DIGITAL LEADERS

Digital Leaders

www.DigiLeaders.com

# DIGITAL IDENTITY LESSONS FOR THE UK'S AI STRATEGY


**ALAN W. BROWN**

**AI DIRECTOR, DIGITAL LEADERS**


**10TH OCTOBER 2025**

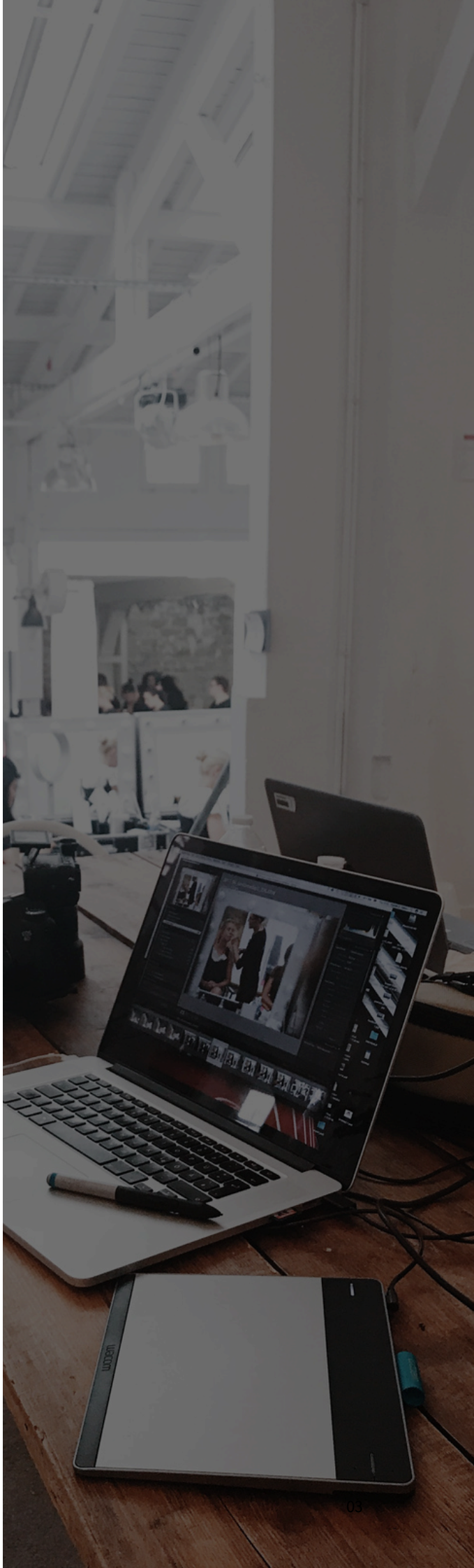
# TABLE OF CONTENTS

# DIGITAL IDENTITY MATTERS

Any broad-based adoption of AI in the UK must be built on a solid foundation. And a core element of this is digital identity. This is essential because without a reliable, interoperable identity infrastructure, AI systems cannot safely verify users, personalize services, or maintain the trust necessary for widespread adoption across both public services and business operations.

A pressing challenge facing the UK today is the inability to reliably identify citizens and accurately match them to the services they receive. This fragmentation undermines effective public service delivery, creating inefficiencies, fraud vulnerabilities, and barriers to coordinated care across health, social services, and benefits systems. Without a unified approach to digital identity, government departments operate in silos, citizens must repeatedly prove who they are, and vulnerable populations fall through the gaps when their needs span multiple services.

Consequently, the UK government's recent announcement to roll out digital identity cards represents more than just a policy shift; it's a strategic recognition that effective AI deployment across public services and business operations demands a reliable, interoperable identity infrastructure. The stakes are exceptionally high: failure to secure this foundation, as witnessed in the Universal Credit programme's troubled digital transformation, means that vulnerable populations may struggle while promised efficiencies remain elusive.



# THE UK'S DIGITAL IDENTITY AMBITIONS

The UK government's embrace of digital identity represents more than just a technological upgrade. It should be seen as a strategic pivot toward an AI-enabled future. The vision is clear: create a digital infrastructure that can support more sophisticated AI applications across both public and private sectors, ultimately driving economic growth and improving citizen access to public services.

This isn't simply about replacing physical cards with digital ones; it's about creating the foundational layer upon which a more intelligent, responsive system of governance and commerce can be built. This infrastructure is crucial for realizing the immense potential of AI to transform healthcare, education, and business operations. Crucially, the success of this strategic pivot depends entirely on getting the infrastructure right from the beginning.

I believe this ambition to be fundamentally sound. The potential for AI to transform how we deliver healthcare, education, social services, and business operations is immense. However, the success of such initiatives depends heavily on getting the infrastructure right from the beginning. To ensure our national digital ambition succeeds, we must leverage international evidence, examining both successes and critical shortcomings.

What can we learn from these efforts, and how should they impact the UK's AI strategy?

# LEARNING FROM THE BALTIC VANGUARD: THE ESTONIA MODEL

Estonia is frequently cited as the gold standard for digital governance, providing compelling evidence that a unified, universally adopted digital identity system is both possible and enormously beneficial. Through its X-Road data exchange layer and mandatory eID, Estonia has virtually eliminated paperwork, saving the equivalent of 2% of its GDP annually and enabling 99% of public services to be conducted online. The core principle of the 'once only' data rule, high transparency (allowing citizens to track data access), and a commitment to digital literacy have ensured deep public trust.

However, UK policymakers must be cautious about replicating this model wholesale. Estonia's success benefited significantly from its relatively small size and a clean slate following its independence, enabling it to build a modern infrastructure with minimal legacy technology constraints. The UK, by contrast, is a nation of vastly greater scale and complexity, grappling with fragmented, deep-rooted legacy systems across government departments.

Furthermore, the UK is defined by a deep-seated cultural pushback against mandatory national ID schemes, a scepticism that has derailed previous attempts and remains a significant political headwind. Estonia's primary lesson for the UK is not what was built, but how it was built: consistently, iteratively, and with trust embedded from day one.

| Characteristic | Estonia | India |
|---|---|---|
| Core Achievement | ***99% of services online***; saves 2% of GDP annually through X-Road interoperability | ***10+ billion monthly transactions***; financial inclusion for hundreds of millions via integrated India Stack |
| Key Success Factor | ***Radical transparency*** so citizens can track all data access; built consistently and iteratively | ***Seamless interoperability*** across identity, payments, and data layers |
| Critical UK Lesson | Trust through transparency and "once only" data principle; ***how*** to build matters more than ***what*** | Mandate interoperability across government and private sector; deliver ***tangible public value*** from day one |
| Major Risk to Avoid | ***Cultural resistance*** to mandatory schemes | ***Digital exclusion*** and ensuring vulnerable groups do not suffer |

# THE INTEGRATED POWER AND PERILS OF INDIA'S DIGITAL STACK

No discussion of digital transformation at scale can ignore India's remarkable journey with what's commonly known as the "India Stack". This isn't a single technology but rather an integrated suite of digital public goods that has fundamentally transformed how services are delivered to over 1.3 billion people.

At its core, the India Stack comprises four key layers. The identity layer centres on Aadhaar, a biometric identification system that has enrolled over 95% of India's adult population. Built on top of this is the payments layer, primarily the Unified Payments Interface (UPI), which has revolutionized digital transactions. The data empowerment layer includes systems like DigiLocker for document storage and Account Aggregator for financial data portability. Finally, the consent layer ensures individuals maintain control over their personal information.

What makes this particularly fascinating is how these components work together. A rural farmer can open a bank account using their Aadhaar identity, receive government subsidies directly through UPI payments, access their land records through DigiLocker, and share financial data with lenders through the Account Aggregator – all through their smartphone. The efficiency gains are staggering: what once took weeks of bureaucratic navigation can now happen in minutes.

The scale of adoption has been remarkable. UPI now processes over 10 billion transactions monthly, handling more digital payments than any other country. The system has enabled financial inclusion for hundreds of millions previously excluded from formal banking, while dramatically reducing the cost of service delivery for both government and private sector organizations.

# THE AI INTEGRATION IMPERATIVE

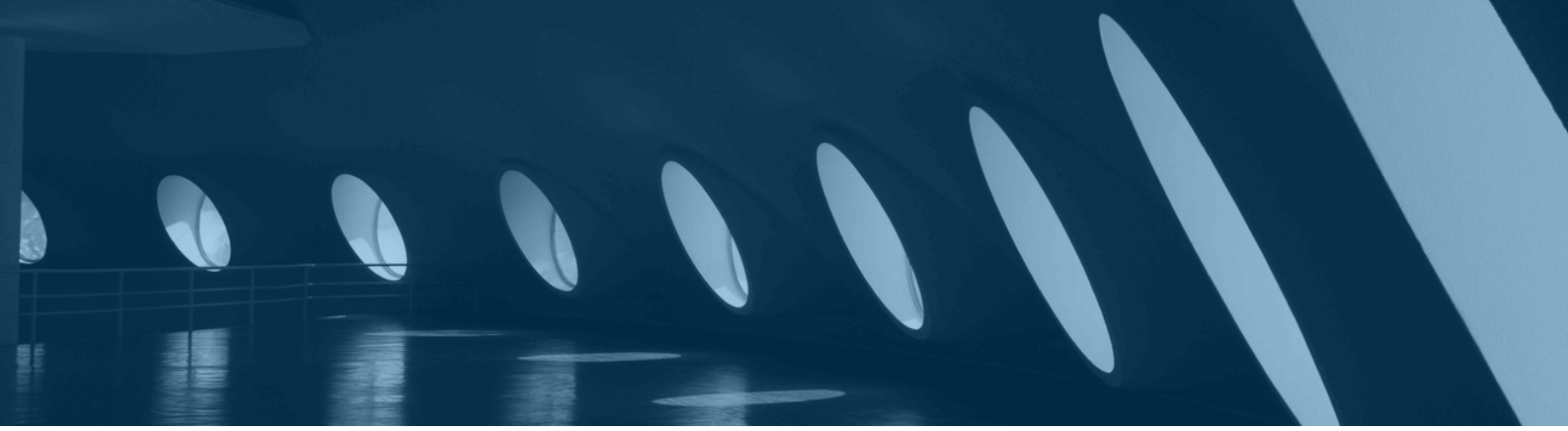
The UK has a unique opportunity to learn from India's digital infrastructure while charting a more ambitious path forward. India's Stack was primarily designed to digitize existing processes, essentially translating paper-based systems into digital equivalents. The UK, however, can go further by reimagining public service delivery entirely through an AI lens from the outset. This means building digital identity infrastructure not merely as a replacement for physical documents, but as an intelligent foundation that anticipates needs, personalizes experiences, and proactively supports citizens.

When digital identity is combined with sophisticated AI capabilities, it becomes exponentially more powerful. Consider how such a system could work in practice: an AI-enabled platform that recognizes when a citizen's circumstances (perhaps a change in employment status, a new child, or a health diagnosis) suggest they might benefit from additional support services they don't yet know exist. Or imagine streamlining the notoriously complex process of applying for multiple benefits by intelligently pre-populating forms with verified information from a citizen's secure digital identity, eliminating redundant paperwork and reducing errors. This isn't about automating inefficiency; it's about fundamentally rethinking how government serves its people.

However, this AI integration amplifies both challenges and risks that must be carefully managed. The UK faces the formidable task of unraveling and modernizing infrastructure deployed over decades. This is a far more complex undertaking than India's relatively newer systems or Estonia's post-independence clean slate. Beyond technical complexity, any new AI system must be designed to avoid perpetuating historical biases embedded in existing data, must make decisions that citizens can understand and challenge, and must not create new forms of digital discrimination that disadvantage vulnerable populations. The stakes are particularly high given the UK's own troubled history with digital transformation, as evidenced by Universal Credit's initial failures.

Estonia's experience offers a crucial lesson for managing these risks: success comes from building consistently and iteratively, with trust and transparency embedded from day one. Rather than attempting a "big bang" rollout, AI capabilities must be phased and rigorously tested at each stage, with clear success criteria before expanding further. This requires the UK's approach to include robust governance frameworks specifically designed for AI decision-making, comprehensive audit trails that allow citizens to see exactly how automated decisions affecting them were made, and meaningful human oversight that provides both accountability and the ability to intervene when systems fail or produce unjust outcomes. Without these safeguards, even the most technically sophisticated digital identity system risks replicating the exclusion and hardship that plagued earlier UK digital transformation efforts.

.



# CRITICAL LESSONS

Having observed Estonia and India's digital transformation, we can see several crucial lessons for the UK's own digital identity journey.

1. **Mandate Interoperability and Ecosystem Design:** The power of the India Stack is not a single application, but its seamless systems. The UK design must ensure deep integration, not only across government departments but also with the private sector. Crucially, the interoperable data exchange system seen in Estonia's X-Road is the proven European model for achieving this efficiency and minimizing legacy data silos.

2. **Embed Trust and Privacy by Design:** Privacy and security must be fundamental design principles, not afterthoughts. The UK has the advantage of existing frameworks like GDPR; these protections must be central as the system evolves. Estonia's experience proves that true public trust is built through radical transparency, allowing citizens to track and control exactly which officials and systems access their data.

3. **Deliver Tangible Public Value:** Building trust requires providing immediate, pragmatic benefits to users from day one. Both India and Estonia achieved success by demonstrating clear, massive efficiency gains (e.g., saving 2% of GDP, or revolutionizing payments) that make the system indispensable. Transparency on data collection, use, and protection is non-negotiable.

4. **Avoid Digital Exclusion:** The UK must actively avoid the consequences of mandatory digital identity leading to exclusion. When technology fails or access is limited, vulnerable populations suffer profound hardship. This risk of exclusion is the critical failure point that the UK's own history (specifically the Universal Credit rollout) underscores. Avoiding any such impacts must be a priority.


# RECOMMENDATIONS FOR RESPONSIBLE IMPLEMENTATION

The UK Government's January 2025 State of Digital Government Review provides sobering context for digital identity implementation. The review found that 47% of central government services still rely on non-digital methods, and 25% of government services are "outdated". More critically, it revealed systemic issues with digital leadership, noting that only four central government departments have a digital leader on their executive committee.

These findings echo the hard-learned lessons from Universal Credit, the UK's most ambitious digital transformation in social services. The Universal Credit programme's troubled history offers crucial insights for digital identity implementation. What began as a "digital by default" benefit system struggled profoundly with user needs, resulting in widespread hardship for vulnerable populations and systematic failures in rule-of-law principles.

Based on these experiences and reviewing international best practices, we can suggest several recommendations for policy makers and business leaders.

**First**, embed user-centred design from day one, not as an afterthought. Universal Credit's initial failure stemmed from treating it as a "technology project" rather than a "human behaviour project". The programme spent £425 million and had zero users by its original 2013 deadline because it failed to understand claimants' needs. Digital identity must be built around genuine user journeys, not administrative convenience.

**Second**, ensure genuine multi-disciplinary teams with executive backing. The 2025 government review's finding that most departments lack senior digital leadership reflects a persistent problem. Universal Credit only succeeded after creating cross-cutting teams that included operational delivery, policy, and security staff working together full-time. Digital identity requires similar integration across departments and skill sets.

**Third**, design for digital inclusion, not digital exclusion. Universal Credit's "digital by default" approach pushed vulnerable people to the margins, creating hardship for those lacking digital skills or reliable internet access. The system's rigid automation caused people to go hungry and fall into debt. Digital identity must include robust offline alternatives and human support.

**Fourth**, implement comprehensive testing with real users in complex scenarios. Universal Credit's algorithm problems only became apparent after rollout, when means-testing failures caused widespread errors. Digital identity systems must be stress-tested not just technically, but against the full spectrum of citizen circumstances and edge cases.

**Fifth**, maintain transparency and accountability mechanisms. Research found that Universal Credit's digital systems routinely breach rule-of-law principles, with opaque decision-making processes that citizens cannot challenge effectively. Digital identity must include clear audit trails, explainable decisions, and accessible appeals processes.

**Finally**, plan for iterative improvement, not big-bang delivery. Universal Credit's problems were compounded by unrealistic timelines and resistance to course correction. The successful turnaround only occurred when teams adopted genuinely agile approaches focused on outcomes rather than deadlines. Digital identity must be designed to meet the Estonian standard of transparency: the system must include clear audit trails, explainable decisions, and accessible appeals processes, allowing citizens to see exactly which officials and systems have accessed their data.

# SUMMARY: LOOKING FORWARD

The UK's move toward digital identity and AI integration represents both tremendous opportunity and significant responsibility. Done well, it could indeed position the UK as a global leader in digital governance while delivering better outcomes for citizens and businesses alike. The lessons from Estonia and  India's experiences (both positive and negative) provide valuable guidance for this journey.

However, success is not guaranteed. It requires sustained political commitment, substantial investment in both technology and skills, and an unwavering focus on serving citizen needs rather than technological possibilities. Most importantly, it requires honest acknowledgment that this transformation will not be without challenges and controversies.

As we embark on this path, I believe we must remain committed to the principle that technology should serve humanity, not the other way around. Digital identity and AI are powerful tools, but they are only as valuable as their ability to create a more equitable, efficient, and human-centred society. The choices we make in the coming years will determine whether we achieve that vision or merely create more sophisticated forms of bureaucracy.

# CONTACT

For more information, or to offer feedback on this report, please contact:

www.DigiLeaders.com

alan.brown@DigiLeaders.com