



IOTA Digital Workshop

Digital Identity and eGovernment in the Tax Domain

22-23 April 2026
Digital Event via Microsoft Teams

GROUP DISCUSSION 1

Thursday, 22 April 2026, 11:45 - 13:00 (CEST)

AIM

The group discussion session will provide participants with the opportunity to:

- Discuss key takeaways from the plenary sessions' presentations, including solutions, challenges and lessons learned
- Exchange practical experiences on digital identity solutions
- Share their approaches on exploring risks and design recommendations when implementing digital identity solutions for cross-border SME taxpayers using digital tax services, particularly under different identity architecture models.

Group discussions will aim to surface practical recommendations that participants can apply in their own work, such as implementation challenges, systems architecture, and possible future developments of digital identity solutions.

FORMAT

The session is intended as a facilitated group discussion. The composition of the group will be published on the IOTA event's dedicated webpage once the registration process closes. The group will have a designated breakout room.

The chairperson will be responsible for moderating the discussion. The chairperson is not expected to be experts who can answer every question. The chairperson should guide the conversation among the group members and contribute to their questions and views, too.

Notes from the group discussions will be generated automatically by Microsoft Copilot tool, reviewed and used for the plenary presentation, in Power Point format. The chairperson will still report the group summary and conclusions at the plenary session and can delegate the reporting role to a volunteer in the group.

TIMING

- Technical check and introduction (5 minutes)
- Group discussion on the following questions (60 minutes)
- Summary and finalising the feedback from the discussion (10 minutes)



REQUIRED INPUT

The participants will discuss the following topics:

- I. **What is the main characteristic of your tax administration's digital identity system? Please shortly answer the question (about 1 minute)**
- II. **Case study scenario and discussion questions**

The participants will discuss the bellow case scenario and debate the related questions.

- **Presentation of the case study**

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

Scenario:

A medium-sized company "SME", registered in **Country A**, sells goods online across several European countries.

The company must interact digitally with the tax administrations of:

- Country A – corporate income tax and domestic VAT
- Country B – VAT registration under OSS/IOSS scheme
- Country C – digital reporting obligations for cross-border sales

SME wants to **manage all tax obligations online** using the tax administrations' e-services.

The company appoints a **tax manager** and an **external accountant** who both need access to the relevant digital services.

Current policy initiative

Country B is implementing a **new digital identity framework for tax e-services** and is considering different architecture models.

The objective is to enable **secure authentication for domestic and cross-border users**, including SMEs and their representatives.

Three possible models are being considered:

1. **Government-centralised digital identity system**
 - State-issued digital identity for businesses and individuals
 - Managed by a national public authority
 - Used across all government services
2. **Private sector identity providers**
 - Authentication through **bank ID / trusted private providers**
 - Government services rely on federated authentication
3. **Hybrid / federated model**
 - Combination of **government identity and recognised private providers**
 - Interoperable through an identity federation framework

The system must also be compatible with **cross-border access for foreign SMEs**.

Exercise Task

Participants are asked to analyse the case and identify key risks, implementation challenges and possible mitigation measures when designing a digital identity solution for cross-border tax e-services.

The participants will prepare:

- 3 key risks
- 1 recommendation



The discussion should consider:

- SMEs operating in multiple jurisdictions
- Cross-border recognition of identities
- Authorisation of company representatives
- Security and fraud risks
- User experience and accessibility

- **Discussion questions**

1. Identity and Access Risks

- What risks arise when authenticating cross-border SME users in national tax systems?
- How should tax administrations manage **authentication vs authorisation** (who the user is vs what they are allowed to do)?
- What risks exist when **multiple representatives** (tax advisers, accountants) access the system?

2. Architecture Model Risks

For each model below, identify **key advantages and risks**.

Government-centralised digital identity system

- What are the strengths of a state-controlled identity?
- What are the scalability or interoperability challenges, particularly for foreign users?

Private identity providers (e.g. bank ID)

- What risks arise from reliance on private providers?
- How could vendor lock-in, liability, or trust frameworks affect tax administrations?

Hybrid / federated model

- What governance or interoperability risks could appear?
- How complex would identity assurance levels and trust frameworks become?

3. Cross-Border Interoperability

- What challenges may arise when foreign SMEs access national tax portals?
- How should systems ensure recognition of foreign digital identities?
- What risks exist if identity assurance levels differ between countries?

4. Security and Fraud Risks

- What fraud or identity-theft risks could arise in cross-border digital tax services?
- How can tax administrations mitigate risks related to: stolen credentials, impersonation, fraudulent company representation

5. SME User Perspective

- What barriers might SMEs face when accessing digital tax services abroad?
- How can systems balance security, usability, and accessibility?

III. Reporting in the plenary session (23 April 2026)

- Main findings based on the discussion questions
- Recommendations
- Key concerns/experiences/outcomes