DIGITALTRUST®
Center of Excellence

POLICY BRIEF

Bridging the Human Skills Gap in Digital Identity and Trust Services

The Case for Competency-Centered Action

Executive Summary

Digital identity and trust services are critical pillars of secure eGovernment and enables of digital transformation across the EU. Regulatory initiatives such as eIDAS 2.0 and the NIS2 Directive underscore their importance, but the human capital needed to support them remains critically underdeveloped.

Despite technological progress, organizations across public and private sectors face an acute shortage of skilled professionals; from identity proofing specialists and PKI & SSI engineers, to trust services managers and compliance officers, the talent gap undermines security, compliance, and digital trust at a structural level.

The **Digital Trust Center of Excellence** (DTCoE) responds to this challenge with a targeted, community-driven initiative to define, validate, and recognize professional competencies. Our approach is vendor-neutral, aligned with the European Cybersecurity Skills Framework (ECSF), and informed by real-world operational needs.

By establishing structured pathways for certification, we support regulatory compliance, strengthen workforce resilience, and foster cross-sector collaboration. These efforts aim to build a more capable, accountable, and future-ready digital trust workforce, essential to delivering on Europe's Digital Decade goals.

Introduction

Digital identity and trust services are central components of eGovernment, cybersecurity, and digital transformation; two inter-related domains that are rapidly evolving under the influence of regulatory frameworks of eIDAS 2.0 as well as the NIS2 Directive.

Despite technological advances, the sector faces a critical shortage of qualified professionals across core roles such as identity proofing, PKI engineering, and compliance auditing.

DTCoE proposes a targeted initiative to define, validate, and recognize competencies through a vendor-neutral framework aligned with the European Cybersecurity Skills Framework (ECSF). This initiative aims to support regulatory compliance, promote workforce development, and build a more resilient digital trust ecosystem.

The Criticality of Human Factor

Technological investments in infrastructure, software, and cryptography often overshadow a critical causal factor: **human error**. We find that incidents such as certificate misissuance or delayed revocations are not just technical errors or malicious acts, but are often rooted in:

- Manual procedural slips
- Misinterpretation of standards and compliance requirements
- Reliance on static configurations
- Incomplete quality assurance
- Organizational silos and governance gaps

These failures are typically unintentional, triggered by complexity, outdated knowledge, or fragmented processes.

Workforce Skills Shortage

DTCoE, having analyzed[1] publicly reported incidents in the WebPKI ecosystem, as well as QTSP-reported incidents, has identified a persistent causal factor of incidents: **human error**. This confirms insights of other researchers as well as ENISA's[2] regarding the widening gap between policy ambition and workforce readiness.

Evidence points to a critical shortfall in skilled professionals:

70% of organizations report insufficient staff for PKI operations, with frequent outages[3]

more than half of global organizations identify **insufficient skills** (52%) and **insufficient resources** (64%) as key barriers to deploying and managing their Public Key Infrastructure (PKI)

human ERROR top among the primary causal factors of **WebPKI** & **trust services** [5,6] incidents

- **Regulatory Misinterpretation**
- **Organizational Misalignment**
- **Poor Quality Assurance Practices**
- **Procedural Oversight and Manual Missteps**

These indicators highlight a specific scarcity in trust-related professions, compromising both capacity and effectiveness.

DTCoE's Strategic Initiatives

There is a unique window to address these systemic challenges through ECSF-aligned credentialing initiatives that promote role clarity, skill recognition, and continuous development. By creating clear professional pathways and competency benchmarks, regulators and institutions can unlock long-term improvements in service quality, compliance, and digital trust.

DTCoE has launched two strategic initiatives:

Industry Insight

The **Industry Insight** initiative serves as the intelligence backbone of DTCoE's mission, focusing on mapping the evolving landscape of job roles in digital identity and trust services.

Recognizing that these roles are foundational yet often poorly defined, DTCoE conducts targeted workforce studies to identify key job functions, required competencies, and cross-functional intersections with compliance, cybersecurity, governance, and engineering.

Our research examines sector-specific skill gaps, talent shortages, and the impact of emerging technologies, such as decentralized identity and AI-based proofing on workforce readiness.

By revealing barriers to entry, reskilling opportunities, and professional pivot points between cybersecurity and digital identity, this initiative informs national and cross-border strategies while laying the groundwork for inclusive, agile career development pathways.

---

[1] Incidents were sought, collected, and analyzed through: (i) Mozilla CA Program bugs, (ii) ENISA CIRAS, (iii) ENISA Annual Reports - Trust Services Security Incidents 2023 & 2024 , (iv) academic papers: Serrano, N., Hadan, H., & Camp, L. J. (2019). A Complete Study of P.K.I. (PKI's Known Incidents). SSRN Electronic Journal., Johnson, S. B., Ferro, K., L. Jean Camp, & Hadan, H. (2021). Human and Organizational Factors in Public Key Certificate Authority Failures., Abbott, J., Johnson, S., Ferro, K., Blasio, P., Swiler, E., & Jean, C. L. (2024, August 2). Pki Incident Reporting Trends: What Can We Learn from Community Reporting?

[2] Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats. (n.d.). ENISA. https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

[3] 2024 PKI & Digital Trust Report. (2024). Keyfactor. https://www.keyfactor.com/resources/digital-trust/2024-pki-and-digital-trust-report.

[4] 2022 Global PKI and IoT Trends Study | Entrust. (2022). Entrust.com. https://www.entrust.com/resources/reports/global-pki-iot-trends

[5] ENISA (2025). Annual Report Trust Services Security Incidents 2024.

[6] Johnson, Ferro, Jean Camp, & Hadan (2021). Human and Organizational Factors in Public Key Certificate Authority Failures

The **Competencies & Skills Validation** initiative transforms complexity into clarity by systematically defining, validating, and structuring professional competence in digital identity and trust services.

Recognizing the fragmented nature of job roles across technical, compliance, policy, and operational domains, **DTCoE** conducts participatory research with practitioners, employers, regulators, and academia to co-create real-world role definitions. These are not theoretical constructs, but evidence-based frameworks grounded in actual practice, capturing knowledge, behavioral, and cognitive dimensions of professional performance.

Outputs include competency profiles, modular frameworks for workforce planning, and credentialing schemes aligned with international standards. Informed by and aligned to the European Cybersecurity Skills Framework (ECSF), this initiative supports the development of qualifications and career pathways that meet the needs of professionals, organizations, and regulators alike. It enables individual growth, organizational readiness, and sector-wide recognition of digital identity and trust as a critical discipline within cybersecurity.

The Digital Trust Center of Excellence provides a comprehensive, vendor-neutral approach to strengthening the digital identity and trust workforce. Our initiatives include multi-stakeholder competency frameworks, evidence-based validation models, and certification programs that align with regulatory priorities such as eIDAS 2.0 and NIS2.

By supporting cross-sector contributors and enabling upskilling and reskilling, we help build resilient, future-ready workforces.

Our work establishes clear career pathways in line with ECSF role profiles, supports public-sector capacity building, reduces risk linked to under-qualification, and improves talent retention, hiring, and workforce mobility across the digital identity and trust services ecosystem.

Why Credentialing Matters

Credentialing and continuous skills validation are not nice-to-haves but essential components of trust.

While technical controls and process frameworks serve as important guardrails, they are only as effective as the people who implement and oversee them. Without a systematic approach to verifying competencies, organizations risk relying on assumptions about knowledge and preparedness. Credentialing not only formalizes essential skill sets but also reinforces a culture of accountability, where trustworthiness is demonstrable and not presumed:

- Standards define roles: Clearly articulated frameworks support hiring, training, and professional development.
- Validated skills prevent errors: Credentialing ensures individuals can handle evolving trust infrastructures.
- Boost confidence and retention: Certified professionals demonstrate accountability and expertise
- Bridge talent gaps: Credentialing creates scalable talent pipelines aligned with sector needs.

Credentialing directly tackles both the quality and quantity issues by reducing human error risk while building workforce resilience.

Alignment with Key Frameworks

To ensure that our efforts serve the broader digital policy landscape, our initiatives are intentionally aligned with major EU cybersecurity and digital identity strategies. By grounding our work in the regulatory, workforce, and risk-reduction priorities set forth by EU institutions, we contribute to a coherent and forward-looking approach to building trust in digital public infrastructure.

Our initiative supports:

- eIDAS 2.0 objectives on workforce reliability and legal trustworthiness
- ECSF roles, knowledge, skills, and tasks.
- ENISA's recommendations for reducing human-factor risks in digital identity systems
- EU/National cyber-skills agendas, linking credentials to capacity building

The following table illustrates how our initiatives directly support and operationalize these strategic frameworks. By translating policy objectives into actionable workforce development measures, we bridge the gap between regulation and real-world capacity building.

Framework	DTCoE Contribution
eIDAS 2.0	Supports workforce reliability through certified roles.
NIS2	Addresses human factor risks through skill validation.
ECSF	Aligns job roles, KSAs, and qualification models.

Call to Action

We invite **working professionals** of all market dimensions – regulators, QTSPs, auditors, and academics to help shape the future of digital identity and trust services workforce.

Share your interest in reviewing competency profiles, participating in delineation studies, developing examination blueprints or supporting awareness efforts.

Take the next step at: dtcoe.org/get-involved

Policy Recommendations

As the EU accelerates its adoption of digital public infrastructure, cross-border eID, and qualified trust services under eIDAS 2.0, there is growing recognition that technical infrastructure must be matched by an equally robust human infrastructure. However, the professionals who design, operate, audit, and regulate digital identity systems remain undersupplied, inconsistently trained, and underrepresented in national and EU-level workforce planning.

To strengthen EU's digital trust backbone, we propose the following targeted policy actions:

Establish Dedicated Workforce Targets for Digital Identity and Trust Services

The Digital Decade targets broadly refer to cybersecurity and ICT specialists. We recommend that the EU introduces specific indicators for the digital identity and trust services workforce, including:

- The number of professionals certified in identity proofing, PKI engineering, and trust services management.
- Workforce diversity and mobility across the public/private/regulated sectors in digital identity roles.
- Institutional capacity benchmarks for supervisory authorities, QTSPs, and conformance assessment bodies.

This will help differentiate the unique human capital needs of trust services from broader cybersecurity roles and allow more tailored investment and monitoring.

Incorporate Role-Based Competence Requirements into eIDAS 2.0 Implementation

The successful rollout of the EU Digital Identity Wallet, qualified trust services, and remote identity proofing hinges on professionals who meet high-assurance criteria and not just technical functionality.

We recommend that:

- eIDAS supervisory frameworks include expectations for certified personnel in specific roles such as Identity Proofing Specialist or Qualified Trust Services Manager.
- Regulatory & compliance frameworks (e.g. eIDAS 2.0, CA/B Forum, Requirements) be enhanced to include voluntary, minimum competency models for digital trust operators, managers, and auditors.
- Role-specific qualifications be recognized in delegated acts, procurement, and service-level agreements.

Support the Validation of Competencies for Emerging Roles

Digital identity is evolving rapidly, bringing new risks and new responsibilities, particularly in areas like biometric identity verification, decentralized identifiers, and AI-supported onboarding. We propose that the EU:

- Co-funds pilot programs that define and validate job roles in emerging areas of digital identity & trust services.
- Aligns these with the ECSF profiles where possible, or contribute to ECSF's evolution with sector-specific extensions.
- Encourages the use of evidence-based credentialing models, based on real-world performance and not just theoretical training.

Ensure Inclusion of Digital Identity Roles in the Cybersecurity Skills Academy

While the Cybersecurity Skills Academy addresses general cyber capability gaps, it currently underrepresents digital identity and trust service roles, which are central to both security and digital sovereignty goals. We recommend:

- Expanding the Academy to include dedicated digital identity learning tracks, with recognition of sectoral nuances (e.g., trust services vs. eID vs. SSI).
- Facilitating partnerships with neutral, vendor-independent bodies that can provide domain-aligned professional development, especially for SMEs and public institutions.
- Simplifying access to training and credentialing through modular, stackable micro-credentials tailored to eIDAS 2.0 ecosystem.

DIGITALTRUST ®
Center of Excellence

For more information:

www.dtcoe.org

About DTCoE

The Digital Trust Center of Excellence (DTCoE) was founded in response to a growing, unaddressed need: the widening gap between the increasing complexity of digital identity and trust services and the availability of skilled, competent professionals to support it.

DTCoE operates independently and transparently, guided by principles of vendor neutrality, scientific rigor, and a clear public-interest orientation, grounded in first-hand experience across technical, regulatory, compliance, and auditing domains. Our founding team comprises professionals embedded in the digital identity and trust services ecosystem, dedicated to advancing professional excellence across all job roles