remme

Distributed Public Key Infrastructure (PKI) protocol and Access Management DApps

Report on business model overview

February, 2018

Contents

1. Executive summary

Key takeaways form report:

1. REMME is an Identity and Access Management (IAM) solution that use X.509 self-signed certificates for authentication and securitization of access for user on device level without need of passwords.
2. REMME solution replace centralized instances of Public Key Infrastructure (such as Certificate Authorities, Registration Authorities, Lightweight Access Directory Protocol, etc.) (PKIX) with decentralized Public Key Infrastructure (DPKIX) empowered with private/hybrid sidechain or public blockchain developing in Hyperledger Sawtooth framework.
3. Centralized PKIX have several point-of-failure that are centralized instances, while REMME DPIKX implement nodes to verify certificates with all features of public blockchains.
4. REMME is service oriented organization that provide services on development and implementation of private/hybrid sidechains for businesses and services of certificates provision on own public blockchain (on-going development) for public usage. Sidechain and public blockchain are not connect that allow business to have full control over their sidechain.
5. REMME DPKIX simplify certificate issue and revocation procedures with its utility token that ensure interactions in private/hybrid sidechain or public blockchain and allow REMME to fix price of certificate despite token circulation (in case of public blockchain).
6. REMME operates on IAM market that have average annual growth more than 7% till 2021 and will reach $8.2 billion, except IAM consulting market.
7. REMME have several competitive advantages over major market players that provide PKI services and address major weaknesses of their approach, but could have lo ability to cannibalize their market shares in short time due to absence of wide adoption, legacy systems connections and lack of skilled specialists on the market.
8. Several blockchain-based solutions with DPKI could be a direct competitor to REMME, but only one of them using X.500 family standards for access, while others oriented on authentication services.
9. Key target clients of REMME can be divided on users of sidechain and users of public blockchain, where major ones is manufacturing and consumer products respectively.
10. There are several limitation of market expansion with financial services, professional services and healthcare due to insufficiency of current legislation regarding blockchain and utility tokens usage.
11. REMME strategy could be based on its strengths that are cover all weaknesses and market threats.
12. Key strengths of REMME solution are:
    - Usage of widely adopted and understandable X.509 self-signed certificates on device level with DPKIX that have improved fault resistance.
    - Simplified revocation technology with simple identification of certificates that are compromised.
    - Availability of hybrid/private sidechain and public blockchain configuration for DPKIX that enable ability of business to penetrate market with passwordless identification and access of its customers.
    - Mix of identity and certificate root validation for access.
    - Ease of migration and no need of pre-existing PKI.

2. Review of REMME solution business model

2.1. High-level overview of REMME business model and solution

REMME solution based on utilization of 3 major technologies that are applicable for advanced IAM services:

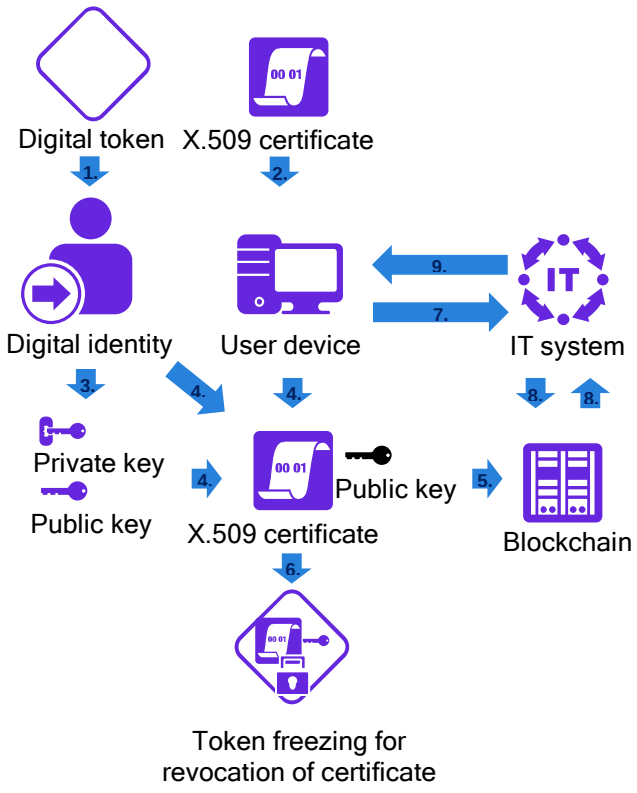
- Public blockchain
- Private/hybrid sidechains[1]
- Digital certificates of identity signature (SSL/TLS) in X.509 standard.

REMME solution is using unique ability of blockchain technology of "double spending attack" with the use of utilization token in public/private network environment.

Utility token is dedicated to special purposes digital token that is key to access blockchain network and instrument to provide information to data tables. Generally, utility tokens are annihilating in case of their usage, but in case of REMME solution due to predefined lifecycle of digital certificates related to each token, they are freezing for certain period of time in unspent blockchain transaction.

To provide more clarification in REMME business model, it is useful to indicate model of user identity in peer-to-peer (P2P) self-signed digital certificates transfer in public network and central certificate issuer-to-user (CCI2U) in private/hybrid sidechains. In figure 1 provide high level overview of P2P IAM with self-signed certificates.

Figure 1. REMME high-level business model



To address logic of business model, there is a description of key steps in solution:

1. **Obtain digital token of REMME environment.** This provide user ability to obtain digital identity in REMME environment and provide additional data for future certificate to be indicated in blockchain.

2. **Certificate distribution.** At this step REMME provide X.509 certificate that have predefined structure to include information about user that will enable verification of him on blockchain.

3. **Key pair generation.** To enable verification of digital identity of user, he/she must generate unique pair of keys (private to store and public to transfer). While private key will be used to sign messages and create digital

[1] Sidechain (both private and hybrid) is a way to implement blockchain that is a public open-source technology. Key difference that sidechain could be configured is such way that it have no need in IT infrastructure that provided by external users. That mean development of quasi-decentralized blockchain, where level of decentralization can be limited by some central authority or by limits of intranet in business IT infrastructure. Despite similarities, sidechains is not a blockchain in their widely adopted definition, even in case of hybrid sidechain (data of sidechain per some amount of blocks transmitted to public blockchain with aim to have up-to-date point to recover sidechain in cases of successful attacks or failure of whole IT infrastructure).

footprint of user, public key is using to provide verification that signature was made with pair private key, without revealing the last one.

4. **Certificate signing.** User fill certificate with all needed information and sign it with his private key. This signature will be used to verify identity with public key, when other information is used for certificate root verification and its permissions management.
5. **Publishing of certificate in blockchain.** This step is one of the main differences from centralized approach. Together with certificate data publishing in blockchain (that is replacing centralized Lightweight Directory Access Protocol as server, other centralized instances and comply with X.500 family standards) there also provided hash value[2] of public key. This value will help system to stop verification for access in case when there is a wrong public key provided to dedicated certificate.
6. **Revocation token freezing.** To ease certificates management, certificate publishing in blockchain always supported with specialized transaction of digital tokens to user that remain unsigned by user until certificate valid. After certificate expiration and without user sign, this transaction also expire. If this transaction is not in the list of blockchain, certificate will treat as invalid. This is one of utilization features.
7. **User requests connection with IT system.** When used want to access to the any IT system, the last one will activate verification of users certificate. In standard approach, IT system verify certificates with trusted certification authority, but in this case IT system address request to blockchain. During this process, IT system obtain users public key and certificates metadata.
8. **Request on verification in blockchain.** To verify users' certificate and his/her digital identity, IT system use received information about certificate and public key to find corresponding certificate in the blockchain. If revocation token is not utilized, certificates data and public key hash value are match, than blockchain check or signature in certificate is made with private key of digital identity that provided public key to IT system. If verification succeed, that blockchain inform IT system that this user is an owner of certificate and public key.
9. **Establishing access.** With verification from blockchain, IT system could grant access of user to the system data.

This approach is the same for CCI2U configuration when company distribute certificates for its clients, but data in certificate could be different due to dedicated usage of it. In case when company distribute certificate to its employees, could be used hierarchical structure of certification and organization will sign certificates instead of employees.

Description of REMME solution features follow next approach:

- Description of blockchain features that utilized in solution
- Comparison of pure utilization tokens with digital token in REMME environment
- Description of features utilized in private/hybrid sidechain configuration
- Comparison of REMME solution with centralized Public Key Infrastructure (PKI) solutions with and without digital certificates

[2] Hash value is an immutable string with predefined length that represent any data. To receive the same value with hash function it require the same data as an input to this function.

2.2. Key features of blockchain technology utilized in REMME solution

Most valuable features of blockchain technology introduced in Bitcoin blockchain and its most popular followers for REMME solution are next:

- Improved distributed hashed tables (DHT) technology
- Consensus protocol for data processing and storage machines (nodes) on data changes
- Determination of data transfers prerequisites (SMART-contracts)
- Depersonalized quasi-anonymous digital identities
- Transparent and accessible history of cryptographically protected data transfers
- Interoperability with all platforms

Improved distributed hashed tables (DHT) technology

DHT technology is widely in use for secure storage of information in decentralized systems. In system where data presented in hash value and distributed by portion on decentralized servers (nodes) network. Data in tables connected by hash values (hash addresses) in each table and protocol of search is finding a least root to target data following references from server to server based on closest value available on reached node to the target value. Blockchain is improve this technology through several changes in technology that presented in table below.

"Double spending attack" is key problem of decentralized storing and changing of information in DHT. This mean that any user, who obtain access to data storage, could designate information to one user to another and persuade the system that this new information is valid. In centralized systems, this avoided by central trusted party that provide arbitration of data, but also became single point of failure in case of attack. Blockchain technology by its design address this challenge.

Table 1. Differences of DHT and Blockchain technologies

Feature	*DHT*	*Blockchain*
Data storage	Data stores on distributed servers in tables	Data stores in digital tokens and stores at user who own this token in that particular time
History of changes storage	Data changes store on server where changes are made, this server also transmit to other nodes changes in case when hash structure is change	All data changes (transfer, transaction of token) store on every node in full amount and writes in form of blocks
Root to find information	Least way to server with target hash value in his table through following references from accessible node	Least block that contain target hash value, all other blocks with this hash value contain useless information for data search
Permits to change data	Server that store part of database where changes are making is the only who permit to introduce changes	Randomly chosen trusted node or node that first solve task on finding hash value of permission – depending from consensus protocol
Resistance to node failure	If node fail, part of data stored there will be lost/unreachable	If node fail, other nodes able to restore whole database
Resistance to unpermitted data changes	Unpermitted data changes on relevant node will compromise entire DHT	Unpermitted data changes can be indicated by conquering node. Compromised block is rejecting. Compromised node is penalizing/excluding from system

Key comments to the table 1:

- Blockchain does not store data as itself; it is store current address and ownership of digital token that can contain any data. Amount of stored in token data depends on blockchain configuration and capacities.
- Through exploring blockchain, user could see data in token only if he have such permission.
- Data transfer in blockchain named transaction due to nature of such transfer – users make transaction of digital tokens. For blockchain data transfer and token transaction is particularly the same definitions.
- During tokens transaction blockchain utilized all tokens from input address and annihilated it – this transaction input. At output it generate tokens with ownership of transaction recipient address (Spent transaction output or STXO) and, if value of transaction lower than amount on input address, it generates remain number of tokens with ownership of input address (unspent transaction output or UTXO).
- Annihilation of all tokens at input is a core feature to prevent "double spending attack", all previous blocks with this token in them treated as container of invalid ownership. To change ownership address in previous block, attacker need to write in blockchain new blocks on top of compromised one with timestamp newer that the last written block of original chain.
- Consensus protocol is core prevention measure from writing of new blocks on top of compromised one.

Due to absence of any proofs that available blockchains were compromised it their core and due to absence of standard of their cyber-security audit, there is no way but to trust that this technology provide security of mention above threats. Despite of that, while protection from "double spending attack" for applicable period have no failures, there are several other attacks have place for blockchain that not an option for DHT. Those attacks related to consensus protocols and described in related section of report.

One of solutions that utilized DHT technology for decentralization of PKI is a KeyChains. This solution related mainly to Pretty Good Protection approach in "web of trust". Idea behind is to create chain of self-signed certificates issues by user and verify by other users that we trust. That mean, if new user try to obtain connection with his certificate and this certificate already connected with other that we trust, so system could trust this user and grant his access.

Comparison of PKI based on DHT with REMME solution of PKI based on Blockchain provided in table 2.

Table 2. Differences of DHT and Blockchain enforced PKI

Feature	*KeyChains*	*REMME*
Certificate identity	Certificate identity root distributed between all users in certificate chains	Certificate identity on all nodes in last block where it mentioned
Verification	Local Minima Search protocol used to find link of certificate with trusted one	Certificate and public key metadata used to verify signature of private key owner
Root to find information	Roots in distributed chains till the generation certificate	Address of blockchain user in last applicable block
Permits to change data	User could change his chain of keys	Randomly chosen node from accessible and allowed nodes
Resistance to node failure	No nodes, only users. If search fail to reach next user, certificate will treat as not trusted	If node fail, other nodes able to restore whole database of certificates
Resistance to unpermitted data changes	Unpermitted data changes could by indicated by users, chain will be broke	Unpermitted data changes can be indicated by conquering node. Compromised block is rejecting. Compromised node is penalizing/excluding from system
Interoperability	Systems must understand and accept certificate type	API friendly system that allow certificate interoperability

Regarding table 1, key benefits of REMME solution on blockchain for businesses are:

1. Ability to interact with wider number of platforms with API
2. Reduced time to check certificate root
3. Ability to rely on own verification nodes as well as on trusted ones
4. Ability to save certificates hierarchies and full roots in case of any certificate revocation.

Consensus protocol for data processing and storage machines (nodes) on data changes

Currently available blockchains are using wide variety of consensus protocols that could be group by its origin:

- Variations on Proof-of-Work (PoW) protocol
- Variations on Proof-of-Stake(PoS) protocol
- Variations of mixing PoW and PoS protocols

Proof-of-Work protocol considered as most stable one and its variations are a major family among blockchains. Under this protocol nodes (and miners to enforce them) receive special tasks to solve at time when block is creating. Tasks is the same for all of them and an idea is to use “rude” force of computational power to find hash value that is lower than target value in the block metadata. The first node/miner that solve this task will obtain ability to valid a block and transmit it in the network. According to this approach, blockchain network have assurance that nodes have some computational power and utilize it for network needs. Major weaknesses of this protocol is 1) useful only work of successful node, other computational power make a competition but not utilized by network, 2) nodes that gain more that 50% of computational power could corrupt entire blockchain and lead other nodes by root with compromised blocks in them.

Proof-of-Stake protocol is a more or less new approach in blockchains, but with wide varieties of implementation. Under this protocol, node must deposit funds (stake) and amount of blocks she will valid equal to share of its stake among other nodes stakes. Some variations apply rule of major vote on block validation (more that 75% of stakes must sign the block). In case when node validate block with compromised transactions in it, stake of this node will be took off and divided between system users or other nodes. Security and reliability of this protocol in public blockchain is not proven and key implementation are at early stage. On the other side, PoS protocol is extremely useful and in times more efficient in private/hybrid sidechains.

REMME as a specialized blockchain as a business-oriented solution have critical requirements:

- Speed of digital token transaction and block creation is a key priority
- Predictable costs to run network
- Transparent and trusted nodes

Table 3 show key features of PoW and PoS protocol and REMME requirements

Table 3. Differences of PoW and PoS protocol in comparison with REMME requirements

Feature	*PoW*	*PoS*	*REMME requirements*
Speed of transaction	Limited by time of block creation	Instant	Instant
Speed of bock creation	Predefined average time, but cannot be instant	Close to instant	Instant
Costs predictability	Unpredictable. Depends from external nodes investments in hardware	Unpredictable. Depends on amount of stake provided by nodes	Predictable
Nodes transparency	Nodes anonymized and anybody can became node	Node partially transparent and access limited by ROI on stake	Transparent nodes with limits to access (private/hybrid version) Partially transparent with strict limitations on access

Regarding table 3, REMME requirements closer to features of PoS protocol. To address differences, REMME is using PoS like protocol, also named Proof-of-Service. Under this protocol, in private/hybrid sidechains will be predefined list of nodes that will handle and process entire blockchain. In public blockchain will be list of nodes that will process transaction and create blocks and access will be obtain only after depositing certain amount of funds (stake). To avoid disproportion of power between nodes, for verification of transactions they will chose in random order.

Determination of data transfers prerequisites (SMART-contracts)

SMART-contracts is special ability of blockchain technology (in full capacity firstly introduce in Ethereum blockchain) to determine prerequisites for transaction. In other words, it is ability of blockchain to execute any business logic in software like manner. To deploy such feature of blockchain it requires using special libraries and allowing in blockchain core execution of loops. Those libraries and loops could became key point of failure for blockchain to secure ownership – attackers could use them to implement malicious code and obtain private key of user.

REMME core (based on Hyperledger Sawtooth[3] framework) by design cannot support SMART-contracts in its environment and have no related to it threads. On the other hand, in hybrid sidechain and in public blockchain implemented feature of cross-blockchain gate. This is a feature of some centralized process, when one or several nodes could read other (for example Ethereum) blockchain and replicate those transaction in REMME chain. For users that want to use SMART-contracts this feature could be applied.

Depersonalized quasi-anonymous digital identities

Blockchain never use data about personality of user, at least in pure form, and presenting his digital identity as an address. Such depersonalization of digital identity is essential for quasi-anonymity of blockchain on one side and enable system serve for real peoples and IoT objects on equal level.

REMME utilize this feature for its solution. As digital certificate could be signed by peoples and by machines it make area application area wider. It is also help to avoid limitation on personal data usage (such as Unified Data Protection Rules in EU). Private Key and certificate signature is belong only to one instance (human or robot) that makes system reliable and significant competitive advantage for REMME over standard PKI solutions.

Transparent and accessible history of cryptographically protected data transfers

Blockchains by design is a transparent and accessible to public or to members of private network. As it mentioned before, it does not contain any personal data and store entire history of digital tokens transactions. All data stored in tokens is cryptographically protected with widely adopted hash functions and have unavoidable permission rules.

REMME utilize this feature to store digital certificates data and set permission rules in its consensus protocol that aim to ensure that any restricted instance (attacker) obtain ability to change this information. In this architecture transparency of data is only a plus and using to verify certificates as well as check root of certificate transfers.

Interoperability with all platforms

Blockchain based solutions do not require any specialized standards to operate with data in blockchain, they are only require software that allow interact with chain. This enable IT systems verify certificates with APIs of interaction with blockchain and ensure interoperability with all platforms (Server, desktop or mobile platforms).

[3] Two business blockchain framework codebases into incubation: Hyperledger Fabric, a codebase combining work by Digital Asset, libconsensus from Blockstream and OpenBlockchain from IBM; and Hyperledger Sawtooth, developed at Intel's incubation group.

In REMME solution, each existent IT system requires only API that it can understand that enable usage of digital certificates on different devices without causing additional problems due to different system standards. For organizations with own certificates it will allow to implement central Key Management instance for all cryptographic subsystems.

2.3. Comparison of pure utilization tokens with digital token in REMME environment

REMME digital token is not pure utilization token as it is not annihilates by blockchain during execution of transaction[4]. Despite of that, digital token is a critical to protect certificates data from attacks that is one of the main features related to utility tokens.

Utility tokens in blockchain are using for:

- **Protection of system from attackers by limiting ability to make transactions.** Key example is Gas that Ethereum SMART-contact absorbing during their execution. Gas is digital footprint of computational power needed and available to execute SMART-contracts by nodes. Idea behind is in protection – theoretically, to corrupt SMART-contract, you must use more Gas that it needed to execute it and provision of Gas is always exact or lower that contract need.
- **Activate certain features of custom blockchain[5].** Key example is a usage of token as a unique key to custom blockchain/SMART-contract. When user want to interact with this system, he must provide token to activate it and token is annihilated.
- **Transfer useful information between address in secure manner.** Approach when some data contained in token and its extraction will lead to token annihilation.

In some cases, where REMME belong, those features could be obtained without digital token annihilation.

Table 4. Utility features of REMME digital token

Feature	*Level of utilization in REMME*	*Level of need in token to enable feature*	*Realization in REMME*
Protection of system from attackers by limiting ability to make transactions	Low	Low to Medium	Blockchain protected with consensus. Certificates protection requires only addresses of token transaction
Activate certain features of custom blockchain	Medium	High	Revocation of certificate and certificate status indicator activated only with depositing token that remain UTXO
Transfer useful information between address in secure manner	Medium to High	Medium to High	Token allow to transfer digital identities and verification string in blockchain

REMME digital token enable features of utilization tokens and at least one of them could not be achieved without tokens and one hardly achievable without it. This lead to conclusion that REMME digital token is an essential part of service and could be treated as utilization token, despite it is not annihilate during it usage.

[4] Commissions for transaction in blockchain is not a utilization of token. It is specialized reward for node to motivate provision of computational power to the network.
[5] Major share of blockchains have general purposes and does not use utility token.

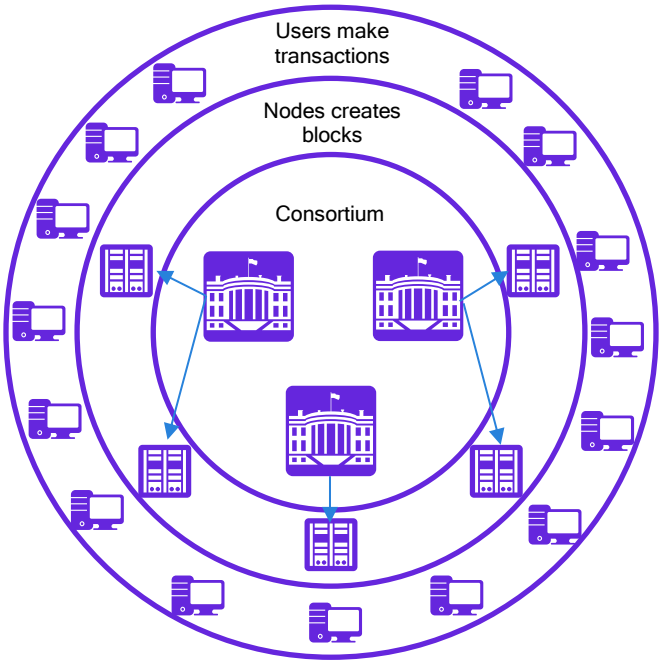
2.4. Description of features utilized in private/hybrid sidechain configuration

REMME developed on Hyperledger Sawtooth framework that enable additional flexibility of solution to create private and hybrid sidechains.

Private sidechain is a custom blockchain based on code of public blockchain, where all nodes controlled by one central organization or by consortium of organizations. In case of one organization, a custom blockchain that use features of public blockchain in organizations intranet, while consortium sidechain operates over internet connection.

Hybrid sidechain is private sidechain with anchoring to public blockchain, when each X (10th, 21th, 1000th, etc.) block of private chain duplicates in public one. In case if private chain will fail, it always have a point for restore, while without anchoring it used to return to genesis block (point of blockchain creation).

Figure 2. Private sidechain:



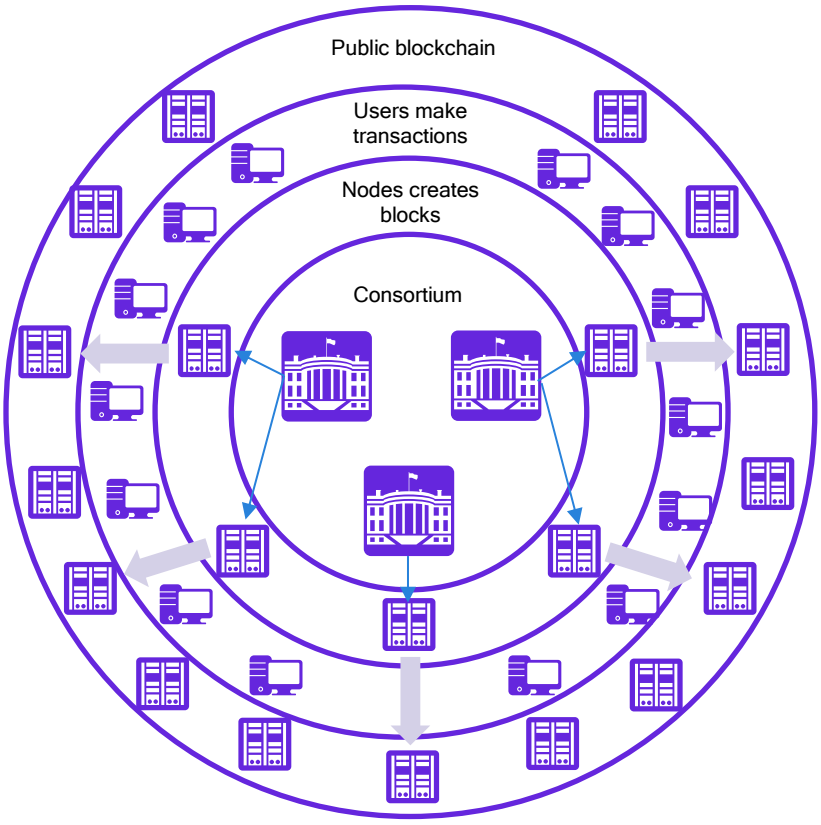
On figure 2 illustrated configuration of consortium ruled private sidechain. In this example, 3 consortium members rule over 5 nodes, where 2 members have 2 nodes each and 1 member only 1 node.

Key feature of this configuration:

1. Consortium members have agreement on blockchain consensus rules.
2. Nodes have equal rights and permissions, trust for them origin from trust between consortium members.
3. Users make transaction that are proceeding by nodes that are chose randomly or pseudo-randomly.
4. Access of any new user only with node permission.
5. Access of any new node only with permission of consortium members.
6. Costs of transactions, token price/value, format of data stored in blockchain are depends from decision of consortium members. In this configuration, nodes could process transaction without rewards and token could have no price/value.
7. Point of failure distributed on shared resources. In this case, instead of when points of failure number equal to number of consortium members, there is can be significantly bigger number of nodes that must fail to lost data by any of organizations. There is no restoration point except genesis block.

In case of one organization it will only distribution of point-of-failure that increase failure resistance of the company, but benefits lower than in case of consortium due absence of shared resources.

Figure 3. Hybrid sidechain



On figure 3 illustrated situation of the same consortium with anchoring to public blockchain. Due to open nature, public blockchain have more nodes to support system that lead to higher ability to withstand attacks on the blockchain. Consortium nodes send each Xth block to public blockchain where will be stored under cryptography particularly footprint of private sidechain current state. This configuration have all private sidechain feature and additional ones:

1. In case of failure of private sidechain it have near to current time restoration point.
2. If consortium indicates fraud of node to late, there is an option to return to more elder state stored in public blockchain.
3. To anchor information in public chain, consortium used to pay commission fee to public blockchain node that is additional costs.

REMME support and deploy both configurations to initiate, store and distribute digital certificates. It is critical to note, that REMME solution could not influence public blockchain transaction fees accept own custom public blockchain. If owner of hybrid sidechain would chose other public blockchain, he fully consider that service prices will not be fixed and predictable.

2.5. Comparison of REMME solution with centralized Public Key Infrastructure solutions with and without digital certificates

REMME solution is an approach to provide decentralized PKI with X.509 certificate standard (PKIX family).

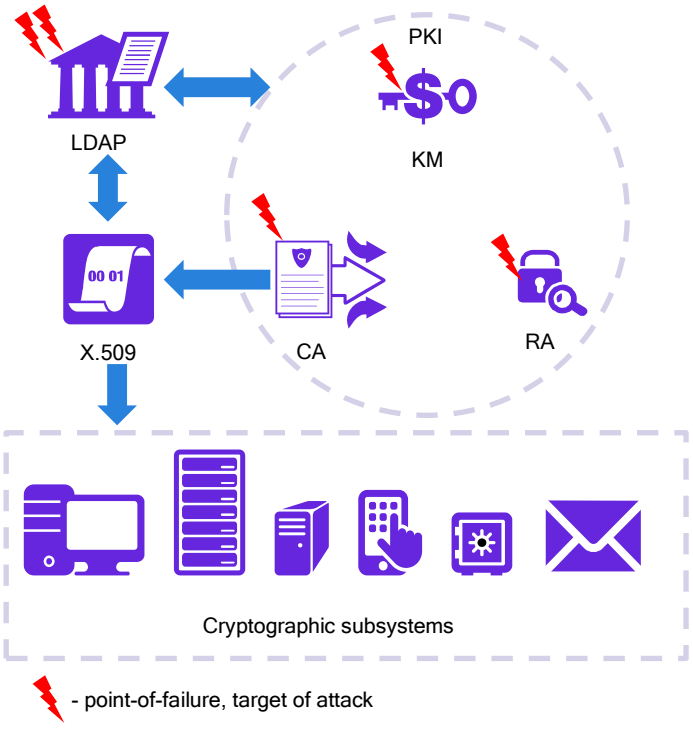
PKIX is a complicated set of sophisticated technologies, that have business value to security teams but also difficult and frustrating to implement. While each piece of a PKIX solution is moderately straightforward, the integration and management of the elements together as a system provide the greatest challenge for most organizations. The primary components of a PKIX system are:

- **Certificate authority** (CA) that issues digital certificates, a highly secure system that generates X.509 certificates for use in various cryptographic systems. Managing CA becomes a significant challenge over time. Additionally, any compromise of a CA can be devastating.
- Digital certificates are required for **authentication and encryption**. An X.509 certificatea digital certificate contains important information that can be used to validate various types of transactions. A digital certificate is a text file generated by a CA that it issues to authenticate an identity or to seed or establish encryption. A common usage of a digital certificate is to establish secure socket

layer/transport layer security (SSL/TLS) connections between websites and browsers. Most firms have allowed these certificates to proliferate unchecked. Additionally, many companies worry about certificate expiration issues. Since it can be disruptive for a certificate to expire at the wrong time, administrators have been known to create certificates with an expiration date 20 to 30 years in the future, thereby ensuring that the cert won't expire on their watch.

- A **registration authority** (RA) registers identities. This is a system that registers identities and determines the types of things that the cryptographic system will enable. An RA receives requests for digital certificates and authenticates users who are part of the system. An RA will be also be involved in revoking certificates that are no longer valid or necessary or are being used incorrectly. An RA is closely tied to the key management system.
- A **key manager** (KM) issues or revokes keys based on business requirements. The KM is the interface between the RA, the CA, and the various cryptographic subsystems that will participate with the PKI system. In the ideal system, the KM would integrate with a firm's directory, such as an Active Directory or Lightweight Directory Access Protocol (LDAP), to understand the identities of the firm's users. The KM would then issue or revoke keys based on the requirements of the business at any specific time.
- **Cryptographic subsystems** are the systems that you want to encrypt. A cryptographic subsystem is any device that must be encrypt or authenticate using a PKIX solution. Each cryptographic subsystem will need to have access to all of the PKIX components. In a traditional PKI model, there is a single CA shared by all crypto systems. In modern systems, each crypto subsystem has its own CA, RA, and KM, and each system is managed independently of each other.

Figure 4. Centralized PKIX for all cryptographic subsystems



On figure 4 indicated potential target for attack, as well as point-of-failure. To compromise all cryptographic subsystems attackers need only to disable or corrupt one of KM, CA, RA or LDAP. LDAP is the weaker point in this system as it fully centralized database of all keys and to ensure system security, replication of this data is least preferable option.

Other pain point of PKIX, is a communication between KM, CA and RA. In major cases, KM is an administrator at client, while CA is a trusted third party that have only contractual arrangements with client.

Additionally, costs of PKIX implementation at organization is not only to issue digital certificate, but also include costs of servers set up for LDAP, KM and, optionally, own RA or CA.

In most cases, costs/benefit ration of PKIX implementation is too high for major share of users.

Figure 5. Own PKIX for each cryptographic subsystem

Figure 5 illustrates approach when each subsystem have own key manager and using self-signed X.509 certificate to create hierarchy of certificates for subsystem.

This approach use X.509 hierarchical root from genesis self-signed certificate. In this case CA is operates as trusted root authority. All subsystems know Public Key of CA, system verify key chain from genesis certificate and lower-level delegated authorities could sing new certificates.

With segmented PKIX for subsystems, LDAP remains main point of failure, but corruption of it could lead only fail of security in one of subsystems.

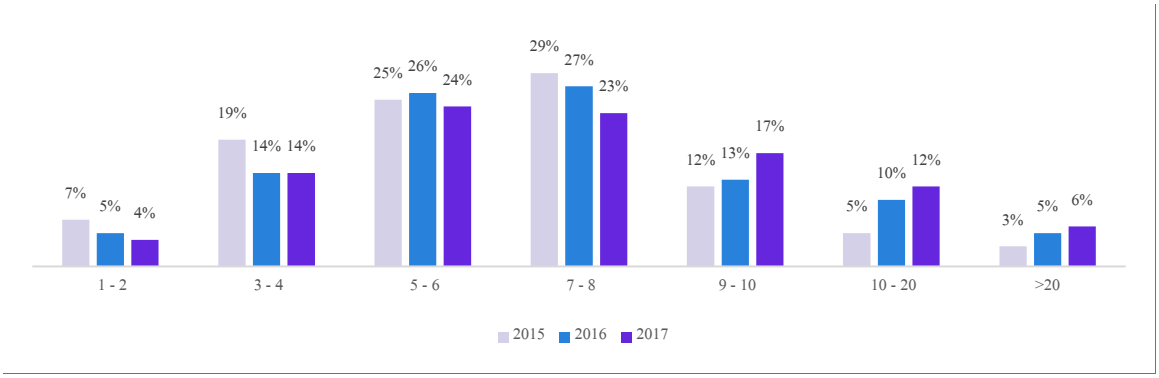
CA or root authority remain one point of failure for system, while lower-level delegated authorities point of failure for all signed by them certificates. This approach increase security of the system, but not significantly.

Costs of implementation are lower, but significant differences occur only when client decide not implement certification of all subsystem. System-by-system approach enable fast deployment of cryptographic protection on most critical systems, but lead to 2 major problems:

- Unprotected subsystems could have data or unsecure connections that enable attacker to obtain genesis certificate private key or put his certificate with fault signature in the root.
- Due to different genesis certificates and not synchronized data in all LDAPs, there is a problem of interoperability between subsystems. Some cases show that client even use different standards of certificates for subsystems genesis certificate.

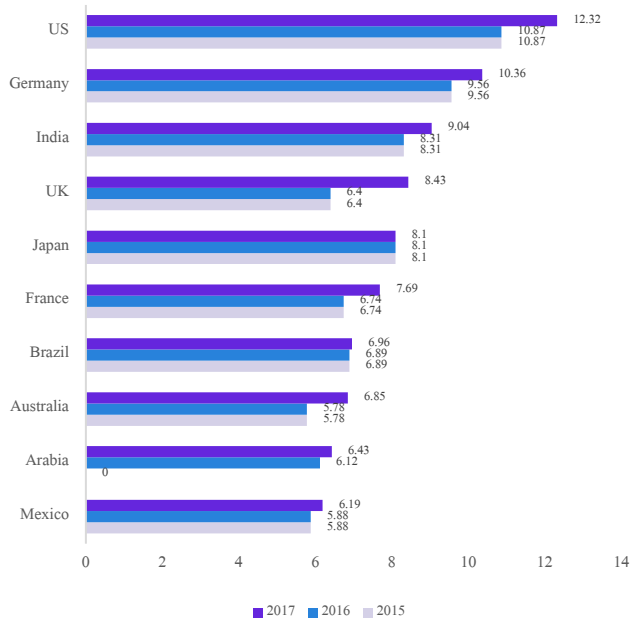
According to Thales PKI Global Trends Study, interoperability of access for subsystems is an important requirement for PKIX providers – on average businesses PKI infrastructure managing on average up to 8.5 applications and its number is growing.

Figure 6. Distribution of applications number that are managing by business PKIX certificates, 2015-2017



This distribution is not homogeneous by geographical split. US and Germany have most complicated architectures of PKIX with more than 10 subsystems to manage, more over this number is grew rapidly during 2017.

Figure 7. Average number of subsystems that are managing with business PKIX, 2015-2017



Trends in Germany, UK and France showing that security and IAM requirements are growing in Europe as well as in US. Continuous increase of architecture complexity is a major limit for wide implementation of PKIX across variety of industries.

Additionally, increasing number of subsystems to manage with PKIX could lead to breaches in whole security system of businesses. It a hard task to prioritize key subsystems to encrypt first and ensure that all links from unencrypted subsystems in secured. Human factor is an increasing concern as well as costs to have specialized staff on board even in case of external certificates providers.

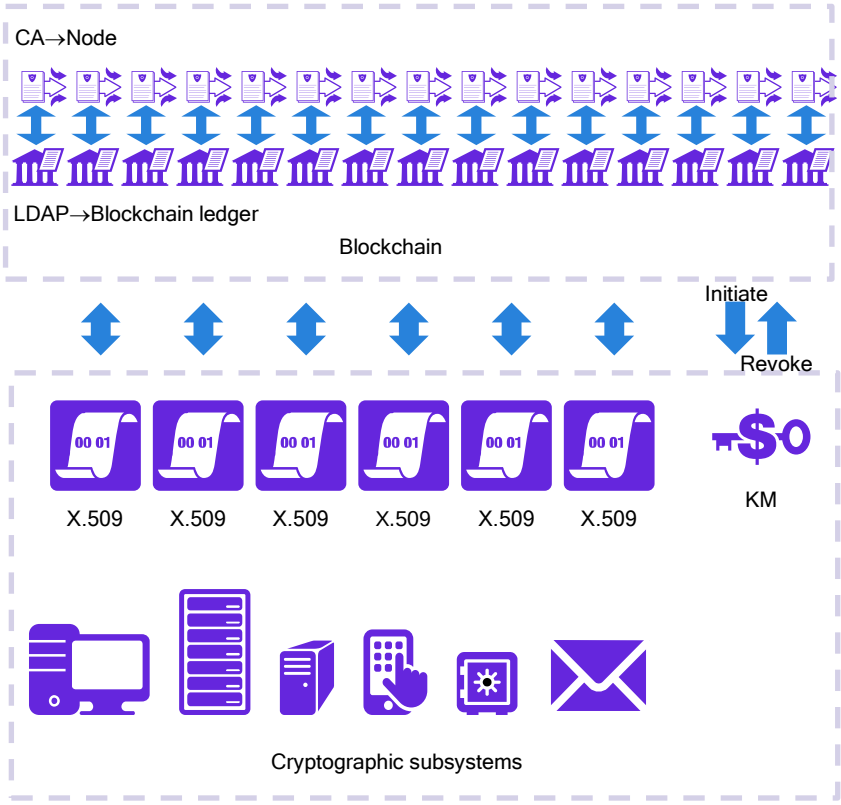
REMME solution enforced by blockchain that lead to significant changes in PKIX under both approach.

On figure 6 illustrated high-level architecture of PKIX with full centralization of KM for all subsystems. Key differences are:

- Device orientation – each device in subsystem have own genesis certificate
- LDAP replacing with Blockchain ledger, all certificates data and status migrating there
- Nodes take a role of CA, role of CA become distributed between nodes that significantly reduce threat of CA failure
- All nodes have the same copy of Blockchain ledger (analogue of LDAP), no single point of attack on database or unpermitted changes without noticing of it
- Due to Blockchain abilities each node verify signature and certificate root together that increase trust to signature (2-factor verification)
- Key management limited only with initiation of certificate and its revocation with transaction

Despite lack of evidences of Blockchain absolute fault-resistance and out-of-class level of security, by design and logic REMME solution improve standard PKIX through distribution of points-of-failure in classical model. Additionally, it could be more user friendly: instead of deploying of expensive infrastructure, hire teams of cryptographers and storage of massive LDAPs user nee only initiate certificate on each device and sign it.

Figure 8. Standard PKIX in REMME solution



Self-signing certificate, traditionally, costs more that his ancestors. This mean, that average cost of certificate in traditional PKIX system for each device will be lower. Otherwise, REMME solution do not require initial investments for infrastructure deployment as well as reduces costs on support and maintain those systems.

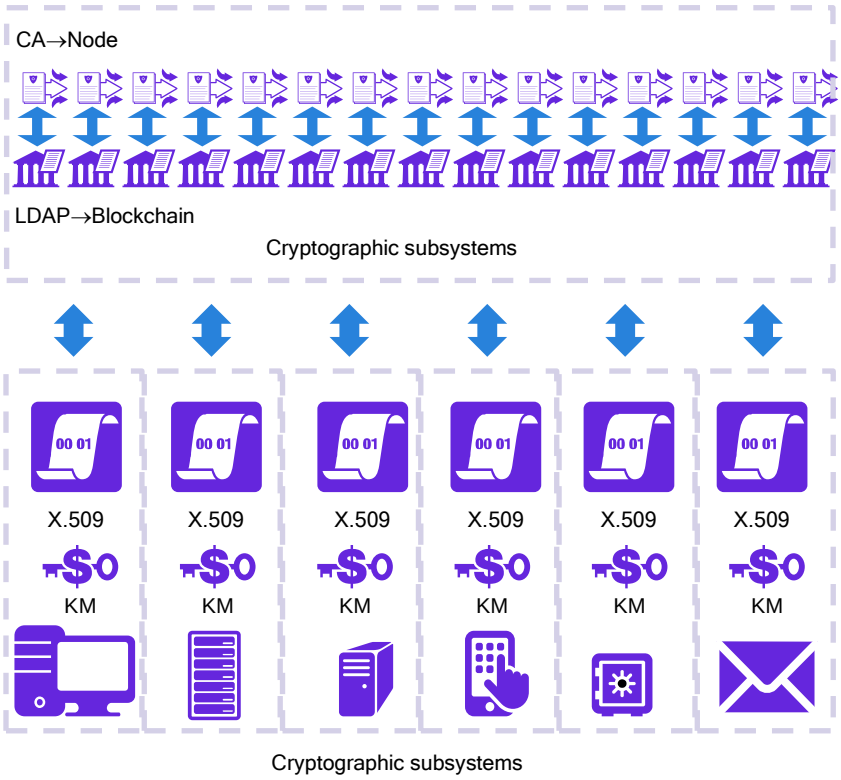
It is recommended to use financial projection to ensure that REMME or standard PKIX more expensive with inclusion of all costs, not only on average certificate price.

On figure 9 illustrated REMME architecture in case of separate key management of subsystems. As it mentioned before, REMME already provide public and root verification, so there is no significant difference from previous model.

This approach only implement several trusted Key Managers that have REMME digital tokens to initiate and revoke certificates in their subsystem. This is more reliable model that previous one due distribution of management rights. In previous model KM is a the most weak point, if attacker obtain it private key it could revoke all certificate that will cost an organization the full cost of new certificates. In addition, this system decrease time of indicating new unidentified certificate and revoke it, if attacker will try initiate new certificate with KM Private Key.

Additionally, this architecture address challenge of interoperability. Blockchain ledger store certificates data in universal manner, certificates of different standards are converting in Blockchain ledger standard to be stored. This enable implementation of APIs to interact with certificates from different subsystems.

Figure 9. Own KM in REMME solution for every subsystem



Blockchain enable universality of solution by implementing interoperable technological layer reachable trough APIs for any platforms.

There are solution of PKI without digital certificates that based on network of users signature. It named Pretty Good Privacy (PGP) standard and related “web of trust” – network of user that trust each other signatures. As it mentioned before, it is similar to KeyChains solution on DHT tables, but instead of certificate verification it verify that user signature was previously connected with signature of user we trust. This system similar to root authority, but it have no central authority to verify root, user by himself check and verify it.

There is no digital certificate, CA, KM, RA and LDAP. Only digital signatures and their roots are matter. Each user can use certify keys for further certification of signatures. It could reduce verification time and cost in comparison with DHT root authentication. Additionally, this approach allow using trusted third party web sites to verify signatures.

This model is something in between of PKIX and REMME solution. Despite long history of existence, PGP have several disadvantages that limiting its wide adoption:

- There is no unified standards of digital signatures that rise interoperability problem
- Signature root could be transparent only at the moment user receive request on connection
- It is social-network like approach to verify signature and have the same treats as a profiles in social networks
- Very high dependence from human behaviour, trusted user could be turned in attacker without any notification that will lead to whole root compromising

Table 5. Comparison of traditional PKIX, root authorities, PGP and REMME solution approach

Element of PKI	*PKIX*	*Root authority*	*PGP*	*REMME*
LDAP	One LDAP per system	Multiple LDAPs, one per subsystem	No LDAP	LDAP replaced with Blockchain ledger, one copy per node/user
CA	One centralized CA	One centralized root authority	Multiple CA, each user is a root authority	Multiple CA, each node is a CA
KM	One KM per system	Multiple KM, one per subsystem	Multiple, one per user	One or multiple, one per subsystem or user
RA	One centralized RA	No RA	No RA	No RA
Certificate standard	X.509, X.500	X.509	No certificate	X.509
Major point-of-failure	LDAP, CA, RA, KM	CA, KM, at some extent LDAPs	User	KM
Major cost components	CA/KM/RA infrastructure, support, services	CA/KM infrastructure, support, services	Digital signature, no support, no services	Certificates, support, services

In table 5 provided summary on comparison of REMME with traditional PKIX solutions with and without digital certificates. REMME solution enable ability to use both certificate and its root verification without any centralized authority and keys databases. It also implement transparency of certificates roots that increase probability of timely indication of any attacks and frauds together with interoperability that make it more advantageous than PGP.

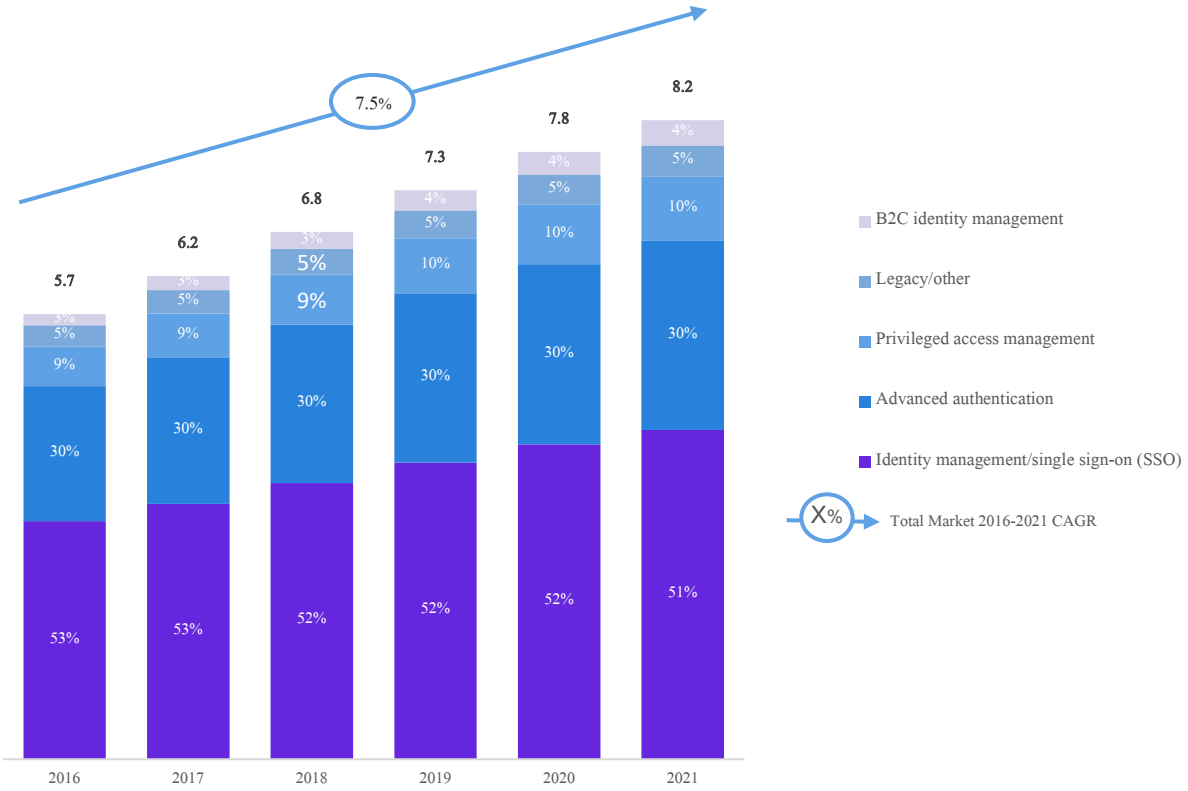
3. Market, competitors and potential clients overview

3.1. Identity and Access Management market overview

Digital certificates and PKI subsector is a part of Advanced Authentication sector that belongs to Identity and Access Management (IAM) market. To this market also relates B2C identity management, Privileged Access Management and Identity management/Single sign-on (SSO). Some legacy systems remain in operation on this market as well.

IAM is a significant submarket of entire cyber-security market worldwide. According to International Data Corporation (IDC) in 2016 total market size was $5.7 bln with 7.5% growth pace per annum till 2021.

Figure 10. Forecasted worldwide IAM revenue (billion USD), market share (%), five-year CAGR (%)



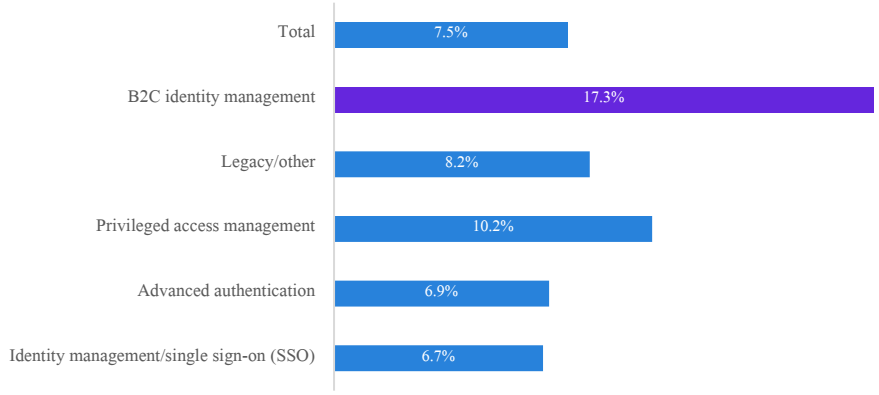
Identification and access management (IAM) market is expected to grow for the next 4 years from $6.2 billion in 2017 to $8.2 billion in 2021. The largest segments of IAM will remain Identity management / single sign-on (SSO) submarket (51% of the worldwide market). The second largest submarket will remain Advanced Authentication (30% of the worldwide market).

There are sub segments of the market, that will grow with different pace:

- Identity management/single sign-on (SSO) sub segment will grow on average 6.7% per year. This management approach under which customer could obtain access to all system with one GUID and password.

- Advanced authentication sub segment will grow on average 6.9% per year. This is a management approach where user is using additional to password (or instead) credentials (incl. biometric information, 2-factor authentication, etc.) or rely on passwordless technologies such as digital certificates and PGP.
- Privileged access management (PAM) will grow on average 10.2% per year. This is a management approach when user obtain access to predefined (pre-ordered) systems after provision of his/her credentials. Additionally, only administrator permission have rights to access to the user session with system.
- Legacy systems support market will grow on average 8.2% per year. 5% of market share in 2016 revealing that significant part of businesses continue to improve their IAM systems.
- B2C identity management will grow on average 17.3% per year and boosting with growth of e-Commerce and on-line services. This type of IAM approach is similar to previous ones, but it is public (anyone could obtain access) and have significant specifics in back-end configurations.

Figure 11. Forecasted IAM market segments CAGR for the period 2016-2021, %



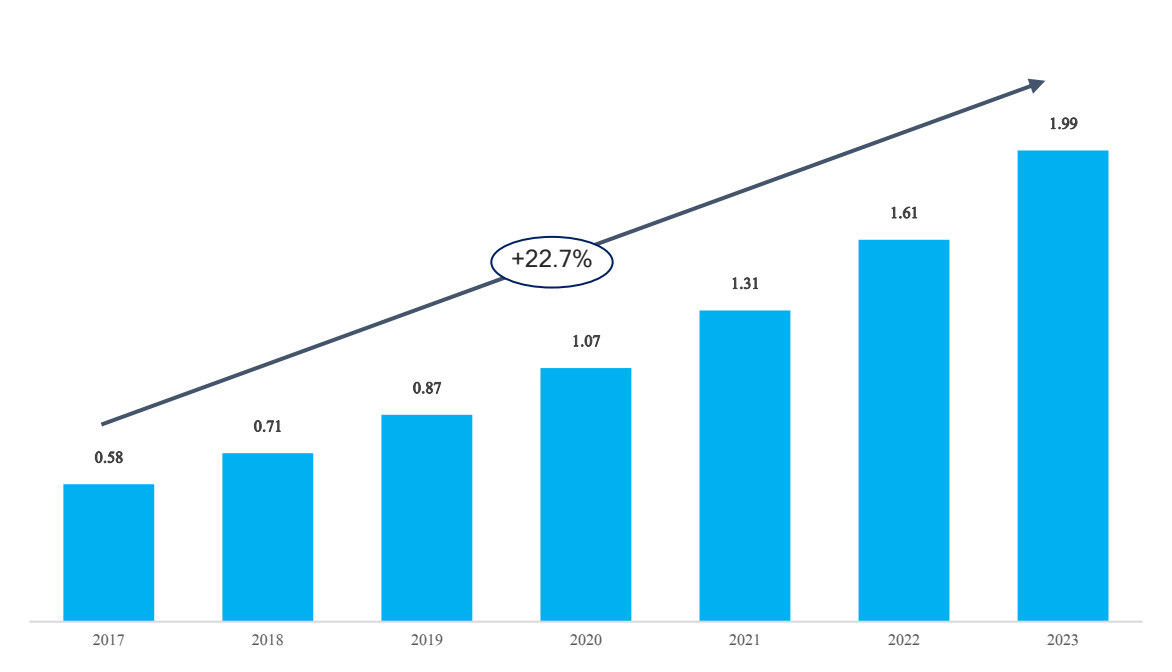
The B2C identity management (B2C) is the smallest submarket of IAM (3% of the worldwide market in 2017). However, its CAGR is the highest in the market (17.3% for the period 2016-2021), which exceeds the overall IAM growth rate (7.5% for the period 2016-2021).

B2C identity segment growth boosting with growth of e-Commerce and cloud based services. This segment is hardly penetrate with traditional PKIX due high costs of infrastructure, but easily accessible by PGP like IAM technology, where REMME could be placed.

By architecture approach and with variety of applicable configurations, REMME solution could cannibalize any of those segments, especially targeting on B2C identity and SSO. By primary competitive market for REMME is a sector of Advanced Authentication in device-system IAM solution. It is no need to compete with providers of User-Device IAM solution of Advanced Authentication (OTP, biometrics, etc.), because 2-Factor Authentication implemented in REMME aim to utilize strength of those technologies.

Accept User-Device IAM, major share of Advanced Authentication technologies is a traditional PKIX.

Figure 12. Global Digital Certificates and Public Key Infrastructure forecasted market revenue (billion USD) and six-year CAGR (%)



Public Key Infrastructure (PKI) type of solutions has a growing trend. They are expected to grow from 0.58 billion USD to 1.99 billion USD in six years form 2017. In 2017 PKIX subsector value is only 31% of all Advanced Authentication technologies value, in 2021 it share in sector will be up to 53%.

This growth mainly drives through implementation of new approaches in PKIX and increasing need of advanced cyber-security features. Additionally, rising interest to cryptography due to cryptocurrencies drive improvement in understanding of cryptographic protection for wider number of users. REMME strategy is to use the momentum and cannibalize share of its competitors and of new market share.

3.2. Key competitors overview

It were identified 3 main tiers of competitors for REMME:

- Tier 1: PKIX service providers
- Tier 2: PKI for Digital signature service providers
- Tier 3: Other IAM services providers

The vendors in the PKI market either issue Certificates on their own or provide users with PKI management tools. The prices for the first type of service vary widely; they depend on contract's duration, number of domains and number of users.

The second type of service can be tailored according to the business needs. Thus, the prices are available only upon request. PKI management tool allows users to control the full life-cycle of Certificate issuance. Vendors offer two- or multi-factor authentication; so that users are able to choose what type authentication they want to use.

Table 6. Tier 1: Key players operating in the global PKI market

Name	Solution	Type of certificate	Type of implementation	Types of authentication	Price	Service	Lifecycle management for business
REMME	Digital certificates with DPKI on blockchain	SSL/TLS (X.509)	On premises, private/public, hybrid	2FA (OTP messages, Software and hardware tokens	1 USD per certificate and services upon request	Available	Available
Comodo Group Inc.	SSL Certification PKI and Certificate management tool (simplifies digital certificate issuance and lifecycle management)	SSL/TLS (X.509)	Cloud	-	from 99.95 EUR per domain per annum	Available	Available
Kofax Ltd.	Electronic Signature Transfer Mailroom automation tool Communication server	SSL/TLS (X.509)	On premises, private/public cloud, hybrid	OTP SMS	Upon request	Available	Available
GMO GlobalSign Inc.	Transferring electronic signatures SSL Certification PKI management tool (Certificate lifecycle, billing, and user management within cloud-based platform)	SSL/TLS	Cloud	VPN, Smart card logon, USB tokens	from 249 USD per domain per annum discounts and corporate rates apply	No	Available
Verisign Inc.	SSL Certification DNS management tool	SSL	Cloud	-	Upon request	No	Available
Gemalto N.V.	Encryption key management tool (consolidates and centrally manages encryption keys, passwords, and certificates) Certificate-based applications (digital signing, network logon and password management) PKI management hardware (usb, cards)	SSL/TLS	On-premises, cloud or hybrid	OTP, Software and hardware tokens	Upon request	Available	Available
Ascertia Company	Transferring electronic signatures PKI management tools (certificate issuance, certificate lifecycle management)	SSL/TLS (X.509)	On-premises or cloud	Hardware token as an addition to certification	For e-signatures: from 12 GBP per month and corporate rates apply	Available	Unknown
Entrust Data Card Corporation	SSL Cerification PKI and Certificate management tools (encryption, digital signature and certificate authentication) PKI management hardware (cards)	SSL/TLS (X.509)	On-premises or cloud	varies from hardware tokens to mobile push OTPs	from 122 USD per domain per annum discounts and corporate rates apply	Available	Available
Identrust Inc.	Transferring electronic signatures SSL Certification Identity authentification tools (identity vetting, administration, validation, certificate manufacturing and storage) PKI management hardware (USB, cards)	SSL/TLS (X.509)	On-premises or cloud	Hybrid PKI/OTP Token, Smart cards	from 75 USD per domain per annum discounts and corporate rates apply	Available	Available
GoDaddy Inc.	SSL Certification	SSL/TLS	-	-	from 43.99 GBP per domain per annum discounts and corporate rates apply	No	No

Table 7. Tier 1: Key players operating in the global PKI market scoring in comparison to REMME

Name	Support of DPKI	Type of certificate	Type of implementation	Similarity of authentication types	Price distance	Service availability	Lifecycle m-nt for business	Score
Comodo Group Inc.	-2	2	-1	0	2	2	2	5
Kofax Ltd.	-2	2	2	1	0	2	2	7
GMO GlobalSign Inc.	-2	2	-1	2	-2	-2	2	-1
Verisign Inc.	-2	2	-1	0	0	-2	2	-3
Gemalto N.V.	-2	2	1	2	0	2	2	9
Ascertia Company	-2	2	0	2	1	2	2	7
Entrust Data Card Corporation	-2	2	0	2	-1	2	2	5
Identrust Inc.	-2	2	0	2	1	2	2	7
GoDaddy Inc.	-2	2	-2	0	1	-2	-2	-5

Table 7 is an another representation of table 6 with scoring methodology applied on it. In this table indicated that Tier 1 competitors not all capture market with similar to REMME features. Solution with similar features (except blockchain DPKIX), could we obtained from Gemalto, Kofax, Ascertia and Identrust. Comodo and Entrust Data Card are more neutral that direct competitors to REMME.

Table 8. Tier 2: Key vendors of electronic signature transfer service based on PKI globally

Name	Solution	Type of signature	Type of implementation	Types of authentication	Price	Service	Lifecycle m-nt for business
REMME	Digital certificates with DPKI on blockchain	SSL/TLS (X.509)	On premises, private/public, hybrid	2FA (OTP messages, Software and hardware tokens	1 USD per certificate and services upon request	Available	Available
Docusign Inc.	Electronic Signature and Payment Transfer	SSL/TLS (X.509)	Cloud	E-mail based, access code, SMS, Federated Identity, Phone,Third-Party, Social Identity, Knowledge-Based, Geolocation Capture	from 10 USD per month discounts and corporate rates apply	Available	Available
Signix Inc.	Transferring electronic signatures	SSL	Cloud	E-mail based, Knowledge-based, SMS-based, pass-through, supplied questions	from 10 USD per month discounts and corporate rates apply	Unknown	Unknown
Secured Signing Limited	Transferring electronic signatures	SSL (X.509)	Cloud	OTP SMS	from 9.95 USD per month and corporate rates apply	No	Unknown

It is possible to distinguish companies that provide only electronic signature transfer service in the cloud on the basis of PKI. Such solutions can be integrated into existing communication systems or used independently (as a feature of PGP). They have to provide highest security levels, because users' electronic signature makes a document legally binding.

Table 9. Tier 2: Key vendors of electronic signature transfer service based on PKI globally scoring in comparison to REMME

Name	Support of DPKI	Type of certificate	Type of implementation	Similarity of authentication types	Price distance	Service availability	Lifecycle m-nt for business	Score
Docusign Inc.	-1	1	-1	2	2	2	2	7
Signix Inc.	-1	1	-1	2	2	0	0	3
Secured Signing Limited	-1	1	-1	1	2	-2	0	0

Table 9 reveille that Docusign Inc. could be, to some extent, direct competitor of REMME solution. Signature services closer to PGP that also make Docusign Inc. a potential threat to REMME solution in term of market shares.

It useful to have high-level overview of key challenges related to standard PKIX solutions and REMME positioning regarding them.

Figure 13. Key challenges for PKI implementation in 2017

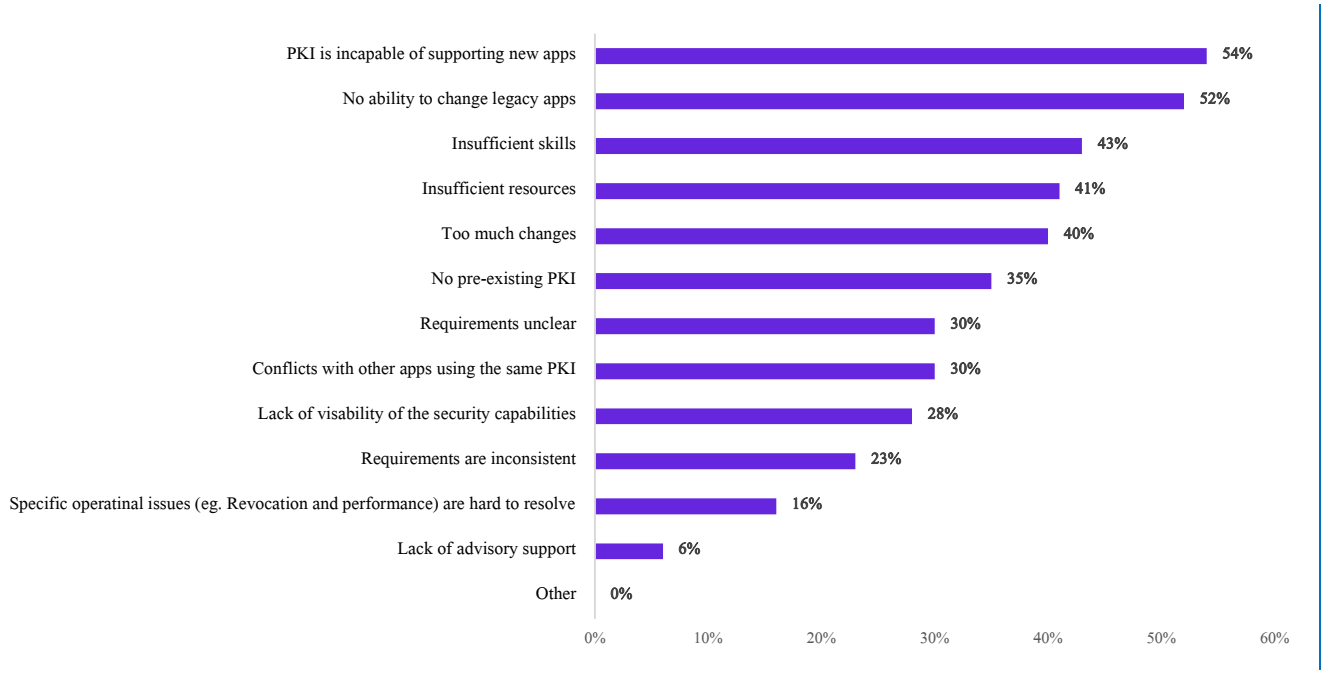
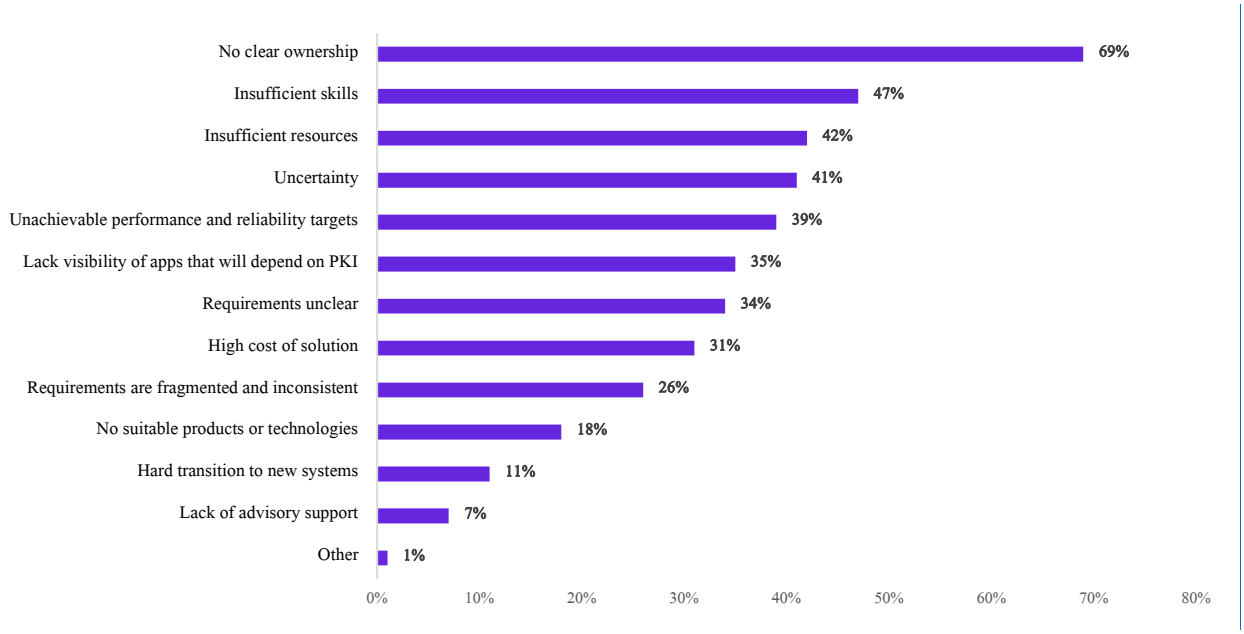


Figure 15. Key challenges of deploying and managing PKI in 2017:



In table 10 enclosed summary of REMME abilities to address those challenges that are familiar to major competitors.

Table 10. REMME features regarding key challenges of PKI providers:

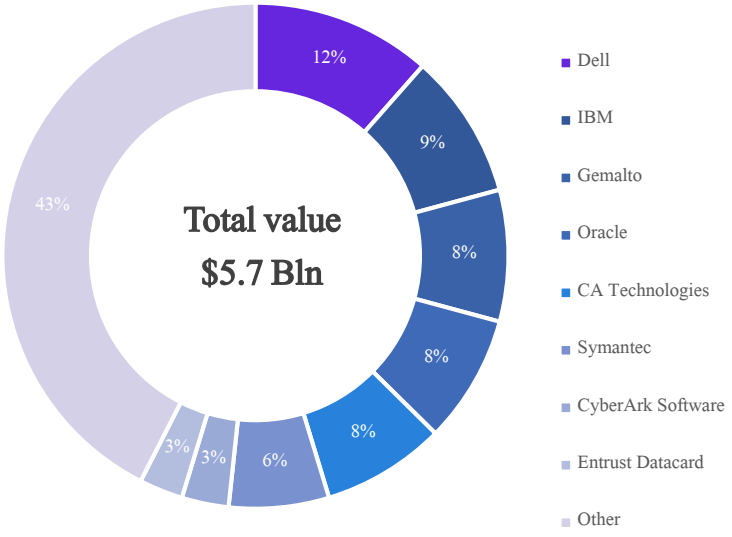
Challenge	*REMME ability to address*	*Level of competitive advantage*
No clear ownership	Using self-signed certificates ownership of which will in transparent and accessible blockchain	High
Existing PKI is incapable of supporting new apps	API like interoperability system, the only requirement is to support X.509 certificate	High
No ability to change legacy apps	Device level security system, there is no need in legacy apps	Medium
Insufficient skills	Hardly addressable due to novelty of technology	Low
Insufficient resources	Using external resources of nodes, no need of pre-existent infrastructure	High
Uncertainty	Remain the same	N/A
No pre-existing PKI	Do not need any pre-existing PKI	High
Unachievable performance and reliability	Achievable due to usage of external nodes	Medium
Lack of visibility of apps that will depend on PKI	Remain the same	N/A
Unclear requirements	Minimum requirements for systems	Medium
Conflict with other apps using the same PKI	Interoperability via blockchain with API will reduce conflicts	High
High cost of solution	Depends on client solution architecture	Low
Inconsistent requirements	Due to novelty of the system, not all requirements are tested	Low
Lack of visibility of security capabilities	Due to novelty of the system there are some biases of business to security capabilities of blockchain	Medium
Specific operational issues (eg. revocation and performance) are hard to resolve	Revocation process is simplified and does not depends from any providers	High

Challenge	REMME ability to address	Level of competitive advantage
No suitable products or technology	Blockchain could address additional abilities to solve problems that depends of Client case	Medium
Hard transition to new system	Solution requires only legacy certificates that lead to simplified transition to new solution	High
Lack of advisory support	Due to novelty of the product and company, currently could be insufficient	N/A

REMME could address main challenges that are existent for major PKI solutions providers. Key strength of solution regarding its competitors are transparency of certificate and PKI ownership, interoperability, external provision of resources, easy of transition and revocation.

Various vendors of other IAM products that could be competitors to REMME and other PKI-based solutions. It is useful to understand key market players and level of their involvement in advanced IAM subsegment.

Figure 16. Worldwide IAM Market value (billion USD) and segmentation by key vendors (%) in 2016



There are lot of other significant players on IAM market that belongs to tier 3 competitors.

Dell and IBM hold largest shares of the AIM Market, 12% and 9% respectively of the overall market. IAM market value was 5.7 billion USD in 2016, which is 11% higher, than in the previous year. More details on revenues, solutions and specification of services of top-10 IAM vendors are provided in the table below.

Most of the vendors provide both cloud-based and on-premises solutions, which can be customized according to company's preferences. In many cases, customization is limited to specific options instead of fully built-in solutions. Some companies also offer consulting services in order to help users to identify business needs and choose the appropriate solutions.

Table 11. Key vendors in the worldwide IAM Market (excl. Gemalto and Entrust Datacard)

Company	2016 Revenue M USD	2016 Share (%)	Growth (%)	Security Solution	Cloud or on-premises	Types of authentication	Service	Lifecycle management for business
Dell	655.4	12%	-2.7	Identity Governance Access Management Priviligged Account Management Identity and Access Management as a Service	Cloud, on-premises, hybrid	OTP: hardware, software, SMS, phone call	Available	Available
IBM	531.5	9%	4.1	Cloud Identity: IDaaS Family Access Management family Identity Governance and Management family Security Service family	Cloud, on-premises, hybrid	vary (biometric, hardware tokens, geolocation)	Available	Available
Oracle	469.4	8%	-3	Identity Cloud Service Identity Governance Access Management tools	Private and public cloud, on-premises or hybrid	Knowledge-based, OTP SMS, bypass code, fingerprints	Available	Available
CA Technologies	451	8%	2.4	Identity Management Application and Payment Security (Priviliged) Access Management Identity as a Service	Cloud, on-premises, hybrid	Federated SSO OTP SMS or e-mail	Available	Available
Symantec (Has Verisign as a subsidiary)	368.4	6%	4.7	VIP Access Manager Enterprise-grade authentication	Private and public cloud, on-premises	Static Risk Authentification Mobile Push Notification Hardware and Software Tokens, SMS, Biometrics, and more	Available	Available
CyberArk Software	170.9	3%	21.8	Enterprise Password Vault Priviliged Session Manager Priviliged Threat Analytics Application Identity Manager	Cloud, on-premises	Tokens, OTP solutions, Smart Cards behavioral biometrics	Available	Available
Okta	153.4	2.7	107.3	Adaptive Multi-factor Authentication Lifecycle Management Universal Directory API Access Management	Cloud	Full range: SMS, Voice, E-mail, OTP, Physical tokens, Biometric factors	Available	Available
SailPoint	131.6	2.3	59.9	Identity Analytics Data Access Governance Identity platform	Cloud, on-premises	Security questions and answers, text, voice, and email	Available	Available
Micro Focus	131.3	2.3	-2.9	Identity Governance & Administration Access Management Privillege Management Change & Configuration Management	Cloud, on-premises, hybrid	Challenge/response, OTP, biometric, cards	Available	Available
ForgeRock	101.5	1.8	32.7	Identity Management Access Management	Cloud, on-premises	Fingerprinting, one-time password, and adaptive risk authentication	Available	Available

Scoring methodology is not applicable to their 3 competitors due huge differences of their business model with REMME one.

Some services also provide decentralized PKIX with blockchain technology, where Emercoin is most advanced one due to availability of own fully deployed public blockchain network. Other services is mostly Ethereum based custom SMART-contracts (in form of quasi-sidechain of Ethereum) and fully depends from his abilities.

Regarding to this, in table 11 showed brief comparison of REMME, Emercoin and Ethereum caracteristics.

Table 12. REMME, Emercoin and Ethereum based solutions comparison

Charcteristics	*REMME*	*REMME (Bitcoin based version)*	*Emercoin*	*Ethereum based*
Consensus	Proof-of-Service	PoW	Mix PoW, PoS	PoW, in future PoS
Time for Block generation	<1 min	~10 min	5-7 min	Unpredictable[6]
Price	Fixed in USD	Bind to current transaction fee	Volatile, bind to token price	Volatile, bind to token price
Additional fees	Only for anchoring	No	No	Gas prise
Instant transactions	Yes	No	No	No
Token utilization	Partially utilize	No, but provide some utility feature	No	Depends from SMART-contract

Below, provided characteristics of key blockchain-based competitors of REMME.

Table 13. Key vendors of blockchain-based IAM solutions

Project/ Feature	Evernym	Cambridge Blockchain	Civic	Authy	Uport	Rivetz	Blockstack	Autoreon	REMME
Blockchain base/ framework	Hyperledger Indy	Cambridge Blockchain	Ethereum	N/A	Ethereum	Rivetz TEE	Browser with access to virtual blockchain	Ethereum	Private/Hybrid Hyperledger Sawtooth, REMME blockchain
PKI	No	No	No	No	Yes	No	Yes	No	Yes
Payments bind to fiat	N/A	N/A	Yes	Yes	N/A	No	No	No	Yes
Support of the two-factor authentication	Yes	Yes	Yes	Yes	Yes	Yes	No	No, changed by double dynamic key	Yes
Platform Application	Windows	Multiplatform	Mobile platforms	Mobile platforms and Windows	Mobile platforms	Mobile platforms	Mac, Windows, Linux	Multiplatform	Main browsers and OS
Passwordless authorization	Yes	N/A	Yes	No	Yes	Yes	Yes	Yes	Yes
IAM subsector	Authorization	Authorization	Authorization	Authorization	Authorization	Authorization	Authorization and access	Authorization	Authorization and access
Price	N/A	N/A	$2.95	No unique price	N/A	N/A	No unique price	N/A	$1/certificate
Type of certificate	No certificate	No certificate	No certificate	No certificate	No certificate	No certificate	X.509	No certificate	X.509
Services (customize)	No limitations	No limitations	Limited	No limitations	Limited	No limitations	No limitations	Limited	No limitations
Lifecycle management for business	N/A	N/A	Yes	N/A	Yes	Yes	N/A	Yes	Yes
State of development	Pilot version	Developed	Ongoing improvement	Ongoing improvement	Ongoing improvement	Developed	Ongoing improvement	Ongoing improvement	Ongoing improvement

[6] Ethereum at pike time process alone almost 50% of all transactions in all blockchains.

There are numerous solutions related to IAM services on blockchain, but major share of them oriented on authorization sub segment and only one competitor is using X.500 family certificates for PKI. Results of similar to previous scoring approach are below.

Table 14. Key vendors of IAM solutions based on blockchain scoring in comparison to REMME

Project/ Feature	Evernym	Cambridge Blockchain	Civic	Authy	Uport	Rivetz	Blockstack	Autoreon
Blockchain base/ framework	-3	-3	-1	0	-1	-2	-2	-1
PKI	+3	+3	+3	+3	-3	+3	-3	+3
Payments bind to fiat	0	0	-3	-3	0	+3	+3	+3
Support of the two-factor authentication	-3	-3	-3	-3	-3	-3	+3	0
Platform Application	+3	-3	0	-2	0	0	0	-3
Passwordless authorization	-3	0	-3	+3	-3	-3	-3	-3
IAM subsector	+2	+2	+2	+2	+2	+2	-2	+2
Price	0	0	-1	+1	0	0	+1	0
Type of certificate	+3	+3	+3	+3	+3	+3	-3	+3
Services (customize)	-2	-2	+2	-2	+2	-2	-2	+2
Lifecycle management for business	0	0	-2	0	-2	-2	0	-2
Score	0	-3	-3	2	-5	-1	-8	4

Blockchain-based systems are closer competitors for REMME, but only 2 of those solutions could be trated as direct competitors. Users are able to choose best solution based on his own perception and with understand of all advantages and disadvantages of each solution.

4. Potential clients and target sectors

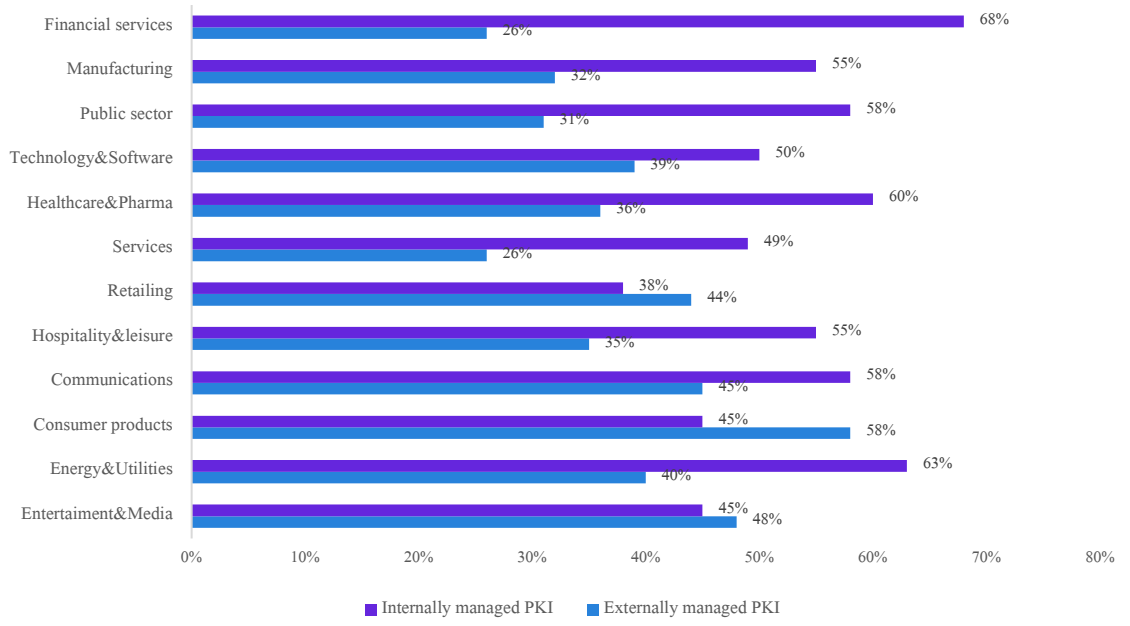
4.1. Key trends and target industries selection

Interest in identity management, encryption, and key management products is surging in Europe and expected increase significantly in the United States as enterprises seek to meet the spirit of the European Union (EU) General Data Protection Regulation, which takes effect in May 2018. GDPR provides for data protection for all individuals within the European Union and protects the export of personal data outside the EU, with the goal of giving citizens and residents control of personal data. GDPR requirements will drive demand for many security products including IAM. IAM is driving market revenue, growing the next five years, from $5.7 billion in 2016 to $8.2 billion in 2021.

From a managed security service (MSS) perspective, organizations are embarking on a digital transformation journey, which is changing how they operate and deliver services to their customers. The Internet of Things also provides a significant opportunity for IAM and other data security and identity management solutions as the number of sensor-equipped and network-enabled devices are skyrocketing. It is need to provide the infrastructure and robust management software required to manage encryption keys and digital certificates used to protect sensitive information, authenticate connections between systems and users, and validate the authenticity of software updates.

In 2017 according PKI Global Trends Study of Thales there are various approach to PKI and PKI-like solutions deployment. Industries in general can be divided on those who are oriented on internal control of certificates and those who are preferred external hosting of certificates control.

Figure 17. Key industries that using PKI and PKI-like systems and distribution of internal and external approaches

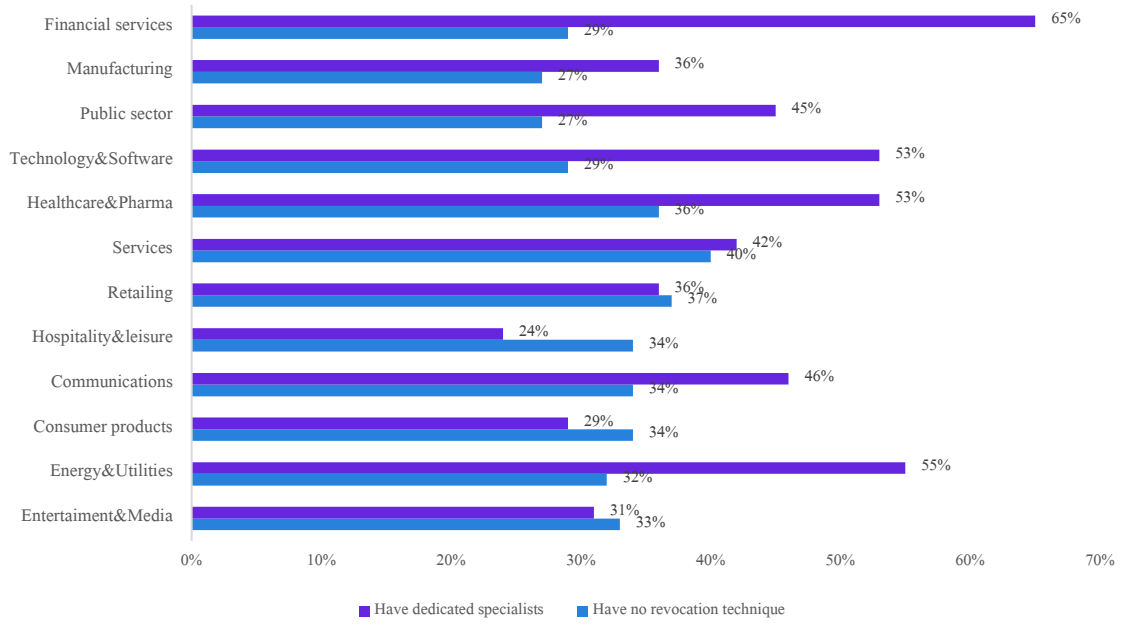


REMME solution currently mostly oriented on private/hybrid sidechains that are internally controlling by business. External control of certificates will be applicable when public blockchain will deploy in full capacity (it is now under development). At that phase of the services development key industries are financial services, manufacturing, public sector, technology and software, healthcare and pharma, services, hospitality and leisure, communications, energy and utilities.

Other sectors are also could be clients of REMME at this stage, but number of services for them are limited. After full deployment of public blockchain those sectors will benefit most of external access verification with resources of nodes.

Each sector have different disciple and resource availability of specialists. Below provided share of companies with dedicated staff across industries. Additionally, as ease of certificates revocation one of key competitive advantages of REMME, provided share of companies that have not implemented revocation technologies across industries.

Figure 18. Share of companies that have dedicated PKI specialists and share of companies without revocation technology deployed



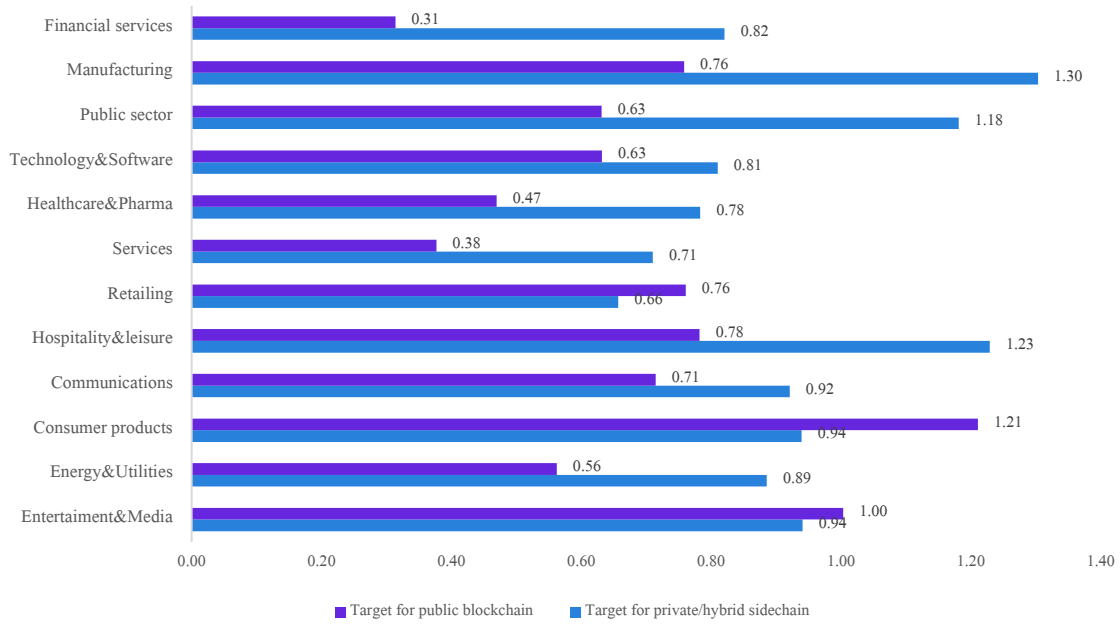
Presence of dedicated specialists on-board mean high level of investments in PKI utilization. Such companies more addicted to legacy and implemented system and could have some issues regarding staff reduction in case of migration. Due to this, under potential clients selection it better to treat as an additional limitations for REMME to provide its services in those industries. On the other side, those specialists are the one who understand limitations of current PKI providers and could be valuable advocates for system migration.

Companies without revocation techniques in place are key potential clients for REMME. Those companies have significant vulnerability in their PKI and hardened management of certificates and, considering competitive advantages of blockchain solution, they will benefit mostly from migration on new DPKIX.

According to information provided above, it is possible to make ranking[7] of industries that could benefit most of migration on REMME solution public or private/hybrid one. Regarding it, key target sectors for REMME are manufacturing, public sector, hospitality and leisure. While major targets for public blockchain will be consumer products, entertainment, media and retail.

[7] Ranking done by multiplying share of external/internal control on share of companies with dedicated specialists and divided on share of companies without revocation technique.

Figure 19. Ranking of industries that will benefit most from private/hybrid sidechain and public blockchain of REMME



Manufacturing is a growing driver for IAM services, and PKI especially, due to Internet of Things, where managing of access include not only human-to-system, by also human-to-robot, robot-to-robot, robot-to-system, system-to-robot that itself mean complication of PKI infrastructure and increase of access apps in more than 4 times.

Public sector becoming an important driver for PKI and IAM services due increase of regulatory environment in developed and developing countries. 2017 was a defiantly a year of new cyber threats and up to 70% of them are related to access management vulnerabilities.

Consumer products industry demand on IAM services is driving by consumer mobile experience, especially when SSL certificates are using for public facing websites and services. Personal cabinets could contain vulnerable private and financial data of user and SSO technique have limited ability to address growing threats. On the other side, management of publicly distributed certificates is one of the most hardest tasks for current PKI infrastructures.

It is worth to point out, that several sectors are hardly achievable targets for REMME. In most cases it is financial sector, services, healthcare and pharma. Reasons for it lying in nature of those businesses, while it is easy to implement transparent DPKI in those businesses for internal systems that in use of their staff, it is not always a good idea to make the same for their clients' access. Blockchain, to stay in legal environment, remain as quasi-anonymous. You could not reveal identity of person by open the database, but you always can apply Big Data analytics tools to analyze connections of blockchain address to identify personalities by their patterns and transactions tracks.

In case of finance, specific legal and professional services and healthcare price of privacy (in financial and reputational terms) are very high. Regarding to this, it will be useful to improve DPKI with additional features that will separate addresses of those services users from addresses those users have to access to other systems. It will be in cost of interoperability and will require additional time and costs on implementation. This motivation is staying behind key customers' industries prioritization.

Additionally, those industries, and technology and software could be add to this, have additional requirements to be comply with Unified Data Protection Rules (UDRP) of EU. It used to have additional

layer of certificate purchasing regarding need to inform that information from certificate will be in use of blockchain that is support by specialized nodes, especially in case of public blockchain.

According to this, REMME better to use service oriented model with prioritization of clients regarding possible configuration of the system.

Table 15. Priorities of industries that will benefit mostly form particular solution type

Priority	*Private/Hybrid sidechain*	*Public blockchain*
1	Manufacturing	Consumer products
2	Public sector	Entertainment and media
3	Hospitality, leisure and travel	Hospitality, leisure and travel
4	Consumer products	Retailing
5	Entertainment and media	Manufacturing
6	Communications	Communications
7	Energy and utilities	Public sector
8	Financial services	Technologies and software
9	Technology and software	Energy and utilities
10	Healthcare and pharma	Healthcare and Pharma
11	Services	Services
12	Retailing	Financial services

Based on applications area of certificates, REMME solution could provide most of its benefits for:

- development of one-point of access for uses in case large numbers of subsystems;
- application of certificates for public facing websites and services;
- establishing of access to private network and VPN;
- device and robots authentication;
- enterprise user authentication;
- access to public/private cloud-based applications and services

It is could be an improvement for email security, document/massage signing and code signing, but that not a core business lines of REMME that not tend to be a straight competitor of advanced systems in those areas.

4.2. Advantages and disadvantages of blockchain empowered solutions

Blockchain refers to the distribution of data held and updated individually by each participating system or node in the network. The database is replicated, shared, and synchronized across these systems. The way Blockchain differs from a usual server-client system is the absence of a centralized server or system to process and store the data. Imagine having a spreadsheet, instead of being stored in a shared drive, each client stores its own spreadsheet with the same contents. When a change is initiated, a consensus between all systems in the distributed network is met before the update takes place. In a Blockchain environment, records are updated and stored at each of the systems independently. The systems also continually check and reconcile the data to ensure consistency.

Blockchain works with trust and permissions depending on the setup of the network to maintain the integrity and security of the data within. In an open or public setup, anyone can connect and make changes to the data within the network. In the case of a private Blockchain, only trusted participants are included as part of the network. Permissions to read and write will also be allocated accordingly. This allows individual sets of data to be validated separately and compared to ensure integrity.

One of the technologies leveraging on Blockchain is smart contract. Smart contracts are a set of predefined actions programmed to be executed when specific conditions are met. The processing of smart contracts

is usually done by the network of computers in Blockchain. In short, Blockchain provides trusted storage capabilities, while smart contracts provide trusted transaction processing capabilities using Blockchain as the skeleton.

A prerequisite for smart contracts to operate effectively is the accurate predefining of contractual terms to be agreed upon and programmed as the conditions of execution in the smart contracts. This will ensure that the self-executing smart contracts process the transactions according to requirements. Any intermediaries required for such transactions can be removed, and human intervention on the processes will also be eliminated, providing a more efficient and error-free process.

REMME as Blockchain empowered DPKIX system reflects all pros and cons of Blockchain technology. SMART-contracts is not implemented in this solution directly (in form as in Ethereum blockhain), but could allow their usage trough gates.

Blockchain and smart contracts were created to enhance the security and efficiency of data recording and processing. The following are some of the main advantages of Blockchain and smart contracts:

- **Transparency.** All participants of the Blockchain will have access to the logic of the smart contract; this provides transparency to what is being agreed in the digital contract. Transactions are also recorded to provide a clear audit trail.
- **Integrity.** Records are reconciled against each other to ensure that no unauthorized changes are being made.
- **Durability.** As records are not controlled by a single system, there is no single point of failure in the entire Blockchain network. This makes a Blockchain network more durable and robust.
- **Resource reduction.** With Blockchain and smart contracts acting as middlemen or agents, resources and time taken for transactions can be reduced. This is especially so in the case of smart contracts in which predefined conditions are agreed upon, and a self-executing process takes place once these conditions are met.
- **Eliminating errors.** With all nodes on the network processing the transactions individually, updating and reconciling the records, errors in calculations can be omitted.
- **Improved fault-tolerance to DDoS.** One of the features blockchain offers is the mitigation of distributed denial-of-service (DDoS) attacks. This is done by offloading the pressure on capacity by sharing the resources in the chain. However, beyond the infrastructure of the blockchain, DDoS attacks are still a threat especially when it comes to the applications or components of services that are not within the blockchain itself.

Limitation and Potential Challenges:

- **Legal and regulatory requirements.** With the nature of Blockchain and smart contracts, legal and regulatory compliance might be a challenge for certain industries. The top concerns in this aspect include where data are stored geographically, are they compliant with data sovereignty laws, are terms and execution of smart contracts legal in court, and so forth. This will be exceptionally challenging, especially in the public and financial sectors, in which technology and security are highly regulated.
- **High implementation cost.** Even though Blockchain and smart contracts will help reduce the operating cost in the long run, it will be costly for organizations to set up an entire private Blockchain. A decentralized network will mean that investment for more nodes has to be made. Smart contracts, on the other hand, will incur a high initial cost for the development of the contracts itself. This will be tied to the next challenge – the effort required for smart contracts.
- **Extensive list of predefined conditions (smart contracts).** Depending on the context of the agreement, the list of predefined conditions could be a long one. This will in term incur more resources during the testing and implement phases.
- **Insufficient adoption rate (nodes and cryptocurrency).** Organizations looking at starting a public Blockchain may face the limitation of low adoption rate. Although there are readily available networks, such as Ethereum, some organizations may wish to start a Blockchain from scratch, and

they will need enough participants in the network. An imbalance on nodes and data might result in performance issues. The other factor contributing to this limitation is cryptocurrency. Should a project involve new cryptocurrency, enough investors must be involved to raise the required funds.

- **Integration issues.** Blockchain and smart contract solutions require a significant change to the infrastructure and operations. Organizations should factor in the cost and effort involved when deciding to adopt Blockchain and smart contract solutions. Other than the technical integration, organizations will also require the buy-in of users and stakeholders to accept and reduce friction of the complete shift of infrastructure and operations.

It is critical for clients to consider those issues while they chose between blockchain empowered DPKIX, novelty DPKIX and traditional PKI/PKIX solutions. Those limitations are inevitable currently, but changes is all of that limitation areas are implementing continuously.

5. Analysis of competitive position and information about REMME

5.1. SWOT-analysis of REMME solution

REMME solution have significant number of competitive advantage and its market and feature open numerous opportunities for market expansion. Otherwise, weaknesses are also have place as well as various threats to limit it market penetration. SWOT-analysis summarize key identified issues with approximate assessment of their influence on its market positions. It was applied simple scoring model to evaluate positioning of solution on the market, where issue with high influence have 3 point, medium – 2 points, and low – 1 point. Everything summarized in figure 20.

Figure 20. Summary of REMME SWOT-analysis factors ranking

Identified 15 strength attributes of market and solution, where:

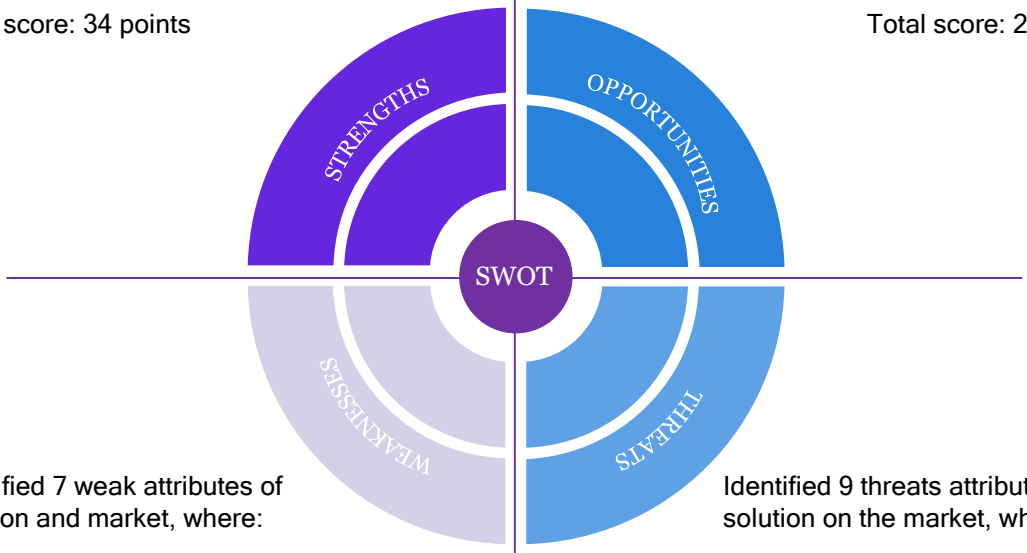
- 7 with high influence of market performance
- 5 with medium
- and 3 with low

Total score: 34 points

Identified 10 opportunities attributes for solution on the market, where:

- 4 with high influence of market performance
- 3 with medium
- and 3 with low

Total score: 21 points



Identified 7 weak attributes of solution and market, where:

- 2 with high influence of market performance
- 2 with medium
- and 3 with low

Total score: 13 points

Identified 9 threats attributes for solution on the market, where:

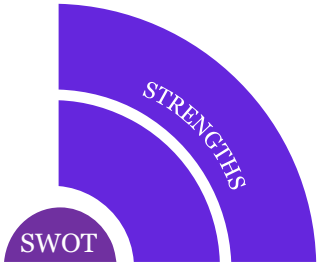
- 2 with high influence of market performance
- 2 with medium
- and 5 with low

Total score: 15 points

According to scoring of SWOT-analysis attributes, REMME have strong coverage of its weaknesses with strength (over 21 points) that determine it strategy on the market is promote strength of the solution. Additionally, regarding REMME business model 1 of 2 major threats of market (lack of skills availability on the market) will addressed with specialized learning program that will be introduce to the market.

REMME solution have significant list of strength:

- **Avoidance of data "double spending" transition in DPKIX** – blockchain (both public and private) enable ability to ensure Proof-of-Ownership for data stored in ledger that is common problem for any decentralized system.
- **Self-signing X.509 certificate** – widely adopted technology that enable uniqueness of user public key and provide Proof-of-Ownership for it.
- **Ease of certificate revocation technology** – revocation with only signing of transaction in blockchain/sidechain provide significant improvement for this technique and one of key competitive advantage of REMME.
- **Availability of hybrid/private sidechain configuration** – controlling of nodes responsible for certificates verification is a major advantage for companies that are highly appreciated security of their intranet without external third parties.
- **Mix of identity and certificate root validation for access** – solution is using 2 major techniques of certificates validation from both PKI and decentralized approaches.
- **Improved fault-tolerance of certificate verifiers** – instead of 1 CA, solution rely on multiple nodes that have equal rights and permissions, as a result, attackers must to compromise all nodes at ones as they can restore entire ledger in case of major share of nodes fail.
- **No unpermitted data change** – nodes are competitors in system and check each other when data changing, if major part of network indicate changes as suspicious and unpermitted – it will be declined.
- **Interoperability through API and API-like connection** – blockchain as technology use binary compilations and require interaction through APIs or other user environment that resulted in ability to manage certificates under open API standards instead of specialized standards of PKI providers.
- **Consortiums and anchoring** – solution could provide joint certificates management for organizations that uniting in consortiums and, additionally, provide ability to periodically write consortium sidechain "as-is" status in public blockchain that allow to recover certificates ownerships in case when consortium member compromise himself.
- **2-Factor Authorization** – additional layout for securitization of access to device that own certificates significantly improve reliability of whole solution.
- **Fixed prices of certificates** – key competitive advantage of solution over other blockchain empowered certificates management that will increase predictability and usability of solution for businesses and private users.
- **No need of pre-existing PKI** – solution rely on X.509 alone and provide open environment of its usage in blockchain that will enable users implementation of certificates without need to invest in PKI infrastructure.
- **Ease of transition** – as it mentioned above, solution do not require any previous PKI configurations, users with previously deployed PKI need only to migrate their certificates that reduce complexity of migration that is common for centralized PKI solutions.
- **Availability of deployed use cases** – solution have previously implemented versions by the team that enable ability to provide quality assurance for their platform.
- **Ability to use resources on Infrastructure-as-a-Service (IaaS) basis** – nodes could provide their computational resources to the blockchain/sidechain as an third party servers or as cloud virtual machines that add to solution features of IaaS services.



Level of influence: - High - Medium - Low

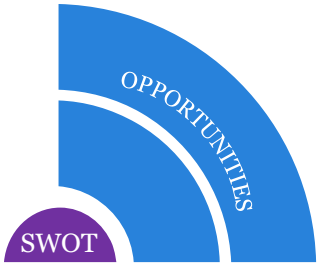
There are weaknesses that related to blockchain technology as well as to solution architecture:

- **Blockchain solution provide ability to use SMART-contract through gates only** – solution in case of SMART-contracts rely on Ethereum network that make quality of those contracts outside of control with the platform and require additional validation of them through centralized gates that could became point-of-failure in this case. 🔴
- **Ability of user identity detection through analyzing of his digital identity with addresses in blockchain** – for some industries could cause some financial and reputational threats due ability of third parties to interact with public blockchain, not related to certificates security, but could be treated as weakness versus competitors without transparent ledgers. 🔴
- **Token not fully utilized** – it is hardly to achieve, but some tokens over time could be used on second time for another user that could mislead nodes with root identification, otherwise it is small probability of that and remain token "unburned" will secure ability to control certificate price fixing. 🔴
- **Currently no direct application as digital signature** – it is possible to use, but architecture will not allow, currently, utilize solution in the same way for signatures that requiring another approach for verification. 🟠
- **Limited company resources against its direct competitors** – company currently cannot match with it resources to biggest players on the market that significantly decline pace of market expansion in near future. 🟢
- **Lack of technology knowledge from side of dedicated PKI specialists that are already available at potential clients** – solution based on cutting edge technology that do not have efficient pool of specialist in field, that can limit solution expansion for reasonable amount of time. Additionally, it is estimate to feel some resistance from those specialist to implement the solution due to necessity of some staff reduction in the future (solution will provide automation of CA and related services). 🟢
- **Legal environment remain insufficient** – solution is using widely adopted technologies of cryptography that could be certified, but several features of blockchain remaining outside legal field in many locations, especially in industry specific regulations. Additionally, several requirement of UDRP could limit implementation in some of targeted industries in EU. 🟠

Level of influence: 🟢 - High 🟠 - Medium 🔴 - Low

Solution perspective of implementation rely on its market opportunities and ability to exceed current market with additional features of product:

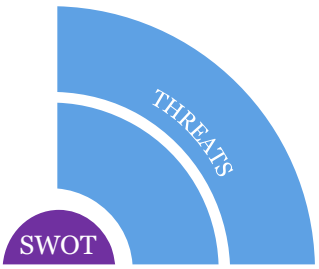
- **Solution have mix of peer-to-peer and centralized PKI architectures** – solution enable security access not only to business controlled systems, but also could be used for personal identification that enforce “web of trust” idea, but without need of trust that built on social relations.
- **Available public blockchain configuration** – business oriented on security of access for publicly available services generally could not afford reliable PKI, while public DPKIX enable reduce investments while ensure significant level of access security.
- **Availability of gate to manage SMART-contracts transaction on Ethereum** – implementation of gates between solution and Ethereum public blockchain introduce ability to use SMART-contracts for certificates distribution and automated revocation, despite absence of full control over those SMART-contracts from solution side, it is creates wide opportunities to increase business applicability of REMME.
- **Significantly high speed of blockchain transaction** – type of consensus protocol in solutions’ blockchain/sidechain resulted in huge amount of transaction processing capabilities that provide opportunity for businesses to establish secured access from scratch in several seconds.
- **Decentralization of PKIX** – ability to have transparent ownership of users certificates will lead to opportunities with businesses that do not trust current CA in centralized PKIX.
- **Device level authentication** – certificates are linked to device that provide ability to establish secured access between each particular machine/robot to any system that allow those certificates, it enable new opportunities in IoT and automation of business.
- **Fast growing market of PKIX and IAM with straight trends of disruption** – pace of growth of IAM services market revealing that that there is a lot of place for new players, while strong need of changes in PKIX services increase ability of new comers to “bite” share from established competitors.
- **Achievable requirements and target performance of the system** – solution requirements for computational power to support whole system remain low, and in hybrid/private sidechains is very low, while performance of the system does not depends of each particular device performance and could be achieved with minimal investments.
- **Growth of IoT market** – solution provide significant benefits for IoT devices access that must be easy, continuous during robots work time and manageable almost on instant basis.
- **Usage of widely adopted cryptography standard** – solution use SHA-256 function for cryptography that adopted widely in the world, understandable and comply with major certification standards that lead to opportunity of wide market coverage.



Level of influence: - High - Medium - Low

There are several threats that could be limitations for solution market expansion and should be elaborated:

- **Usage of tokens could lead to connection with cryptocurrencies** – token in solution used to provide easiness of whole blockchain/sidechain management and fast connection between user and provider of certificate, but it is use approach to transfer data as in transactions of cryptocurrencies, that threats provides to face some biases regarding it and misleads of legislation in several countries. 🔴
- **Nodes opportunistic behavior in public blockchain** – public blockchain rely on external nodes that will process all data transactions, there are strict rules and nodes competition are implemented to ensure that nodes provide services with trust of network, but threat of opportunistic behavior cannot be eliminated in any public blockchain. 🔴
- **Legacy systems domination** – solution do not connect to any legacy PKIX and IAM systems that could limit market due to affection of business to its legacy applications that already adopted on the market. 🟠
- **Low availability of skills on the market** – blockchain based solution providers facing lack of specialists with required skills on the market that could supress pace of market intervention due to limited resources of REMME to implement several solution at time and support them timely. 🟢
- **Biases against blockchain security** – due to lack of experts in field worldwide, information about security breaches of projects related to blockchain that are not in blockchain itself, lead to extrapolation of those problems on all field of technology and could raise biases of business against blockchain itself. 🔴
- **Available blockchain-based solutions with similar properties** – there are already deployed services of identification with certificates that use blockchain in their core and this will lead to tough competition with them, despite orientation on access securitization, when business adopt one of competitors service it will be hard to persuade him to change system. 🔴
- **Implementation of hybrid/private sidechain could exceed financial expectations** – implementation costs of hybrid/private sidechain can be identified on particular business case basis, it could cost a fortune in one business or be minimal in similar one. With increasing of system adoption, it would be hard to manage expectations of clients. 🟢
- **Uncertainty of SHA-256 future** – despite SHA-256, and all SHA-2 family, we are at the beginning of SHA-3 family implementation trend. Those standards of cryptography still need proofs of their security and several improvements, but with time, it could be a need to update solution with new standards of cryptography. 🟠
- **Limitations of security standards compliance** – due to novelty of blockchain, there are no certification and standardizations of it. Businesses in several industries have strict rules to comply with regarding security of their systems. Those issues will be resolved with time, but for now remain as limitation for market expansion pace. 🔴

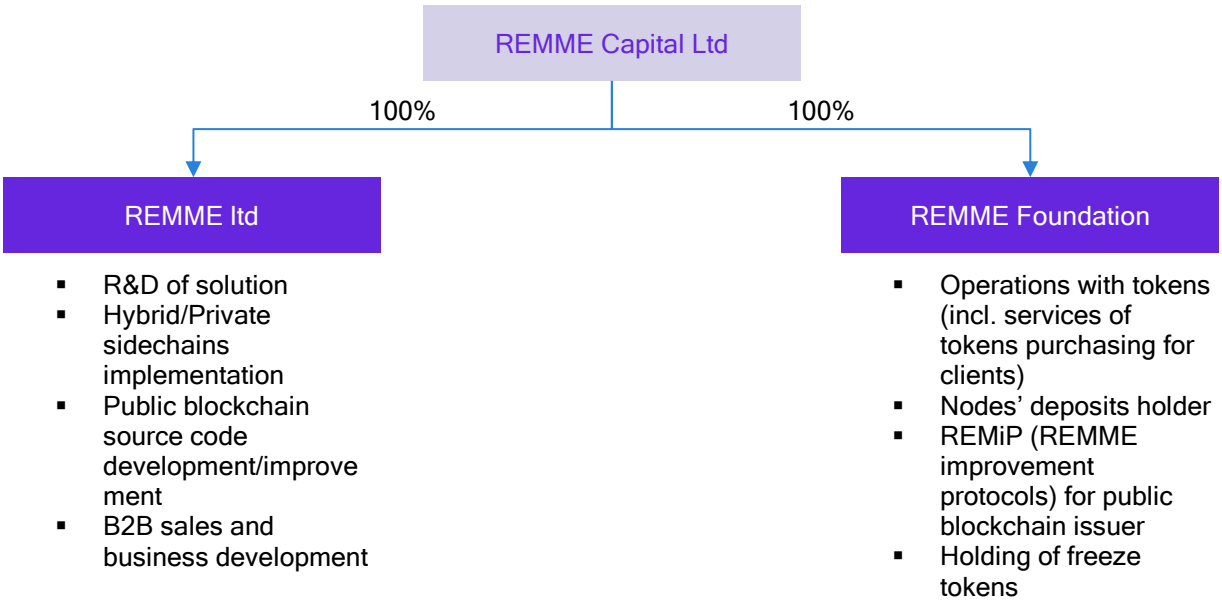


Level of influence: 🟢 - High 🟠 - Medium 🔴 - Low

5.2. Legal structure overview

REMME legal structure is simple and consist from 2 separate organizations where one responsible for services and business operations, while another one involved in REMME tokens operations. It is understandable that some clients have concerns about operations with tokens in public blockchain and REMME will support them with services on tokens purchasing trough separate organizations. It also provide ability to conduct operations in countries with different readiness of legislation regarding public blockchain tokens operations.

Figure 21. High-level legal structure of REMME and operational spit



With further development of company, there are plans to set up sales offices worldwide that will enable opportunity to arrange agreements with Client under their native legislation through direct contracting with sales offices.

remme

The Report may contain estimates of future solution performance or opinions that represent the authors view of reasonable expectations at a particular point in time. However, such information, estimates or opinions are not provided as predictions or assurances that events will occur in exact way presented in The Report. The actual performance of solution may differ from the expectations in the Report due to on-going development of platform.

Authors have not carried out any auditing procedures with respect to data provided in connection with this Report. As such, there is no additional opinion in relation to data.

Authors assumed that obtained facts and information about future platform development, along with explanations are honest and true and, as such, did not verify them independently. Authors reviewed the materials and source information to check coherence and to eliminate obvious errors.

In the course of our analysis, we relied upon information obtained from the solution Owners and from various public, market, and industries sources.

The Report constitutes a whole and none of its parts or pages should be read and interpreted without reading the entire Report, particularly its disclaimers and limitations.

Authors would like to emphasise that the responsibility for achievement of the expected results of the solution rests with the solution Owners.

This Report has been prepared solely for the purposes described in the Authors and REMME ltd and may not be used, in whole or in part, for purposes other than those included in the Agreement. Agreement conducted with all needed KYC and RM procedures from both sides.

Authors accept no liability to anyone, other than to the party indicated in the Agreement, in connection with services and deliverables, unless otherwise agreed by Authors in writing.

Report version 1.0 as at 02/2018