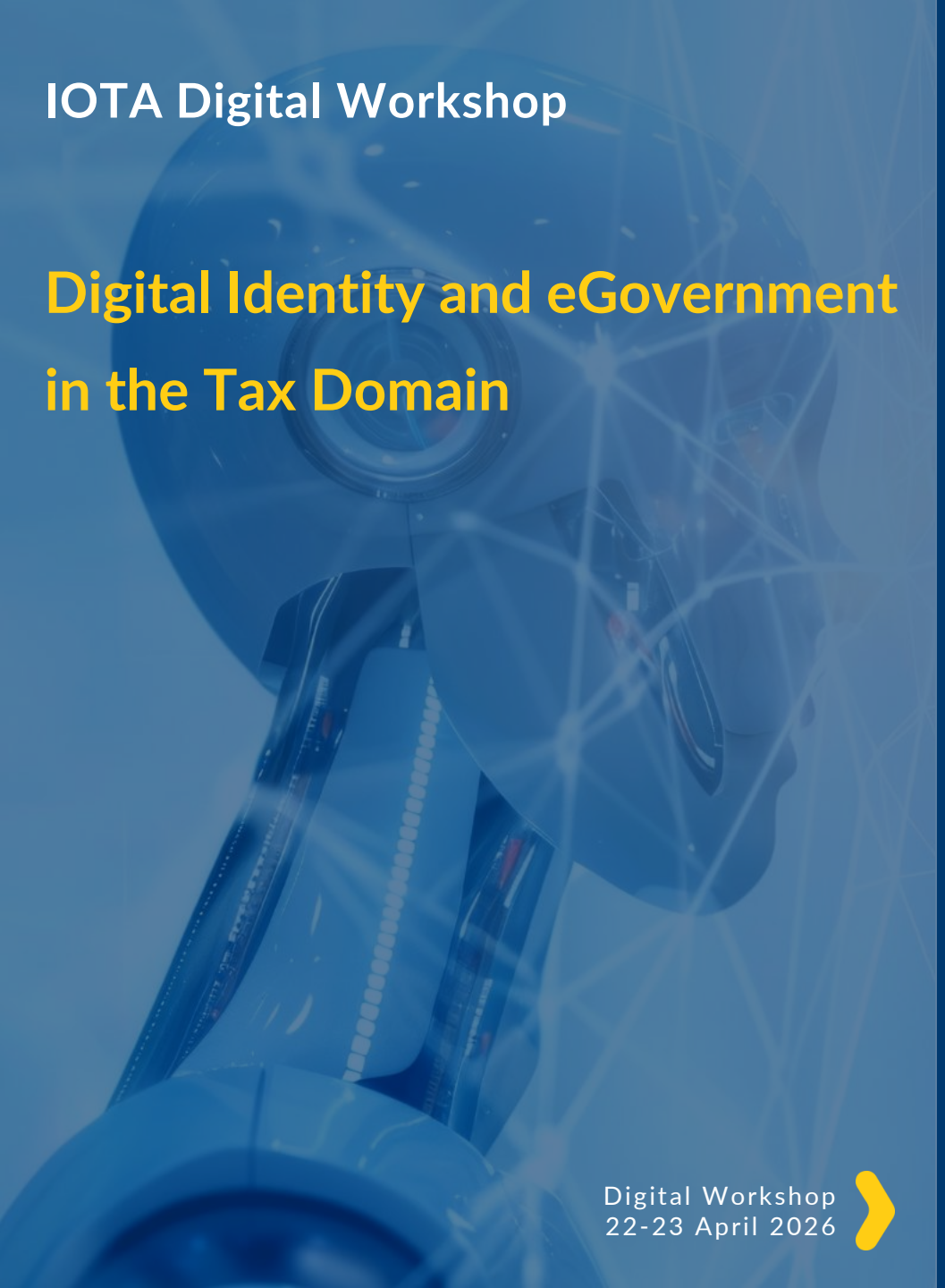
Future EU wallet solutions look promising
The EU Digital Wallets for individuals and businesses have many benefits, but they are not yet operational enough to solve the problem today on managing cross-border interactions.

Strongest recommendations:

- Create a common cross-border trust framework for digital identity of businesses and representatives.
- Use the EU interoperable wallet/business identity solutions when they become operational, while finding solutions for today and for the non-EU cross-border interactions.

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain



Digital Workshop
22-23 April 2026

Main characteristics of national digital identity systems

- **Strong domestic digital identity systems**
  Identity management can work well inside national ecosystems, in various architectures.
- **Main weakness**
  Difficult to manage the proof of non-resident companies' representatives.
- **Usability concern**
  Some company-access solutions introduce costs or an extra burden for business users.
- **Implication**
  Digital identity should be designed as a layered identity-and-authorisation ecosystem.

IOTA

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

Digital Workshop
22-23 April 2026

1. Identity and Access Risks

Design response

- Separate authentication and authorisation as different layers.
- Use fine-grained, role-based mandates for company representatives.
- Allow revocation and limited scope for each authorised user.
- Retain fallback onboarding, but keep it risk-based and streamlined.

Key takeaway

How to build digital identity solutions to ensure **trusted proof of representation.**

IOTA

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

2. Architecture Model Risks

- **Government-centralised**
  Strong public trust and consistency, but risks include interoperability problems, foreign-user onboarding difficulty, and dependence on national identifiers.

- **Private identity providers**
  Can improve usability and reach, but raises concerns about reliance on external providers, governance, cost, and vendor lock-in.

- **Hybrid / federated**
  Some company-access solutions introduce costs or an extra burden for business users.

Leaning of the discussion group

- Each of the architecture models has advantages and constrains, but the management of cross-border companies is a problem in each of the models.

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

3. Cross-Border Interoperability

Main findings

- Create a common cross-border trust framework for business identity and representatives
- Recognise core attributes: company existence, representative status, and scope of authority
- The EU Digital Wallets for individuals and businesses will have many benefits and will solve some of the problems within EU

Key takeaway

- Need to find solutions to manage digital identity for cross-border interactions NOW

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

4. Security & Fraud Risks

- **Major concerns included fraudulent company representation and cybersecurity** - identity theft, stolen credentials, and misuse of public company data
- Manual onboarding can reduce risk but does not eliminate forgery or impersonation
- Participants also emphasised auditability, anomaly detection, and the need to share actionable information across administrations when abuse is detected

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

SME User Perspective

- SMEs face high administrative burden, poor scalability of manual checks, and sometimes cost barriers for access.
- Usability was treated as strategic, not cosmetic: solutions should work on mobile devices and require minimal repeated data entry.
- The group argued that better user journeys also make tax administrations more efficient by reducing back-office handling.

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

Cross-Cutting Recommendations

Most important recommendation

Develop a trusted cross-border business identity framework that verifies the representative, the company, and the scope of authority.

Separate core functions

Authentication and authorisation should be different layers, with granular mandate controls.

Electronic fallback route

Keep fallback channels for users who cannot use standard digital identity options, but make them streamlined and risk-based.

Resilience

Avoid single points of failure and support alternatives.

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Case Study

Digital Identity management for a cross-border business company (EU/non-EU)

Digital Workshop
22-23 April 2026

Cross-Cutting Recommendations

- Most important recommendation
  Develop a trusted cross-border business identity framework that verifies the representative, the company, and the scope of authority.
- Separate core functions
  Authentication and authorisation should be different layers, with granular mandate controls.
- Electronic fallback route
  Keep fallback channels for users who cannot use standard digital identity options, but make them streamlined and risk-based.
- **Resilience** - Avoid single points of failure and support alternatives.
- **Reduce SME burden**
  Limit unnecessary local-representation requirements, paid onboarding, and repetitive manual evidence.
- **Strengthen monitoring**
  Use audit trails, suspicious-behaviour detection, and better information sharing across borders.
- Operational path
  Adopt wallet/business identity solutions once they become operational at scale, but find solutions for today.

Bottom-line recommendation:

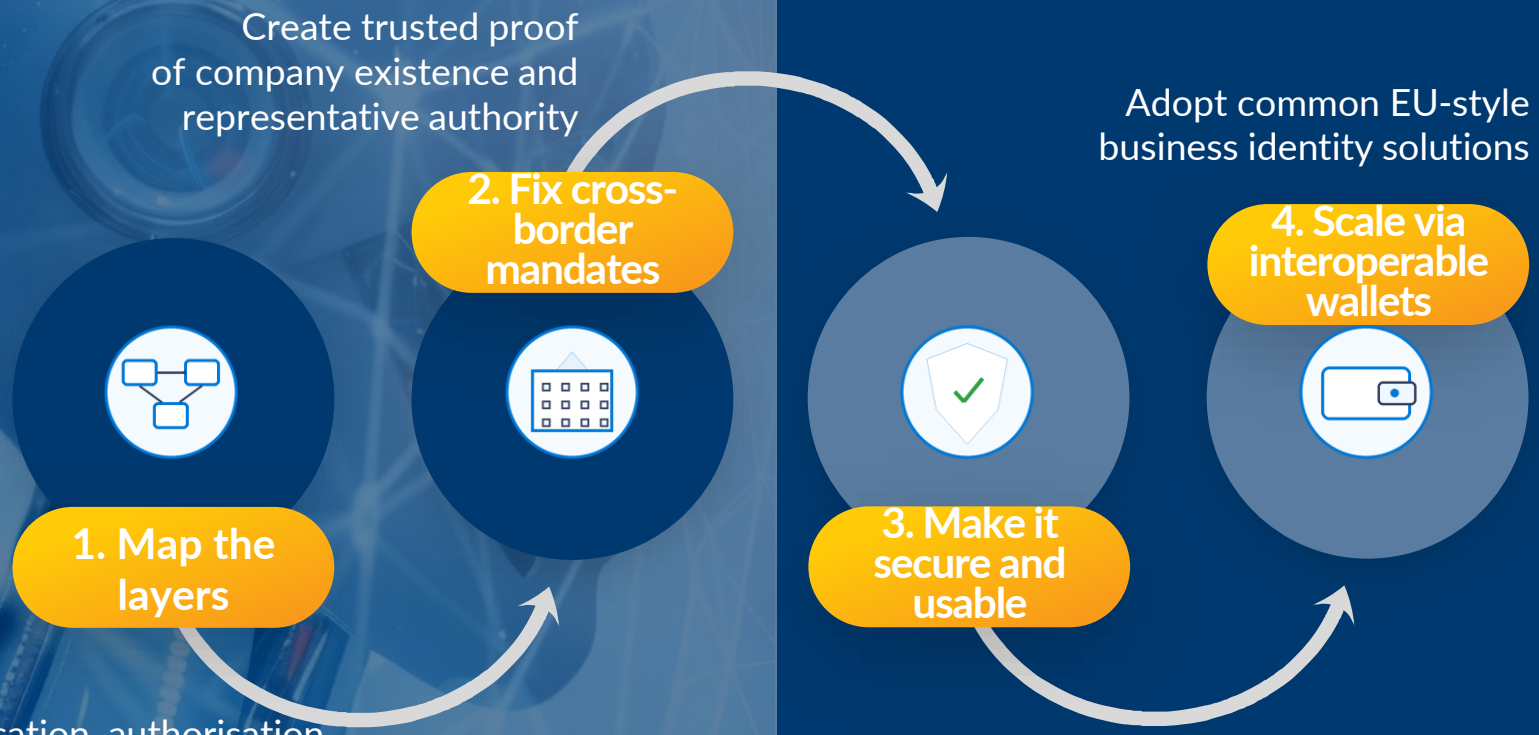
Prioritise a common cross-border trust framework while maintaining practical electronic fallback arrangements.

IOTA

IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

Closing Roadmap



Final message

Domestic digital identity is comparatively mature, but trusted cross-border business representation remains the unresolved challeng and we need to find solutions now. Progress depends on combining trust, usability, and interoperability.

IOTA