

**The
Alan Turing
Institute**

**CYBERSECURITY RISKS &
THREATS ACROSS THE IDENTITY
STACK**

**Trustworthy Digital Infrastructure for
Identity Systems**



Agenda

- Cyber Threats Observatory for National Identity Systems (Prof. Carsten Maple)
- Cross-Border Identity Federation and Measuring Trustworthiness using DISTAF (Dr. Mirko Bottarelli)
- Enhancing the cyber resilience of digital ID ecosystems (Dr. Zhijun William Zhang)
- The Reliability Problem in AI-Driven Identity Proofing (Dr. Idris Zakariyya)
- Panel: Securing Trust Across the Identity Ecosystem (Prof. Jonathan Crowcroft)

**The
Alan Turing
Institute**

**Cyber Threat Observatory
for National Identity
Systems**

Prof. Carsten Maple




In the News

Reuters World Business Markets Sustainability More My News

UN report urges stronger measures to detect AI-driven deepfakes

By Olivia Le Poidevin
July 11, 2025 11:32 PM GMT+1 · Updated July 11, 2025



Figurines with computer graphics. 2024. REUTERS/Dado

digwatch [Subscribe](#)

TOPICS TECHNOLOGIES PROCESSES TRENDS EVENTS ANALYSIS POLICY PLAYERS

[Home](#) | [Updates](#) | Deepfake and AI fraud surges despite stable identity-fraud rates

26 Nov 2025

Deepfake and AI fraud surges despite stable identity-fraud rates

A new report finds that while overall identity-fraud attempts have dipped, AI and deepfake-powered "sophisticated fraud" is rising fast, increasing by 180 percent.

[f](#) [x](#) [in](#)

Gen AI is ramping up the threat of synthetic identity fraud

Awareness critical as criminals use all available tools to commit financial fraud



BUSINESS DAY

TRACKING TRENDS | INFORMING D

Companies & Markets Economy Hek Tax Calculator BD Conferences BD Foundation BDTV Live

0.000000 (0.00%) **NGNOE** **NGNJPY** 0.10726 +0.000033 (+0.31%)

Home Technology Africa enters high-skill fraud era as deepfakes surge 967% in Zambia, 367% in DRC

Africa enters high-skill fraud era as deepfake surge 967% in Zambia, 367% in DRC

Royal Ibeh - December 2, 2025

Infosecurity Magazine [Log In](#) [Sign Up](#)

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

Infosecurity Magazine Home News AI and Deepfake-Powered Fraud Skyrockets Amid Identity Fraud Stagnation

NEWS 25 November 2025

AI and Deepfake-Powered Fraud Skyrockets Amid Identity Fraud Stagnation



The Cyber Threats Observatory

- Early-warning for governments
- Shared intelligence pool
- Evidence-based policy making
- Focus on critical infrastructure
- Strengthen cross-border cooperation



Dissemination Channels

The Alan Turing Institute

Home Events News About us Research Skills

Trustworthy Digital Infrastructure Cyber Observatory Trustworthiness Assessment Tool Guides

Cyber Threat Observatory for national identity systems

The programme's flagship observatory focuses on offering timely insight and analysis of cyber threats that have potential to negatively impact identity systems globally.


Introduction

Having a robust and secure National Digital ID System can be crucial for any nation. However, the infrastructure are increasing at an alarming rate. The number of bad actors globally pose significant digital identity systems being no exception.

LinkedIn profile for Cyber Threat Observatory

Search

Home My Network Jobs Messaging Notifications



Cyber Threat Observatory ✓
Cyber Threat Analysis at The Alan Turing Institute
London, England, United Kingdom · [Contact info](#)
[CyberObs @ Turing](#)

The Alan Turing Institute

Cyber Threat Observatory | Alan Turing Instit @TuringCyberO1 · Nov 11 ...

Monitor for malware staging in directories such as %HOME%\datax and unusual executions of legitimate software. Ensure robust endpoint logging with tools like PowerShell logging for enhanced detection.

Source:



Inside look:

**Generative AI and the rise of credential Fraud in
Digital Public Infrastructure**

Key Findings Snapshot

Rising Identity Vulnerabilities

Identity-related CVEs and CWEs have surged 300% from 2020 to 2025, increasing security risks.

Synthetic Identity Fraud Surge

Synthetic identity fraud in the UK rose by 500% over three years, posing major fraud challenges.

Deepfake-Enabled Breaches

Deepfake technology breaches now impact identity, finance, health, and government sectors.

Escalating Cross-Border Crimes

Cross-border financial crime and disinformation campaigns are increasing, demanding coordinated defense.

Data Sources

Vulnerability Databases

Identity-related CVEs and CWEs were sourced from the National Vulnerability Database covering 2020 to 2025.

Sectoral Reports

Reports from finance, healthcare, and government sectors provided industry-specific insights for the study.

Academic and Industry Literature

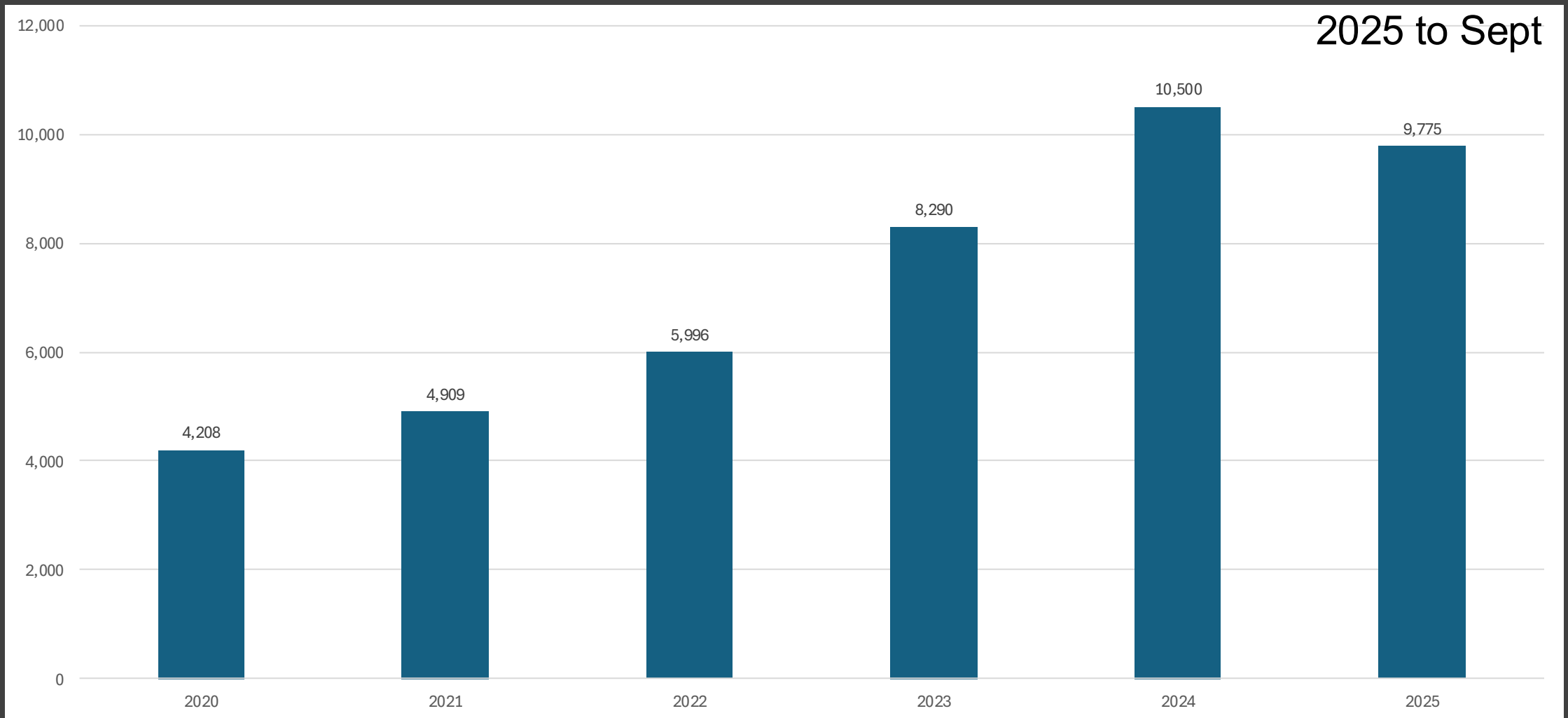
Research from ENISA, NIST, and other institutions enriched the study with academic and industry knowledge.

Policy Frameworks

Analysis included DPI Safeguards, NIST SP 800-63, OWASP API Security Top 10, and UK Cyber Assessment Framework for standards alignment.



Yearly Deepfake Relevant CWEs



Emerging Trends

- **AI-as-a-Service and Deepfakes**
- **Synthetic Media Marketplaces**
- **Industrialised Cybercrime Models**
- **Cross-sector Breach Propagation**



Emerging Technologies and Regulatory Challenges

- Designing Inclusive AI-Enabled Public Service Delivery
 - Tiered Access Model, fallback mechanisms, inclusive identity design, regulatory safeguards and monitoring redress
- Safeguarding Privacy in AI-Powered Accessibility Tools
 - Privacy risks, design and governance solutions, Contextual Consent Mechanisms regulatory and ethical safeguards and inclusive governance

Implications for DPI Security

Amplification of Security Risks

Identity systems amplify risks in DPI, causing cascades like financial fraud and healthcare data breaches.

Secure Design Principles

Architects must prioritize CWE-informed secure design and adopt secure-by-design for identity systems.

Continuous Monitoring and Threat Modelling

Regular CVE monitoring and threat modeling frameworks are essential to mitigate identity system risks.



Cross-Domain Vigilance & Continuous Monitoring

- Interlinked vulnerabilities demand unified **intelligence sharing**
- A **breach** in one sector can **cascade** into others
- **Continuously track** emerging CVEs that span multiple domains



The Digital ID Safety Pack

Technical Controls

- Multi-Modal Biometric Verification
- Liveness Detection and Anti-Spoofing Algorithms
- Secure API Design and Rate Limiting
- Encryption of Biometric Templates
- AI-Based Deepfake Detection

Governance and Policy Measures

- DPI Safeguards Integration
- Regulatory Alignment and Standards Adoption
- Cyber Assessment Framework (CAF) Adoption
- Mandatory Disclosure and Incident Reporting
- Synthetic Identity Simulation Exercises

The Digital ID Safety Pack

Cross Border Collaboration

- Threat Intelligence Sharing
- Public-Private Partnerships
- Cyber Workforce Development

Future-Proofing Identity Systems

- AI Use and Governance Programme
- Post-Quantum Cryptography Readiness

Key Takeaways

Global Security Priority

Identity security is a critical concern worldwide, demanding urgent attention across all sectors and countries.

Collaboration and Sharing

No entity can defend alone; cooperation and intelligence sharing are vital to counter identity threats.

Security-by-Design

Embedding security principles from the start ensures better protection and accountability in systems.

Proactive Risk Mitigation

Active strategies are needed to address risks from generative AI and credential fraud effectively.



**The
Alan Turing
Institute**

**Cross-Border Identity
Federation**

Dr. Mirko Bottarelli

mbottarelli@turing.ac.uk



Rationale

Global Mobility

- Over 280 million international migrants worldwide (UN DESA, 2020) and rising
- Individuals increasingly interacting with services across borders, in several sectors
- Services rely on identity verification mechanisms, highlighting the need for interoperable and portable digital identity solutions.

Challenges

Regulatory Momentum

- European Digital Identity Framework established by Regulation (EU) 2024/1183 provides for interoperable cross-border digital identity wallets. The African Union's Digital Transformation Strategy for Africa (2020–2030) points in a similar regional direction on interoperability and digital governance.

Siloed IdPs

- Existing IdP deployments serve single-country scenarios. There is no production-ready mechanism for Country A's relying party to authenticate a citizen of Country B, due to **Technical** and **Trust** constraints among countries.

Trust Requirements for Interoperability

Trust Relationships

- Six explicit levels must be governed: User↔IdP, User↔RP, IdP↔RP, RP↔RP, and their inverses.

Levels of Assurance

- Three tiers (Identity / Authentication / Federation Assurance Levels 1–3) covering identity proofing strength, authentication factors, and federation assurance. High-sensitivity sectors (finance, healthcare) require Level 3.

Trust Framework

- Built on ecosystem rules, technical standards, legal structure, compliance & enforceability, compliance recognition & communication.

Cross-Border Trust

Standards-Aligned Assessment Framework for Interoperable Identity (SAAFI) A standards-aligned framework for assessing cross-border digital identity interoperability

- **Pre-engagement analysis** — Helps jurisdictions understand each other's digital identity and trust landscape before formal discussions.
- **Structured dialogue and alignment discovery** — Provides a neutral, standards-aligned vocabulary to identify alignment and divergence without imposing a single model.
- **Risk-informed cooperation scoping** — Helps governments assess feasible interoperability options and where further governance or institutional development is needed.
- **Preparation for mutual recognition or pilots** — Supports evidence-based discussions on assumptions, constraints, and sequencing before formal agreements.

Technical Requirements for Interoperability

Protocol Translation

- Bidirectional, lossless, SAML or OpenID Connect

Credential Management

- Secure enrolment, update & revocation, W3C-compliant attributes, one identity per person (no duplicates)

Scalability

- Assertion caching, load balancing, optimised for low-bandwidth environments

Security

- TLS everywhere, private keys hardware-protected, schema validation

Privacy

- Data minimisation · differential privacy · only essential attributes disclosed

Standard eSignet: Single-Country OIDC Flow

SINGLE COUNTRY TRUST BOUNDARY

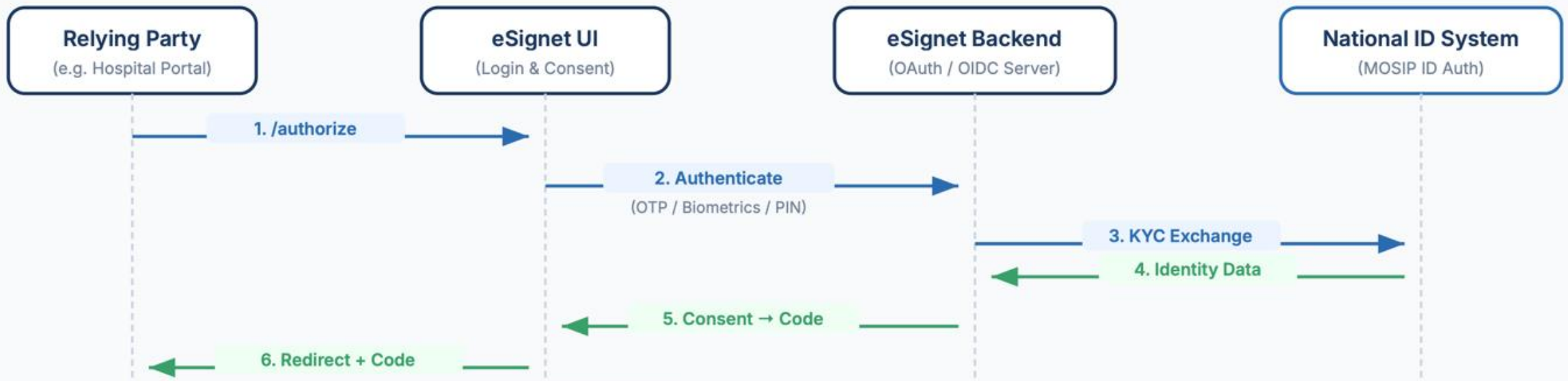


Standard eSignet: Single-Country OIDC Flow

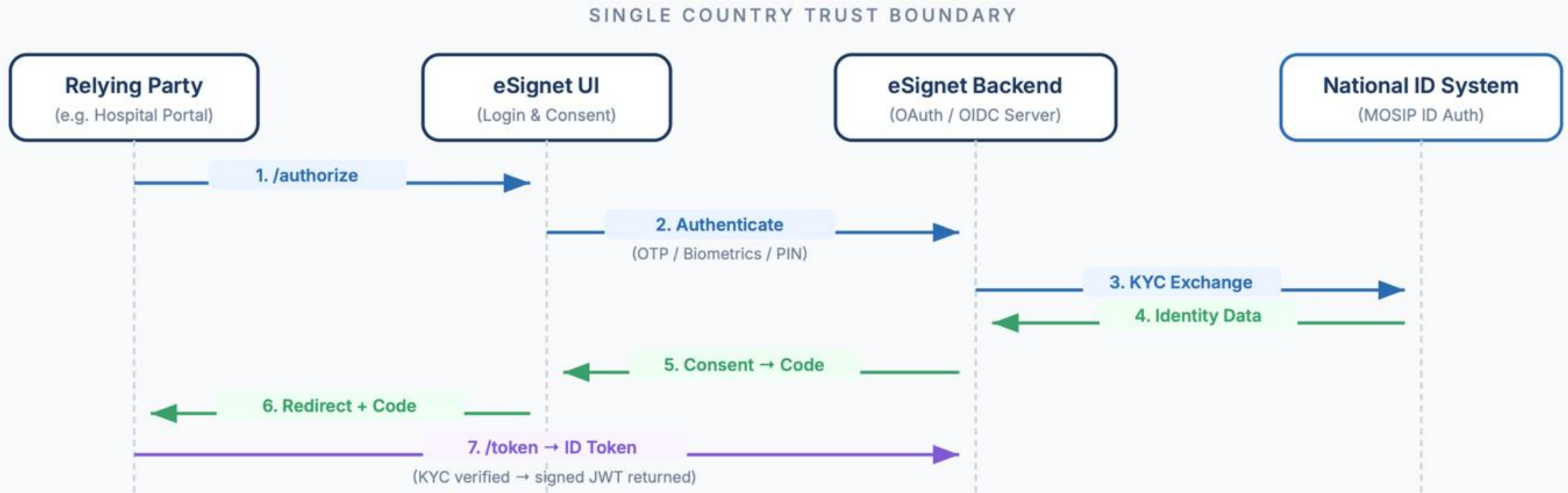


Standard eSignet: Single-Country OIDC Flow

SINGLE COUNTRY TRUST BOUNDARY

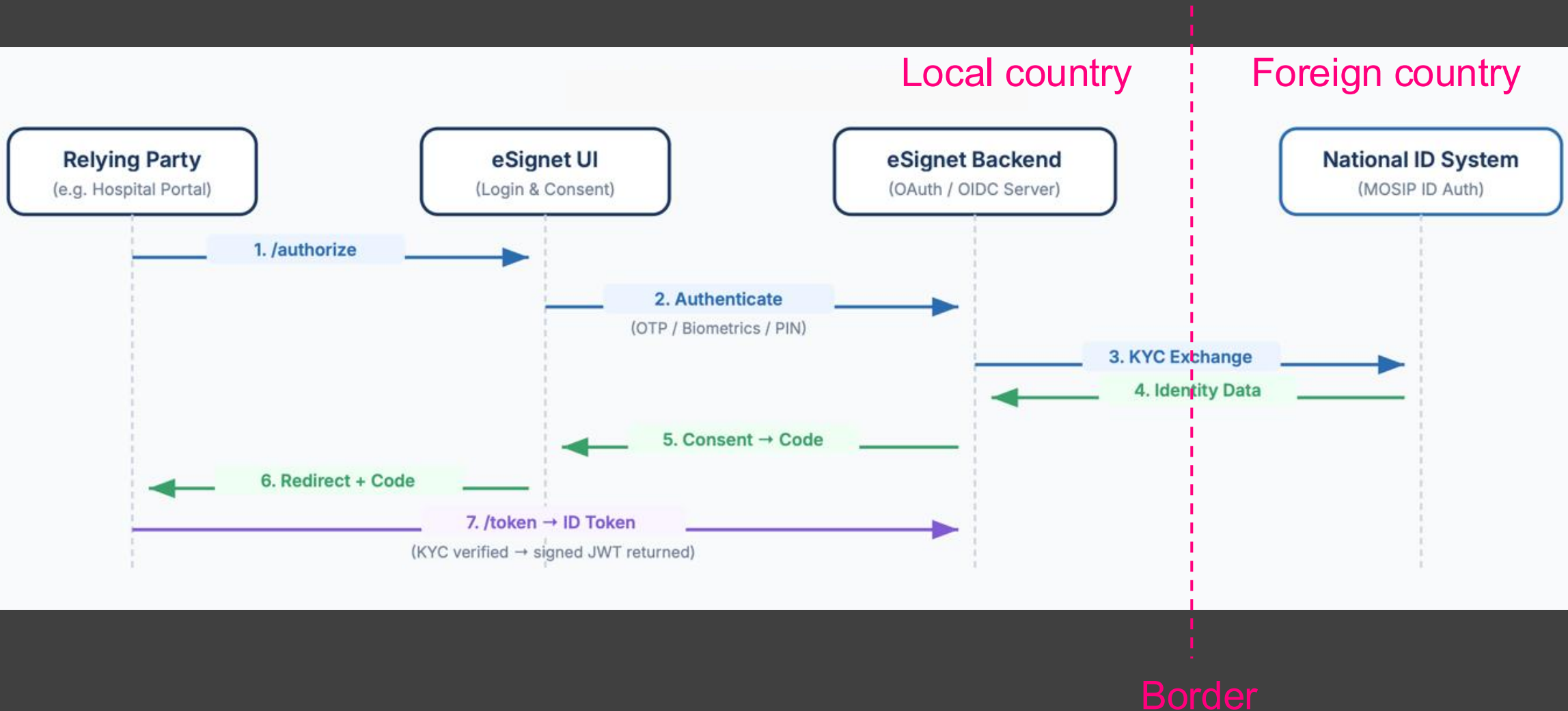


Standard eSignet: Single-Country OIDC Flow

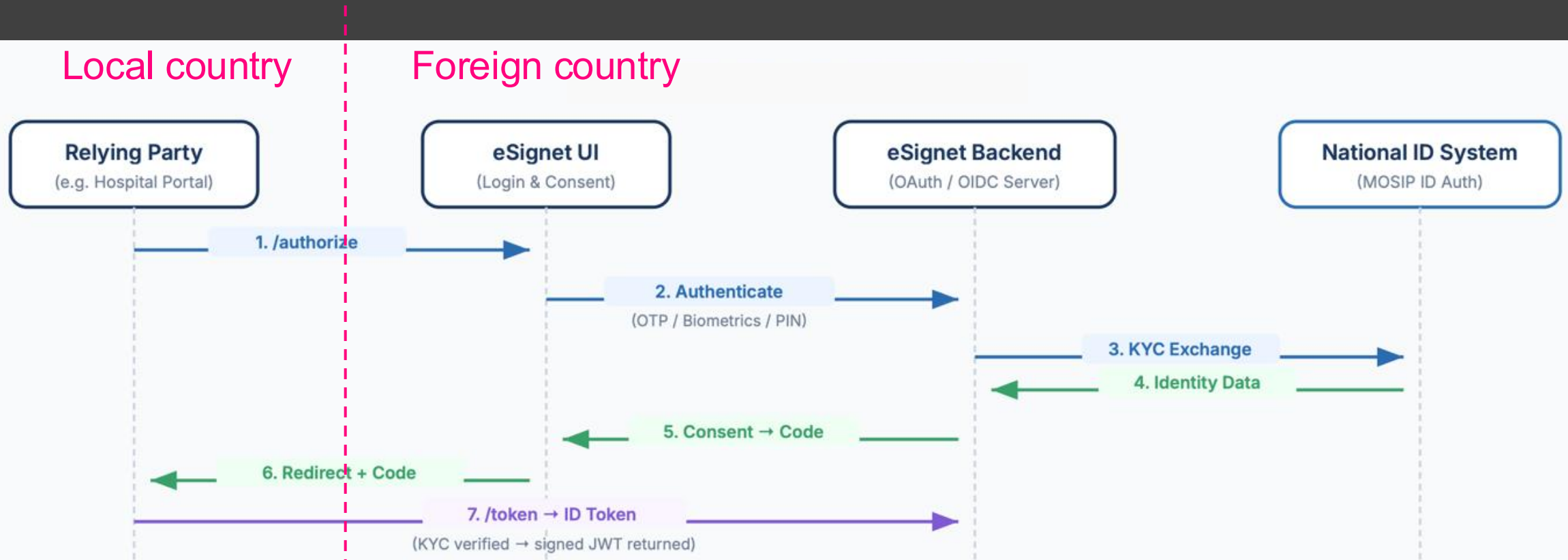


LIMITATION: Single trust boundary -- RP, eSignet, and ID system all within one jurisdiction

Standard eSignet: Can we make it cross-border? [1/2]



Standard eSignet: Can we make it cross-border? [2/2]

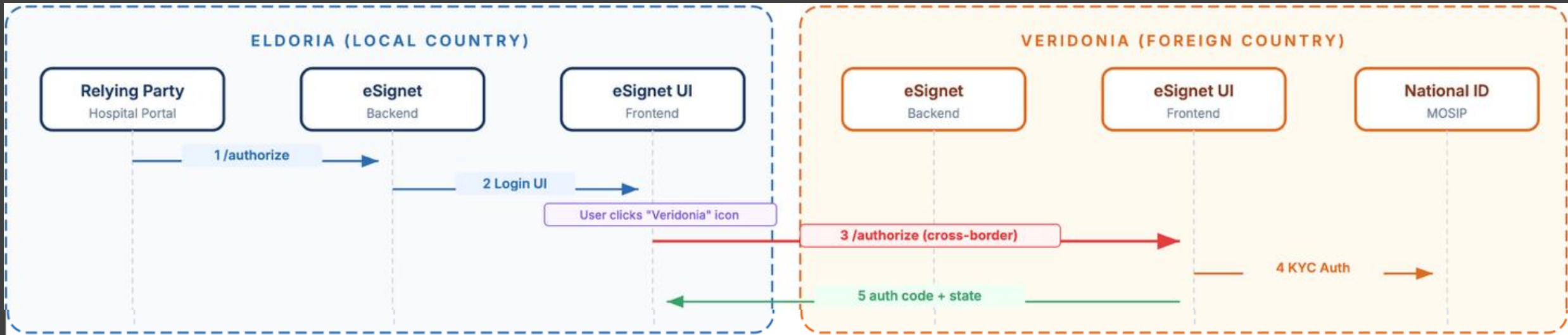


Border

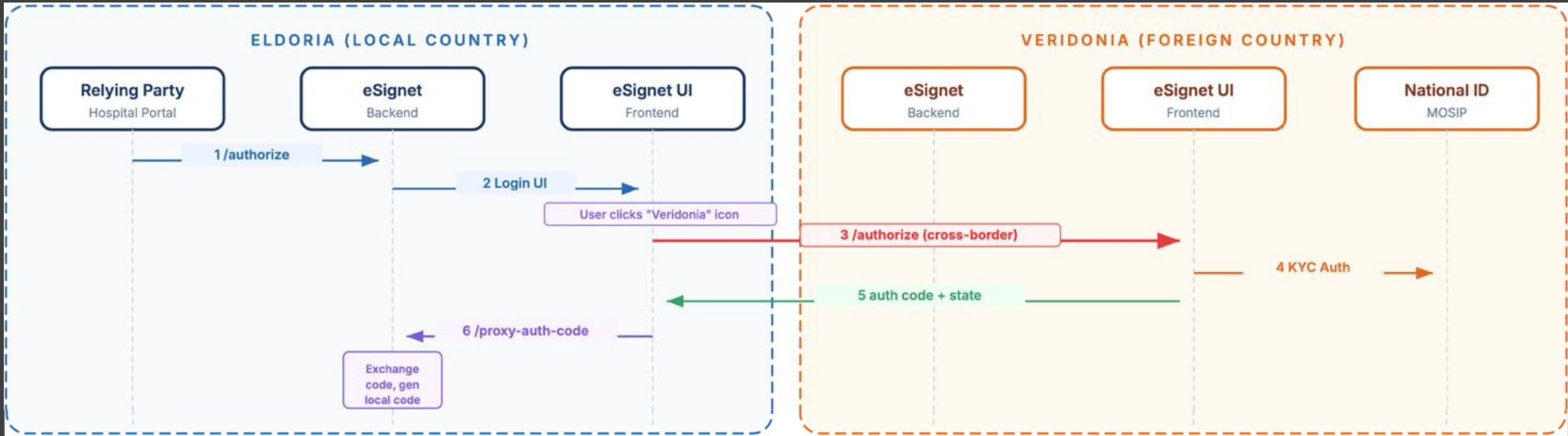
Cross-Border Proxy OIDC Flow



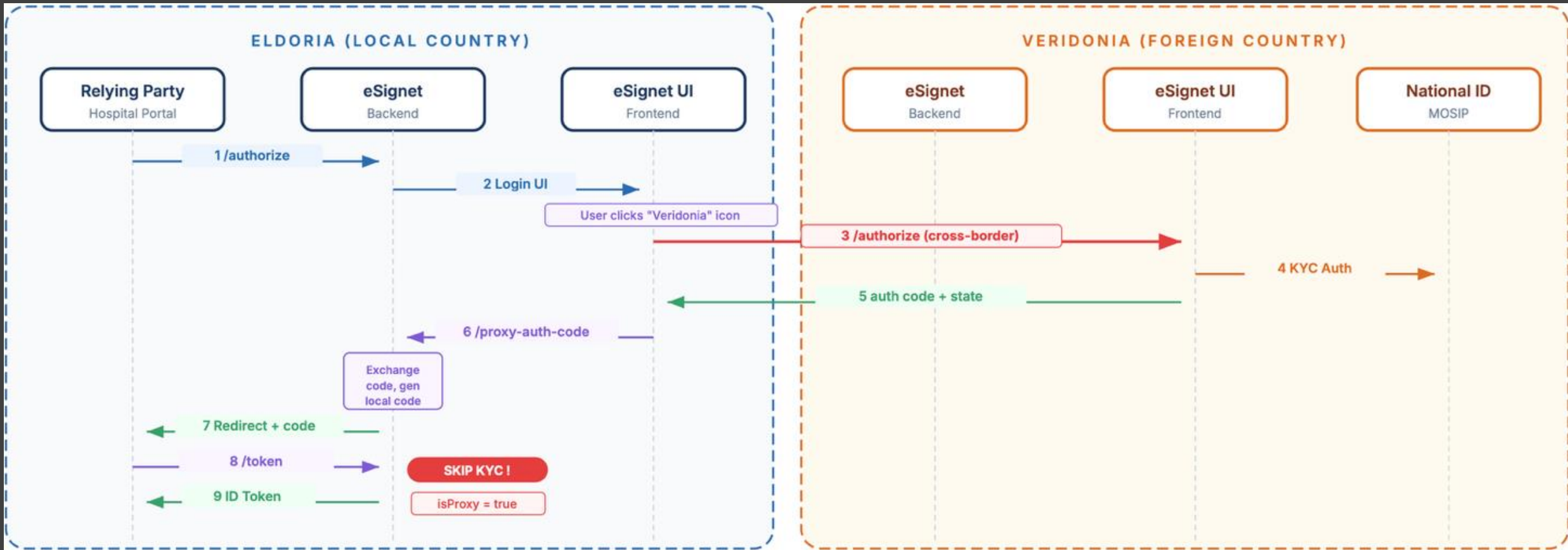
Cross-Border Proxy OIDC Flow



Cross-Border Proxy OIDC Flow



Cross-Border Proxy OIDC Flow



Key innovation: chain of OIDC authentication, where eSignet can collaborate with local IdP or delegate to foreign one.

Cross-Border Proxy OIDC Flow

Demo Placeholder

DPI Cyber Signals Exchange

- **Building on the Cyber Threats Observatory**
 - Evidence and insight on emerging risks
 - Early warning and prioritisation
 - Actionable guidance for decision-makers

What this would mean

1. Stronger evidence and assurance for safe, secure AI in DPI
2. Better governance, accountability, and protection of citizen rights
3. Reduced large-scale harm, fraud, and service disruption
4. More resilient and secure public services across linked systems
5. Greater public trust and confidence in DPI

Get involved

- Your opinion matters
- TDI@turing.ac.uk

