Digital identity governance on blockchain

for data, applications, processes, user management and IoT

Technical Brief

Executive Summary

The Issue

In the modern digitally evolving world, traditional approaches to Access Management (AM) and Identity Governance and Administration (IGA) are no longer efficient due to the following critical hardships:

- Identifier works only in the organization that confirmed it;
- The issue of trust to certification authorities of all levels;
- Necessity to check the entire chain of certificates by a user (up to the root);
- Problems associated with synchronizing Online Certificate Status Protocol (OCSP) servers;
- Complexity and cost of operation and development of multi-vendor integrated systems Identity and Access Management (IAM) especially if there are already working IAM systems;
- The complexity of integrating existing systems with new cloud identity or access management as a service (IDaaS) or RaaS (Registration as a Service) solutions.

Trends

Most IAM providers expand their deployment models beyond the local network by using cloud technologies with the ability to support system operation in a rapidly changing business environment. In this case, the blockchain can solve the problem of providing an additional layer of reliability and flexibility for introducing such systems and avoid costly maintenance of the local system.

At the same time, customers are increasingly taking the personally identifiable information (PII) storage and handling method. Basic regulations (such as GDPR, PSD2, etc) require enhanced measures to regulate and validate user data. Such measures apply to both IAM providers and organizations that use PII.

This means that the platform owner needs a solution with PII management, which allows you to ensure confidentiality when storing, processing and transferring data. Blockchain is a solution that can provide a reliable identification system in the multi-partners environment while respecting the security policy regarding the confidentiality of user data.

Mission statement about the concept

There is a completely decentralized approach based on the concept of web-of-trust. The essence of the approach is that users organize a peer-to-peer system, and each of them deals with the identification and certification of other network participants (i,e., each user decides whether or not to trust the identifier of another user). This method of organization has undoubted advantages, such as inability to influence the system alone and more objective information about whether an identifier corresponds to a system participant.

But this approach also has a number of limitations that reduce the effectiveness of these systems:

- The long process of rebuilding the network of trust (in case of changing the user ID, the system update will take a very long time because 1) the majority of system participants must update the identifier 2) and because it is necessary to convince the participants that it is the target user, not an attacker, who initiates the change of an identifier;
- Users are not ready to provide all their data associated with the identifier in the public domain.

There are a number of proposals based on the use of the same standard X.509 but with an application of blockchain technology. In this case, public key certificates are being added to the blockchain that is maintained independently by certification authorities. Such an approach makes the process of certificate authorities synchronization easier and ensures the immutability of the certification authorities activity history. However, the central certification authority still remains; in such a case, the security of the entire system is relied on this center (keys compromise of the root certification authority would entail the need to re-issue all child certificates). While an end user still needs to check the entire chain of certificates.

The TOKEND blockchain software platform (www.tokend.io) provide efficient solutions to these challenges, mitigate threats and increase digital identity and certification efficiency:

- Company receives a white-label infrastructure solution (with user key storage, modules for the user certification, identity storage and an administrative interface) that it fully customizes and creates new opportunities for digital identity and certification;
- Company can use their own Know Your Customer (KYC) provider or entrust the identity to another company;
- Compared to the traditional approach, a client does not need to go through the identification procedure in each service used. Rather, it is enough to confirm their identity once (most often the data required by the KYC coincide for many areas of

activity);
- The record of each transaction is easily traced (who identified the user, who issued the certificate, etc.);
- A public blockchain does not store personal data of users but only proof that this data was provided and a public key certificate.

Benefits of the TOKEND blockchain platform for digital identity and certification:

For the IAM platform owner:

- Multi-partner identity ecosystem;
- It is not necessary for each company to hire its own KYC provider.

End-Customer (certificate owner):

- One app for all services of multi-partner companies;
- One identifier for all services of multi-partner companies;
- One-time KYC procedure (no need to register separate identifier for different services).

Proof of value for blockchain in identity and certification

- Doesn’t presume a single point of failure as well as centralized censorship;
- Stored identification data can be provided to another party only with the consent of a user;
- There is no need to disclose your personal data to all participants in the system;
- Fast and efficient functioning;
- Compatible with various systems.

Blockchain advantages

- Single source of truth for all participants is provided without intermediaries as well as without compromising privacy and competitiveness;
- Reduced transaction costs, which are the result of disintermediation.
- Shared data enables near-real-time updates across the network for all parties;
- Unambiguous perception of user IDs by all services.

Digital Identity for Internet of Things

IoT also requires the use of robust identification and certification mechanisms to support normal operation. Each of the individual sensors must communicate correctly with the rest of the system components. For secure communication between system components, they must exchange encrypted messages with an ability to check data integrity and authenticate the sender object. And this is only possible with a reliable certificate infrastructure.

As the number of such components grows, it is becoming increasingly difficult to organize a reliable mechanism for identifying data and data sources. It also often becomes the task of organizing rights and permissions depending on the identifiers received in the system:

- policy and role management;
- maintaining rules governing the automatic assignment (and deletion) of access rights;
- ensuring visibility of access rights for selection in access requests;
- periodic permission checks to ensure compliance of access in accordance with the system security policy.

Expanding Digital Identity and Certification with Blockchain

Concept overview

Being a blockchain-based platform, TOKEND creates an immutable and time-stamped distributed database entry of every single transaction ever made. This makes transactions and their records easily traceable, irreversible as well as prevents from double spending, fraud, abuse and any other type of manipulation.

In the traditional, centralized approach, each of the certificate authorities performs the identification and certification of its own clients (using available methods and resources: it could conduct KYC personally or use external KYC providers). This center must also store KYC data provided by a user in a local secure storage.

After certification, such a center adds a corresponding entry to the blockchain—that it has identified and certified a user with such a public key. In addition, a hash of user data is added to the entry as proof of the passage KYC procedure. Note that the transaction is signed by the center conducted the identification.

If a user needs to access the services of another system that also holds one of the validator nodes, then a user refers to it using their own identifier. The system, in turn, applies to blockchain and verifies who verified this user.

The owner of each system determines themselves how much they trust certificates issued by another system. If the level of trust is maximum, then the system provides the user with a service based on their identifier. If the trust in the system is lower, then the validator can query the KYC user data (and verify that the received data match the blockchain using a hash value). Note that access to personal KYC data is made only after the user's approval. If the provided data is sufficient, the system provides the user with access; if not (for example, additional data is needed), then the system individually identifies the user with the corresponding entry in the registry.

KYC procedure and obtaining a public key certificate

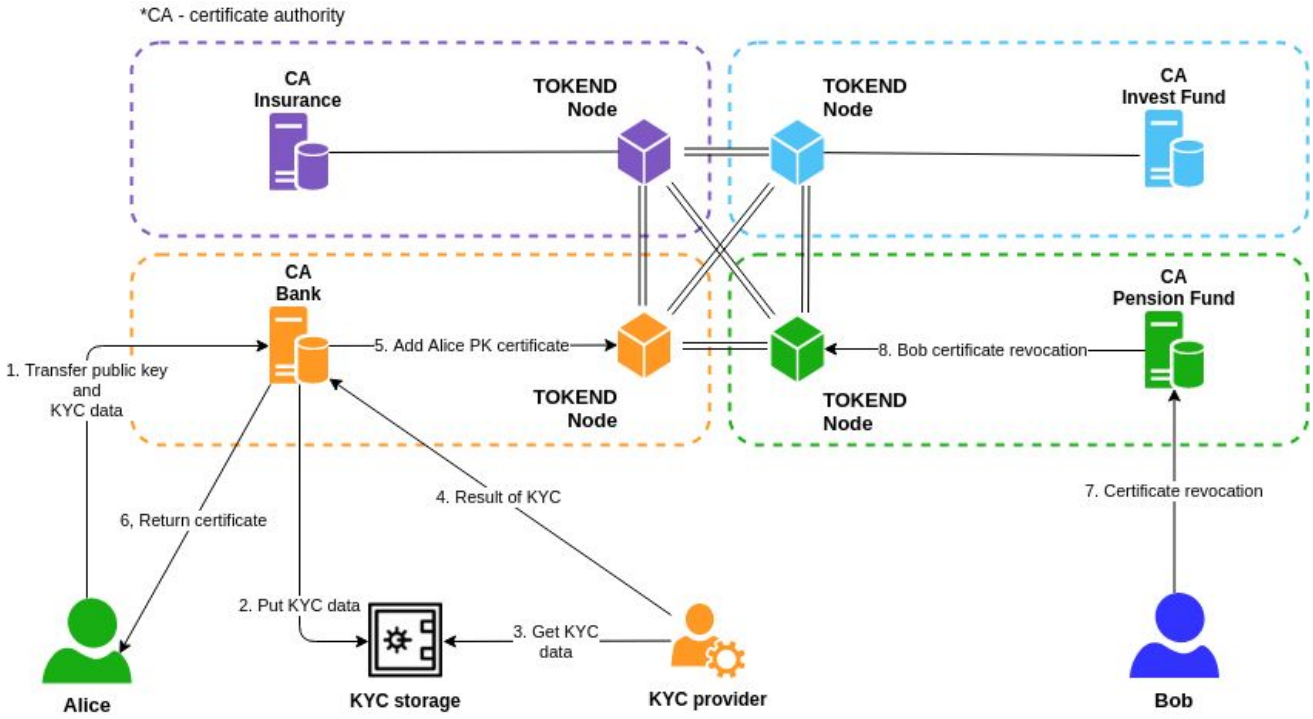

Figure 1. Process of KYC procedure, obtaining and revoking a public key certificate

1. Alice sends her own public key and data necessary for passing the KYC procedure to the certificate authority of bank.
2. The bank places the received user personal data in a secure KYC storage, compatible with the GDPR. Note that KYC data is encrypted by the bank and only it can directly access the data of the storage. To obtain KYC data by a third-party organization, it needs to contact the bank, which, before providing this data, request the user's approval.
3. KYC provider gets access to user data and conducts a KYC procedure.
4. After that, the KYC provider passes the bank the results of the KYC procedure. If the procedure was not successful, the bank informs the user about it, the user adds the missing data and repeats step 1.
5. If the KYC procedure was successfully completed, the bank creates a transaction that contains the user's public key certificate (which is signed by the bank key) and the hash value of all user KYC data (as proof of the storage of these data). TOKEND Bank Node processes the transaction and adds it to the blockchain.

6. The bank returns to Alice a signed public key certificate. Alice can verify that the corresponding record was added to the blockchain and that the hash value in the transaction matches the data she sent.
7. If Bob wants to revoke his public key certificate, he informs his certification authority about this (in our case, it is a pension fund certification authority).
8. The pension fund creates a transaction that contains information that the previously valid certificate has been revoked, and adds it to the blockchain. TOKEND Pension Fund Node processes the transaction and adds it to the blockchain, as a result of which the certificate becomes invalid for all system participants.

   8.1. If the user does not renew the certificate, his personal data is deleted from KYC storage.

Using an identifier for access to services from other organizations

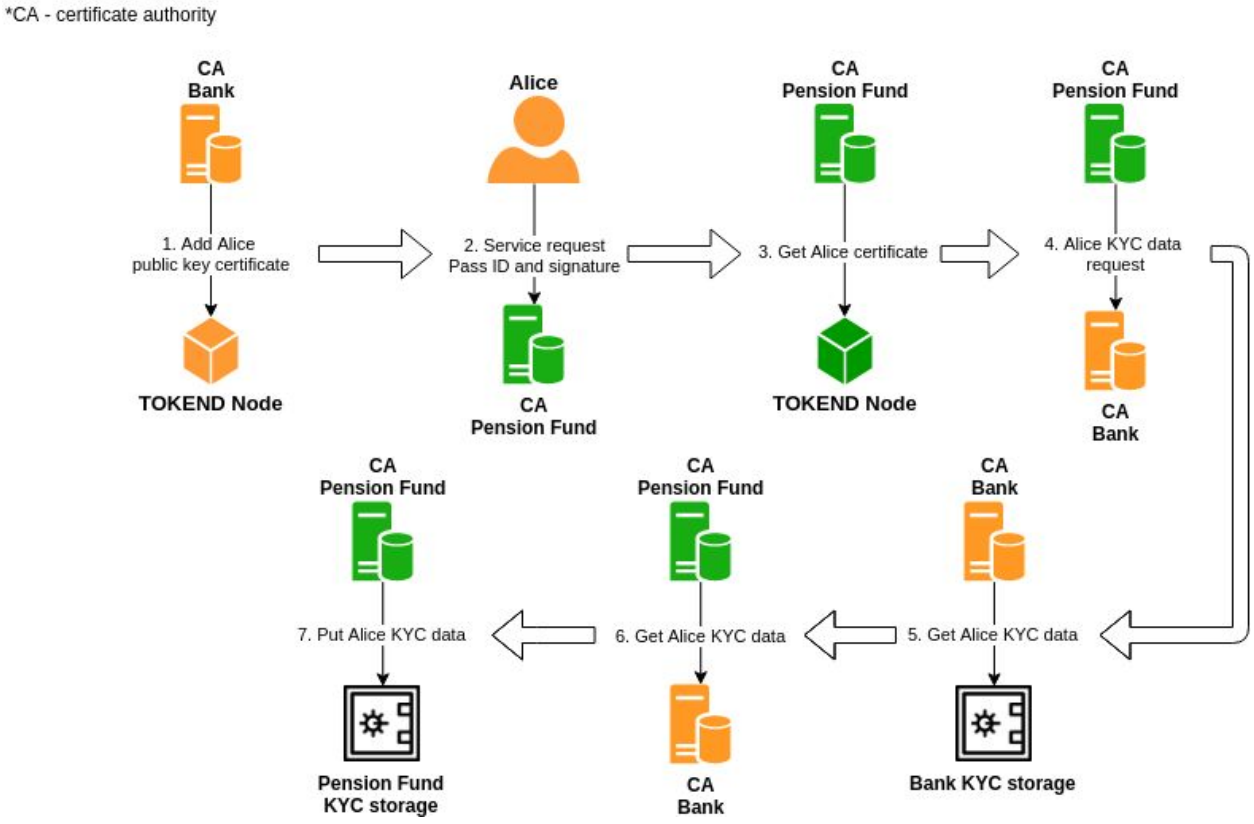

Figure 2. Process of access to other organization service

1. Beforehand, the bank adds the Alice certificate to the distributed database as we described above.

2. Alice wants to conduct an action with a pension fund. She has not registered on it, but the pension fund is a partner of the bank. She requests the pension fund, sends him her identifier (public key) and signs the request with the secret key, which proves ownership of the identifier.
3. The pension fund through TokenD Node verifies that Alice's public key certificate is in the blockchain and is signed by the bank. If the pension fund trusts the bank to identify and certify users, it immediately provides the appropriate service to Alice.
4. If the pension fund does not sufficiently trust the bank (for example, the bank is a young company), it can request the Alice KYC data from bank (if Alice gives her approval).
5. In this case, the bank retrieves the data from the storage and passes it to the pension fund. Note that Alice should grant permission to access KYC data when she requests access to pension fund.
6. The pension fund receives data and can verify their validity (the hash of data stored in the blockchain), after which fund gives Alice access to him services.
7. Pension fund is required to store this information, so it must fetch it right away and store it on it's own storage

Alice verification of the certificates of Bob and Carol

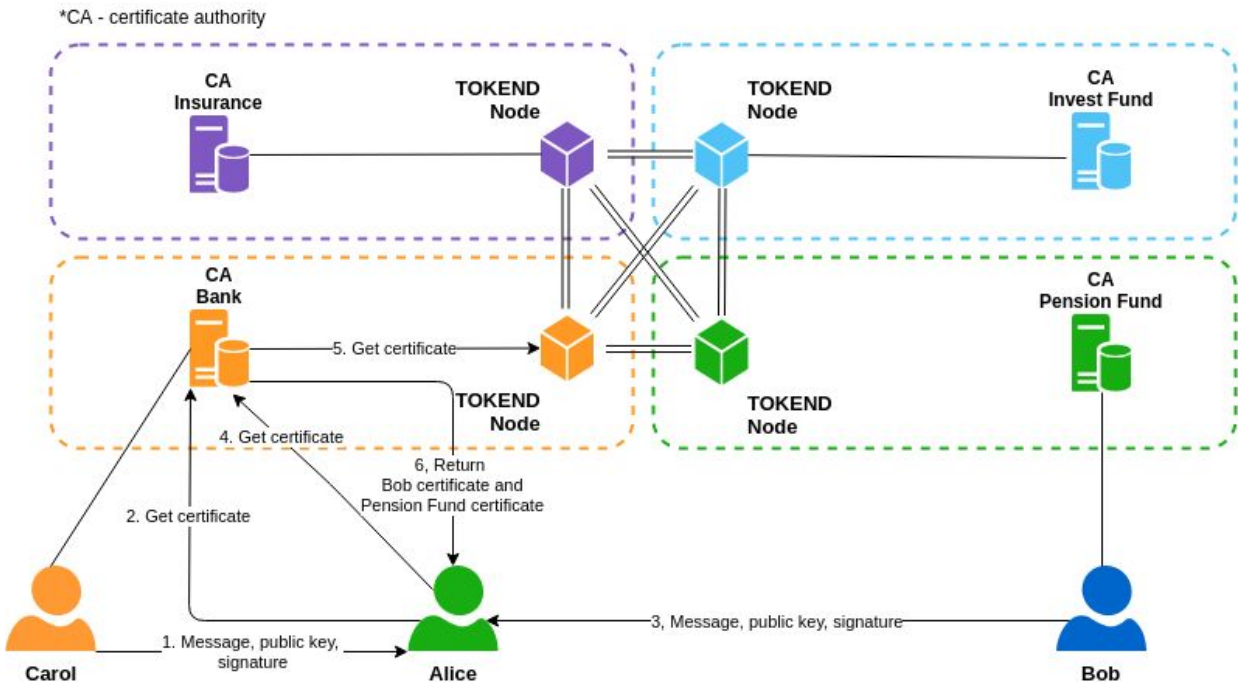

Figure 3. Process of certificates verify

1. Alice receives a signed message from Carol and a public key that can verify the integrity of the received message. In order to make sure that the message was signed by Carol, Alice needs to make sure that the received public key is indeed Carol's key.
2. Alice contacts the bank's certification authority to obtain a Carol public key certificate. Since Carol is also a bank customer, he can immediately provide a signed certificate to Alice. Alice verifies the signature of the bank, and if it is correct, she believes that the message was actually received from Carol.
3. Alice receives a signed message from Bob and a public key that can verify the integrity of the received message. In order to make sure that the message was signed by Bob, Alice needs to make sure that the received public key is indeed Bob's key.
4. Alice contacts the bank's certification authority to obtain a Bob public key certificate. However, in this case, Bob is not a bank customer.
5. Therefore, the bank accesses the blockchain through TOKEND Bank Node and see if there is a Bob public key certificate. If such a certificate is available, the bank checks by whom it was signed. The bank determines that the certificate was signed by the pension fund (bank partner).
6. The bank returns to Alice Bob public key certificate (signed by the pension fund) and the pension fund public key certificate (which was signed by the bank and indicating that the bank trusts the issuance of certificates to the pension fund). Alice verifies both received certificates and makes sure that the message was actually signed by Bob.

Key compromise by a single organization

The process of restoring the certificate of one of the centers after the key has been compromised is as follows:

1. Eve steals the secret key of the bank (the bank key is compromised).
2. The bank informs other organizations that its private key has been compromised. All certificates previously signed by the bank are invalidated.
3. Each organization revokes a bank certificate. From this point on, all participants in the system consider the bank certificate and certificates of all its clients to be invalid.
4. The bank distributes the new public key to partner organizations.
5. Each organization creates a new certificate of the public key of the bank and adds the corresponding entry to the blockchain. Now the bank certificate is valid and it can sign new certificates with a new private key.
6. The bank signs new certificates of its customers (with new keys) and publishes corresponding transactions in a blockchain.
7. The bank distributes certificates to users. From this point on, the functioning of bank users with other network members is restored.

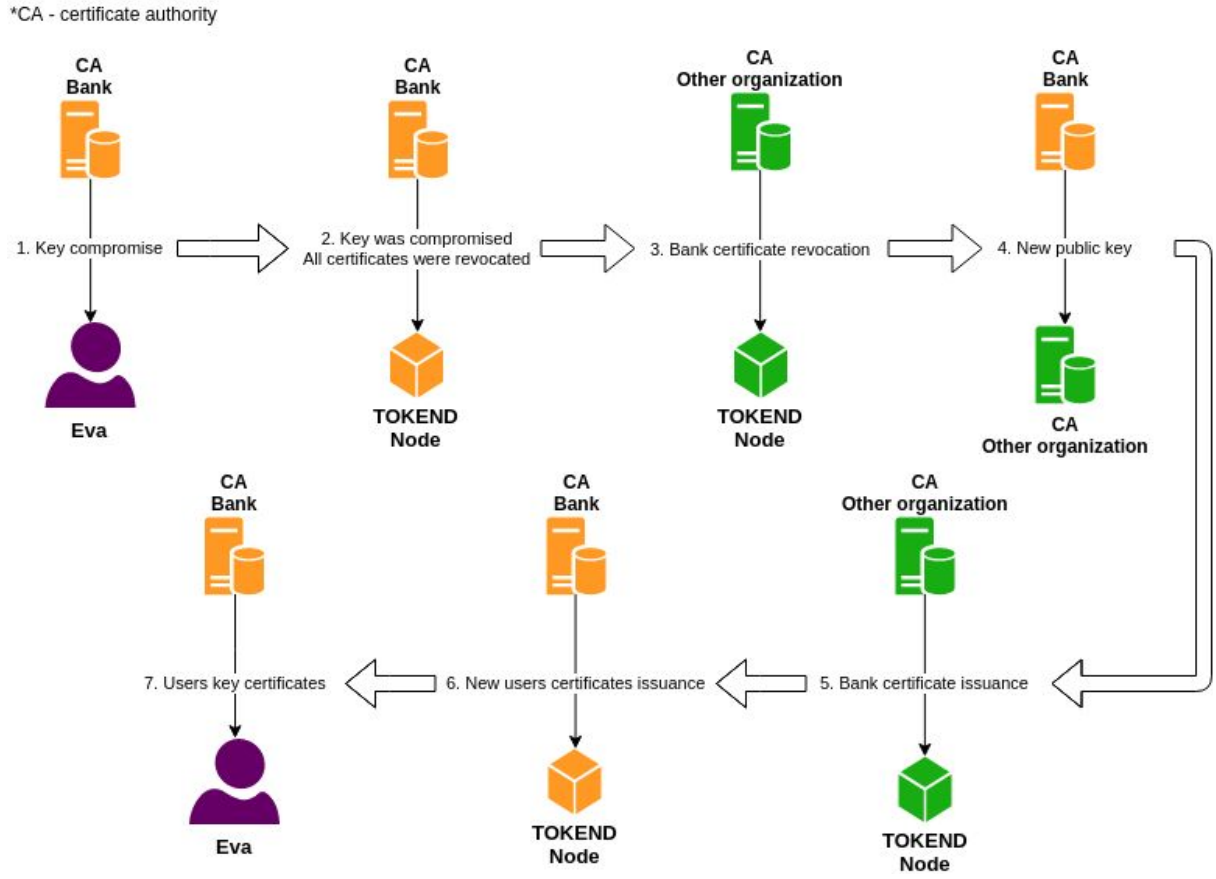

Figure 4. Process of certificate revocation and recovery

Digital Identity for IoT

There are nine major applications of the Internet of Things:

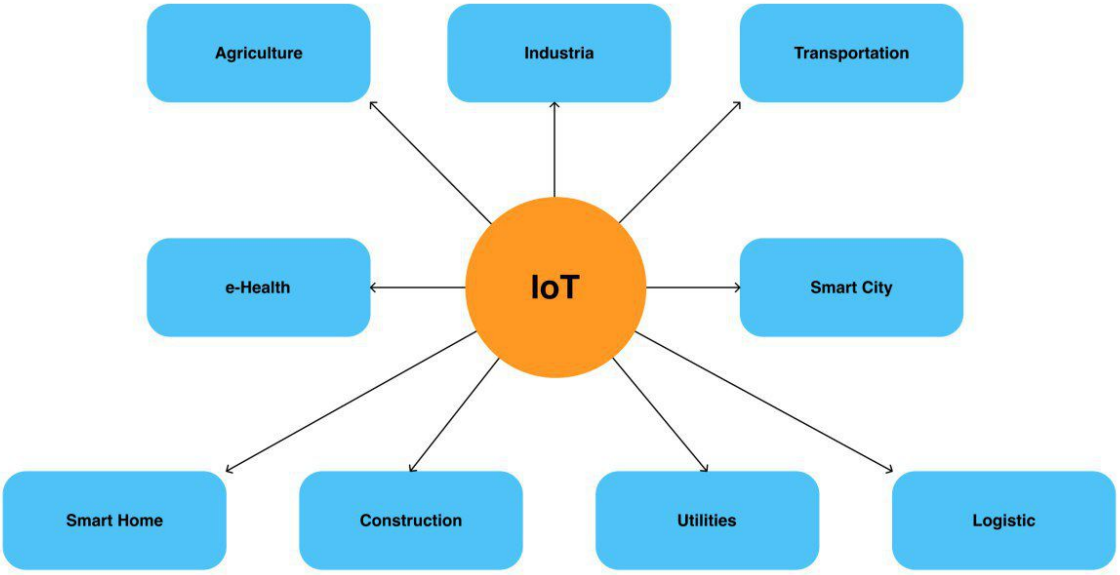

Figure 5. Main Internet of Things domains

The TOKEND platform can provide an identification and certification system that is suitable for everyone: in e-Health for reliable information exchange of medical equipment items, in Industrial for data authentication, its providing components and their manufacturers, etc. As an example, let us consider how it is possible to organize an identification system containing information about the vehicle's sensors.

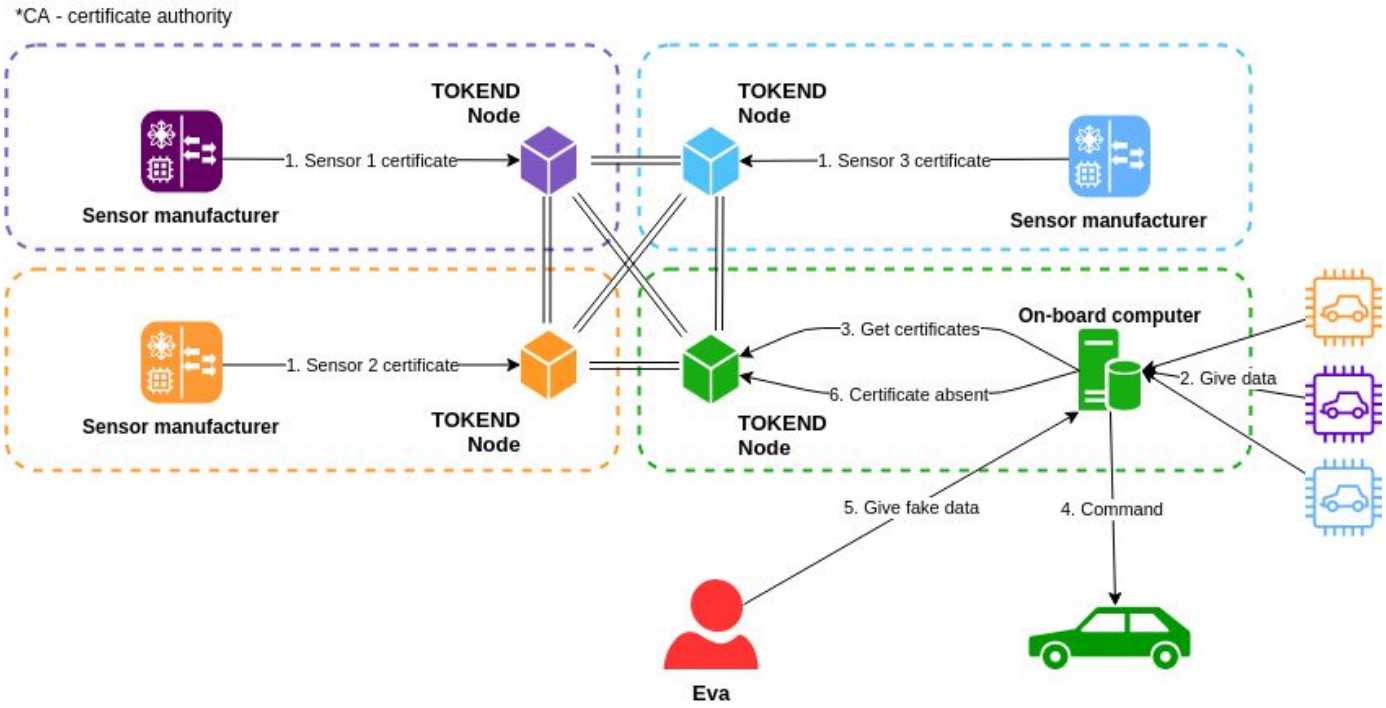

Figure 6. Process of getting information from separate sensors

1. Sensor manufacturers place the blockchain public key certificates of their products.
2. Sensors transmit information to the on-board computer of the car while signing all the transmitted messages.
3. The on-board computer accesses blockchain and checks the validity of the sensor certificates through the TOKEND Node
4. Based on the information received, the on-board computer gives commands to the mechanisms of the car.
5. Eva wants to send fake information on behalf of one of the sensors.
6. The TOKEND Node is requesting a public key certificate that matches the received identifier and signature value. Since there is no Eva certificate in the system, the on-board computer will not process the information received. Moreover, in the event of a breakdown of one of the components, the user will have a transaction with which you can confirm the fault of one of the sensor manufacturers.

If we present the scheme of interaction between the components of IoT in the layer model, then the TOKEND platform occupies an intermediate level between the Edge Layer (manufacturers and information supplied from them) and the application level - a logical level at which the obtained data is analyzed and all important decisions are made regarding the operation of the final device.

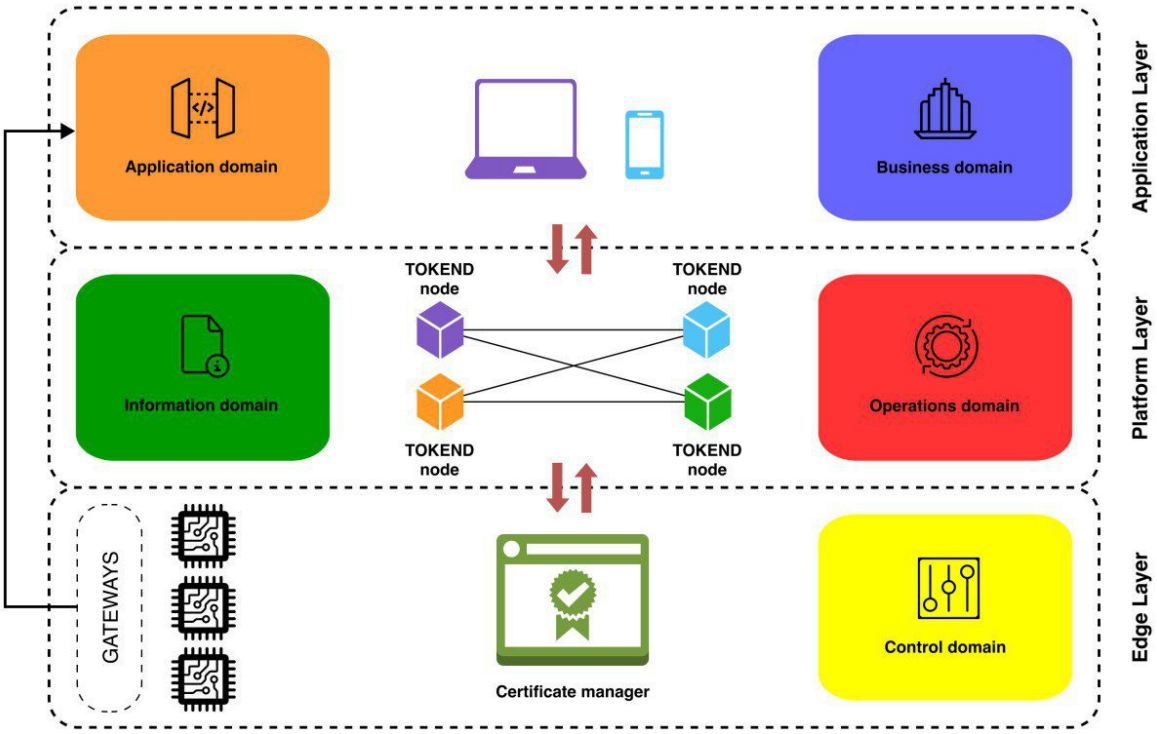

Figure 7. Interaction between different layer components in IoT

Summary

TOKEND provides a platform capable of organizing a digital identification and certification infrastructure to manage both user roles and split permissions for IoT platforms. TOKEND allows you to easily and quickly integrate a corporate blockchain with an existing system and provide a number of advantages, such as:

- The minimum trusted intermediaries. Changing the hierarchical structure of certificates with a single head center to a decentralized structure with equal certificate authorities;
- Transparency. Information on all certificates is available to all participants in the system. At the same time, all personal data of users are outside the chain of blocks and are reliably protected;
- Integrity. Certificate information cannot be retroactively changed. Certificate renewal or revocation is also accompanied by transactions in the blockchain;
- Security. The impossibility of modifying a blockchain increases security when communicating the IoT components together.

Learn More

https://tokend.io/

https://tokend.io/downloads/

enterprise@distributedlab.com

About TOKEND

TOKEND is a white label blockchain software platform that consolidates best practices of tokenization solutions. It allows you to issue, transfer and exchange your assets with a high level of privacy, security, and auditability while following regulations of your jurisdiction. TOKEND is designed for enterprises who are willing to take advantage of tokenization or experiment with the blockchain technology without the need for maintaining the expensive team of blockchain experts and within the shortest time to market.

© Copyright 2019 Sakor LTD. Available under CC BY 4.0 license. The information contained herein is subject to change without notice. The only warranties for Sakor LTD products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Sakor LTD shall not be liable for technical or editorial errors or omissions contained herein. TBTDIDN001PK, April 2019