Fostering Professional Excellence in Digital Identity & Trust Services

Building Competence for the Future Global Workforce

Position Paper

DIGITALTRUST
Center of Excellence

Executive Summary

Introduction

Digital trust is the invisible currency of the digital world. Every interaction — from signing a contract online to validating a citizen's identity — relies not only on technology or legal frameworks, but also on the competence and integrity of the professionals who make these systems work. Technology and cryptography, as well as legal frameworks and governance models, form two core pillars of digital trust. Yet it is the competence and integrity of practitioners that serve as the cross-cutting pillar. Without skilled and accountable professionals, neither technology nor regulation alone can deliver an adequate level of trust.

Global View on Digital Identity Initiatives

Governments worldwide are developing their digital identity initiatives and regulated trust services. The EU advances eIDAS 2.0 and the European Digital Identity Wallet; the US sets identity standards through NIST while several States are pioneering mobile driver's licenses (mDLs); India operates Aadhaar; Singapore manages NDID; Bhutan has launched its flagship NDI, and Canada promotes the Pan-Canadian Trust Framework. Despite their differences, these initiatives converge on a principle: digital identity is a matter of trust, governance, and assurance — not technology alone.

However, the workforce behind digital trust remains undefined and unsupported. Unlike medicine, aviation, or auditing, there is no global framework to define, validate, or credential professionals operating in this high-assurance domain. This gap results in fragmented competence requirements, barriers to cross-border recognition, and incidents often linked to skills gaps and human error.

Aligning with Europe's Digital Decade

Europe's Digital Decade 2030 sets a dual ambition: by 2030, 80% of adults should have basic digital skills and Europe should lead in secure digital infrastructure, including cross-border digital identity and trust services. While progress on infrastructure and regulation is advancing, the specialized workforce required to operate and govern these systems remains undefined.

The EU Cybersecurity Skills Framework (ECSF) contributes directly to the Digital Decade skills target by harmonizing role profiles and training pathways for cybersecurity professionals. However, trust service professionals are not included within its scope. Roles such as PKI engineers, identity proofing specialists, and qualified trust service managers, are essential to the security and reliability of Europe's digital trust infrastructure but remain outside existing frameworks.

The Mission of the Digital Trust Center of Excellence (DTCoE)

The Digital Trust Center of Excellence (DTCoE) was founded to close this gap. Firmly believing that digital trust is only as strong as the people who run it, our mission is the professionalization of this workforce, contributing directly to Europe's Digital Decade, complementing the ECSF, and strengthening confidence in digital trust services worldwide.

The Definition of Digital Identity & Trust Services

Digital identity and trust services is not a subset of any single technical discipline. It is a regulated and auditable ecosystem, where legal, technical, and governance frameworks converge to enable confidence in the digital economy.

Digital trust services form the foundation of Europe's Digital Single Market and are increasingly central to global digital transformation. Under eIDAS 2.0 and related frameworks, digital identity, qualified electronic signatures, seals, timestamps, certificates, digital identity wallets, and qualified electronic attestations of attributes (QEAAs) are recognized not as technical add-ons, but as regulated services essential for cross-border trust.

These services are built on strong cryptographic and legal foundations, but their reliability ultimately depends on the competence, ethics, and accountability of the professionals who operate them.

Unlike other regulated fields, there is today no recognized credentialing framework to define, validate, and professionalize the digital trust workforce, in an objective and scientifically valid way, ensuring the possession of minimum qualifications and competence, ethics, and professional integrity of those operating these trust services.

Without such a framework, the digital trust ecosystem remains exposed to fragmentation, uneven competence, and risks arising from human error — even when the technical and regulatory layers are sound.

The Workforce Gap

Today, there is **no global framework** to define or validate the competence of professionals in **digital identity and trust services**. As a result:

- Competence requirements differ across jurisdictions.
- Cross-border interoperability is blocked by inconsistent skillsets.
- Regulators set standards for systems, **not for the workforce** behind them.
- Incidents in trust services (mis-issuance, non-compliance) are often caused by **skills gaps and human error**[1].
- **eIDAS 2.0** and **NIS2** require skilled personnel[2] but offer **no structured validation path**.

Unlike other fields, there is **no body of knowledge, no credentialing framework, no career pathway**. This creates:

- Fragmentation across countries and industries.
- Barriers to global interoperability.
- Inconsistent competence in high-stakes, regulated services.

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

[2] eIDAS 2.0 Article 24 – Requirements for Qualified Trust Service Providers, Annex II – Requirements for Qualified Trust Service Providers, and NIS2D Article 7(f) – Responsibilities of Member States, Article 21(g) – Cybersecurity Risk Management Measures, Recital 78.

Human Error is a Causal Factor

DIGITALTRUST
Center of Excellence

Increasing incidents caused by human error in PKI & Trust Services:

OVER 70% of WebPKI misissuance incidents involve human or organizational error[1]

- Incomplete QA Cycles
- Procedural Oversight & Manual Missteps
- Regulatory Misinterpretation
- Organizational Misalignment
- Dependency on Static Configuration

of global organizations identify **insufficient skills** as a key barrier to deploying and managing their Public Key Infrastructure[4]

4 mil user hours lost[2]

Human Error top among the primary causal factors of incidents[3]

[1] 2022 Global PKI and IoT Trends Study | Entrust. (2022). Entrust.com. https://www.entrust.com/resources/reports/global-pki-iot-trends

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

[3] Incidents were sought and collected via: (i) Mozilla CA Program bugs during the period 2009-11 to 2025-07, (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?

[4] 2024 PKI & Digital Trust Report. (2024). Keyfactor. https://www.keyfactor.com/resources/digital-trust/2024-pki-and-digital-trust-report

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.

- **Demonstrates Verified Competence**: confirms professionals possess the necessary technical and regulatory expertise for high-stakes roles.
- **Drives Continuous Learning**: promotes ongoing upskilling to keep pace with evolving threats and standards.
- **Raises Accountability Standards**: signals commitment to professional integrity and responsible practice.
- **Reduces Compliance Risk**: minimizes human errors and regulatory breaches through structured knowledge assurance.
- **Strengthens Stakeholder Trust**: builds confidence among regulators, employers, and the public in digital trust services.
- **Reduces Talent Gap:** provides structured pathways to build and validate a capable, scalable workforce.

Remark:

Credentialing does not claim to certify mastery. It assures that individuals meet the **minimum**, **demonstrable** competencies required to responsibly and effectively perform their duties.

The Mission of DTCoE

DIGITALTRUST
Center of Excellence

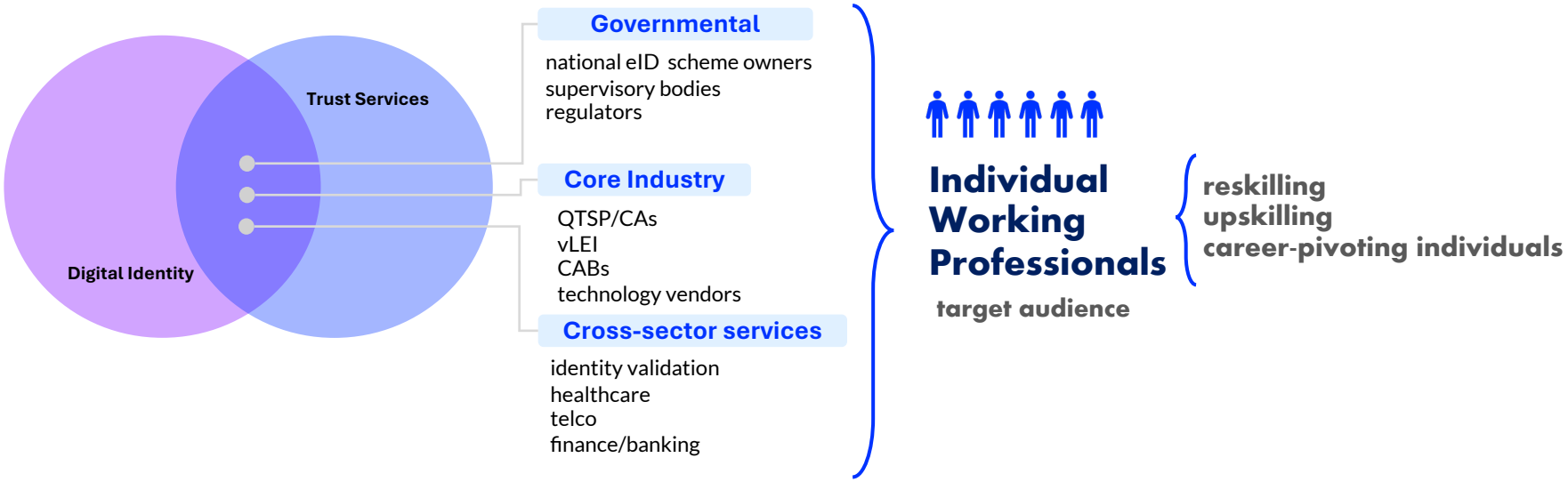
Digital Trust Center of Excellence

https://dtcoe.org

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

Mission

- Define peer-validated competency profiles in digital identity & trust services, aligned with regulatory and industry frameworks worldwide to ensure scientific validity and domain-specific relevance.
- Develop peer-validate credentialing schemes for natural persons that validate competence in areas such as identity proofing, PKI & SSI engineering, qualified trust services management, compliance auditing, and cross-border assurance.
- Foster a global community of digital trust professionals, advancing shared knowledge, ethics, and best practices.



Call to Action

Digital trust is now a global public good. But without a competent, credentialed workforce, even the strongest regulations and infrastructures cannot guarantee trust.

Together, we can ensure that digital trust is not just a technological framework, but a professionalized discipline sustained by competence, ethics, and accountability.

We invite:

Practitioners to engage with DTCoE & help define professional standards.

Regulators & Policymakers to collaborate in aligning workforce competence with evolving regulatory frameworks.

Industry Leaders to support the development of credentials that strengthen trust in digital markets.

Academia to partner through advisory roles.

DIGITALTRUST
Center of Excellence

References & Key Sources*

Regulatory Frameworks

Regulation (EU) 2024/1183 – amending Regulation (EU) 910/2014 as regards establishing the European Digital Identity Framework

Directive (EU) 2022/2555 – on measures for a high common level of cybersecurity across the Union

EU Digital Decade 2030 Programme

EU Digital Decade Targets

Ecosystem Standards & Specifications

European Digital Identity Wallet – Architecture and Reference Framework (ARF)

ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1 Requirements for Trust Service Providers issuing Certificate – General Requirements

ETSI EN 319 411-2 – Requirements for Trust Service Providers issuing Certificates - Policy Requirements

ETSI EN 319 471 – Policy and Security requirements for Providers of Electronic Attestation of Attributes Services

CA/B Forum – Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

W3C Verifiable Credentials Data Model

OID4VC – OpenID For Verifiable Credentials

OID4VP – OpenID for Verifiable Presentations

OID4VCI – OpenID for Verifiable Credentials Issuance

DIF Specifications

ToIP Foundation

Key Event Receipt Infrastructure (KERI)

Verifiable Legal Entity Identifier (vLEI)

Skills & Workforce Frameworks

EU Cybersecurity Skills Framework (ECSF) – ENISA, 2022

European e-Competence Framework (e-CF) – EN 16234-1

International References

NIST SP 800-63-4 – Digital Identity Guidelines (US)

ISO/IEC 18013-5:2021 – Mobile Driver's License (mDL)

Pan-Canadian Trust Framework – PCTF

Bhutan National Digital Identity (NDI)

Swiss Confederation – e-ID Information (fedpol)

Reports, Studies & Academic Papers

Trust Services Security Incidents 2024 Report – ENISA, 2024

Remote Identity Proofing Good Practices – ENISA, 2024

PKI & Digital Trust Report – Keyfactor, 2024

Global PKI and IoT Trends Study – Entrust, 2022

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?

ABOUT US

The **Digital Trust Center of Excellence** (**DTCoE**, www.dtcoe.org) is an independent, vendor-neutral organization established to professionalize the digital identity & trust services workforce. Founded by practitioners with expertise across identity, PKI, SSI, regulatory compliance, and credentialing. DTCoE operates with a public mission: to ensure the competence and recognition of digital trust professionals worldwide.

DISCLAIMER

This document has been prepared by DTCoE to support awareness, education, and dialogue on the professionalization of the digital trust workforce. The material reflects DTCoE's perspectives at the time of publication and is intended as a guidance resource, not as a prescriptive or exhaustive standard. While every effort has been made to ensure accuracy and relevance, the content may not cover all circumstances, regulatory environments, or technical variations. Readers are encouraged to apply their own professional judgment and adapt the ideas presented here to their specific organizational, regulatory, and technological context. DTCoE accepts no responsibility for outcomes resulting from the direct or indirect application of this material.

RESERVATION OF RIGHTS

*the list is not intended to be exhaustive