# VERIFYTT: EMBEDDING TRUST IN THE DIGITAL ECONOMY OF TRINIDAD AND TOBAGO

White Paper

iGovTT

National Information and Communication Technology Company Limited

March 2026

**Attribution**

This white paper was prepared by iGovTT as part of its mandate to design, implement, and steward national digital infrastructure initiatives.

Lead Author:
Irwin Williams

Head of Software Development, iGovTT

# Executive Summary

Trinidad and Tobago does not lack digital adoption. Internet penetration reached approximately 84.7 percent of the population in early 2025[1]. Mobile connections exceeded total population levels, with more than 2.0 million active cellular subscriptions—equivalent to roughly 135 percent penetration[2]. These indicators reflect widespread smartphone access and sustained digital engagement across the population. Online banking, digital job applications, mobile authentication, and web-based service portals are routine components of everyday interaction.

The challenge is therefore not access to digital channels, but the absence of embedded digital trust. Credentials may be exchanged electronically, yet verification remains manual. Documents are digitized, but assurance is not.

VerifyTT establishes a national digital trust rail — a reusable Digital Public Infrastructure (DPI) building block that embeds cryptographic assurance directly into digital credentials. It eliminates the trade-off between speed and integrity by making trust instantaneous, portable, and machine-verifiable. Education is the pilot; trust infrastructure is the objective.
VerifyTT represents Trinidad and Tobago's first operational DPI component and establishes a scalable foundation for digital verification across sectors.

# The Trust Maturity Gap

In the absence of a national digital verification infrastructure, credential exchange commonly relies on scanned documents and direct institutional confirmation.

In tertiary credential workflows, verification may require direct institutional confirmation and introduce measurable administrative delay.

Verification often requires manual review or contact with issuing institutions, introducing institutional burden and slowing downstream decisions. Employers must either defer hiring decisions pending confirmation or accept unverifiable digital artifacts. When trust must be negotiated transaction by transaction, it generates recurring cost.

# From Digitization to Infrastructure: Evaluating the Options

Digitizing documents is not equivalent to embedding trust.

[1] DataReportal, *Digital 2025: Trinidad and Tobago* (January 2025), https://datareportal.com/reports/digital-2025-trinidad-and-tobago
[2] DataReportal, *Digital 2025: Trinidad and Tobago*

Scanning a paper certificate into a PDF reduces physical handling but does not eliminate the need for independent verification. A digital document remains dependent on institutional confirmation unless its authenticity can be verified computationally.

International digital government frameworks distinguish clearly between digitizing documents and transforming verification models. The OECD has emphasized that true digital transformation requires moving from document-centric workflows toward data-centric and reusable service architectures[3].

If Trinidad and Tobago seeks to modernize credential verification, there are three structurally distinct approaches.

**Option 1: Enhanced Manual Digitization**

Institutions may improve existing workflows by:

- Providing downloadable PDF certificates
- Establishing centralized verification hotlines
- Offering email-based confirmation services
- Expanding registrar verification teams

This approach preserves institutional control and minimizes structural change.

However, it does not eliminate human mediation. Verification remains dependent on manual review or direct institutional confirmation.

Administrative burden research demonstrates that compliance processes requiring repeated human validation generate measurable time and effort costs for both institutions and service users[4]. The OECD has further identified administrative burden as a driver of service delay and institutional inefficiency when processes rely on repetitive verification steps[5].

Scaling such systems typically increases staffing requirements proportionally to transaction volume. The transaction cost is not removed; it is redistributed.

Digitization improves format. It does not alter the trust architecture.

**Option 2: Proprietary Vendor-Based Verification Platforms**

[3] OECD, The OECD Digital Government Policy Framework, 2020.
[4] Herd, Pamela & Moynihan, Donald, Administrative Burden: Policymaking by Other Means, Russell Sage Foundation, 2018.
[5] OECD, Reducing Administrative Burden in Public Services, 2021.

A second approach involves contracting a commercial provider to operate a credential verification platform.

This model can provide:

- Rapid deployment
- Managed infrastructure
- Commercially mature tooling

Proprietary credential services are widely used internationally in higher education and workforce sectors.

However, international digital governance literature highlights several structural considerations associated with vendor-dependent digital identity and credential ecosystems:

- Recurring licensing and subscription costs
- Long-term switching barriers
- Data portability constraints
- Limited interoperability across sectors
- Dependence on continued vendor viability

The World Bank's Identification for Development (ID4D) program emphasizes the importance of open standards, interoperability, and vendor neutrality in foundational digital systems to avoid lock-in and preserve sovereign flexibility[6].

Similarly, the GSMA Digital Identity framework underscores the need for portability and ecosystem-wide interoperability to support cross-sector trust frameworks[7].

A proprietary solution may resolve verification within a defined institutional boundary, but it does not automatically establish reusable national infrastructure.

**Option 3: Public Digital Infrastructure (DPI)**

A third approach is to establish a standards-based, modular digital trust layer as public infrastructure.

[6] World Bank, ID4D Principles on Identification for Sustainable Development, 2020.
[7] GSMA, Digital Identity: A Framework for Interoperability, 2019–2022.

Digital Public Infrastructure (DPI), as articulated in international frameworks including GovStack and the UNDP DPI Safeguards Framework, is characterized by:

- Open standards
- Modular architecture
- Separation of core functional components
- Interoperability by design
- Public-interest governance

DPI enables credentials to be cryptographically signed and independently verifiable without requiring direct institutional mediation.

The World Bank and UNDP have both emphasized that foundational digital systems benefit from modular, open architectures that support cross-sector reuse and long-term scalability[8].

Unlike enhanced manual processes or proprietary platforms, DPI establishes a reusable trust rail that multiple sectors can adopt without architectural reinvention.

The policy choice is therefore not between digital and non-digital systems.

It is between:

- Digitizing manual verification
- Outsourcing verification into a closed ecosystem
- Establishing open, reusable national trust infrastructure

VerifyTT adopts the third approach.

## TRUST AS INFRASTRUCTURE

Trust moves opportunity. VerifyTT treats trust as a public utility — modular, reusable, and sector-agnostic. While education is the initial use case, the infrastructure extends to professional licensing, healthcare credentials, financial onboarding, and civil registry extracts.

### THE DIGITAL TRUST RAIL

[8] UNDP, Digital Public Infrastructure Safeguards Framework, 2023; GovStack Initiative, Building Blocks Architecture Overview, 2022.

The digital trust rail enables verified information to move securely between issuers, holders, and verifiers without repeated human mediation. Verification becomes a cryptographic integrity check rather than a manual negotiation.

# Architecture and Open Standards

Built on the open-source Inji Verifiable Credentials Stack and compliant with W3C standards, VerifyTT separates issuance, storage, and verification. This ensures interoperability, data portability, and protection against vendor lock-in.

## Architectural Model

VerifyTT operates on a three-role trust architecture consistent with global verifiable credential standards:

- **Issuers** generate cryptographically signed credentials using controlled signing keys.
- **Holders** store credentials in digital wallets or secure repositories under user control.
- **Verifiers** validate credentials independently using published verification keys and standardized protocols.

This separation ensures that trust does not depend on real-time institutional mediation. Once issued, a credential can be verified independently without requiring the issuing institution to be contacted for confirmation.

## Cryptographic Trust Model

Each credential is digitally signed using asymmetric cryptography. The issuer controls a private signing key, while a corresponding public verification key is made available through a trusted registry mechanism. Verification confirms:

- The credential has not been altered (integrity check).
- The issuer is recognized and valid.
- The credential has not been revoked.

This model converts trust from a human confirmation process into a computational validation process.

**Modular Infrastructure Components**

The infrastructure consists of distinct but interoperable components:

- **Issuance Module** – Generates credentials based on defined schemas.
- **Credential Store (Wallet / Web Locker)** – Enables user-controlled storage and presentation.

- **Verification Module** – Performs cryptographic and issuer validation checks.
- **Issuer Registry / Key Management** – Maintains trust anchors and public verification keys.

Because these components are modular, additional issuers or sectors can be onboarded without redesigning the core trust mechanisms.

## WHY THE INJI STACK?

VerifyTT is built on the open-source Inji Verifiable Credentials Stack. This selection was guided by architectural and governance considerations rather than vendor preference.

Inji complies with W3C Verifiable Credential standards and supports cryptographic signing, revocation, and portable machine-readable formats. This ensures interoperability across systems and future compatibility with other digital identity and credential ecosystems.

As an open-source stack, Inji supports sovereign hosting, code transparency, and long-term flexibility. Foundational trust infrastructure benefits from auditability and the ability to evolve independently of proprietary licensing constraints.

Inji's modular design separates issuance, storage, and verification functions. This enables asynchronous adoption across institutions and sectors without requiring architectural reinvention.

The selection therefore reflects a standards-aligned, modular, and vendor-neutral approach consistent with international Digital Public Infrastructure principles.

## EVALUATION CRITERIA FOR VERIFIABLE CREDENTIAL STACK SELECTION

The selection of the Inji Verifiable Credentials Stack was guided by defined architectural, governance, and sustainability criteria.

| Evaluation Criterion | Rationale for National Trust Infrastructure | Inji Alignment |
|---|---|---|
| **Standards Compliance** | Must comply with globally recognized VC standards (e.g., W3C Verifiable Credentials) to ensure interoperability and future compatibility. | Fully compliant with W3C VC specifications and cryptographic signing standards. |
| **Open-Source Governance** | Foundational infrastructure benefits from code transparency, auditability, and avoidance of proprietary dependency. | Open-source stack with publicly accessible codebase and community governance. |

| Evaluation Criterion | Rationale for National Trust Infrastructure | Inji Alignment |
|---|---|---|
| **Modular Architecture** | Separation of issuance, storage, and verification enables sector-wide reuse and asynchronous adoption. | Native separation of issuance (Certify), wallet (Web/Mobile), and verification modules. |
| **Vendor Neutrality** | Infrastructure must not depend on a single commercial operator for long-term viability. | Stack can be hosted sovereignly and integrated with multiple service providers. |
| **Data Portability** | Credentials and schemas must remain exportable and usable outside a single ecosystem. | Supports portable, machine-readable credential formats (e.g., JSON-LD). |
| **Interoperability Potential** | Must enable cross-sector and potential cross-border verification. | Standards-based architecture supports interoperable verification. |
| **Deployment Readiness** | Implementation should not require foundational re-engineering from scratch. | Mature DPI-aligned stack supported under DaaS engagement. |
| **Scalability Across Sectors** | Architecture must support expansion beyond education without redesign. | Designed as reusable trust layer across domains. |

# POLICY ACTIONS FOR NATIONAL ADOPTION

The architectural case for VerifyTT is strongest when matched by a clear policy pathway for adoption. If VerifyTT is to function as national trust infrastructure rather than a pilot implementation, policy action will be required across three areas: legal recognition, institutional adoption, and operational sustainability.

## LEGAL AND REGULATORY RECOGNITION

Trinidad and Tobago already possesses a partial legal foundation for digital records through the Electronic Transactions Act, 2011, which recognizes electronic records, electronic signatures, and the legal validity of information retained in electronic form. Relevant provisions addressing the legal recognition of electronic records, retention of information, original form requirements, and admissibility of electronic evidence should be reviewed to determine whether cryptographically verifiable credentials can operate within existing statutory language.[9]

A complementary review should consider the Evidence Act (as amended 2021), which already provides mechanisms for establishing the authenticity of electronic records through certified digital evidence.[10] In addition, the Data Protection Act should be examined in the context of selective disclosure and wallet-based credential presentation to ensure compliance with principles governing personal data processing and disclosure.[11]

The review should also extend to sectoral administrative rules where statutory instruments continue to require “certified copies,” “original documents,” or wet signatures in licensing, recruitment, or registry procedures. The objective is not to replace statutory authority but to allow verifiable credentials to operate alongside existing documentary requirements as legally recognized digital representations of issued records.

Comparable approaches have been adopted internationally. The European Union’s eIDAS 2.0 framework extends existing electronic identification and trust service regulations to recognize digital identity wallets and verifiable credentials across public and private services.[12] Similarly, the U.S. state of Utah has enacted legislation directing state agencies to pilot and recognize digital verifiable credentials as official government records.[13]

## INSTITUTIONAL ADOPTION

Digital trust infrastructure becomes valuable only when multiple institutions participate in the same verification ecosystem. Early adoption strategies should therefore focus on sectors where verification is already routine and administratively burdensome.

[9] Electronic Transactions Act, 2011, Trinidad and Tobago.
[10] Evidence (Amendment) Act, 2021, Trinidad and Tobago.
[11] Data Protection Act, Trinidad and Tobago.
[12] European Union, Regulation (EU) 2024/1183 (eIDAS 2.0) – European Digital Identity Framework.
[13] Utah Legislature, Digital Verifiable Credentials Act, 2023.

International public administration research has shown that repetitive verification processes create measurable administrative burden for both institutions and citizens.[14] Consistent with the OECD's "Once-Only Principle", governments increasingly seek to reduce repeated document submission and redundant verification across services.

For Trinidad and Tobago, this suggests a pragmatic adoption pathway:

- Establish measurable onboarding targets for the first 24 months, including at least two additional regulated sectors beyond education;
- Conduct structured outreach to employers, professional bodies, and financial institutions to expand verifier participation;
- Launch public communication emphasizing the practical benefits of verifiable credentials, including faster verification, reduced fraud exposure, and improved administrative efficiency.

International deployments have followed similar sector-focused strategies. In British Columbia, digital credentials have been introduced through partnerships between government and professional regulators, allowing lawyers to present verifiable credentials for secure court system access.

Early adoption should prioritize high-volume government workflows where credential verification already occurs frequently. Demonstrating reduced processing time and administrative handling in one such workflow can accelerate broader institutional adoption.

## SUSTAINABILITY AND ECOSYSTEM DEVELOPMENT

Long-term success requires VerifyTT to operate as durable infrastructure rather than a time-limited pilot. This requires clear institutional and financial arrangements.

Policy considerations include:

- Defining a transparent operational funding and cost-recovery model for the trust infrastructure;
- Establishing a public–private collaboration framework allowing participation by professional bodies, financial institutions, and other credential issuers;
- Creating an international advisory mechanism to support standards alignment, capacity development, and ecosystem partnerships.

[14] Pamela Herd & Donald Moynihan, Administrative Burden: Policymaking by Other Means, Russell Sage Foundation, 2018.

International initiatives such as GovStack and the World Bank's Identification for Development (ID4D) program demonstrate the value of coordinated international advisory and technical networks in supporting national digital infrastructure development.

Taken together, these policy actions would enable VerifyTT to move beyond pilot implementation toward becoming a stable national capability for trusted digital verification.

## Governance and Safeguards

VerifyTT operates under MPAAI strategic oversight, implemented by iGovTT, with CDPI advisory support and Deloitte under the DaaS framework. Safeguards include cryptographic signing, revocation capability, role-based access controls, and structured export readiness.

Institutional alignment, verifier adoption, sustainability planning, and legal recognition are acknowledged as structured implementation considerations. These are managed realities, not structural weaknesses.

## Scaling Beyond Education

The underlying credential infrastructure — including cryptographic signing mechanisms, verification protocols, wallet integration, and issuer registry services — remains consistent across use cases. Expansion into additional sectors does not require rebuilding these foundational components. Instead, new credential types are introduced through the definition of sector-specific schemas that operate within the same standards-based framework.

In practical terms, this means that onboarding a professional licensing body or a healthcare authority requires governance alignment and schema configuration, not architectural redesign. The verification logic, cryptographic validation process, and presentation mechanisms remain unchanged.

### Five Years On: Institutionalization of the Trust Rail

Within five years, the measure of VerifyTT's success will not be the volume of credentials issued, but the normalization of embedded digital verification across sectors.

The foundational components — cryptographic signing, verification protocols, wallet integration, and issuer registry services — will remain unchanged. What evolves is sectoral participation.

#### *Education as Default Digital Issuance*

Tertiary institutions will issue digital credentials as a routine complement to physical artifacts. Verification will occur through computational validation rather than direct institutional confirmation. Manual confirmation will shift from standard practice to exception handling.

### *Regulated Sector Onboarding*

At least one additional regulated domain — such as professional licensing or healthcare credentialing — will operate on the same trust infrastructure. Onboarding will require schema definition and governance alignment, not architectural redesign.

Issuers will retain authority over issuance and revocation. The infrastructure will standardize verification, not alter regulatory control.

### *Verification Embedded in Workflows*

Verification will increasingly be integrated into institutional systems — recruitment platforms, licensing checks, and compliance processes — rather than conducted through ad hoc document review.

Trust will become an automated validation layer within existing workflows.

### *Governance Maturation*

Issuer accreditation processes, schema approval mechanisms, and revocation governance will be formalized. Operational oversight will shift from project implementation to infrastructure stewardship.

The trust rail will function as a stable public capability rather than a pilot initiative.

## Methodological Note

This white paper is based on a structured analysis of Trinidad and Tobago's digital ecosystem, documented institutional workflows within the tertiary education sector, and internationally recognized Digital Public Infrastructure (DPI) design principles.

The evidence base draws on:

1. **Publicly available national digital indicators**, including internet penetration, mobile connectivity, and broadband adoption data published by internationally recognized sources such as the International Telecommunication Union (ITU), the World Bank, and global digital monitoring reports.

2. **Documented institutional practices** observed within the tertiary education credentialing environment during the design and implementation of the VerifyTT pilot. These observations include paper-based issuance processes, manual verification workflows, and administrative handling procedures.

3. **International DPI standards and governance frameworks**, including W3C Verifiable Credential specifications and open-source modular credentialing architectures, which inform the technical and architectural analysis presented.

4. **Comparative institutional logic**, drawing on established public administration and transaction-cost principles to assess the systemic impact of manual verification processes.

Where quantitative national statistics are available, they are cited. Where direct institutional workflows are described, they reflect documented operational practice within the pilot scope. Analytical conclusions are derived from the structural implications of these practices rather than from generalized national surveys.

This paper does not claim to provide exhaustive sector-wide statistical measurement. Rather, it presents a policy and infrastructure analysis grounded in documented practice and internationally recognized standards to articulate the rationale for establishing a national digital trust infrastructure.

## CONCLUSION: TRUST AS PUBLIC UTILITY

VerifyTT marks a shift from manual verification to embedded assurance. By embedding trust directly within its digital economy, Trinidad and Tobago transitions from negotiating trust to sustaining it as infrastructure.