Digital Identity & Trust Services Roles & Credentials Aligned with the ECSF

DTCoE's Contribution to the EU Cybersecurity Skills Framework (ECSF)

DIGITALTRUST
Center of Excellence

About Us

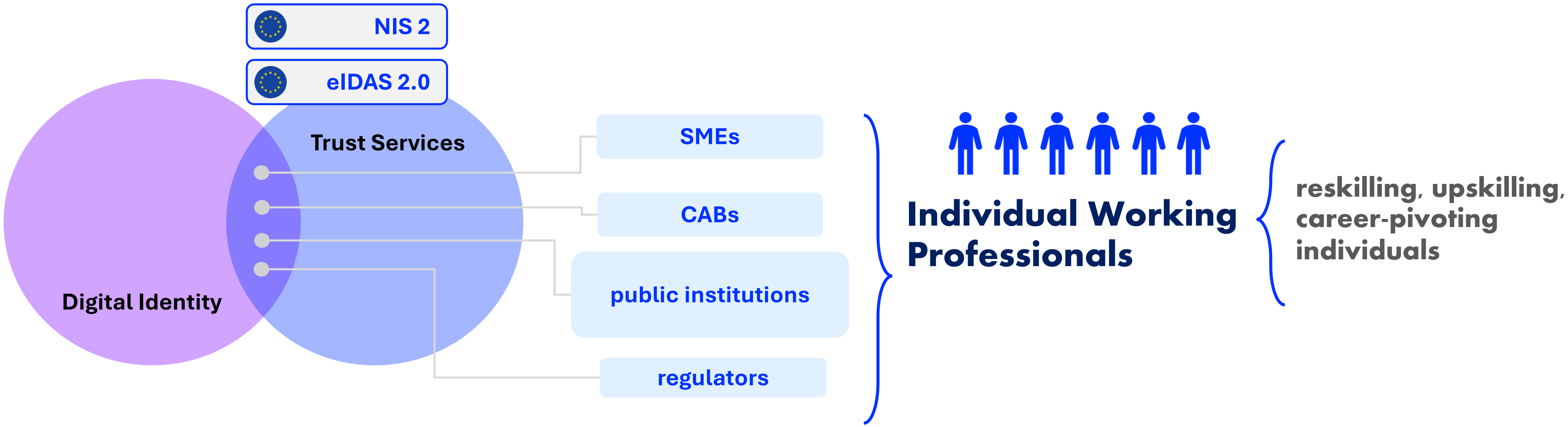
Digital Trust Center of Excellence

Independent, vendor-neutral credentialing organization, founded by working professionals in the field of conformity assessment and engineering for digital identity and trust services.

Public-Interest Mission:

- the **reduction of the skills & gender gap** in the digital identity & trust services workforce;
- **matching workforce demand with supply**, by developing credentials that are aligned with existing job roles of the industry and conform to peer-reviewed learning objectives.

Target Audience:



NIS 2

eIDAS 2.0

Trust Services

Digital Identity

SMEs

CABs

public institutions

regulators

Individual Working Professionals

reskilling, upskilling, career-pivoting individuals

Problem Definition

- Qualified Trust services incidents (misissuance, non-compliance) common causative factor: **human error** & **skills gaps**[1]
- **eIDAS 2.0**[1] **& NIS2**[2] introduce obligations for skilled personnel but offer no structured validation path.
- Skills gap undermines security, compliance, and public trust.
- No structured approach exists today to define or validate these role-based competencies for digital identity and trust services.

> **Without professional skills validation, we cannot ensure the sense of trust into human processes.**

[1] ENISA CIRAS, ENISA Annual Reports - Trust Services Security Incidents 2023 & 2024.

[2] Article 24 – Requirements for Qualified Trust Service Providers, Annex II – Requirements for Qualified Trust Service Providers.

[3] Article 7(f) – Responsibilities of Member States, Article 21(g) – Cybersecurity Risk Management Measures, Recital 78.

DIGITALTRUST
Center of Excellence

Current Progress

Developed **job roles** that make the digital identity & trust services **labor market more transparent** for SMEs, public authorities, and professionals.

↓

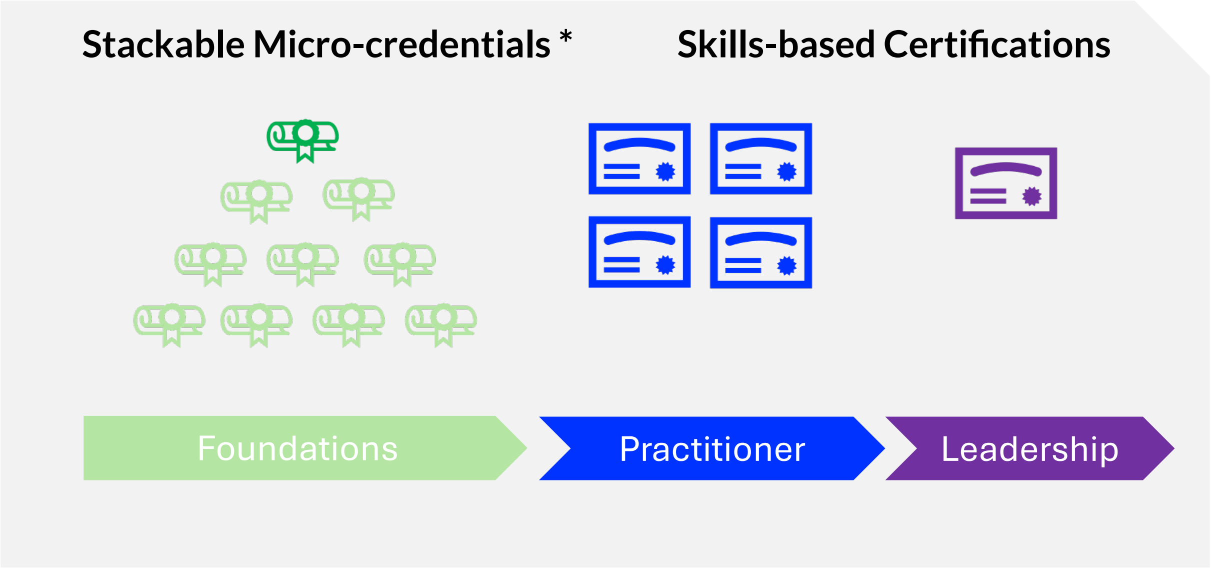
Identified **KST gaps and overlaps** between ECSF and DTCoE's roles.

↓

Identified **career trajectory maps** showing how people from adjacent IT/cybersecurity fields can enter and progress into trust services roles.

↓

Developed a **tiered credentialing offerings** catalog. →



* aligned with EC Recommendation of 16/06/2022 on setting out a European approach to micro-credentials for lifelong learning and employability.

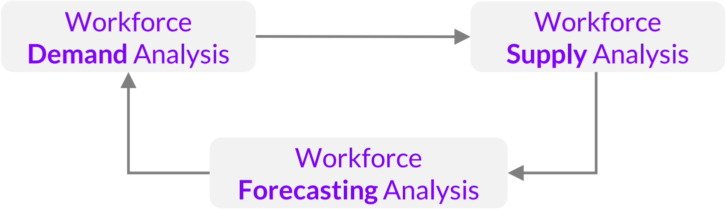
Roles Development Methodology

DIGITALTRUST
Center of Excellence

Our methodology* integrates ECSF principles into the definition and validation of real-world job roles in digital identity and trust services.

ⓘ Methodology key elements and steps remain confidential and have been abstracted from the presentation.

1. Source Inputs (Multi-layered Evidence Base)



Workforce **Demand** Analysis
Workforce **Supply** Analysis
Workforce **Forecasting** Analysis

Regulatory context: eIDAS 2.0, ETSI EN 319 standards, WebTrust for CA, CA/B Forum Requirements.

Operational & labour market artifacts: Role descriptions from audits, job postings, process manuals.

Knowledge elicitation: Structured interviews, focus groups, and incident analysis with subject-matter experts.

Output: **Draft functional profile per role**

2. Job Practice Analysis

Utilize **CEN/TR 16234 (e-CF)** as a taxonomy and initial competencies framework: use a common competencies vocabulary for the in-scope roles.

Elicitation of cognitive demands/KSTs through structured surveys and psychometric interviews.

Mapping each role into e-CF **Competencies** and **Proficiency Levels**.

Output: **Draft competency profile per role**

3. ECSF Integration

Utilize **ECSF** as a target, e-CF anchored, role mapping framework.

Mapping each KST element to one or more ECSF roles, with annotations where roles are hybrid or cross-functional.

Retaining KSTs that are needed for the role but do not exist in ECSF.

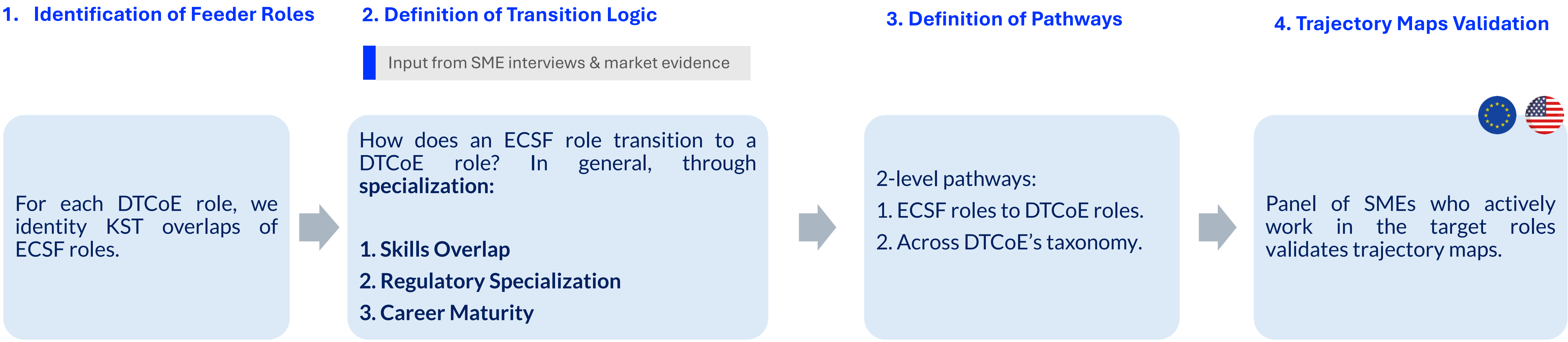
Validating initial profiles via participatory workshops with stakeholders across public, private, and regulatory sectors.

Output: **Final validated role profile**

Trajectory Maps Development Methodology

Our methodology* integrates ECSF principles into the definition and validation of real-world job roles in digital identity and trust services.

ⓘ Methodology key elements and steps remain confidential and have been abstracted from the presentation.



1. Identification of Feeder Roles

For each DTCoE role, we identity KST overlaps of ECSF roles.

2. Definition of Transition Logic

Input from SME interviews & market evidence

How does an ECSF role transition to a DTCoE role? In general, through **specialization:**

1. Skills Overlap

2. Regulatory Specialization

3. Career Maturity

3. Definition of Pathways

2-level pathways:

1. ECSF roles to DTCoE roles.
2. Across DTCoE's taxonomy.

4. Trajectory Maps Validation

Panel of SMEs who actively work in the target roles validates trajectory maps.

Output: **Trajectory map per role**

DIGITALTRUST
Center of Excellence

Indicative Use Cases

DTCoE Profiles to ECSF Roles & KSTs mapping

Digital Trust Services Manager

Sector-Specific

- Knowledge
- Skills
- Tasks

Leads the governance, compliance, and operational integrity of digital trust services under. Ensures that trust services operate within regulatory, security, and policy boundaries and that they maintain continuous conformity for audit and supervision.

Role Trajectory Map

Certification Scheme

ECSF Alignment

2.1 Chief Information Security Officer	Knowledge	Skills	Tasks	e-CF Mapping
2.3 Cyber Legal, Policy & Compliance Officer	Knowledge	Skills	Tasks	
2.6 Cybersecurity Auditor	Knowledge	Skills	Tasks	
2.10 Cybersecurity Risk Manager	Knowledge	Skills	Tasks	

Regulatory/Compliance Context

Digital Trust Services Engineer

Sector-Specific

Knowledge

Skills

Tasks

Designs, implements, and maintains the technical infrastructure that underpins qualified trust services, ensuring cryptographic security, availability, and compliance with sectoral and industry requirements. Bridges engineering practice with policy, operating within rigorously controlled environments.

Role Trajectory Map

Certification Scheme

ECSF Alignment

2.5 Cybersecurity Architect	Knowledge	Skills	Tasks	e-CF Mapping
2.8 Cybersecurity Implementer	Knowledge	Skills	Tasks	
2.2 Cyber Incident Responder	Knowledge	Skills	Tasks	

Regulatory/Compliance Context

Digital Trust Services Auditor

Sector-Specific

- Knowledge
- Skills
- Tasks

Performs independent conformity assessments or internal audits of qualified trust services and WebPKI infrastructures against sectoral and industry requirements. Ensures trust services meet regulatory, technical, and assurance requirements, and produces audit opinions recognized by supervisory authorities and market gate-keepers.

Role Trajectory Map

Certification Scheme

ECSF Alignment

2.3 Cyber Legal, Policy & Compliance Officer	Knowledge	Skills	Tasks	e-CF Mapping
2.6 Cybersecurity Auditor	Knowledge	Skills	Tasks	

Regulatory/Compliance Context

DIGITALTRUST
Center of Excellence

Wider Impact

- **Sectoral Extension**: ECSF is extended to the digital identity & trust services domain, through the mapping of ECSF roles to domain-specific roles.
- **Career Pathways**: our effort defines seniority paths in the digital identity & trust services domain but also introduces entrance pathways from adjacent cybersecurity roles defined in ECSF.
- **Credentialing**: ECSF becomes the reference backbone for training aligned to certification for digital identity & trust services credentials.
- **Policy Alignment**: demonstrates to policymakers how ECSF-aligned roles help with **compliance capacity**. In this way, ECSF becomes a tool for **regulatory workforce planning**, not just HR.

DIGITALTRUST
Center of Excellence

Thank You!

www.dtcoe.org