TRUST Over IP FOUNDATION

Case Study

Bhutan NDI (National Digital Identity) & ToIP Digital Trust Ecosystems

21 May 2024

This publicly available Case Study was approved by the ToIP Ecosystem Foundry Working Group on 21 May 2024. The ToIP permalink for this document is: **Case Study: Bhutan NDI & ToIP Digital Trust Ecosystems**

The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 400 organizational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Table of Contents

Document Information

Authors:

Pallavi Sharma, Bhutan National Digital Identity Project, Druk Holding & Investments

Eric Drury, Director, Forthco.io

Contributors:

ToIP Ecosystem Foundry Working Group members

Druk Holdings & Investments NDI project team

Terms of Use

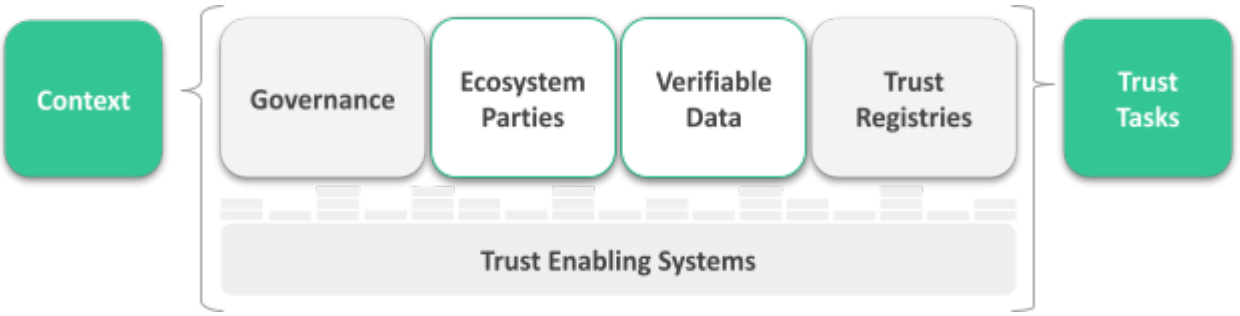
Bhutan NDI: Digital Trust Ecosystem

Bhutan NDI, the Kingdom of Bhutan's national digital identity system, officially launched in 2023 and introduced *Self-Sovereign Identity* as a foundational element underpinning a national digital trust ecosystem which connects the government, individuals, and the private sector in their digital interactions.

In this Case Study we examine the Bhutan NDI system through the digital trust ecosystem (DTE) lens. In doing so, we are able to gain both a high-level overview of the ecosystem, while also getting detailed insights into the specific ecosystem components.

NDI's Digital Trust Ecosystem Building Blocks

This Case Study is a collaboration between the *Trust Over IP Foundation* and Bhutan's NDI team. The structure of this Case Study follows the Trust over IP Foundation's *Digital Trust Ecosystem Building Blocks* framework of: (1) Context, (2) Governance, (3) Ecosystem Parties, (4) Verifiable Data, (5) Trust Registries, (6) Trust Enabling Systems, and (7) Trust Tasks.



The DTE Building Blocks framework helps us to examine Bhutan NDI from several broad perspectives, while providing a holistic view of the ecosystem and its key components, and highlighting the most innovative characteristics of the ecosystem, including:

- A forward-thinking approach to identity at population-scale;
- early adoption of self-sovereign identity principles and verifiable data technologies;
- a progressive and modern governance architecture;
- a commitment to the highest level of security, privacy, and inclusivity;
- all underpinned by advances in decentralized / distributed systems.

Together, these principles power the Bhutan NDI trust ecosystem, ensuring accessible and equitable digital services for a multitude of use cases across the Kingdom.

The Building Blocks of the Bhutan NDI Digital Trust Ecosystem (DTE) are:

BUILDING BLOCKS	DESCRIPTION
Context	A National Digital Identity system based on SSI (self-sovereign identity) principles to support the emergence of a national digital trust-based ecosystem connecting Bhutan's citizens, government and private sector, and propelling the Kingdom towards a future digital economy.
Ecosystem Parties	The Ecosystem Parties participating in Bhutan's NDI digital trust ecosystem are grouped into three categories: ● Government ● Individuals ● Organizations
Verifiable Data	The current verifiable data that can be issued, exchanged, and verified in the NDI ecosystem includes: ● Foundational IDs, Residence Permits, Tourist Visas, Employment Credentials, Academic Credentials, Telephone credentials, Self-attested email and allergy credentials
Governance (Human Trust)	● The *National Digital Identity Act (NDI Act)* is the overarching governance anchor for the NDI DTE, establishing the purpose and vision of the ecosystem. ● The *NDI Governance Framework* is the reference for how the ecosystem is governed. ● Additional governance anchors include: Department of Civil Registration, and Census, Department of Immigration, Registrar of Companies…
Trust Registries (Technological Trust)	Technological Trust is derived via two main registries: ● NDI Trust Registry: Contains a list of Organizational Public DIDs for authentication and verification purposes ● Verifiable Data Registry: Stores Issuer's public keys, DID documents, and other schema and cryptographic metadata.
Trust Enabling Systems	The supporting standards and protocols which underpin trust in the NDI system include: ● W3C Verifiable Credentials (VCs), Anoncreds, Digital Signatures (CL Signature), Decentralised Identifiers (DIDs), Distributed Ledger Technology, Sharding, QR codes, Deeplinks, Acentrid…
Trust Tasks	The major trust tasks that enable trust to flow through the NDI DTE include: ● Onboarding ● Connecting with other parties ● Issuing & Receiving Credentials ● Credential exchange for Passwordless Login, eKYC

1. CONTEXT

In 2020, the Kingdom of Bhutan, led by the Prime Minister's Office, initiated the Digital Drukyul Flagship Program that aimed to transform public service delivery.

As a foundation for the Digital Drukyul Flagship Program, the National Digital Identity (NDI) Project was initiated upon the Royal Command issued to the Government Technology (GovTech) Agency (then Department of IT & Telecom). The project was officially launched in 2021 in collaboration with the Department of Civil Registration & Census (DCRC), the Department of Immigration (DOI), and Druk Holding and Investments (DHI).

The project, from its inception, was guided by His Majesty the King's personal vision to provide every citizen with the right to privacy. Therefore, one of the key decisions made early on was to adopt SSI (self-sovereign identity) principles as the basis for the National Digital Identity program.

The decision was made with the understanding that for public service delivery to truly transform, *trusted identity* would need to be at the root of every digital interaction. And if trusted identity were to be introduced at the population scale, it needed to be both practically and perceptibly extremely trust*worthy*. Self-sovereign identity responded to these needs.

By introducing a trusted digital identity framework, the Kingdom was putting in place the first building block that would serve as the foundation for its budding digital economy.

And so the initial remit of transforming public service delivery was expanded, and national digital identity would serve the broader purpose of supporting a national digital trust-based ecosystem connecting Bhutan's citizens, government, and private sector, and propelling the Kingdom towards a future digital economy.

Bhutan NDI was launched nationwide in October 2023, less than three years after its conception. This was the beginning of the creation of a truly national digital trust ecosystem in Bhutan.

Scope: National Digital Identity spans a wide and diverse range of use cases, actors, objectives, and interests. The expectations and demands relating to privacy, transparency, security, and connectivity fall along every point of the trust spectrum.

A National Identity ecosystem must accommodate the highest concerns of a sovereign nation, as well as the most intimate needs of its citizens. It must serve the interests of businesses while protecting the rights of individuals. The scope is both extremely broad and very specific.

While the NDI system was conceived in the context of the need to streamline, via integrated user interface (UI) and user experience (UX), access to public services - which up until now has been extremely fragmented - it also needed to pave the way for trusted peer-to-peer interactions between individuals, government, and organizations, accelerating digital adoption and access to financial and other services, so that all citizens can participate in the global digital community and digital markets.

Social Context: Bhutan is a landlocked country in the Himalayan range, nestled between India and China. The population of approximately 750,000 is scattered across 20 districts, divided by rugged terrain and limited physical infrastructure. Approximately 80% of the population are involved in agriculture, and rural residents usually travel long distances to access government, business, and financial services.

Having digital access to public and professional services in remote villages is especially appealing, and important in ensuring the NDI system is truly inclusive.

Safeguarding the privacy of individuals, as related to the disclosure of personally identifiable information (PII) during G2C (Government to Citizen) interactions was paramount, so SSI's data minimization and privacy-preserving principles are a good fit.

Economic Context: The decision to adopt SSI Digital Identity also had an economic incentive. Originally, the plan for the national identity infrastructure was to be PKI-based, but the program was able to lower development and implementation costs substantially by adopting a standards- and software-based decentralized architecture.

Lower implementation costs was especially appealing since the Bhutanese economy has limited access to the global market, other than via its major trading partner, India, and so cost was a key part of the decision to adopt SSI.

Technological Context: For most of its history, Bhutan was isolated from the rest of the world, only opening trade and diplomatic ties in 1975. Bhutan introduced television, broadcasting, and the internet in 1999 and mobile phone services in 2003. Mobile and agency banking were introduced much later, in 2015. In 2020, Bhutan revamped its technology strategy, pivoting its focus to Web 3.0 technologies and investing in decentralized and distributed ledger technologies.

High-speed internet is still a challenge, especially in many of the remote villages, which highlights the importance of addressing *offline* solutions to ensure the NDI system fulfills its mission to be inclusive.

2. ECOSYSTEM PARTIES

NOTE: In this Case Study we will sometimes refer to ecosystem parties as 'trusted' or 'trustworthy', but it is important to note that the trustworthiness of an ecosystem party can only truly be determined by a verifier after an authentication and verification process - and even then, it is ultimately up to the verifier to make a 'trust' determination based on their own internal decision-making policies.

The parties participating in Bhutan's NDI digital trust ecosystem are grouped into three categories: **Government, Individuals,** and **Organisations**.

Ecosystem Parties are considered 'trusted' because they each go through an initial authentication process and commit to abide by the ecosystem's terms and conditions as embodied in the NDI Governance Framework, after which they receive a unique, persistent, reusable, and verifiable identifier that they use to authenticate themselves during interactions with other parties in the ecosystem.

Trust is limited to very specific actions which each party performs within the ecosystem, such as issuing, requesting, presenting, or verifying credentials.

- **GOVERNMENT**: The Royal Government of Bhutan is the ultimate trusted party. The government's trust and authority are bestowed via legislation, which it then delegates to Secretaries, Offices, or Departments through its Ministries.

  All governmental parties that participate in the NDI ecosystem receive *Organizational DIDs* (Decentralized Identifiers) as *agents*.

  Government parties in the ecosystem include:

  - **Department of Civil Registration and Census (DCRC)**: Trusted to issue Foundational IDs and Permanent Address verifiable credentials (VCs) to Bhutanese citizens. The VCs issued to citizens by DCRC act as the source of truth and usually serve as the basis for all other verifiable credentials.
  - **Department of Immigration**: Trusted to issue digital versions of visas and permits to non-nationals for tourism, residency, work, study, and other purposes. In the NDI ecosystem, these are referred to as Foundational IDs for non-Bhutanese participants of the ecosystem.
  - **Government Technology Agency (GovTech Agency)**: Trusted to authenticate the Foundational IDs of citizens for passwordless login to their integrated government-to-citizen (G2C) services portal that facilitates public service delivery.

- **ORGANIZATIONS**: Organizational trust is established either via Bhutan's Registrar of Companies (ROC), where companies register for a business license, or via the Royal Monetary Authority for financial institutes. Eventually, any entity that has a vLEI (verifiable Legal Entity Identifier) will also be considered a trusted party.

  Organizations are onboarded into the ecosystem as *agents* and receive *Organizational DIDs*. After onboarding, organizations appear in the NDI Trust Registry (currently a backend microservice), from where their legitimacy and status can be verified by other ecosystem parties.

  Organizations from a variety of sectors currently participate in the NDI ecosystem, including:

  - **Financial Institutions**: Bank of Bhutan (BOB), Royal Securities Exchange of Bhutan
  - **Telcos**: TashiCell InfoComm Pvt Ltd.
  - **Education**: Royal University of Bhutan, Bhutan Council for School Examination & Assessment
  - **Human Resources**: Druk Holding and Investments (DHI), Royal Civil Service Commission
  - **Transportation**: Road Safety & Transportation Authority

  Organizations from several other industry sectors will join the ecosystem in the near future, including:

  - **Media**: ***Samuh***, an Over-the-Top (OTT) media platform
  - **Healthcare**: *Bhutan's National Healthcare Services*
  - **Aviation**: *Drukair*

- **INDIVIDUALS**: The NDI trust ecosystem accounts for three categories of individuals:

  - **Citizens**, where trust is derived via their inclusion in the national DCRC database and established via a biometric verification process and verification of CID (Citizen ID), household, and THRAM number (address). The process of matching data from the DCRC with the individual providing the biometrics creates a binding that serves to establish the individual as a trusted party.

    Most of the credentials issued to individuals come from the government or organizations, but individuals can also issue credentials to themselves (such as the *allergy, email, and temporary address* credentials), meaning they fill in this information themselves, and that information is stored as a 'self-attested' credential.

    At the moment, citizens can receive various types of credentials, including:

    - *Foundational ID*
    - *Permanent Address*
    - *Mobile Number* credential
    - *Academic* credentials
    - *Employment* credentials
    - *Driver's License* credentials
    - *Vehicle Registration* credentials

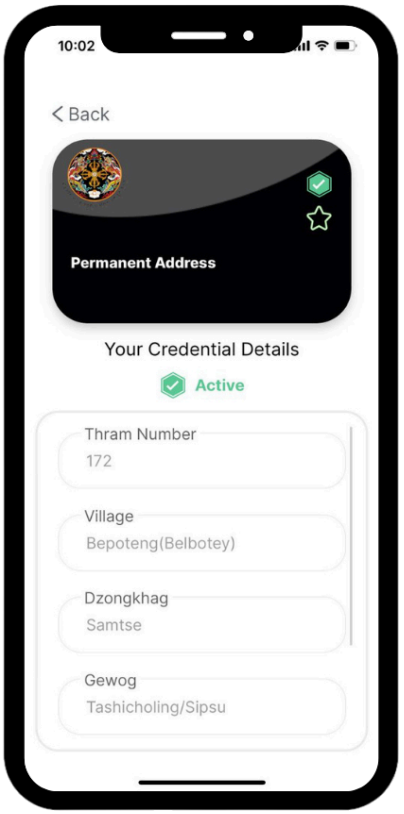
- **Non-national residents** (expats with worker permits, international students, spouses, etc.), where trust is derived via their status in the Department of Immigration's database. Non-national residents can receive various credentials, including:
    - *Work Permit* credential
    - *Nationality* credential.
- **Tourists** (in the near future), where trust will be derived via their electronic visas issued by the Department of Immigration. Tourists can receive:
    - *Tourist Visa* credential

---

3. VERIFIABLE DATA

One of the core functions of the NDI ecosystem is to be able to exchange verifiable, *trustworthy* data among ecosystem participants, i.e. in a secure, privacy-preserving, consent-based, and transparent manner. The verifiable data that flows through the ecosystem is in W3C Verifiable Credential format (see *Section 6. Trust Enablement Systems*).

The current verifiable data that can be issued, exchanged, and verified in the NDI ecosystem includes:



- **Foundational ID**: Issued to an individual and digitally signed by the DCRC (citizens) or DoI (for foreigners) at the time of the individual's registration for NDI. To receive a Foundational ID, an individual validates their personal information and completes a biometric facial scan - which is matched to their biometric details stored in the DCRC database.

  A Foundational ID provides the recognition of an individual's existence through the validation of their name, date of birth, and gender, as well as other crucial information about their legal status, such as their citizenship, household number, work permit number, etc. Foundational ID for citizens, residents, and visitors is considered the source of truth upon which other service-specific verifiable credentials are issued.

- **Permanent Address:** Issued to citizens and digitally signed by the DCRC at the time of the individual's registration for NDI; an individual validates the permanent address details, which the DRCR compares to the details submitted at birth or during the annual census to match the source to validate their proof of residence for compliance with sector-specific regulatory mandates.

- **Academic Credential**: Issued and digitally signed by the Royal University of Bhutan. Student ID and university certificates are issued as verifiable credentials to the students and alumni of the university to validate their professional credentials during the employment processes.

- **Employment Details**: Issued and digitally signed by an employer (*Druk Holding & Investments and the Royal Civil Service Commission for the moment*) to confirm employees' designation, grade, salary, and other relevant information related to the individual's employment.

- **Mobile Number:** Issued and digitally signed by TashiCell InfoComm Pvt Ltd. to confirm subscribers' mobile numbers, and in the near future leased line and broadband numbers.

- **Driver's License**: Issued and digitally signed by the Road Safety & Transportation Authority to confirm an authorized individual's permit to drive either light, heavy, two-wheeler, or taxi vehicles along with other information related validity and type of permit.

- **Learner's License:** Issued and digitally signed by the Road Safety & Transportation Authority to confirm an individual's permit to learn driving on public roads for a specific time period.
- **Vehicle Ownership:** Issued and digitally signed by the Road Safety & Transportation Authority to validate vehicle ownership details along with details about the vehicle and its roadworthiness.
- **Audit Clearance**: Issued and digitally signed by the Royal Audit Authority to provide certification for a no-conflict/no-objection clearance.

SELF-ATTESTED CREDENTIALS

Individuals can also self-attest credentials on the Bhutan NDI digital wallet to make claims about themselves and present these during the eKYC or authentication processes required by service providers. Examples of self-attested credentials currently available in the NDI ecosystem include:

- **Telephone Credential**: For non-TashiCell users, individuals can also attest one or more mobile numbers as a verifiable credential.
- **Email Credential**: Individuals can add one or more email IDs as self-attested verifiable credentials.
- **Allergy Credential**: Individuals can make claims about one or more allergies by adding them as verifiable credentials.

4. **GOVERNANCE** (HUMAN TRUST)

Governance in the NDI ecosystem is multiple, layered, and overlapping, with several bodies contributing to the overall governance of ecosystem activities.

While the ecosystem inherits governance from existing sector-specific policies, regulations, and legislation, there is a need for additional governance to address the complexities that arise when introducing new technologies and new ways of exchanging data in a digitally native ecosystem.

For the NDI ecosystem, it is the *National Digital Identity Act of Bhutan 2023* which addresses these areas.

National Digital Identity Act: The NDI Act of Bhutan, passed in July 2023, is an Act of the Parliament and the deepest governance anchor which establishes the legitimacy of Bhutan NDI to provide for "an innovative National Digital Identity Infrastructure to encourage the use of secure, privacy-enhancing digital credentials and / or data, support development of digital trust between digital economy participants, while adhering to the kingdom's environmental, social, governance, and sustainability objectives."

The NDI Act sets the overarching principles for information security, privacy, and digital signatures.

The NDI Act authorizes the drafting of the *NDI Governance Framework*.

NDI Governance Framework (NDI GF): Details how the NDI ecosystem is governed through five key aspects:

1. Overall Ecosystem Objectives and Conduct
2. Governing and Administrative Authorities
3. Technical, Security and Privacy Requirements
4. Participants (*who* can, and *how* to) in the NDI Ecosystem
5. Trust Flows in the NDI Ecosystem

1. **Overall ecosystem objectives and conduct:** The NDI GF ensures that the ecosystem operations are consistent with the principles laid out in the NDI Act, and are expanded on in the detailed code of conduct, desired outcomes, and other sub-sections.
2. **Governing and Administering Authorities:** The NDI GF establishes the formation of, and mandate of a Governing Body and an Administrative Body who are responsible for the technical, security and privacy requirements of the ecosystem architecture, as well as the conduct of members.
    - The *Governing Body* is an ad hoc body responsible for overseeing the NDI ecosystem and its technical infrastructure, and ensuring adherence to the Governance Framework.

- Includes Head of GovTech Agency (the sponsor of NDI), 2 members of the Royal Civil Service Commission, and 2 members of industry independent individuals.
- Functions independently from the Administrative Body, which is the Bhutan NDI company.
- Approves regulations for Issuer, Verifier, Holder onboarding.
- Accords foreign electronic identification schemes recognition for cross-border interoperability.

- The *Administrative Body* is the Bhutan NDI company, whose function it is to develop the technology, and oversee the day-to-day operations of the NDI ecosystem. The Administrative Body:
  - Is responsible for onboarding participants into the ecosystem: Issuers, Holders, and Verifiers.
  - Drafts the NDI Ecosystem Governance Framework (a family of governance documents) and submits to the *Governance Body* for approval.
  - Develops and operates the NDI ecosystem infrastructure: mobile app, APIs for issuance/verification, Trust Registry, Revocation Service, etc.

3. **Technical, security, and privacy requirements**: The NDI GF lays out the requirements for NDI architecture and infrastructure as related to security, privacy, accessibility, Trust Service Providers, incident reporting, etc.

4. ***Who* can participate in, and *how* to participate in the NDI ecosystem**: The NDI GF outlines: the processes for onboarding into the NDI Ecosystem so they can be included in the list of ecosystem parties, i.e. considered a 'trusted party'; how trust is *asserted* and assured in the ecosystem (via detailed Governance Framework control documents); how trust is assured through certification documents; and how the integrity of active parties, their status, and revocations (if any) is ensured.

5. **How trust flows through the NDI ecosystem**: The NDI GF outlines the parameters for the issuance, exchange, and verification of credentials and data, and their compliance with tangential sector-specific or jurisdictional governance frameworks. Each professional ecosystem party also adheres to sector-specific governance.

Other key sector-specific governance anchors in the NDI ecosystem are:

- **Department of Civil Registration and Census**: Under the Ministry of Home Affairs, the DCRC develops and maintains accurate and complete information on population and demography via the Civil Registration and Vital Statistics System. DCRC governs and maintains Bhutanese citizens' legal status.
- **Department of Immigration**: Enforces the Immigration Act of the Kingdom of Bhutan and contributes to nation building. DoI governs and maintains foreign residents' and visitors' legal status within the borders of Bhutan.
- **Registrar of Companies** (Corporate Regulatory Authority of Bhutan): a Statutory Regulatory Authority under Chapter 14 of Companies Act, 2016, is responsible for incorporation or registration of corporate and private entities, and supervision of all corporate entities including listed companies, entities created under Royal Charter, special laws, etc. Registrar of Companies governs and maintains corporate and private businesses' legal status.
- **GLEIF**: All private and corporate organizational entities that participate in the NDI ecosystem will be vetted according to the GLEIF governance framework.

5. **TRUST REGISTRIES** (TECHNOLOGICAL TRUST)

NDI's trust registries, acting as technological trust anchors, enable the fundamental technical assurances necessary for secure interactions between ecosystem parties. They are used to validate the identifiers of parties involved and ensure the integrity of data exchanged.

In the NDI DTE, the two main trust registries are the *NDI Trust Registry* and the *Verifiable Data Registry.*

- **NDI Trust Registry**: Contains a list of trusted *Organizational Public DIDs* for authentication and verification purposes. It interacts with the Bhutan NDI wallet and the verifiable data registry (see below).
- **Verifiable Data Registry**: Built on Hyperledger Indy blockchain and the Indicio run network (soon migrating to Polygon). It stores Issuer's public keys, DID documents, and other schema and cryptographic metadata (signed by issuer's private key).

The NDI trust registries enable *transitive trust*, so that the integrity of an ecosystem issuer's claims - as presented in the form of a verifiable credential - can be verified without the need for direct connection to the Issuer.

For example, when an individual presents their *Foundational ID* credential to a business service provider in order to authenticate themselves and gain access to a service, the business (listed as a ecosystem party in the Trust Registry) must first verify that the issuer of the *Foundational ID* credential (in this case, the DCRC) is present in the NDI Trust Registry.

The business provider verifies the status of the *issuer* of verifiable credentials on the NDI Trust Registry to validate the trustworthiness of a verifiable credential presented by the individual.

For the business service provider to trust that the individual presenting, for example, the *Foundational ID* credential is indeed the rightful holder, it must check the Verifiable Data Registry to determine whether the issuer's signature on the *Foundational ID* credential is the same as the signature which is stored on the Verifiable Data Registry.

In this way, the NDI Trust Registry and the Verifiable Data Registry anchor the bindings of the ecosystem parties and data and allow trust to flow through the ecosystem.

To facilitate the interactions with the ecosystem's trust registries, NDI has developed several micro-services based on SSI roles and actions, including:

- **Client Services**: Issuer Services, Verifier Services, and Agent Services
- **Core Services**: Revocations Services, Trust Registry Service
- **Onboarding Services**: Foundational Services, Biometrics Service

6. TRUST ENABLING SYSTEMS

Trust enabling systems ensure the integrity, reliability, and interoperability of digital interactions to allow trust to flow among parties. The NDI ecosystem relies on a variety of open standards, protocols, and technologies to support these trust flows, including:

- **W3C Verifiable Credentials (VCs**): Verifiable data in the NDI ecosystem is designed around the specifications and standards approved by the World Wide Web Consortium (W3C).
- **Decentralised Identifiers (DIDs)**: DIDs provide unique identifiers for all the ecosystem parties. The NDI ecosystem currently runs on the did:sov method to create, manage, and resolve DIDs and their associated private and public keys. The NDI ecosystem is built on decentralized identifiers technology using the Indicio Network and Hyperledger Indy blockchain.
- **Distributed Ledger Technology (DLT)**: Driven by the philosophy of SSI, Bhutan NDI is built on the Hyperledger Indy blockchain. Hyperledger Indy's distributed ledger technology stores and manages DIDs and public keys, eliminating the need for intermediaries to manage identity data.
- **Anoncreds**: Currently, the NDI ecosystem leverages Anoncreds-based verifiable credentials. Using the Anoncreds-supported credential definition, parties in the NDI ecosystem can exchange verifiable data supported by zero-knowledge proof (ZKP) protocols. For example, individuals can confirm that they are above the age of 18 without disclosing their actual age, but at the same time validating the authenticity of the hidden attribute i.e., their age which may be required for a digital interaction.
- **CL Signature** (cryptographic trust proof). To provide technical trust for variable data exchange designed around ZKP protocols, the VCs are issued with CL signatures. The CL signatures, further, enable parties to selectively disclose information through a proof request during a trusted interaction, i.e. a trusted party can issue a VC with a CL signature for an individual who can then selectively disclose attributes, based on the proof request, from one or a combination of VCs without presenting all the attributes listed under all credentials.

  With the migration to the Polygon network, the NDI ecosystem will also support JSON-LD-based verifiable credentials.
- **Revocation Services**: Bhutan NDI's identity information system is supported by its Revocation Services to manage the statuses of credentials and other certificates. Currently, the revocation mechanism reflects the status of a credential under one of the following categories:
    - *Active*: To indicate that the credential/certification is valid.
    - *Suspended*: To indicate that the credential/certification has been temporarily suspended. For most suspended credentials, the status will automatically update to active after the suspension period lapses. For instance, when a driver has violated a traffic regulation, suspending his/her right to drive for a certain period.
    - *Revoked*: To indicate the credential/certification has permanently been invalidated. For most revoked credentials, the individual will need to initiate the request for a

new credential. For instance, when a driver's license expires after the validity of the permit.

- **Sharding**: Backup and restoration of the Bhutan NDI wallet are facilitated by sharded systems that enable encrypted data distribution. During the backup process, the wallet is distributed across several shards and stored on undisclosed servers. During the restoration process, parties need to retrieve data from multiple encrypted shards to recover verifiable data previously stored in their wallet.

- **QR codes:** The NDI ecosystem leverages QR codes to complete a trust task. The QR codes can only be generated and scanned by agents established as ecosystem parties. The use of QR codes is dependent on two devices, i.e., to access services or a portal through a different device other than the device where the Bhutan NDI wallet is installed.

- **Deeplinks:** The NDI ecosystem also leverages deeplinks to complete a trust task. The access request to a portal or a service through deeplinks can only be authenticated through the Bhutan NDI wallet. The use of deeplinks is dependent on a single device, i.e., to access services or a portal through the same device where the Bhutan NDI wallet is installed.

- **Acentrid:** The NDI platform is built on Acentrid, a customized protocol layer developed using a fork from Evernym's Verity platform which was open-sourced. Acentrid currently connects NDI's ecosystem layer with the Hyperledger Indy blockchain to perform core functions, including issuance of verifiable credentials, generating proof requests, sharing proofs, and facilitating DID communications.

7. TRUST TASKS

Trust tasks are where trust in the ecosystem becomes tangible, as ecosystem parties connect with each other, exchange information, and conduct transactions.

Trust tasks might be thought of from the perspective of UX (user experience), where humans interact with the applications and digital interfaces in the digital trust ecosystem. These interactions are the moments where the trustworthiness of the entire ecosystem is challenged and has the opportunity to prove its integrity.

One of the NDI ecosystem's primary objectives was to streamline, via unified and integrated UI and UX, access to public and private services, which up until now have been extremely fragmented.

The NDI Wallet

Trust tasks are use-case specific, but the majority of trust tasks in the NDI ecosystem today occur via the *NDI Wallet* and involve scanning a QR code or accessing a deeplink, consenting to connection requests, and sharing verifiable credentials upon requests.

In most cases trust tasks are integrated into existing ways of working, and in other cases they introduce new processes and workflows.

Examples of trust tasks in the NDI ecosystem include:

1. **Onboarding into the NDI ecosystem**: For obtaining an Organizational DID or a Foundational ID
2. **Connecting with other parties in the NDI ecosystem**: For authentication and verification, including determining the status of an ecosystem party
3. **Issuing & Receiving Credentials**: For mutual trust establishment
4. **Sharing Credentials**: For passwordless login, eKYC/customer identification, access management…

1. ONBOARDING INTO THE NDI ECOSYSTEM

Government entities, organizations and individuals can all become participants in the NDI ecosystem through an onboarding process.

Onboarding is considered a trust task because it establishes an individual, an organization, or a government entity as a 'trusted party' in the ecosystem, and because participants must make assumptions about trustworthiness of the ecosystem when onboarding.

INDIVIDUAL ONBOARDING: OBTAINING A FOUNDATIONAL ID

When an individual onboards into the NDI ecosystem, they obtain a *Foundational ID*, which is stored in their NDI Wallet, and which establishes them as a 'trustworthy' ecosystem participant.

When an individual decides to onboard into the NDI system, they implicitly make certain trust assumptions:

- The individual trusts that the NDI Act will protect their interests.
- An individual trusts that the NDI system will provide a private and secure environment for the storage of the personal details they share during the onboarding process, via the wallet that is created on their phone.
- The individual also trusts that NDI does not and will not store any of their personal identifiable information (PII) on the NDI database, and that NDI only acts as a *facilitator* of digital interactions.
- An individual trusts that their *Foundational ID* will enable them to connect and interact with other parties in the ecosystem with those same privacy and security guarantees.

GOVERNMENT & ORGANIZATIONAL ONBOARDING: OBTAINING AN ORGANIZATIONAL DID

When an organization or government entity onboards into the NDI ecosystem as an agent, they obtain a Public DID, and are registered in the NDI Trust Registry, which establishes them as a 'trusted' ecosystem party. Furthermore:

- An organization or government entity trusts that with the *Public DID* they are assigned, and via the agent services that the NDI system provides, they will be able to connect, communicate and interact securely and privately with other agents and ecosystem parties.

2. ESTABLISHING A TRUSTED CONNECTION: Login with Bhutan NDI

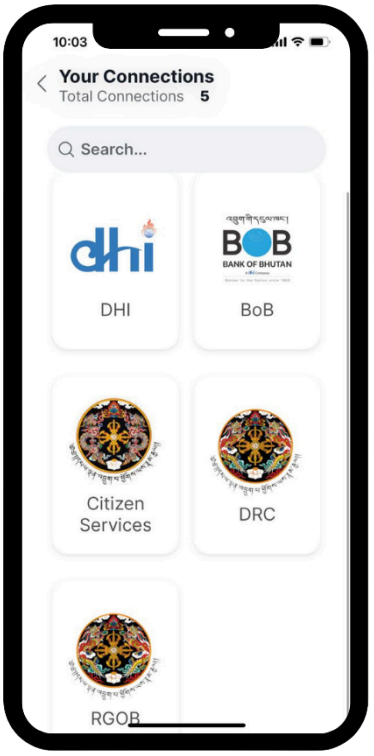
When one party wishes to connect with other parties or agents in the NDI ecosystem, they implicitly trust the NDI system to ensure that their connections are private and secure and that all connecting parties are also already established as trusted ecosystem participants.

The NDI wallet enables this mutual trust by assuring that only parties that are present in the NDI Trust Registry and the Verifiable Data Registry can connect with each other. In other words, if all necessary information and keys of *both connecting parties* are not present in either or both of the NDI trust anchors, a trusted connection cannot be established.

In the NDI ecosystem, two types of connections can be established: a *persistent connection*, or an *out-of-band (OOB) connection*.

Establishing an initial, persistent connection

- An initial and persistent connection is useful in cases where one of the parties needs to store the other party's details (with consent, of course) for regulatory compliance or other reasons, or where there is regular ongoing authentication and verification between two parties - for example when an individual needs to login to their bank.
- A persistent connection improves user login experience, since once a persistent connection is established, subsequent user logins are quick and easy, with no usernames or passwords, and without sacrificing privacy or security.
- Establishing a persistent P2P connection is a one-time procedure that generates a *relationship DID* which is then stored in a user table, usually maintained by the service provider (for example, the bank), and which is then used for authentication / verification of the individual on subsequent logins and service access.
- In the context of banking, for example, this *relationship DID* replicates the CIF (Customer Information File) requirement in a digital format.



Example of using 'Login with Bhutan NDI' for a banking app.

- On the **mBOB** (Bank of Bhutan's mobile banking app), individuals can choose the option to 'Login using Bhutan NDI'
- Opting for this login option will open the individual's Bhutan NDI wallet.
- The Bhutan NDI wallet manages the connection by:
    - ensuring the connection request is from a ecosystem party;
    - clearly displaying the attribute(s) from one of the verifiable credentials which is requested by mBOB for authentication purposes - in this case the CID number attribute from the *Foundational ID*;
    - allowing the individual to consent to sharing that information - which the bank uses to match to its existing customer records.
    - ***Note***: As part of this verification process, in order to fully trust the *Foundational ID* credential which was issued in the past and determine whether that credential is *still* valid, the Bank queries the credential's status:
        - It checks the NDI Trust Registry to ensure the *Organizational DID* of the issuer of the *Foundational ID* is indeed in the NDI Trust Registry.

        - It then checks with the Revocation Service Provider to ensure the *Foundational ID* has an 'active' status, i.e. has not been suspended or revoked.
        - Once these two steps are done, a *Relationship DID* is generated and the individual is redirected back to the mBOB app for a successful login.
    - After the persistent connection is established, the individual can use the 'Login with Bhutan NDI' option for quick and easy subsequent logins to the mBOB app, via *session-based authentication*.
        - BOB requests an attribute (CID number) from an individual's Foundational ID.
        - BOB, simultaneously, checks the *Relationship DID between the individual and the bank at the backend.*
        - Individual consents to sharing the attribute from the Foundational ID.
        - If both the attribute and the *Relationship DID* are successfully validated, the user is redirected back to mBOB with a successful login.

Passwordless Login via an Out-of-Band (OOB) connection

- OOB connections are used for passwordless login for Government-to-Citizen (G2C) connections via the G2C Portal. OOB connections are only used for authentication and verification purposes during the login process, and no data is stored by the authenticating government office.
- Individuals wishing to access a G2C service will establish an OOB connection when they 'Login with Bhutan NDI':
    - When logging in to a G2C website via browser:
        - The individual scans a QR Code which is shown on the G2C webpage:
            - The individual's NDI wallet shows a pop-up, requesting a connection;
            - The individual consents to the connection request, and then sees another pop-up requesting an attribute (CID number) from their *Foundational ID* to be shared;
            - The user consents, and a successful authentication and verification will automatically log the user in to the G2C portal.
    - Accessing the G2C portal via mobile phone follows the same flow, but instead of a QR Code, a deeplink redirects the user to their NDI Wallet to complete the passwordless login process.

3. ISSUING / RECEIVING A CREDENTIAL

Issuing a credential is a trust task because the issuer needs to trust that they are issuing the credential to the appropriate recipient.

Receiving a credential is a trust task because the recipient must trust that the party that wishes to issue them a verifiable credential is a trusted, authentic, verified ecosystem participant and that the credential they will receive will be safe and legitimate, i.e., will not be infected, spam, a trojan horse, etc.

The issuance / reception of a credential follows a similar pattern, no matter the sector (banking, telecommunications, education, etc.). For example:

- Two parties establish a P2P connection via their Bhutan NDI wallets;
- One party receives a notification on their Bhutan NDI wallet that their connection "would like to send a credential";
- The receiving party accepts the credential, which is then stored in their Bhutan NDI wallet.

Student ID VC example: An example of issuing / receiving a credential is seen with the Royal University of Bhutan (RUB), which can connect with their students and issue a *Student ID VC* (verifiable credential), which the student stores in their NDI Wallet and uses to login to the RUB portal.

4. EXCHANGING CREDENTIALS: REQUESTING & SHARING

In the NDI ecosystem, credentials can only be requested and shared by official ecosystem parties, i.e. parties that are onboarded into the NDI ecosystem.

The most common trust tasks involving the exchange of credentials are passwordless login, access management, and eKYC compliance.

- **Passwordless Login**: Replaces username and password for authentication and verification purposes when providing access to government and business services**.**
- **Access Management**: Parties in the Bhutan NDI ecosystem leverage the unique identifiers and attributes from individuals' Foundational IDs or those issued by service providers to manage the access rights of individuals on portals, websites, and applications based on their roles in the system.
    - Access management using Bhutan NDI is a sub-feature of passwordless login. During the login process, the unique identifier used for providing access to a portal/website/application categorizes access rights based on the individual's role.

- For example, individuals, brokers, and internal employees of the Royal Securities Exchange of Bhutan provide access rights based on their role in the company.

- **eKYC:** ecosystem parties such as banks, telecommunication companies, or any other party in the NDI ecosystem requiring customer identification for regulatory / compliance reasons can use NDI's eKYC as part of their onboarding / account opening, mobile number registration, etc. eKYC service has been customized for each sector to meet the regulatory requirements of that sector.

Conclusion

We hope this Case Study has provided useful insights about both the Bhutan NDI Digital Trust Ecosystem, and Digital Trust Ecosystems (DTEs) in general.

And we hope that by using the Trust over IP Foundation's *Digital Trust Ecosystem Building Blocks* framework, it makes it easier for readers to conceptualize how their own DTEs use cases might be architected and designed.

The Building Blocks framework allows DTE use cases to be considered from various perspectives, by answering a variety of questions, i.e.:

1. **Context**: What is the purpose, and vision of this DTE? What problems or challenges are to be solved, or what are the opportunities to be taken advantage of in building a DTE?
2. **Ecosystem Parties**: Who is involved in the DTE? Who are the participants necessary for the DTE to be of value?
3. **Verifiable Data**: What kind of data, or value will be exchanged in the DTE?
4. **Governance**: What are the rules, or terms of participating in the DTE? How is the integrity of the data which is exchanged assured, and how are the participants governed? *Who* governs, and who administers the DTE - based on what authority?
5. **Trust Registries**: How are the trust lists built and managed, in order that they provide the essential technological bindings which assure the integrity of the verification processes?
6. **Trust Enabling Systems**: What are the new digital trust technologies that the DTE should adopt in order to establish the most up to date, secure and indeed, *trustworthy*, DTE?
7. **Trust Tasks**: and finally, how is the value of the DTE made tangible? How does trust actually flow through the ecosystem, in the real world?

In answering these questions for the Bhutan NDI use case, we have seen:

Context: A population-scale national digital identity program was envisioned to support a national digital trust ecosystem connecting the government, individuals, and the private sector in their digital interactions.

Ecosystem Parties: We learned that this ecosystem makes it possible for government institutions, individuals, and the private sector to share a wide range of verifiable data …

Verifiable Data: … and that data, in the form of verifiable credentials, is used in domains ranging from national ID, banking, academics, and employment, to transport, telecommunications and others.

Governance: We have seen a modern approach to governance, in the form of *The NDI Act of Bhutan 2023*, which established the legitimacy of Bhutan NDI to provide for "an innovative National Digital Identity Infrastructure to encourage the use of secure, privacy-enhancing digital credentials and / or data, support development of digital trust between digital economy participants, while adhering to the kingdom's environmental, social, governance, and sustainability objectives."

Trust Registries: We have seen two Trust Registries, The *NDI Trust Registry* and the *Verifiable Data Registry*, designed to enable the fundamental technical assurances necessary for secure interactions between ecosystem parties, used to validate the identifiers of parties involved and ensure the integrity of data exchanged.

Trust Enabling Systems: We found that the NDI ecosystem adopted a variety of open standards, protocols, and technologies to support these trust flows among parties, including decentralized identifiers, verifiable credentials, distributed ledger technology, and others, which ensure the integrity, reliability, and interoperability of digital interactions in the ecosystem.

Trust Tasks: And we have seen the culmination of all of this work made tangible when ecosystem parties connect with each other, exchange information, and conduct transactions via the NDI wallet, which has become a core component of the Kingdom's digital trust ecosystem.

With these fundamental building blocks in place, we expect the Bhutan NDI ecosystem to continue to grow, bringing an enormous amount of value to the Kingdom and its citizens, while providing a shining example of what a truly trustworthy digital ecosystem looks like.

Acknowledgements

The National Digital Identity Project was conceptualized as the foundation for digital transformation and inclusion in the Kingdom of Bhutan. This case study was completed less than a year after the nationwide launch of Bhutan NDI in October 2023. The NDI ecosystem continues to evolve as citizens and residents continue to onboard into the ecosystem and the service sectors continue to expand. The envisioned goal, with Bhutan NDI, is to create a thriving and inclusive digital ecosystem rooted in trust.

We extend our heartfelt gratitude to all those who contributed to the completion of this comprehensive case study on Bhutan NDI and its pioneering digital trust ecosystem. Their collective experience, efforts, expertise, and unwavering support have made the case study a success.

We express our sincere appreciation to His Majesty the King of Bhutan, the Prime Minister's Office in Bhutan, the Government Technology Agency Bhutan, Druk Holding & Investments, and the Department of Civil Registration and Census, and the Department of Immigration in Bhutan for their continued support of Bhutan NDI.

We extend our gratitude to the Bhutan NDI team for their guidance and encouragement at every stage of this research endeavor. Special thanks are due to key members of the Bhutan NDI team – Jacques Von Benecke (Chief Technology Officer), Suprit Pradhan (Project Manager), Anand Acharya (Product and Technical Project Lead), Dev Raj Dungana (Governance and Policy Lead), Kinzang Dorji (Technical Lead) and Tshendu Gyeltshen (Backend Lead) for their cooperation and provision of essential data and insights, without which this case study would not have been possible.

We are deeply grateful to the Trust Over IP Foundation, the Ecosystem Foundry Working Group, and the numerous stakeholders and participants who shared their perspectives and expertise during interviews and consultations. Special thanks are due to Steve Magennis, Carly Huitema, Drummond Reed, and Scott Perry. Their invaluable contributions have influenced the depth and breadth of this case study, shedding light on the multifaceted aspects of the Trust Over IP Foundation's Digital Trust Ecosystem framework.

This case study stands as a testament to the collaborative spirit, dedication, and passion of all those involved, reflecting our collective commitment to advancing knowledge, fostering innovation, and driving positive change in the realm of Digital Trust Ecosystems.

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in understanding
- Use Cases to illustrate implementations
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.

Licensing Information:

All Trust Over IP Foundation deliverables are published under the following licenses:

Copyright mode: Creative Commons Attribution 4.0 International licenses

http://creativecommons.org/licenses/by/4.0/legalcode

Patent mode: W3C Mode (based on the W3C Patent Policy)

http://www.w3.org/Consortium/Patent-Policy-20040205

Source code: Apache 2.0.

https://www.apache.org/licenses/LICENSE-2.0