OFID

The Future Platform for Your Identity Asset

Blockchain + Trusted Computing + Open Algorithm

White Paper Beta 0.8

https://ofid.io

Abstract

With the advent of computers in the 80s and the dotcom revolution in 90s, digitalization of data has become an inevitable option for every organization. While digital data revolutionized the way organizations store and manage data, it came with a price. As the data moved online, hackers found ways to steal the identity of a person and perform fraud transactions. To mitigate identity frauds, the government has imposed financial regulations in the form of Know-your-customer (KYC) and Customer-Identification Program (CIP). To conform to government regulations and secure customer data, organizations are turning to identity verification services.

The current Identity Verification (IDV) solutions come with multiple challenges. Focus on authentication, the potential risk of centralized storage and less financial return are a few of them. The blockchain-based OFID IDV platform offers a revolutionary solution to current IDV challenges.

The block chain technology was originally designed for Bitcoin. However, looking at the amazing benefits offered by this technology, developers are now extending the functionality of block chain technology to every industry. The IDV segment is not excluded. Leveraging the disruptive block chain technology and augmenting it with Ethereum smart contracts, OFID platform brings an IDV eco system that makes it easy for end-users to share personal identity information (PII) data while being rewarded for the same. Similarly, validators can turn their years of hard work in building PII databases into revenue generators by selling the attestations without actually sharing the PII databases. For service providers, IDV comes at reduced costs. The OFID IDV platform improves operational efficiencies, increases security while rewarding the participants of the IDV eco system.

List of Acronym

AIK	Attestation Identification Key
AML	Anti-Money Laundering
API	Application Programming Interface
CA	Certificate Authority
CIP	Customer-Identification Program
EK	Endorsement Key
HLA	Homomorphic Linear Authentication
IC Design	Integrated Circuit Design
IDV	Identity Verification
IMA	Integrated Measurement Architecture
KYC	Know Your Customer
M-Server	Management Server
OAT	OpenAttestation
OPAL	Open Algorithm
PBFS	Peer Based File System
PCR	Platform Configuration Register
PII	Personal Identity Information
RDBMS	Relational Database Management System
RK	Root Key
RMS	Rights Management Service
RP	Representative Payee
SDK	Software Development Kit
SP	Service Provider
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
Wlist	Whitelist

I. Introduction

Introduction to IDV Services

With increasing identity fraud incidents across the globe, businesses now face a tough challenge of implementing a trusted infrastructure that can cost-effectively verify user identities and perform background checks. Identity Verification Services (IDV) rightly fit in here.

An Identity Verification Service is a 3rd party service used by businesses, financial institutions and government organizations to check whether the customer data is real and authentic. These services verify physical identity documents such as Passport, driving license, bank details against trusted sources such as credit bureau data. Employee screening and background check is an important requirement in the hiring process of every organization.

Identity verifications services can be offline or online. For instance, online websites perform an online check to prevent under-age signups, spam signups or sock puppetry. Similarly, when you open a bank account, bank authorities verify the authenticity of identity documents. While IDV services might not be a common-man term, a common instance of this service is the government regulation for financial institutions regarding “Know Your Customer”. To get an approved bank account, customers are required to produce identity documents in support of the KYC program. When it comes to non-documentary identity verification, the IDV services check the information against private and public databases to match it. Since the world is rapidly getting digitalized and as we tend to enjoy services through the Internet, online identity verification services become an inevitable option.

The state of Identity Verification Services Industry

According to a Smithers Pira report, personal identification verification market was worth $8.7 billion in 2016. This value is expected to reach $9.7 billion by 2021, growing at a CAGR of 2% between the year 2016 and 2021. Global Market Insights reports that the Personal Identity Management market was valued at $6.5 billion in 2015. This value is expected to reach $34 billion by 2024, growing at a CAGR of 20%.

According to ABI Research, the Online Identity and Authentication market in the banking vertical would reach a market value of $1.6 billion by 2018, increasing by 945% in comparison to its value in 2012. Among others, software applications would account for 81% of this market.

The Need for IDV Services

The need for IDV services stems from several factors. Here are a few of them:

- **Increasing Identity Frauds and Thefts**

According to Javelin Strategy & Research 2017 Identity Fraud Study, the overall fraud incidents in the US have affected 15.4 million citizens in 2015. This value grew by 16% in 2016. Frauds types have grown too. Among them card-not-present fraud and account-takeover losses increased by 60%. Overall, $16 billion was stolen by fraudsters in 2016 which is an increase of $1 billion from the previous year.

Figure 1 (Source: Javelin Survey)

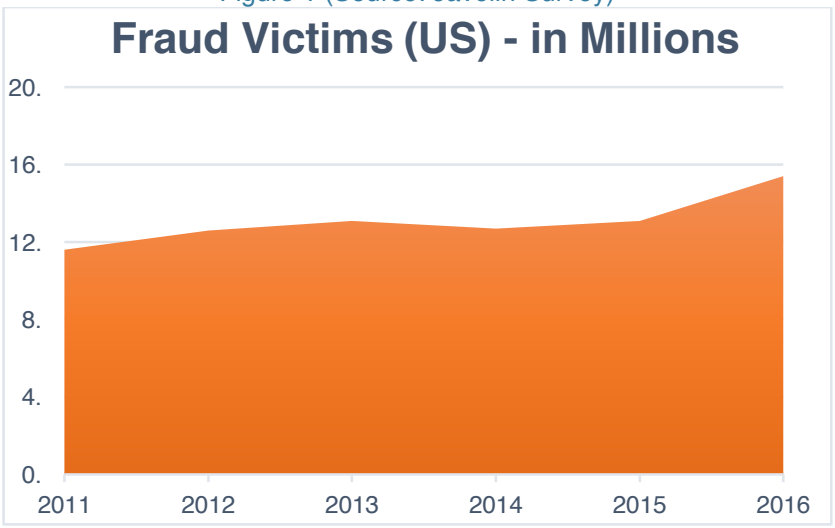


Figure 2 (Source: Javelin Survey)

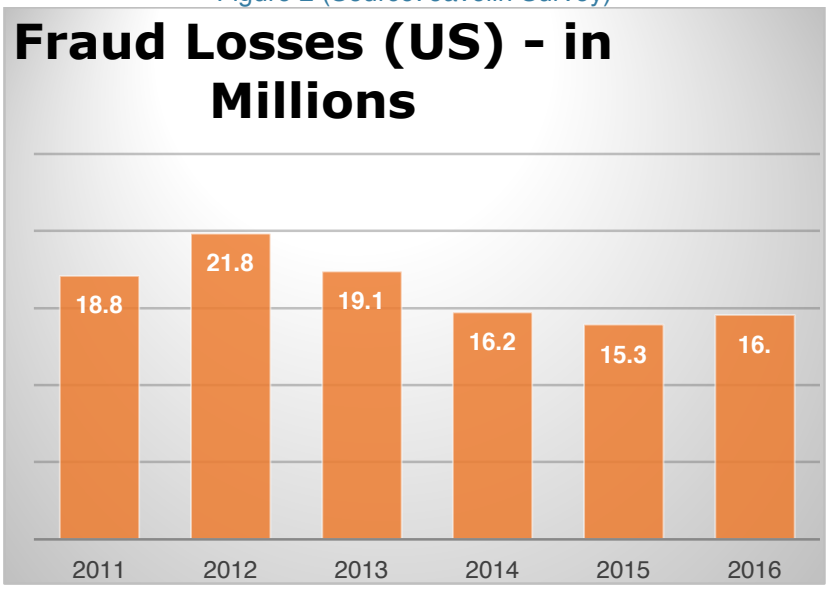
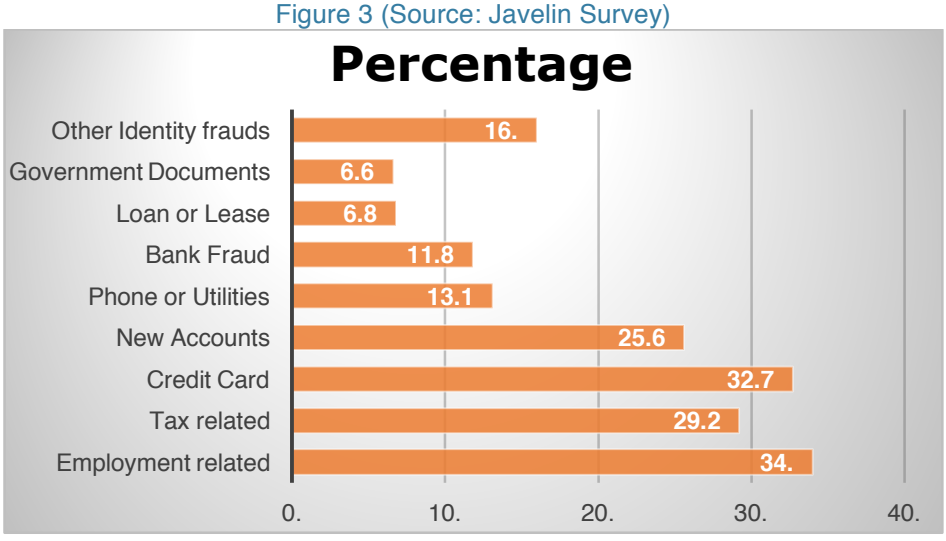


Figure 3 (Source: Javelin Survey)



This problem is widespread in the developing countries. The identity of a Chinese man was stolen in 2012 and it was later found that his name was registered in 32 legal proceedings and 80 million Yuan of debt was pending under his name.

(source: http://www.scmp.com/news/china/society/article/2022600/chinese-man-cited-32-civil-suits-after-having-identification). In India, often known as the IT capital, the cybercrime has become no less than a routine, so much that the identity theft hardly creates a headline. Yet, almost 1001 cases were registered alone in the year 2015, which comes out to be approximately 3 cases daily. Most of the complaints related to 'cheating by impersonation', followed by those of identity theft. (source: http://www.indiaspend.com/cover-story/impersonation-identity-theft-most-common-cyber-crimes-reported-in-bengaluru-68907)

Identity Verification Services effectively solves all these challenges. That is why, many corporations, financial institutions and government organizations are aggressively implementing IDV services. In the future, we believe that there would be a continuous demand of identity verification services.

- **Privacy Issues**

Actually, in most of the cases, the customers themselves don't control their personal data and leave it with the services provider while availing the services. In addition, the service provider also owns any new data generated during the serving procedure. It is also common that most cloud services don't delete customer data immediately after terminating the contract, which is a great threat to the personal privacy.

Every other day we can hear about any breach of customer data that is shared with or sold to the third party. The hacking of Sony Pictures, back in November 2014, clearly revealed the magnitude of the problem, as well as established the fact that it was no longer just the individuals and the small groups of hackers that perpetrate the hacks. An enormous amount of employee data inclusive of salary information, personal records, email correspondences as well as movie scripts and unreleased films was obtained.

(source: http://time.com/3639275/the-interview-sony-hack-north-korea)

An identity verification system is able to cost-effectively provide identity verification services with minimal personal identity information while not compromising on the privacy and security of user data. In recent years, people are paying more attention to privacy of their personal data which means the IDV market would be in great demand, going forward.

- **Financial Regulation Requirements**

In the United States, the Bank Secrecy Act introduced in 1970 required all banks to maintain customer data for effective monitoring or money laundering issues. BSA was improvised with Anti-Money laundering (AML) laws in 1980s. In 2002, the Secretary of Treasury finalized regulations that made Know-Your-Customer (KYC) mandatory to banks and all financial institutions. In 2013, Customer Identification program (CIP) became a mandatory requirement wherein financial institutions should verify the identity of individuals intending to perform financial transactions.

However, banks are increasingly facing pressures that did not previously exist and the traditional ways of verifying identity are simply too slow and cumbersome – not to mention, costly – to keep up with the demands of the modern world. The costs inherent in verifying the identity of a new customer today can be extremely high. Averages for full KYC are in the $15-20 range and costs are continuing to rise.

Globalization pushes this issue to a further extent. Today's middle class is no longer confined to a single city or region but is instead a global citizen with an expectation of service regardless of the locale. When citizens transition their locale, it is still incumbent upon financial institutions to take all the necessary steps and decisions to ensure that they are best servicing their customers while still remaining cognizant of the need to protect financial institutions from risk. However, this often means that an individual is forced to wait days and weeks, without access to accounts and funds since identity verification rules and regulations vary across regions, countries and nationalities.

When changes are forced from a corporate perspective – company transfers – there is often an available buffer for the move to ensure that the individual is not significantly inconvenienced. Unfortunately, similar options do not exist for private moves and in these cases, the costs can be significant!

This ongoing increase in costs has had a significant impact on the bottom line of many financial institutions worldwide. In fact, many businesses have reported significant savings due to efficiencies and asset growth but a simultaneous decrease in overall profitability due to ever increasing costs of compliance. This decreasing profitability has led to many institutions reducing product offerings as well as the sizes of their customer service teams as they struggle with smaller discretionary budgets.

Today, there is a greater need for an identity verification system that improves the efficiency of KYC services while being cost-effective.

- **Emerging Market**

In a world where proof of identity is essential for access to credit and finance, users in developing countries continue to struggle without official identity documents or comprehensive credit history. In developing countries, government issued ID documents are considered luxuries and privileges, not rights granted under law, primarily due to a lack of resources and infrastructure.

People in these emerging markets are not as concerned with fraud, theft or even privacy, here identity verification serves a different purpose – a way to financially empower the poor.

For an industry to flourish and become successful, there should be an emerging market with a huge market capacity. This is what is exactly happening with the IDV industry, especially in the developing countries. To tap the increasing IDV market, many companies are jumping on board to offer IDV services in recent times.

- **High-Trusted Sharing Economy**

The sharing economy is quickly evolving to become a major part of global economy in recent times. The rapid growth of Airbnb and Uber is an example of this trend. According to Brookings, the shared economy market earned a revenue of $14 billion in 2014. This value is expected to touch $335 billion by 2025. eMarketer estimates that 56.5 million people in the US will use a shared economy service in 2017. More forms of shared economy are expected to come up in recent times. As sharing economy relies heavily on trust among peers, the IDV system has a greater role to play here, extending beyond the financial services sector.

(Source: https://www.brookings.edu/research/the-current-and-future-state-of-the-sharing-economy/)

(Source: https://www.emarketer.com/Article/Uber-Airbnb-Lead-Way-Sharing-Economy-Expands/1016109)

Insufficiency of the Current Solutions

With the evolution of Internet today, an array of services has appeared on the market, promising to resolve the issue of identity usage and sharing. Before going into these details, it is important for you to first distinguish among the following three concepts:

- **Identity Certification**

Identity certification refers to the process wherein the identity provider(s) create identity systems for individuals , legal entities and assets holding trusted information. The Identity Provider securely stores certified attributes that common tractions require. Such attributes can be the inherent attributes like name, date of birth, nationality, national identification number and assigned attributes like address, etc.

• Authentication

Authentication is the act that confirms the truth of the identity provided. It might include the validation of the documents shared by the identity. Service Providers, (like Telecom Operators, Banks, etc.) first validate their users before they provide services by partnering with an ID verification service.

• Identity Verification

It is a process wherein the service provider verifies the validity of the submitted user credentials before offering a product or a service to the user. Eg: access to social assistance (like the Old Age Security Pension, unemployment insurance, etc.). The service provider is required to validate the accuracy of the attributes information, which is known as the identity verification.

The traditional financial service instruments, like insurance and credit, completely depend upon the accuracy of the user's personal data. More knowledge of the preferences and habits of the customers can help the financial institutions deliver the right offers to the customer.

CASES

- **Government Sector Solution, Sweden**

Sweden has developed an eID system that gives its citizens and businesses access to more than 300 private and public services. Certain private entities, including big banks and prominent telecommunication providers, issue digital identities. Identity Validation services are bought by the public sector from the private sector. The service providers in the private sectors can join the BankID system after signing contracts with eID providers for validation. Currently, this solution has become very popular and is used by more than 9 million citizens.

- **Private Sector Solution, Finland**

TUPAS, the bank identity system, was created by the Federation of Finnish Financial Services in order to improve user's experience to online services.

As it is with the majority of the banks, the users would first need to approve and validate the data that is transferred from the Bank to the representative payee (RP), abolishing any risk of liability for the ID platform. A new revenue stream has been established by TUPAS for banks. Though there are few other competitors in Finland, TUPAS processes 95% of all online service logins as of Feb 2015. The majority of government organizations have adapted TUPAS services.

- **Business Solutions, ShoCard**

ShoCard helps users and enterprises in establishing their identities with one another securely and in a verified manner. Be it login, sharing personal information, or making a financial transaction, ShoCard ensures that all transactions are completed proficiently, quickly and peacefully. You can either create a ShoCard ID either through the App, or even by building the technology in your existing Apps through ShoCard Software Development Kit.

https://shocard.com/

- **Business Solutions, CIVIC**

Civic is an IDV platform that providers a multi-factor validation without any username, password, third party authentication or any hardware key.

https://www.civic.com/

Figure 4

		Non-Blockchain			Blockchain	
		Government		Private		
		Passport Agencies	eID	TUPAS	ShoCard	CIVIC
SOLUTIONS	Certification	✓	x	X	X	X
	Authentication	x	✓	✓	✓	✓
	Verification	X	X	X	✓	✓
Data Storage		Centralized	Centralized	Centralized	Distributed	Distributed
High Capacity		✓	✓	✓	x	x
Create and Transfer Assets		x	x	x	✓	✓

Although there have been some government or commercial solutions in the field of identity, the disadvantages of these solutions are obvious. Such as:

- **Focus on Authentication**

The majority of solutions focus on identity verification. However, the Internet World contains ample of personal data of the people (like the browsing history, watch history, geographical location, transaction data, healthcare data, and much more). The Service Providers, thus, require more accuracy and comprehensiveness in the personal data validated by third party. Definitely, it is much more difficult and valuable to establish the identity verification platform than identity authentication.

- **Potential Risk of Centralized Storage**

Centralized Identity Systems are best suited to offer Identity Certification to Individuals, lawful entities, and assets on a bigger scale. However, it is risky in the identity verification domain. Inadequate data protection leads to data breach and data leakage, causing huge losses to the organizations as well as to the users.

- **Less Financial Return**

Various organizations, especially the ones in the private sector, treat the user data that was generated during a process as their own asset. They believe that data is an asset and expect maximum returns on it. Though, a huge amount of data is “owned” by the organizations, there are only a few opportunities wherein they can generate revenues from that data. It means this data can neither be consolidated nor can be a new source of revenue for the organizations.

Ideal Verification System

In the ideal ecosystem, no data provider can play a leading role, and the lack of any unique data can be a loss. The ideal verification system should endogenous a set of appropriate incentive system to promote the sharing of data to enhance the value of identity data.

- **For Users**

The basic concept of user-centricity is having a key component that aligns the stakeholder's interests and comprehends the vision of personal data ecosystem. This holistic approach helps acknowledging the fact that the end users are crucial and independent stakeholders in co-creating and exchanging the value of services and experiences.

In addition, the end user-centricity signifies a transitioning opportunity. It aims to consolidate varied personal data in a way which was earlier impossible. This is possible only by keeping the end user at the centre of four major principles:

- ➢ Transparency: Individuals expect to know what data is being captured about them, the manner in which such data is captured or inferred, the usage it will be put to and the parties that have access to it.
- ➢ Trust: It is the confidence that individuals have with respect to the factors of availability, reliability, safety and integrity embedded in the applications, systems and the service providers that will gain access to their personal data.
- ➢ Control: It is the capability of the individuals to commendably manage the extent to which the apps, system and service providers share their personal data.
- ➢ Value: It is the user's understanding of the worth of the usage of their data and how they are being compensated for the same.

- **For Service Providers:**

Complex verification procedures such as 'Know Your Customer' (KYC) or Anti-Money Laundering (AML), empower users to make use of the Internet for financial investments. The verification results can also be shared with other organizations.

- **For Validators:**

Validators (which include notaries, banks, passport agencies, hospitals, etc.) will complete the identity verification service for the service providers which would allow the monetization of Verification-as-a-Service via fees per verification or any other business prototypes.

This vision includes a future where:

- ➢ Individuals exercise superior control over their personal data, digital identity and online privacy, and would receive better compensation for providing access to their personal data.
- ➢ It will now be easy to exchange contrasting features of personal data with validators and government agencies in order to increase efficacy and trust among people, private and public sectors.

Considering all these aspects, OFID has created a decentralized blockchain-based IDV platform that makes the ideal IDV platform a reality.

II. OFID – A Blockchain-based Decentralized IDV Platform

OFID is a blockchain-based decentralized Identity verification (IDV) platform that offers low-cost identity verification services to users. Built on the blockchain technology and augmented by features such as encryption and authentication, OFID significantly enhances security and privacy while removing inefficiencies. Not only does it provide reliable IDV services, but it also rewards users participating in the ecosystem.

How It Works?

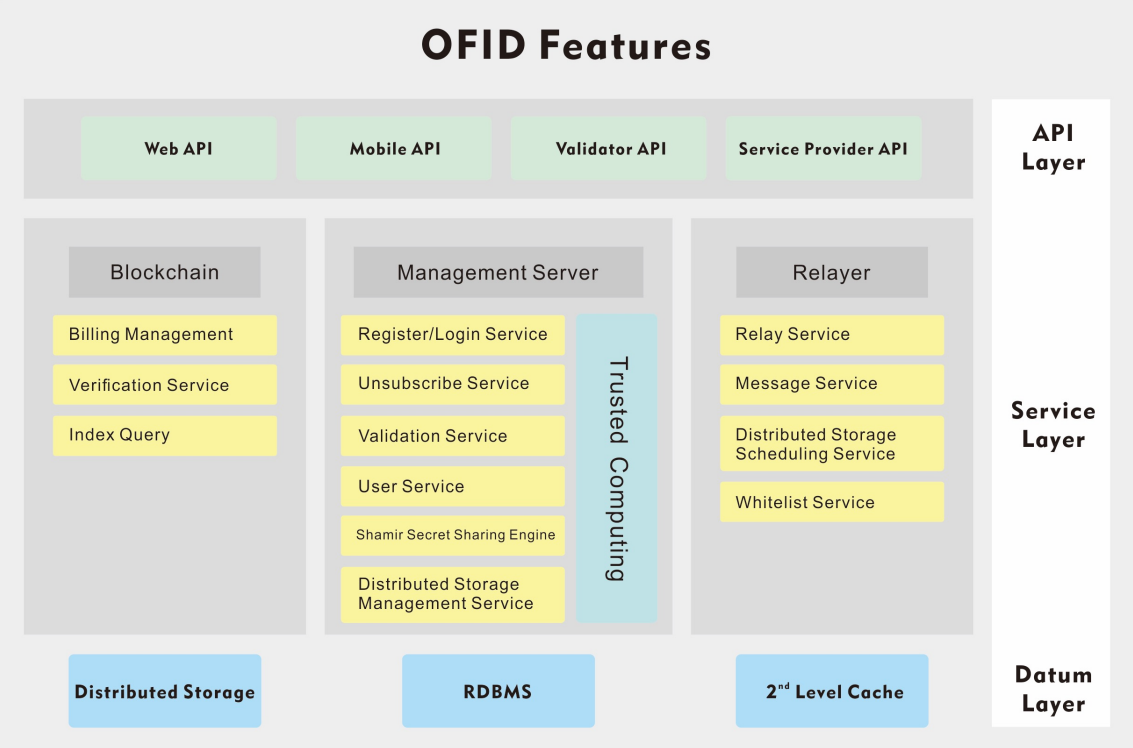
OFID is designed with ease of use in mind while not compromising on security. Registering with OFID and navigating through the app is pretty simple and straight forward. To register with OFID, users simply download the app on their personal device, provide their personal identity information (PII) and get it verified. The user PII is thoroughly verified and attested by OFID partners.

When the user applies for a product or a service, the service provider requests the user to share the PII through the OFID app. The user reviews the request. If the request is genuine, the user unlocks the app, scans the QR codes and shares the required information. Otherwise, the user can reject that request.

The best thing with OFID platform is that the PII is locally stored on the personal device of the user. It means the user has the total control over his or her own PII data. It is the user who decides whether or not to share the PII with the service provider. The first thing the user is supposed to do is to securely store the public/private key pair. The private key is known only to the user. When this digital signature is applied, it authenticates and validates the user's identity to requesting parties confidentially and securely.

OFID Architecture

Picture 1



The OFID architecture consists of the following components:

1. Interface Layer
    a) Web Interface
    b) Mobile Interface
    c) Validator Interface
    d) Service Provider Interface
2. Service Layer
    a) Blockchain Service

It offers three important services: Payment Service, Certificate Service, Index Storage and Query

    b) Management Service

OFID is an open-source IDV platform. Be it a user, validator or a service provider, all participants of the ecosystem can access the platform. OFID takes care of the operation and maintenance of the platform.

    c) Relayer

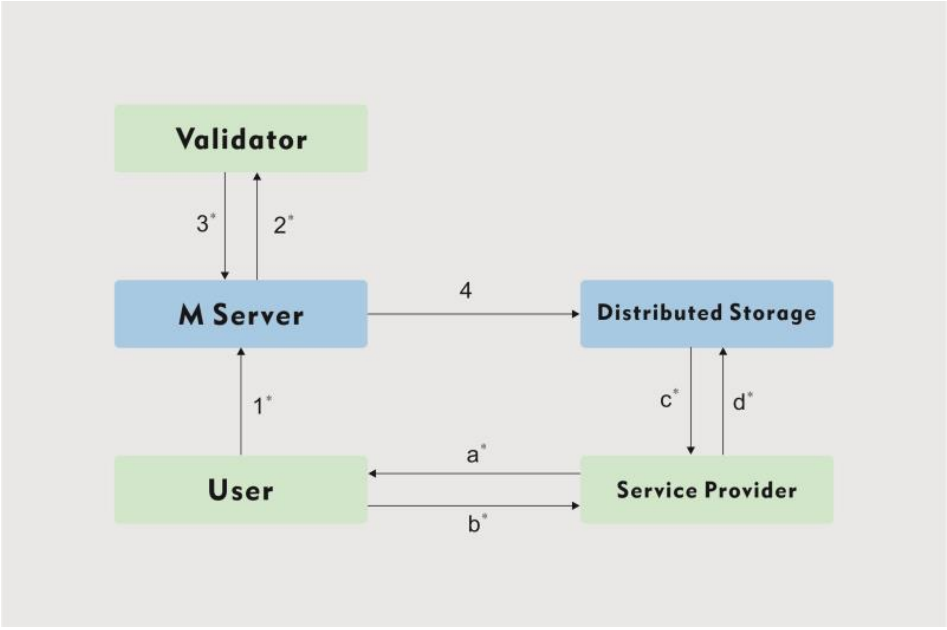
Relayer is the unified interface, which is composed of proxy server, messaging server, whitelist server and distributed storage server.

3. Data layer
    a) Distributed storage server
    b) RDBMS (Data storage and retrieval)
    c) 2ND Level Cache (designed to implement multithreaded applications)

The Role of the Platform

This is how the verification process works on OFID.

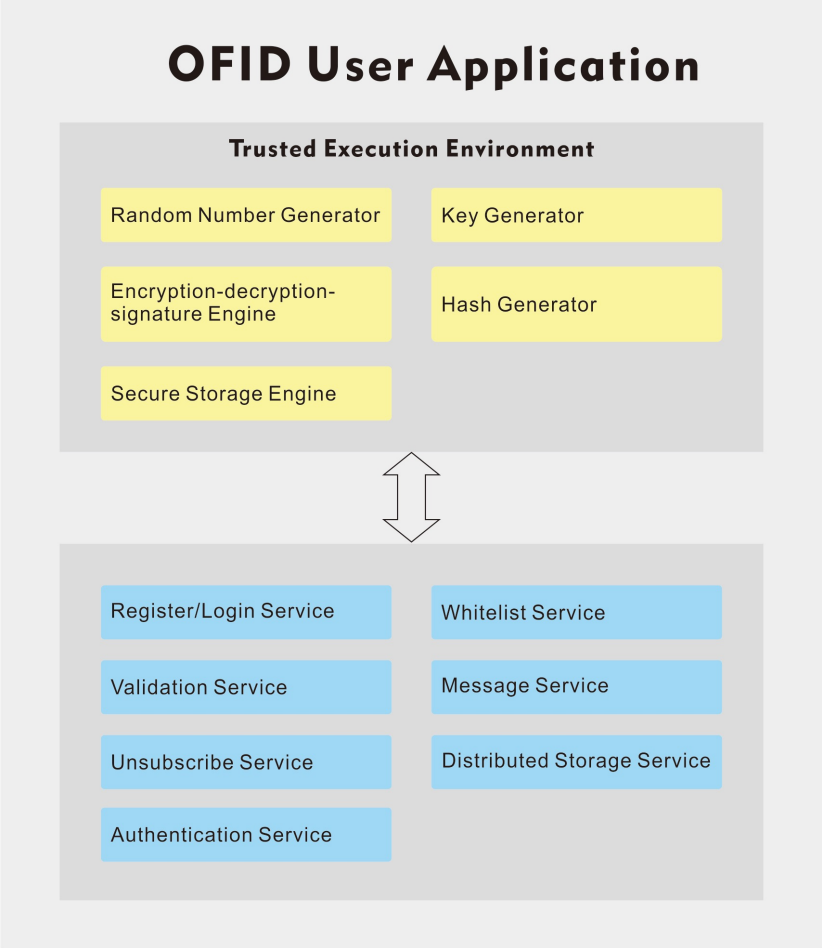
Picture 2 （ All communication is done through the Relayer Server ）



- **User**

Users can access OFID IDV services via the mobile app. The PII data is stored in mobile devices as well as in the distributed cloud for enhanced security.

Picture 3



A set of software components support the Trusted Execution Environment(TEE) on users' mobile devices, which provides safety behaviours including registration, login, certification, authentication and distributed storage. A whitelist cache is also maintained on mobile devices, serving as the backup of the remote whitelist server.

The messaging service facilitates communication between the relayer and the user application.

- **Service Provider**

When a user applies for a service or a product from a service provider, the service provider needs to verify the user's PII. The user provides the hash values of the attestation details. Using these hash values, the service providers verifies the attestation and contacts the validator to get the attestation details. After being paid a mutually agreed price, the validators provide the attestation details to the service provider. With OFID platform, service providers enjoy the following benefits:

1. Casts off trivialities of verification while lowering operational costs
2. Reliable validators boost authenticity of the platform
3. As there's no necessity for the service provider to store sensitive personal data, IT infrastructure costs are reduced.

- **Validator**

In most cases, verification service is not validators' main business. Managing millions of customer records does not bring considerable revenues for validators. However, OFID enables validators to transform their years of hard work in building PII database into revenue generating opportunities.

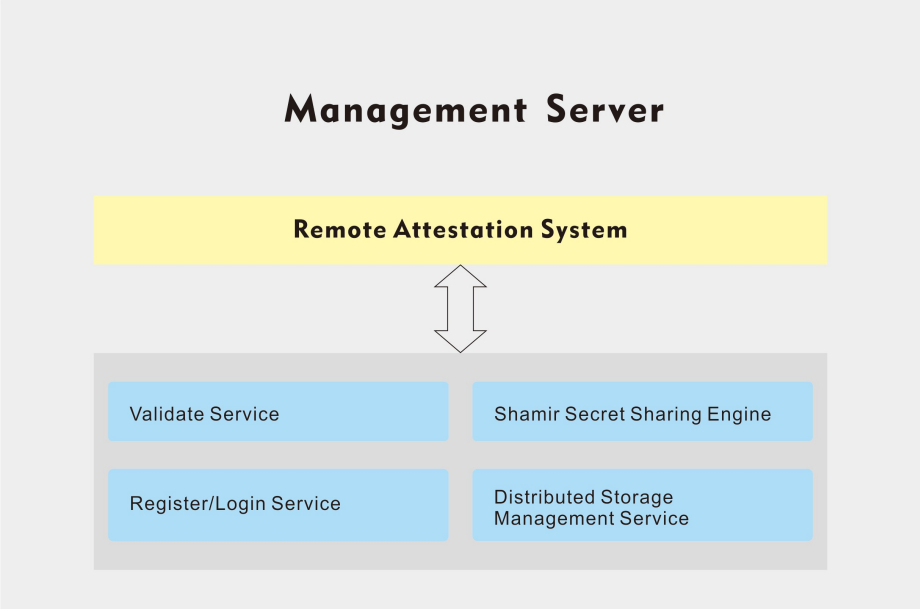
There are two kinds of validators:

1. Authority organizations such as the National Identity System, academic institutions, financial institutions etc.
2. Commercial organizations that provide verification based on their trading or consumption records.

- **M-Server**

M-Server is Management Server

Picture 4



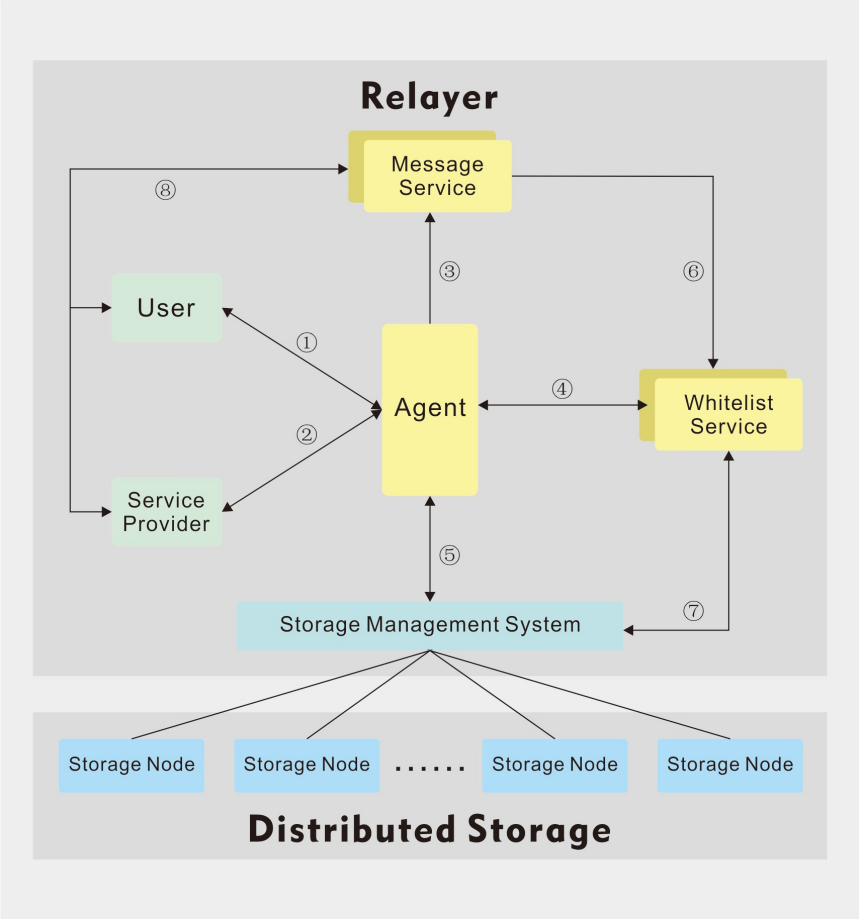
The management service performs the registration and validation processes. The registration data and validation data is stored on a distributed cloud via Shamir Secret Sharing engine. The remote attestation system records the operation status of the whole system, demonstrating all servers' credibility.

In order to avoid fraud and phishing attacks, a user needs to check the legality of the validator before sending the application to the validator. Users can verify the validator whitelist record to verify the credibility of validators. The same whitelist mechanism is also used for verifying the credibility of service providers.

- **Relayer**

In order to decrease latency, OFID uses a proxy server as an intermediary among user, service provider and distributed cloud.

Picture 5



The Relayer system is composed of four components:

1. Proxy Service

Proxy servers are used as an intermediary to handle requests from clients seeking resources from other servers. Proxy servers prevent malicious attacks and block unsolicited traffic while offering cache services, increased security and better administrative control.

2. Whitelist Service

A whitelist service is a kind of positive security model that allows only trusted requests to be processed. It is a standard that define what type of requests can be allowed for execution. Anything that is not included on the whitelist cannot be executed. The distributed cache system brings high throughput, predictable scalability and continuous availability to the whitelist service.

3. Messaging Service

The messaging system is a generic one that be used across multi-systems. The messaging architecture is optimally designed to deliver higher scalability and reliability.

4. Distributed Cloud

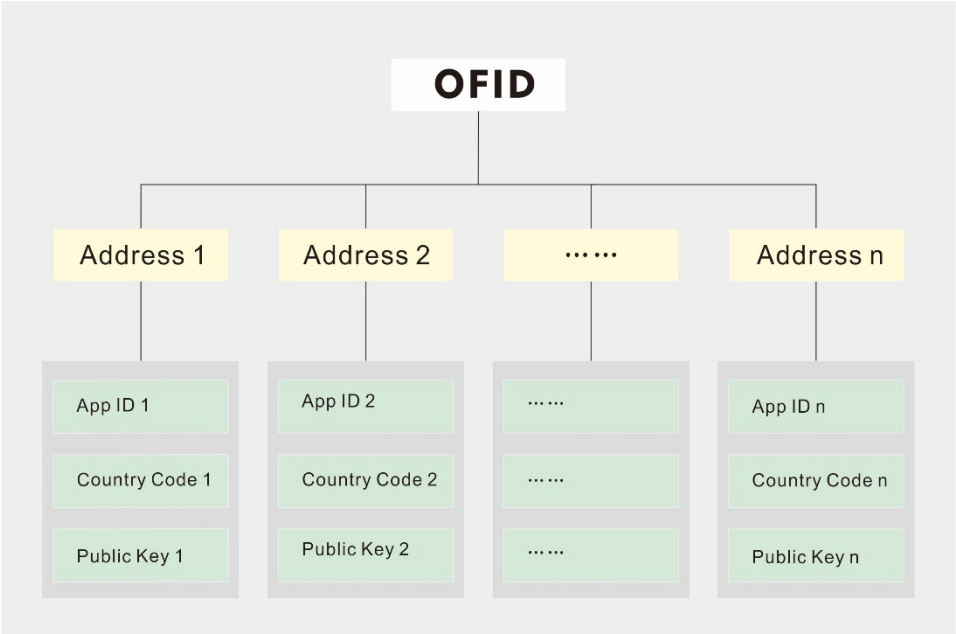
Distributed storage systems provide reliable access to data through redundancy spread over individually nodes. The master server running on a dedicated node is responsible for coordinating storage resources and providing strong consistency while balancing availability and consistency at the same time.

5. OFID number

The OFID platform issues a OFID number to every user. Each OFID number is mapped to multiple identity addresses. Each identity address is used solely to correspond with one service provider.

This methodology ensures that user identity is not comprised by identity theft even through data mining.

Picture 6



Each identity address is composed of three parts: public key, national ID, service provider ID

Identity Address = hash (public key + country code + SP id)

Whether you are a user, validator or a service provider, the OFID platform rewards everyone participating in the ecosystem. The operations and maintenance of the platform is taken care by the OFID team.

Work Flow

- **Registration and Certification**

1. Installation

User downloads the OFID App.

2. Basic Certification

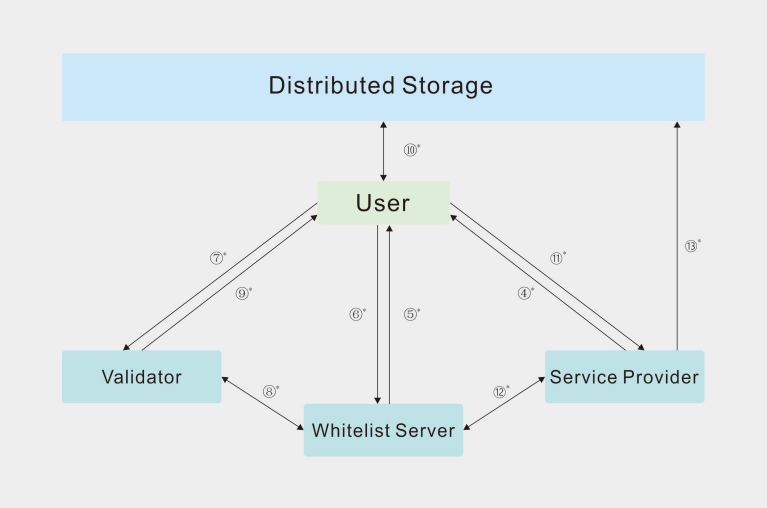
User chooses his or her country code and enters a phone number to register with the OFID system. After allocating the OFID number and the public key to the user, Management Server will record these details along with the phone number and stores them on the mobile device and the distributed cloud.

3. Secondary Certification

User needs to upload PII details such as name, ID card number and hand-held ID card photos and verify details via face recognition and video authentication. After that, Management Server will record all the information and store them in the mobile device and the distributed cloud.

- **Verification Work Flow**

Picture 7 (All processes should pass through the Relayer.)



The user applies for services from a service provider but the verified information does not meet the service provider requirements:

1. The service provider submits a request to the user with the service provider's signature to provide a list of details related to the identity data of the user.
2. The user requests the whitelist server to verify the validity of the service provider and applies for the validator's whitelist.
3. The whitelist server provides the validator's whitelist to the user.
4. The user requests the validator to verify his or her identity data. Before sending the information to the validator, the user signs the information that has been filled and encrypts it with the validator's public key.
5. The validator receives the user's verification request and asks the whitelist server to verify the validity of the user. After successful verification, the validator decrypts the information with the private key and deals with the user's request.
6. When the verification is successfully completed, the validator stamps the timestamp of the verified information, specifies the validity period, and signs it. After creating the Bi-directional Signature, the validator encrypts it with the user's public key, and sends it to the user.
7. After receiving the verification information, user decrypts it with his or her own private key and stores it in the device and uploads it to the distributed cloud.
8. User sends a signed access license to the service provider.
9. The service provider requests the whitelist server to verify the validity of the user.
10. The service provider uses the access license to retrieve the user's identity data from the distributed cloud.

Here is an example of how the user's authenticated information is stored:

- ➢ Telephone number "+86 13900012345" is verified by Telecom Operators, bound to "China Mobile, Beijing".
- ➢ ID Card number "110101200001010001X" is verified by the Public Security Bureau, bound to "Chinese Citizen."

- ➢ Social Security Number “19293949N” is verified by the US Internal Revenue Service, bound to “US citizen”.
- ➢ Blood type “RH+AB” is verified by the medical system, bound to “TRUE”.
- ➢ Graduated school “Japan Waseda University” is verified by Japanese Ministry of Education, bound to “2017, Medical PhD, Excellent grades”.
- ➢ Email address “someone@gmail.com” is verified by Gmail, bound to “Certified Users, OLD”.

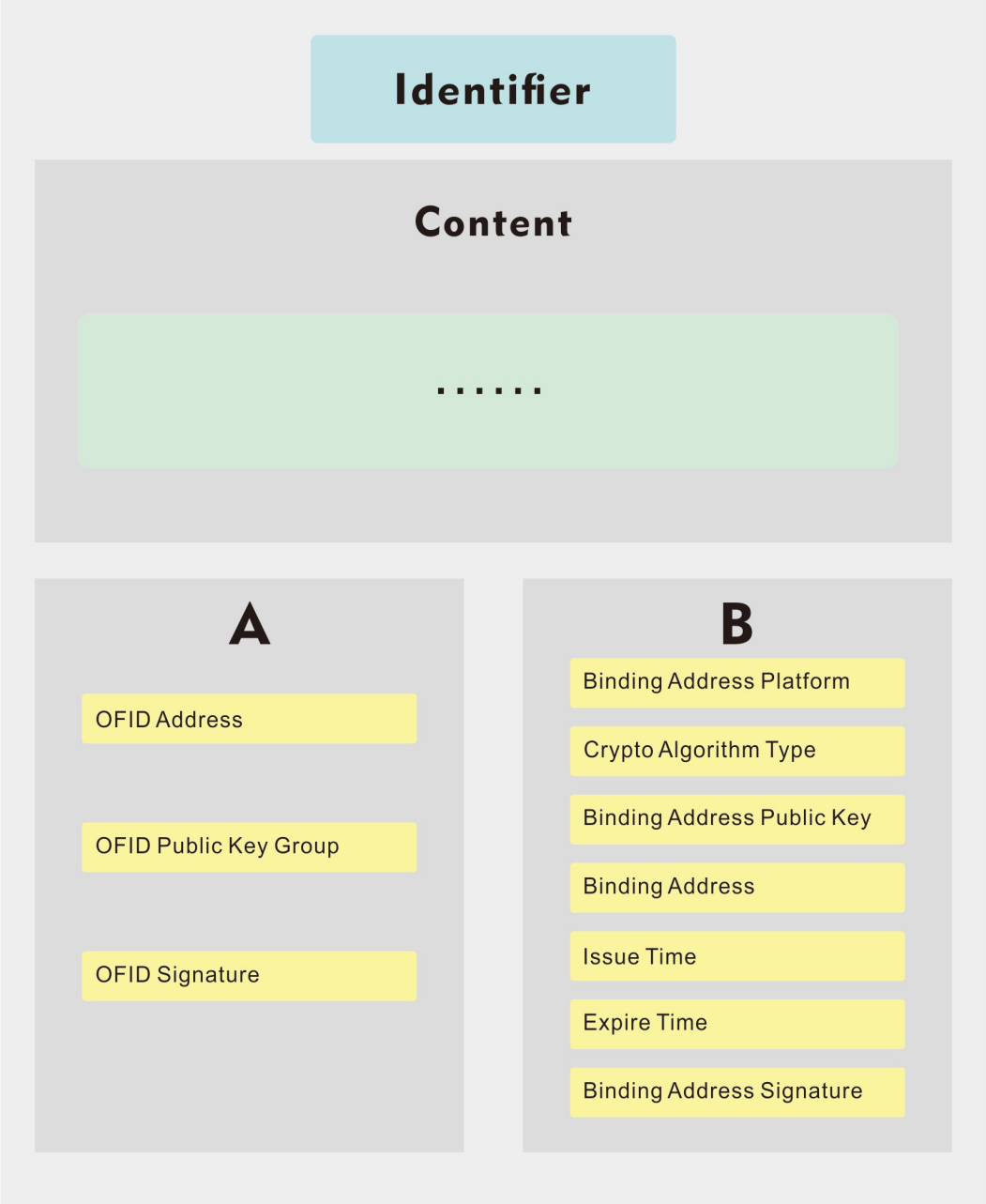
III. The Key Technologies behind OFID Platform

Bi-directional Signature

Bi-directional Signature is a confirmative proof that both parties have approved the signed content.

The architectural design of Bi-directional Signature is explained as follows:

Picture 8



Why is Bi-directional Signature used in the OFID System?

1. To mark the consent of both parties

When the User submits the signed PII, a certificated validator signs the data again to verify the validity of the data.

2. To form a correspondence between addresses

The data validated on an application corresponding to an address under the same OFID number can be used on an application corresponding to another address under the current OFID number without having to re-validate it.

3. To correspond an anonymous blockchain address to a real name OFID address

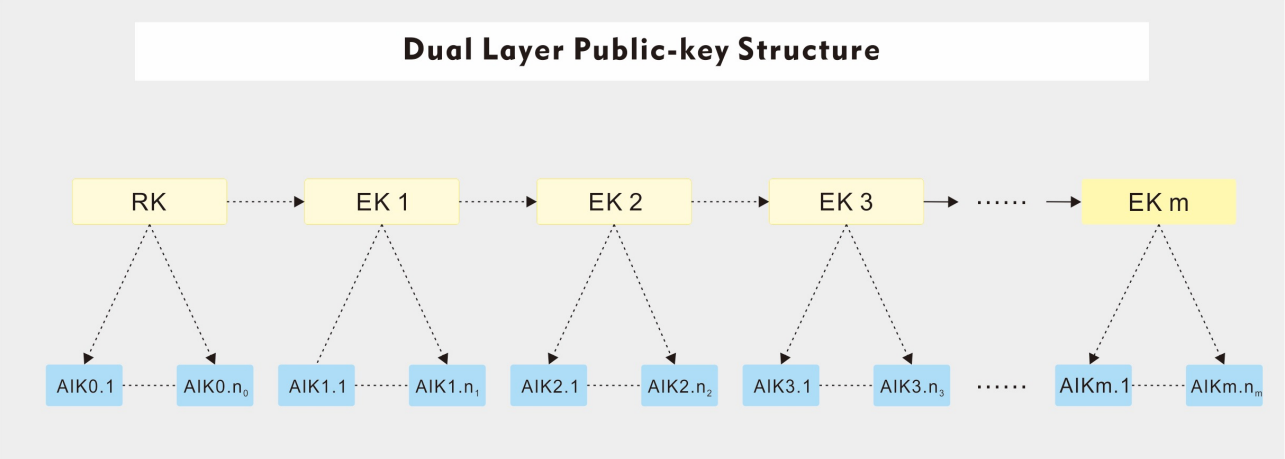
Attributes such as skill, character, and quality etc. lack official certification. However, the OFID platform allows public to recognize and confirm such attributes of a user. OFID allows multiple users to endorse a single user. In such cases, there would be multiple Bi-directional Signatures on the same content. In this way, an unofficial verification and evaluation system can be established.

The Double-Layer Public Key Structure

The existing technology that protects data on the Internet is mainly dependent on discrete algorithm logarithm problem. However, the rapidly increasing computational power of quantum computers combined with the shor algorithm can crack the current public-key cryptography schemes. It means the current encryption algorithms are no longer safe. This is where the double-layer public key structure comes to the rescue. Leveraging this double-layer public key structure, the OFID platform has upgraded the existing encryption algorithm to implement the latest security standards, effectively resisting external attacks.

This is how the Dual-layer public key structure works:

Picture 9



A Root Key (RK) is used to protect the user's original key pair, and to produce a trusted root certificate authority (CA). An effective RK can sign one Endorsement Key (EK) and multiple Attestation Identification Keys (AIK). The RK becomes invalid once the EK is signed.

EK is the node in the CA Chain. In this chain, the latter one can only be signed by the former one (e.g. EKn is signed by EKn-1). EK1 is signed by RK. The effective node is only the last one (EKn), and the former ones are all ineffective. An effective EK can sign one EK and multiple AIKs.

AIK is a key pair with time limit, signed by effective RK and EK. During the validity period, AIK can be used to sign the information.

In the future, OFID will develop a blockchain-based distributed storage file system PBFS (peer based file system) to store a variety of data to ensure data security, reliability, privacy and high-performance computing.

Trusted Computing

The most vulnerable segment of the verification system is the management server. Identity data is stored on a distributed cloud. If a separate node is hacked, it will not affect the Identity data. However, if the management server is hacked or invaded, the data will be lost. Trusted computing offers a perfect solution to this challenge.

Trusted computing and blockchain share one commonality; they both provide a trusted environment. Blockchain achieves this goal through consensus protocols, wherein everyone comes to a consensus working on open information. Trusted computing, on the contrary, is a hardware-based mechanism, which establishes a cryptographic chain of trust to protect data integrity and confidentiality.

Trusted computing is a paradigm aimed at enforcing trustworthy behaviour on computing platforms by identifying a complete ‘chain of trust’ and a list of all hardware and software that has been used. This chain of software can then be compared to a list of known ‘good’ applications.

Trusted computing includes a number of distinct proposals and initiatives with the general goal of engineering more security into commodity computing systems.

Here are some important features of trusted computing:

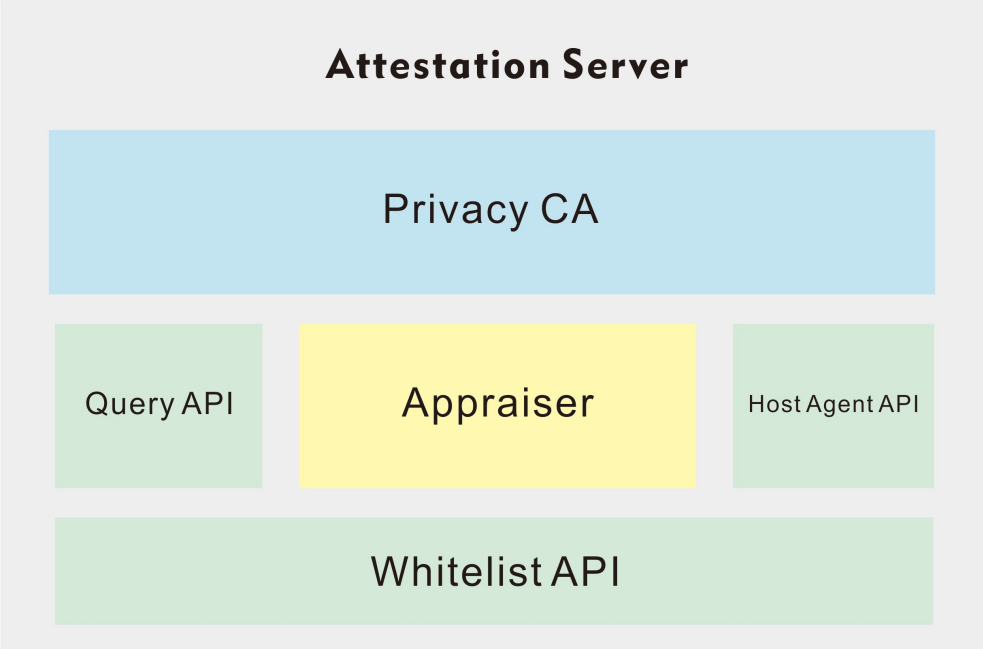
- ➢ Boot into defined and trusted configuration using Secure boot
- ➢ Strong memory isolation by curtained memory wherein other operating systems and debuggers cannot read the memory
- ➢ Cryptographically secured data via sealed storage
- ➢ Key-stroke loggers, screen scrapers and other I/O thwart attacks are blocked.
- ➢ Offers integrity measurement
- ➢ Perform remote attestation

Trusted Computing Unit :

- **Attestation Server**

An attestation is described as a request made by the attester to a third party, called an appraiser regarding its properties and providing proof to support that claim. The appraiser makes a decision based on the provided evidence.

Picture 10

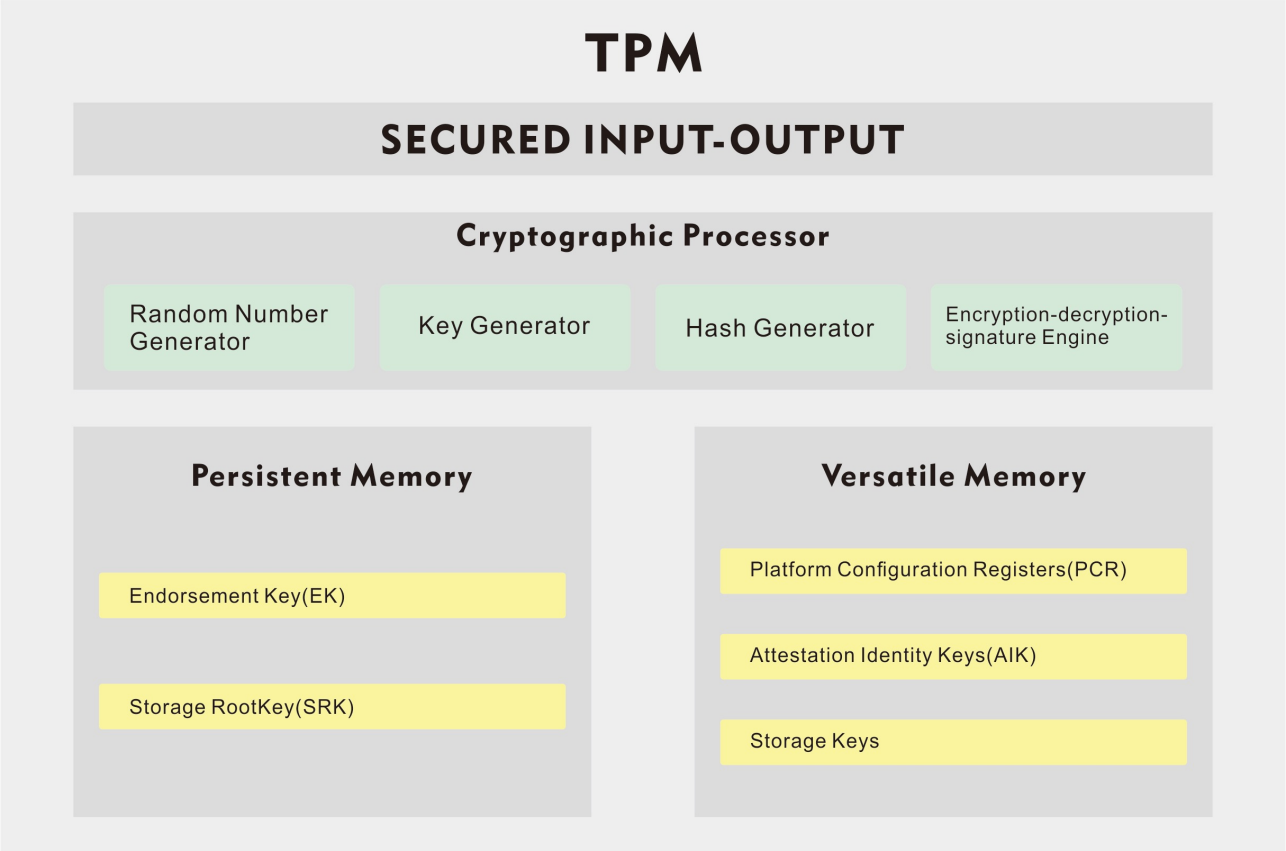


1. Query API ：Query API returns result to the attester.
2. HostAgentAPI：HostAgentAPI enables the attester to communicate with management server.
3. PrivacyCA：PrivacyCA is the privacy certification authority who serves as third party service pseudonyms.
4. An Appraiser acts as a gatekeeper for the protected resource. The attester will provide some measurement data that represents the state of the device as evidence of its integrity. Upon receipt of this evidence, the appraiser checks whether the device is in the whitelist. If there is a matching entry in the whitelist, the appraiser grants access to the resource.

- **Trusted Platform Module(TPM)**

Trusted Platform Module (TPM) is a hardware-based cryptographic solution that enables organizations to enforce strong security measures. With a tamper-resistant piece of cryptographic hardware, TPM provides highly secure solutions that cannot be tampered by malicious software. Serving as a local root of trust, TPM via the internal co-processor handles all cryptographic operations right from hashing and asymmetric key generation to asymmetric encryption and decryption. It offers primitive cryptographic functions wherein you can built more complex features on it.

Picture 11



TPM is manufactured with two keys pairs. The first one is the Endorsement Key (EK) that is unique to the TPM. It is maintained inside and is inaccessible by software. Each TPM has its own ER and is signed by a trusted Certification Authority. Attestation Identity key (AIK) is the second key that ensures that unauthorized software does not modify the device settings.

With increasing security threats, organizations are forced to increase security budgets. TPM optimizes security costs by offering highly secure solutions that can be implemented on multiple platforms, owing to its vendor-neutral architectural specifications. This flexible TPM IC design facilitates interopability and allows flexible implementation of the solutions.

With strong security policies, TPM ensures that transactions are securely processed across multiple devices including mobile devices. the highest security measures offer greater security for networks without affecting the productivity levels. The benefits of TPM are also extended to the storage system. Using its disk encryption features, organizations can setup trusted devices and securely manage data across the organization.

- **Integrated Measurement Architecture (IMA)**

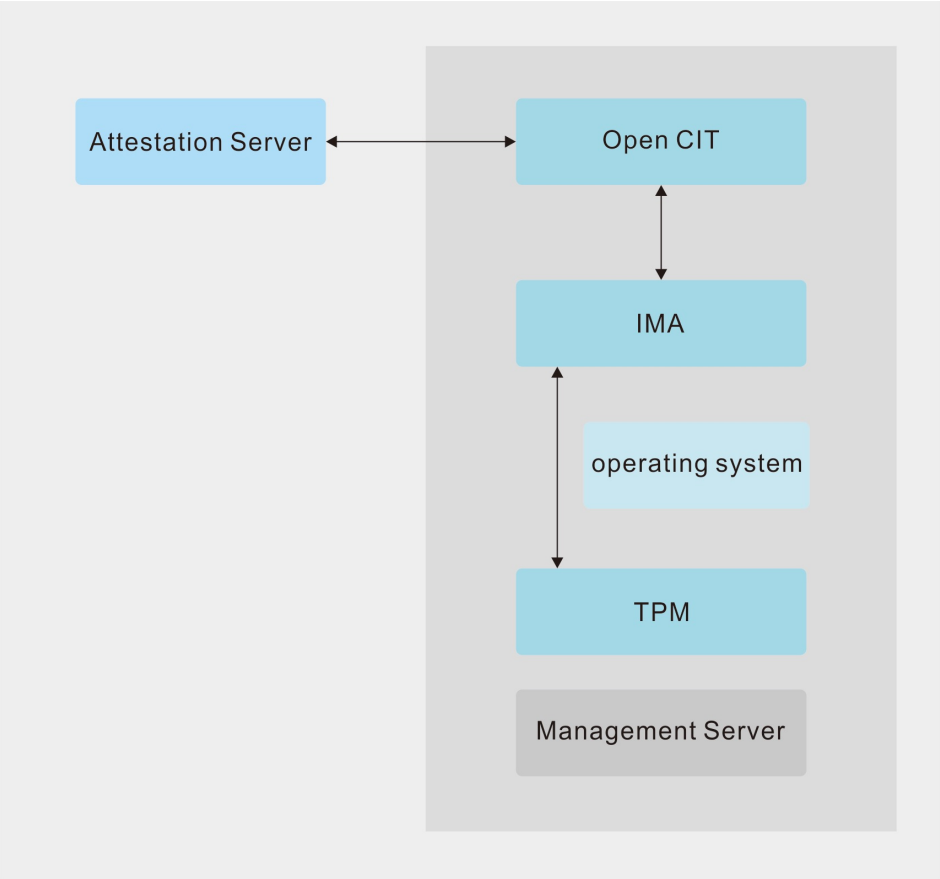
Integrated Measurement Architecture (IMA) is a trusted mechanism for remote attestation processes. It ensures a remote party that only approved executables are executed on the system. Using a trusted boot system, IMA can be used to check and attest the system's runtime integrity. When a program is executed, IMA saves a hash of the file. When the remote system requests for the integrity of the system, it provides the list of executed programs along with their hash values. This mechanism ensures that vulnerable programs haven't comprised the system.

- **Open Attestation**

Open Attestation is project that is initiated by Intel that is designed to verify the integrity of the host system. It offers a SDK that enables you to manage host integration verification. Open attestation uses TCG-defined remote protocol to verify the integrity of the target system.

OAT (Open Attestation) comprises of various tools like whitelist tables that hold known good platform configuration (PCR values), host agents and APIs to support host queries, a certificate authority and appraiser, table provisioning and host agent communication.

Picture 12



The verification management system is based on TPM 2.0 standard.

Upon successful verification, the data is stored on multiple nodes. The distributed cloud's uptime is monitored by the management node to ensure availability on a regular basis. In a case wherein a security threat is identified or if a group of nodes storing a specific record reach a threshold value, the management node refactors the storage plan and deletes old information on those nodes to ensure storage protection.

- **Trusted Execution Environment(TEE)**

This is a secure area of the main processor which is in an isolated execution environment that provides security features like integrity of trusted applications and isolated execution alongside confidentiality of their assets. The Trusted Environment also known as TEE guarantees the confidentiality and integrity of the code and data loaded inside the TEE.

Encryption and decryption inside the TEE executes some user tasks like login, authentication or verification. Due to this hardware based mechanism, the data is well protected. During registration, users generate and store keypairs in the TEE so as malwares do not invade.

Distributed Storage

Many organizations store the confidential data like PII in their data centers and storage area networks. However, data centers are the most vulnerable elements in an organization. When a security breach occurs on the storage server, sensitive data gets into the hands of the attacker causing huge losses to the organization and people. This is where distributed storage comes to the rescue.

Distributed storage comprises of three things; data owner machine, multiple storage servers and the link that will connect the two.

Distributed storage system has adopted secret sharing scheme which is widely used to split secret data into various different kinds of pieces and stored at different locations. To retrieve this data, you should gather the plural pieces and construct that data. This method is known as Shamir's (k, n) threshold scheme. The main idea is to split a secret S into n pieces (shares) for storage. To retrieve that data, a number of k pieces should be gathered for reconstruction. This theoretic security furnishes information that even if an attacker collects shares as far as they are less than the given threshold being represented by k, then they cannot get any information.

- **Shamir's Secret Sharing Algorithm**

In the original Shamir's Secret Sharing scheme, the data D is divided into n pieces which has shares fD (a1), fD (a2)……fD (an) wherein fD represents a random polynomial degree at most k – 1 with a free coefficient representing the secret data D itself while a1, a2 all the way to an are public values. Using langrage interpolation, k or more pieces of fD (ai) makes D computable. D value cannot be determined when you only have the knowledge of any k – 1 or fewer pieces of fD (ai). Shamir Secret Sharing Algorithm securely stores data as it is not possible for attackers to retrieve original data with less than the threshold k of shares even by using unlimited computational resources.

OFID uses Shamir's Secret Sharing algorithm along with public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preservation data security. We achieved high level privacy through random masking technique. The proposed algorithm is very efficient and strong algorithm through which we have achieved confidentiality, integrity, and availability of cloud data.

Blockchain

OFID system is going to leverage the blockchain technology to enhance data security. This is how the attested user PII is stamped to the blockchain.

1. The user PII is returned from the Validator with a Bi-directional Signature. At the same time, a hash value is created based on that data. The system processes the hash into a Smart Contract. Through Smart Contract, the hash value is written on the blockchain finally. When the service provider needs this PII, an index from the blockchain can help service provider take the PII from the distributed cloud. The processing of the query through the blockchain increases the security of OFID system.
2. The Double-layer Public Key structure would be updated only when the authoritative record generates a new EK public key. The blockchain is an ideal way to record this new EK public key making the previous public key invalid.
3. The payment and the transfer of OFID Tokens are implemented through Smart Contracts.

Security Design

OFID platform integrates many security aspects into its system.

1. RMS security model secures remote attestations.
2. The security of user data is handled by TEE.
3. Storage function is managed by distributed cloud. Verification data is sliced into pieces and stored on distributed cloud.
4. In the Relayer system, whitelist can be traced back to the trusted root certification authorities. At the same time, whitelist is isolated from user's privacy data.
5. End-to-end encryption ensures that data is transferred securely between endpoints. All messages are encrypted by receiver's public key.
6. For those mobile devices that currently do NOT support TPM (such as Apple™ iOS®), we will relay on its own security mechanism, such as Secure Enclave to protect and restrict the usage of the stored private keys with the strictest limitation under OFID APP's own user-space.

IV. The Leading Technologies Planned for OFID Platform

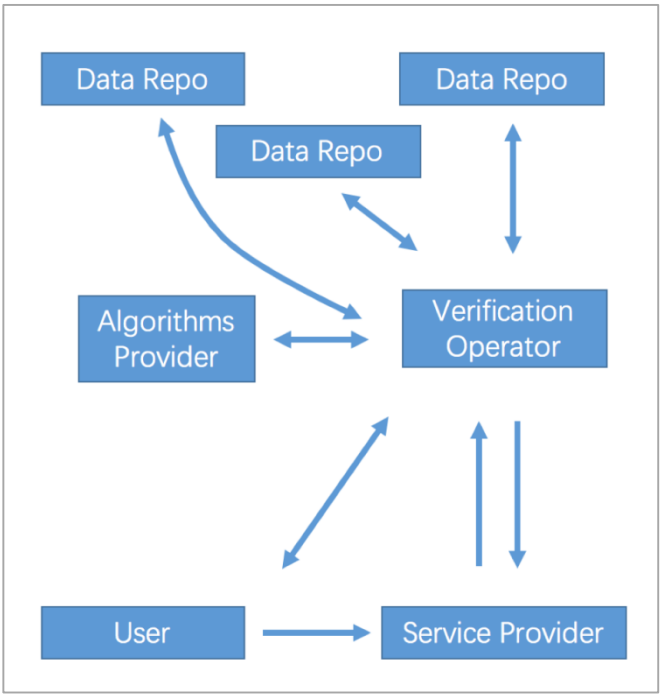
Open Algorithms (OPAL)

The OPAL project is an advanced model that aims at creating an extensive list of available data to be inspected and analyzed without violating personal data privacy. Open Algorithms paradigm involves moving algorithm to the data and implementing at the data repository location so that the unprocessed data is never out of its repository. Only cumulative answers are reverted. Another main aspect is that the algorithms must be scrutinized by experts to be “secure” from any privacy requirement violation.

OPAL’s core is comprised of an open technology platform and open algorithms that directly run on the servers of partner companies, at the back of their firewalls. OPAL aims to develop data services on the basis of grander confidence between all the parties involved.

In future, OFID aims to use the open algorithms pattern to facilitate sharing of more rich information by the participants in the ecosystem. The OFID platform eventually shifts from an attributes-based unidirectional model to a richer algorithms-based interaction.

Picture 13



The Algorithm providers establish smart codes on the blockchain to store their safe algorithms, which is scrutinized by specialists.

When the user requests access to resources or services, the option to request for implementation of one or more audited-algorithms lies with the service provider as a part of the user-authentication process. The verification operator then authenticates the user for providing secure responses to the service provider. During the execution of an algorithm on a data-set, the repository of data always give answers that are “secure” from the perspective of privacy.

This new pattern provides an improved way forward for the identity-protection society, more appropriately to report the main issues surrounding identity silos. Data fusion can lead users to use their data in a better way and offer comfort by developing a powerful source of information, which is more flexible and accurate than any of the original data sources.

Open Platform

Why a Sole-operator system is insufficient for the Identity Verification Industry? The Identity Verification Industry is a special industry wherein a sole-operator system doesn't make sense.

- **Here are some of the challenges with a sole-operator system:**

1. Lack of Competition

Competition always results in innovation. As a contrast, the lack of competition will result in a monopoly rule. It means the operator is not obliged to spend money and time on improving the quality of services or updating the whitelist. Without properly updated whitelists and validator accounts, the authenticity of data becomes questionable over a period of time.

2. Legitimacy of the System is at Stake

When there is no alternative, users are bound to use the only available IDV platform regardless of the quality and efficiency of the service. As the sole-operator doesn't face a crisis management situation, the legitimacy of the system would be at stake.

3. Usability doesn't Matter

In today's competitive business world, organizations that value user interactions would stay in the competition. However, when the IDV platform is operated by a single company, it means realigning the usability of the app to suit user's demands becomes an option instead of a requirement.

4. Low Quality of Data

Inefficient processes of data aggregation and low usability discussed above will result in weakening the overall efficiency and authenticity of the IDV platform

Thus, the sole-operator system has to stand down. In order to increase the efficiency of the system while improving the quality and quantity of data, OFID has come up with an ideal IDV platform that supports multi-operators.

- **Using the OFID SDK, operators can build the OFID platform and perform the following tasks:**

1. Maintain users PII database that includes primary and secondary identity data
2. Design their own customized apps to suit their company branding
3. Create whitelists and regularly update them
4. Develop a list of authorized validators and design ranking rules
5. Manage a list of legitimate service providers and effectively mitigate phishing attacks to obtain user's PII data
6. Have access to the OFID cloud to store data

V. Ecosystem & Token

The OFID Token

A token is a key element of any blockchain ecosystem. The OFID token facilitates smooth functioning of the OFID ecosystem while rewarding all the stakeholders of the platform for their time and efforts.

There are two ways to acquire OFID tokens:

1. A certain amount of tokens can be purchased from the OFID platform. Users and validators are rewarded in the form of OFID tokens for their participation in the ecosystem.
2. Cryptocurrency exchanges.

OFID tokens are issued via smart contracts. While the users and validators are rewarded for their participation in the form of OFID tokens, service providers purchase OFID tokens to avail identity verification services. As all transactions are performed via smart contracts, they can easily tracked and monitored.

- **Here is how OFID tokens are distributed on the OFID platform:**

1. Operators:

Operators can sell OFID tokens to users at the market price. In addition, they can airdrop tokens to potential users to expand their user base.

2. Users:

When new users register with the OFID app, the OFID platform issues few tokens as a reward for joining the platform. When users apply for a product or a service, the service providers verify the PII data with the validators. When the service providers pay the validators for the identity verification service, a portion of that fee is given to the user as a reward for their participation in the ecosystem. If the user wants to access any value-added services of the OFID platform, they can pay for those services in OFID tokens. Users can sell their OFID tokens at cryptocurrency exchanges.

3. Validators

Validators have spent several years in creating verified user data. Now, the OFID platform enables them to convert that effort into revenue-generating entities. When service providers want to verify the PII data, they have to pay OFID tokens to validators for the identity verification service. By rewarding validators with OFID tokens, the OFID platform wants to accommodate as many validators as possible to provide identity verification services.

4. Service Providers

When a user applies for a service, that service provider is going to receives user's PII data which has been verified by a validator. The service provider has to pay OFID tokens to the validator to obtain its service.

- **The Voting System**

Be it activating an arbitration, rating a validator or moving to an open-source platform, key decisions related to the OFID platform are determined by the voting system. All stakeholders of the OFID platform would participate in the voting and decide whether to approve or reject an idea.

Here are a few typical use cases:

1. Activating Arbitration: When a dispute arises, users can request for an arbitration service. The decision to activate an arbitration would be determined by the votes casted by other stakeholders.
2. Rating Validators: When more than one validator validate PII data, other participants can participate in a voting event and rate the validator. Based on these ratings, service providers can choose the best validator. This process improves the quality of the identity verification services offered on the OFID platform.
3. Decision-making: A decision to make changes to the ecosystem can be determined through the voting system. Examples include updating the technology, implementing new technologies, rejecting validators, approving new procedures and policies etc.

VI. Next Step

Product Roadmap

- **The First Phase**

We are planning to testrun the OFID platform in January 2018. Subsequently, the app will be available on Android store and Apple store, enabling users to download and check the performance of the app. We are planning to launch OFID IDV operations initially in China and Japan and then extend the functionality to other regions. We are getting associated with local organizations such as China's Ministry of Public Security to provide IDV services to users.

- **The Second Phase**

Commercial operations will begin from June 2018. Validators who may include commercial banks, central banking credit systems, financial institutions, utility companies and government organizations can join the OFID ecosystem. Validators can use the self-service feature of the app to access the OFID system.

- **The Third Phase**

The inter-user verification function that is based on social information algorithms will be introduced in this phase. This inter-user verification function will increase the credibility of the identity data validated on the platform.

- **The Fourth Phase**

Enterprise verification feature would be implemented in this phase. Using this feature, small and medium enterprises can verify their assets, shareholdings and customer base to acquire higher credit-ratings and thereby avail higher credit.

- **The Fifth Phase**

Multi-operators will be accommodated on the OFID platform.

- **The Sixth Phase**

The system technology will be fully upgraded to the next stage, namely "Open Algorithm System".

Development Plan

- **Sep 2016 – Dec 2016:**

Project Initiation, Requirements Analysis, Architecture Design

- **Jan 2017 – Aug 2017:**

Development of Distributed Storage Infrastructure, of Smart Contract Payment System, and of Transfer Server Infrastructure.

- **Sep 2017 – Dec 2017:**

APIs for Service Provider and Validator, Beta Version of OFID app, which can provide basic verification services.

- **Jan 2018 – May 2018:**

Implementation of Trusted Compute Management Service and Challenger Platform. Optimizing Trusted Compute Module on app, which can support premier verification services.

- **June 2018 – Oct 2018:**

Development of Social Product Module. Optimizing Function of Validator and Service Provider Whitelist System.

- **Nov 2018 – Mar 2019:**

Design and Development of Transfer Server System and Distributed Storage Clustering.

- **April 2019 – Sep 2019:**

Implementation of the Third Party Storage on OFID Platform, which can make the system more secure and trusted. Implementation of Video Verification System.