Introduction of China RealDID System

Red Date Technology

Traditional Password-Based Authentication vs. Modern Key Signature Verification

VS

Traditional Password-Based Authentication

Modern Key Signature Verification

What Exactly Can a Public-Private Key Pair Do?

Signing with a private key

Encrypting with a public key

Only the corresponding public key can verify signatures made by its private key

Only the corresponding private key can decrypt files encrypted with its public key

China National Digital Identity Infrastructure - CTID System

CTID Platform

The Trusted Identity Authentication Platform (CTID Platform) is the only national identity infrastructure in China supporting all Chinese identity authentication. It is constructed and managed by the Ministry of Public Security and with the support and guidance of the Central Cyberspace Administration, the National Development and Reform Commission, and the Ministry of Science and Technology. CTID is the only legal source in China for authenticating Chinese citizen identities.

中华人民共和国国家互联网信息办公室 Cyberspace Administration of China

中华人民共和国国家发展和改革委员会 National Development and Reform Commission

中华人民共和国科学技术部 Ministry of Science and Technology of the People's Republic of China

中华人民共和国公安部 Ministry of Public Security of the People's Republic of China

56 Billion

Legal Identity Data

Authoritative data source from the Ministry of Public Security

- **Safety**
- **Convenience**
- **Authority**
- **Legality**
- **Legitimacy**

China RealDID Project

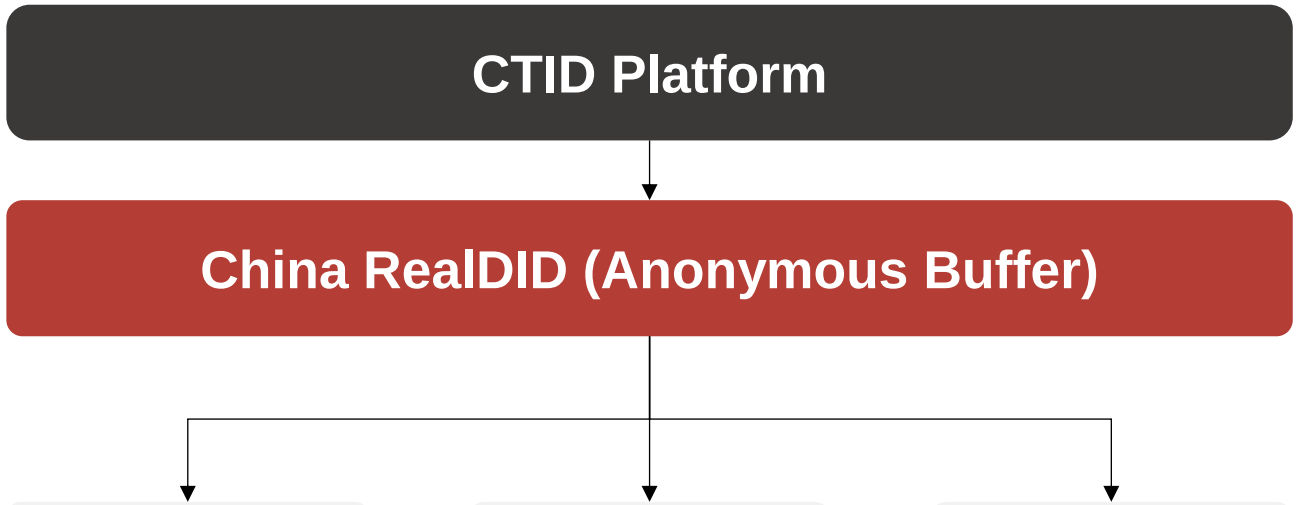
BSN实名DID服务
China RealDID by BSN

中盾安信 ANICERT

中国移动 China Mobile | CMDI 中国移动设计院

Jointly developed by Anicert (a wholly-owned subsidiary of the Ministry of Public Security), Red Date Technology and China Mobile Group Design Institute, the China RealDID project fully integrates the capabilities of the Blockchain-based Service Network (BSN) and the CTID Digital Identity Chain Platform, two national infrastructures in China.

MPS issues real-name DIDs after the CTID platform authenticates individual data and supports embedding multiple public keys to the single RealDID document. The private keys corresponding to these public keys are held by the individuals. Any third party can utilize the publicly accessible public keys in the DID document to perform data encryption and signature verification.

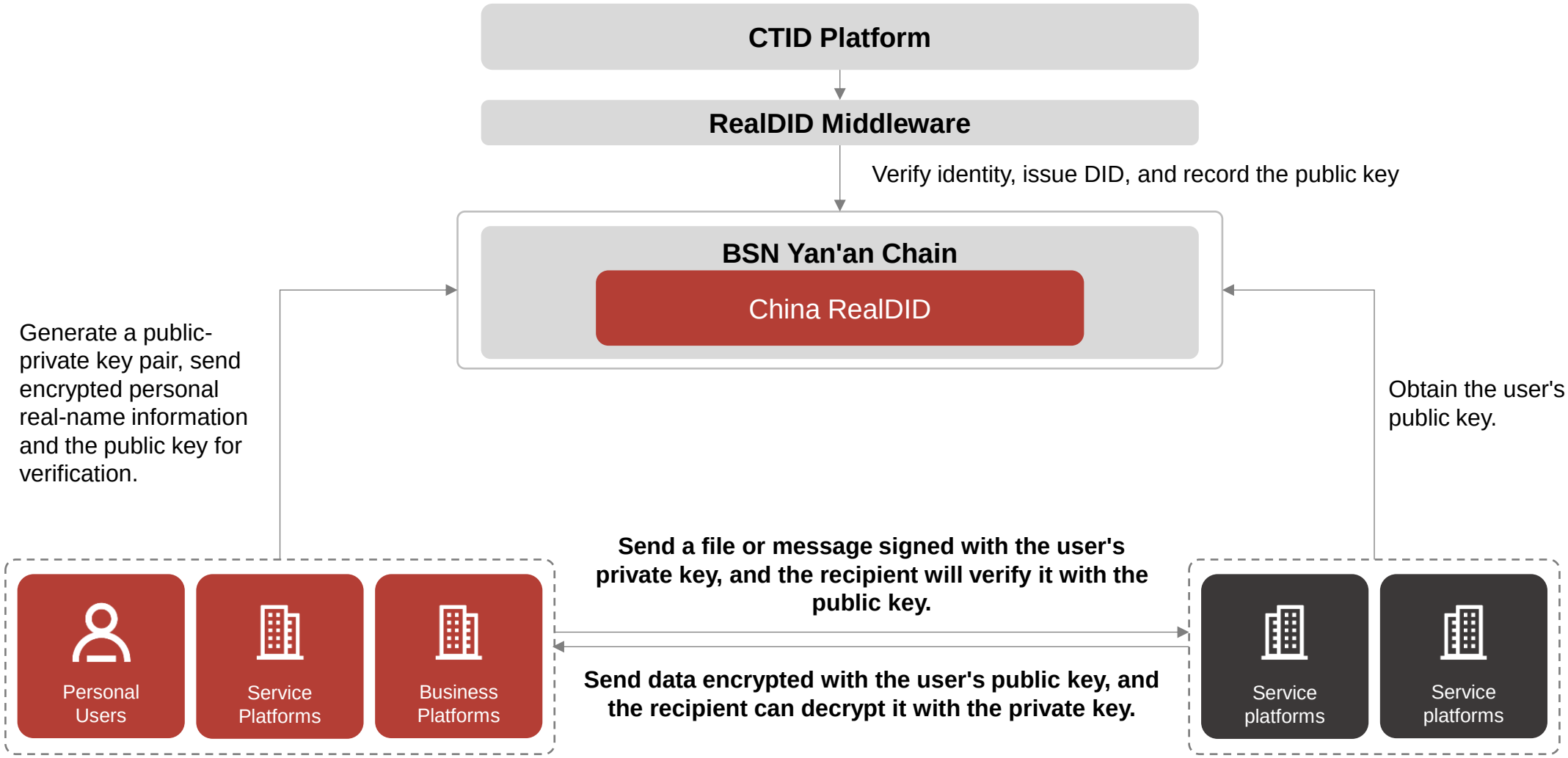


The document contains up to 120 public keys. This becomes an anonymous buffer to CTID.

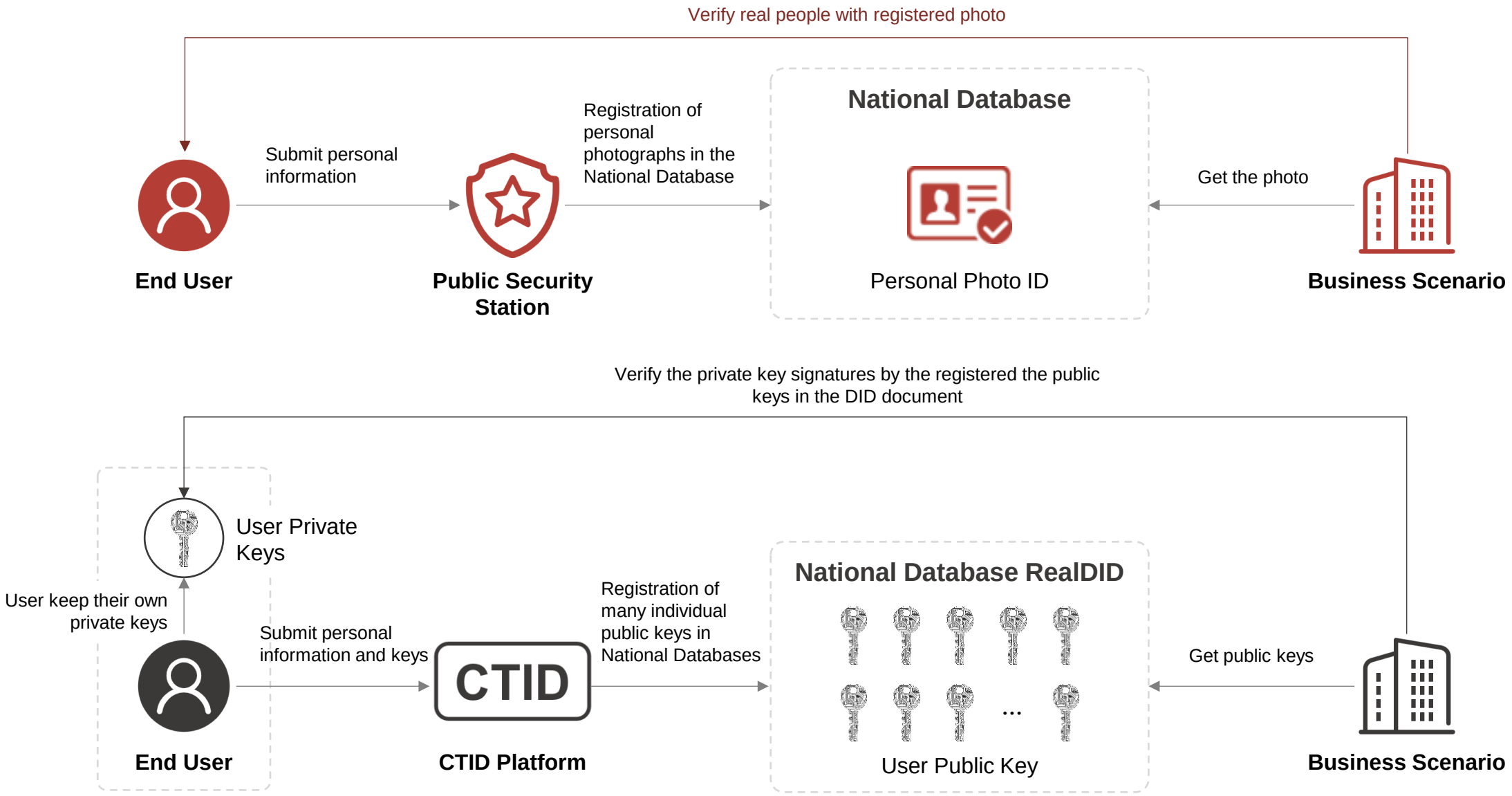
The VCs are issued by CTID based on pre-set templates and approval from DID owners

Each DID owner can link the DID to an online storage for private data and share with authorization.

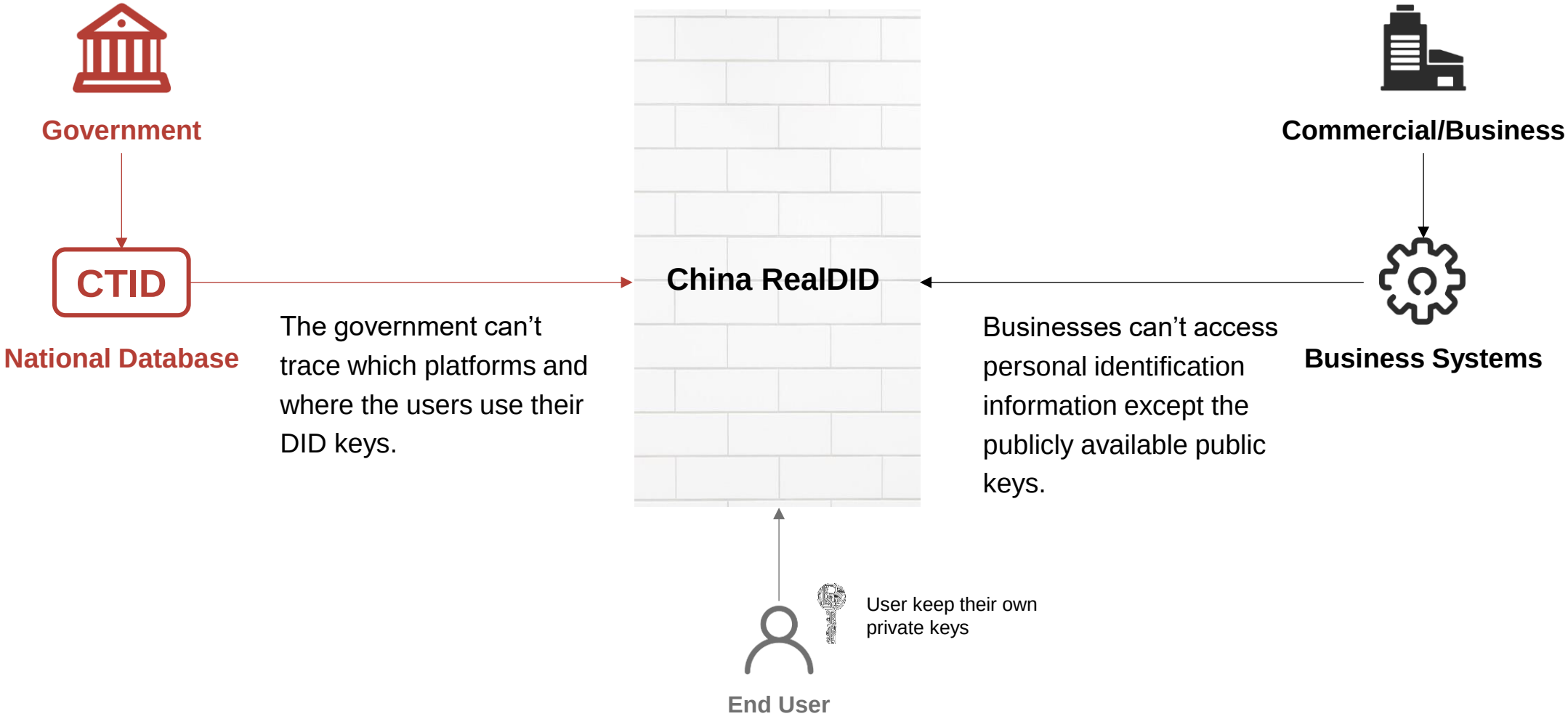
Technical Logic of China RealDID



Business Logic of China RealDID



Two-Way Anonymity



Case Studies

RealDID Digital File Copyright Protection Service

The most popular service the RealDID enables is to put a digital “watermark” on all digital/binary files generated, such as pictures, PDFs, MS office files, with RealDID private key signatures. Since the corresponding public key is registered into the CTID national database, and the “watermark” can be verified by publicly accessible DID Address. This provides a digital file copyright protection mechanism that proves the ownership legally by government registered data and can be upheld in courts. This service is being used by traditional image/picture protection service websites and short video generation services. No web2 technologies can achieve the same result this efficiently.

RealDID End-to-End Digital Encryption Service

Since the DID document is publicly accessible and no cost is involved for accessing it. People can use each other’s public keys in the document to encrypt any digital files and messages, and only the owner of the RealDID who holds the private key can decrypt and read them. A use case is a plugin on outlook. The sender can input both the recipient’s email address and DID address, the plugin will retrieve the public key from the DID document, and encrypt the message then send it out. The recipient is the only one in the world who can read the message because he/she has the private key. The email service provider can’t even read the content of the emails.

RealDID Anonymous KYC-based Registration and Login Service

The RealDID acts as an anonymous buffer on top of the national CTID database, so Chinese citizens can use the private keys they hold to prove their citizenship on the internet after the verifiers access the public keys in the DID documents to authenticate. This immediately enable “Anonymous KYC-based Registration and Login” mechanism. Users can register on any commercial platform by submitting their DID address and private key signature, and the platform can verify them with the DID document data and complete the registration process. The commercial platform doesn’t have any personal identifiable information, but since the government still knows the identity from the DID address, so the process is still in compliance with any KYC requirements.

Challenges and Requirements for Government-issued Real-name DID

01.

It must be authenticated and issued by a national authority with digital ID database.

02.

There must be national legislation regarding personal privacy and personal data.

03.

Ultimately, individuals must have full control over their own private keys.

04.

The DID documents must be stored in a public network environment where anyone can freely access and read them.

China RealDID Official WeChat “Mini Program”

China RealDID KYC Trials in Hong Kong

To show the potential of the China RealDID to be the game changer in identity technologies, we have been running four trials in Hong Kong with partners. These trials demonstrate how Chinese mainland visitors can use the China RealDID to cross the border, register in a financial service app, purchase a financial product, and transfer digital currency anonymously without revealing any personal identifiable information (PII), but still in compliance with KYC rules, in the jurisdiction of Hong Kong.

Track#1

Access Point Entry Inspection

A DID holder can access the Hong Kong border control by generating a “Hong Kong Border Control Verifiable Credential” with RealDID APP and use it to pass the access point with minimal exposed PII.

Track#2

Anonymous Registration on Regulated Stablecoin App

The DID holder can register on the IDA Stablecoin APP anonymously with China RealDID. The only information submitted during the registration is the DID address and private key signature.

Track#3

Purchase token-based Financial Products and Taxation

The DID holder can use the IDA Stablecoin to buy tokenized financial products anonymously on Franklin Templeton website. The return can still be traced by the tax authority with the DID submitted.

Track#4

Enable Anonymous “Travel Rule” between Financial Institutions

RD stablecoin is transferred between two financial institutions. The originator bank can only share the DID to the beneficiary bank. It complies with the travel rule without exposing customer info.

Trial Participants

During September and October 2024, Red Date and partners will perform end-to-end trials for mainland visitors to have “Anonymous KYC Authentication” in multiple real-life use cases.

Use Case	
Track#1: Access Point Entry Inspection	
Track#2: Anonymous Registration on Regulated Stablecoin App	flare
Track#3: Purchase token-based Financial Products and Taxation	
Track#4: Enable Anonymous “Travel Rule” between Financial Institutions	

Organizers

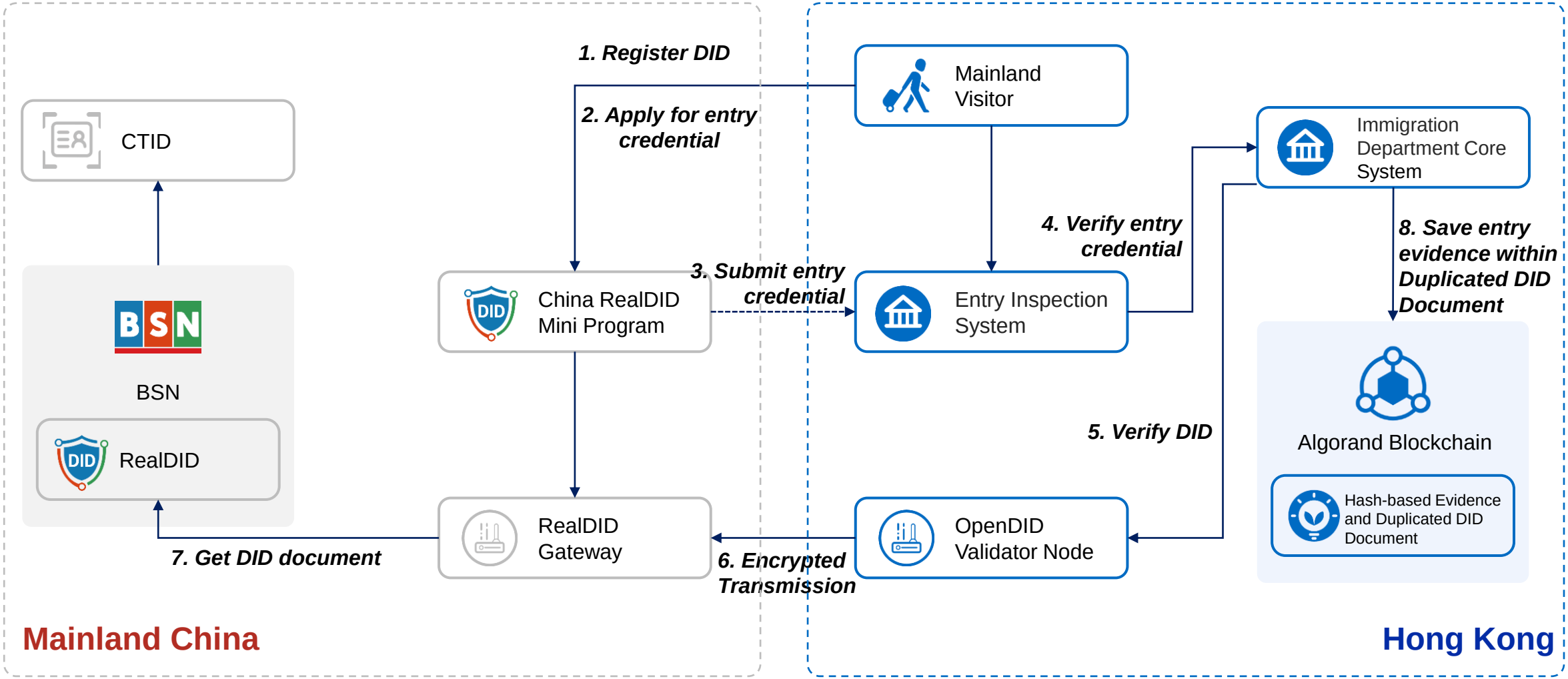
公安部第一研究所 THE FIRST RESEARCH INSTITUTE OF MINISTRY OF PUBLIC SECURITY OF P.R.C

国家信息中心 State Information Center

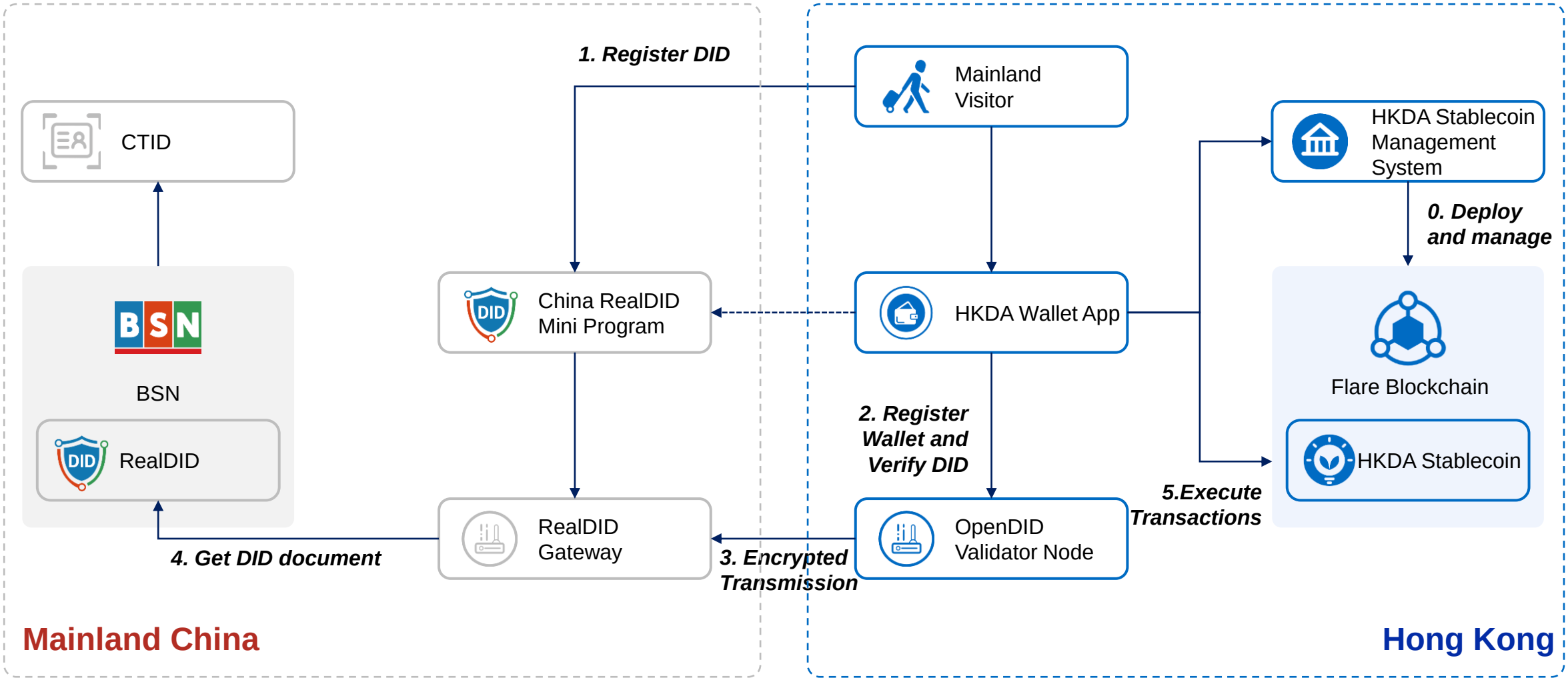
OpenWallet FOUNDATION

Red Date Technology

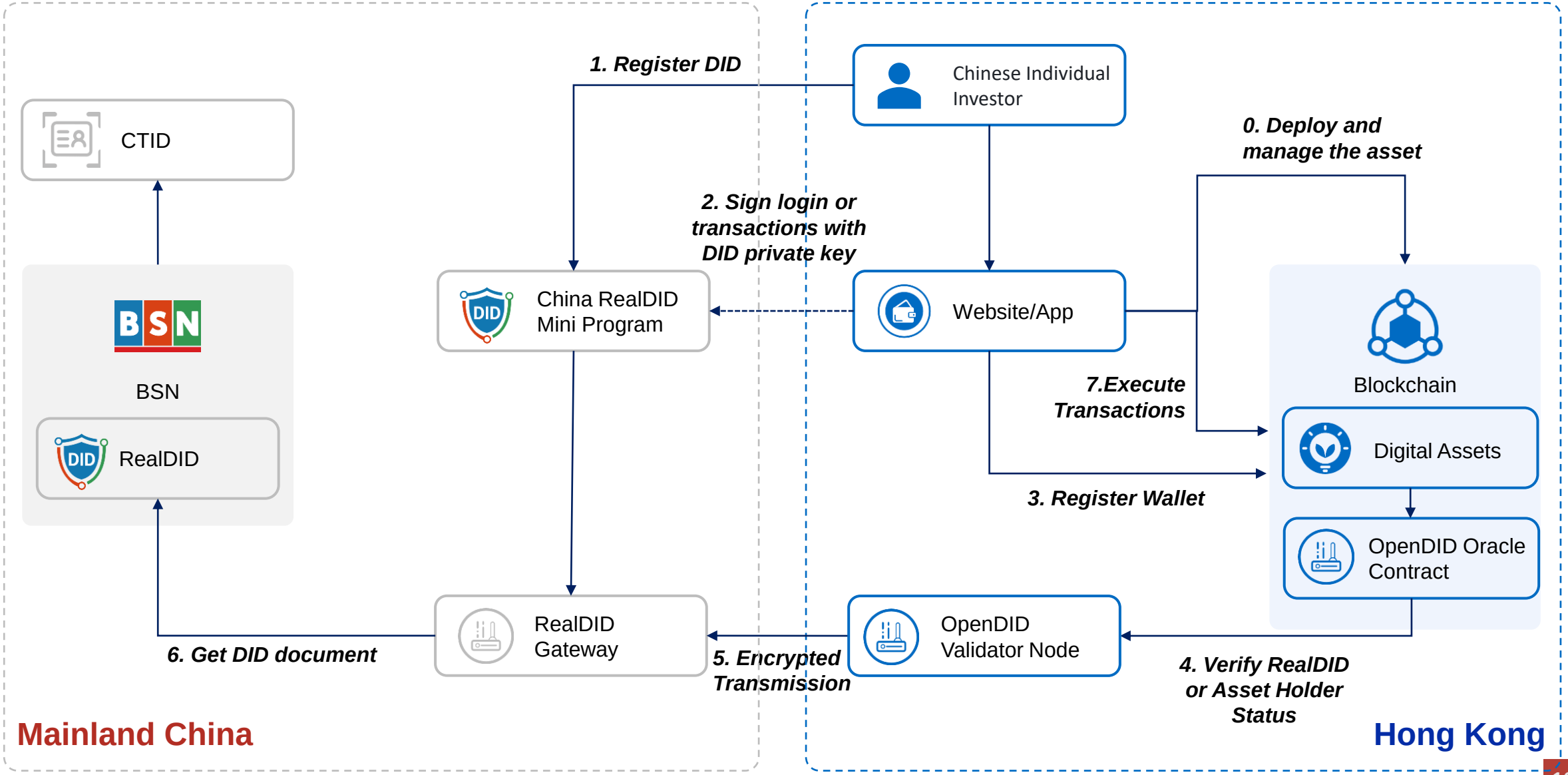
Track#1: Access Point Entry Inspection



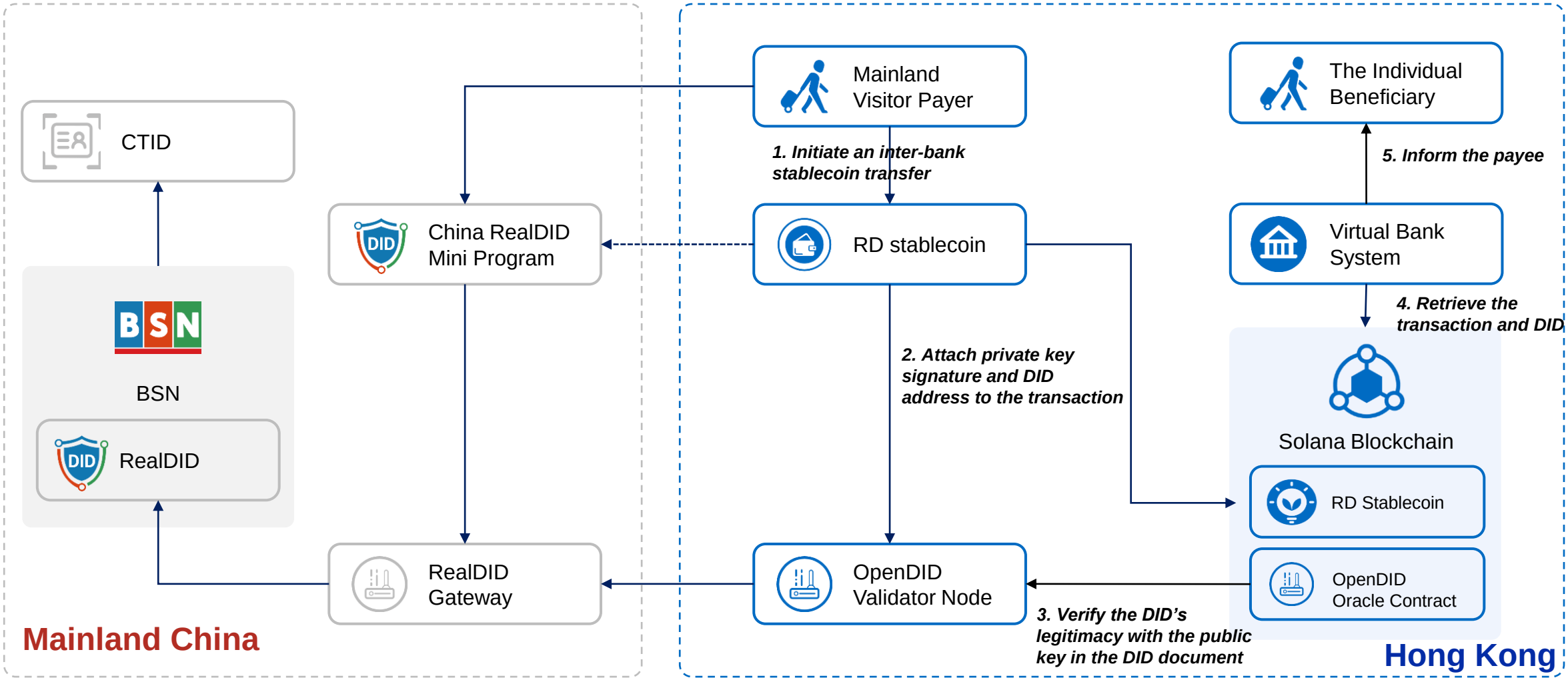
Track#2: Anonymous Registration on Regulated Stablecoin APP



Track#3: Purchase token-based Financial Products and Taxation



Track#4: Enable Anonymous “Travel Rule” between Financial Institutions




Thank You!