

Project SHIELD: A Privacy-First, Employer-Focused Solution to Illegal Work Enforcement

Executive Brief

A secure, scalable, and citizen-respecting digital framework to ensure right-to-work compliance without a national ID card.

Executive Summary

Project SHIELD offers a targeted, cryptographically secure alternative to a national digital ID, enabling employers to verify right-to-work status instantly and privately, thereby strengthening enforcement while protecting civil liberties.

1. Problem Statement

The current paper-based right-to-work verification system is burdensome for employers and vulnerable to fraud, while the proposed national digital ID card (BritCard) introduces disproportionate surveillance risks to civil liberties.

2. Core Solution Thesis

By empowering individuals to hold a secure, verifiable digital credential of their work status, we can enable employers to instantly and privately confirm eligibility without accessing any underlying personal data, thus preventing illegal work without creating a mass surveillance system.

3. 90-Day Pilot Plan

Week(s)	Milestone	Objective
1-2	Stakeholder Alignment & Technical Scoping	Finalise pilot participants (Home Office, select employers, tech provider). Define technical specifications for the Verifiable Credential (VC) and the verifier app.
3-4	Component Development (Alpha)	Develop the issuer portal (Home Office), the holder wallet (citizen app), and the verifier app (employer). Issue test DIDs and VCs.
5-6	System Integration & Testing	Integrate components and conduct end-to-end testing in a sandbox environment. Begin independent security and privacy audits.
7-8	Pilot Deployment & Onboarding	Deploy the system to pilot participants. Onboard a small cohort of employers and volunteer employees. Provide training and support materials.
9-10	Live Pilot Operation & Data Collection	Conduct live verification checks for new hires within the pilot group. Monitor system performance, usability, and core metrics.
11-12	Analysis, Reporting & Recommendations	Analyse pilot data against core metrics. Finalise audit reports. Draft a final report with recommendations for a phased national rollout.

4. Core Pilot Metrics

- **Verification Speed:** Time from scan to confirmation (target: less than 2 seconds)
- **Employer Adoption:** Percentage of pilot employers actively using the system
- **User Experience:** Satisfaction scores from both employers and employees
- **Privacy Preservation:** Confirmation of zero personal data transfer during verification, verified by audit log
- **System Security:** Number of identified vulnerabilities (target: 0 critical)
- **Cost-per-Verification:** Estimated cost compared to manual checks

5. Minimal Technology Stack

Project SHIELD is built on four established, open-standard technologies:

1. **Decentralized Identifiers (DIDs):** Gives individuals a self-owned, independent digital identity, eliminating the need for a central government database of citizens.
2. **Verifiable Credentials (VCs):** The Home Office issues a digitally signed, tamper-proof VC to the individual, which simply states their right-to-work status. This is stored in the individual's secure digital wallet.
3. **Zero-Knowledge Proofs (ZKPs):** When an employer needs to verify status, the candidate presents a ZKP. This cryptographically proves they hold a valid VC from the Home Office without revealing the credential itself or any personal data—the employer's system simply gets a 'Yes' or 'No'.
4. **Immutable Audit Log:** Every verification request is recorded on a distributed ledger, creating a tamper-proof, publicly auditable record that a check was performed, by whom, and when, without revealing who was checked. This ensures accountability and transparency.

6. Legal & Inclusion Safeguards

- **Data Protection by Design:** The system is architected to be fully compliant with GDPR, processing the absolute minimum data necessary.
- **No New Powers:** SHIELD requires no new surveillance powers or data retention mandates. It is a verification, not a tracking, system.
- **Voluntary & Inclusive:** The system is opt-in for citizens. Non-digital and offline alternatives will be maintained, ensuring those without smartphones or digital literacy are not excluded.
- **Statutory Oversight:** The immutable audit log will be made available to an independent oversight body to monitor for misuse or discriminatory patterns.

7. Project SHIELD vs. BritCard

Feature	Project SHIELD	BritCard (Proposed)
Data Model	Decentralized (citizen-controlled)	Centralized (government-controlled)
Citizen ID	Not required	Compulsory national ID card
Data Revealed	Nothing (Zero-Knowledge Proof)	Name, photo, status, other linked data
Function Creep	Difficult (limited by design)	High risk (designed for data linking)
Surveillance	No tracking	Enables mass surveillance
Trust Model	Trust in cryptography	Trust in government administration
Cost	Low (leverages existing devices)	High (national infrastructure rollout)

8. Press-Ready Materials

Headline: "Project SHIELD: Privacy-First Alternative to National Digital ID Protects Workers and Employers"

Subhead: "New framework enables instant right-to-work verification without surveillance or civil liberties violations"

One-Line Pitch: "SHIELD proves employment eligibility through cryptographic verification, not citizen tracking."

9. Publication & Submission Checklist

- ☐ Publish Executive Brief to a dedicated GitHub repository
- ☐ Generate a PDF version for formal submissions
- ☐ Post the brief to a public Notion page for easy sharing
- ☐ Submit the PDF to the Home Affairs Select Committee and the Joint Committee on Human Rights
- ☐ Distribute to key civil society stakeholders (Big Brother Watch, Liberty, etc.)

- [] Share with technology and policy journalists

Authored by Obinna Patrick

Under the Sovereign Architect Framework

© 2025 — Released for public implementation