Whitepaper

Public ver. 1.2 (EN)

https://www.crypviser.net

Düsseldorf, Germany

1. Preamble

Not only business people and politicians, but also consumers have been realizing lately that our economies and societies are undergoing dramatic changes due to the so-called "digitalization". The term "digitalization" refers to a variety of different phenomena with a strong impact on our daily life's and the way value is created in our economies. The future research company "Z-Punkt" uses another term and writes about "Connected Reality 2025".[1]

A major trend that is currently turning the "Connected Reality 2025" into reality is the "Internet of Things". It is a "network of internet-connected objects able to collect and exchange data using embedded sensors.[2]" An example which is repeated quite often in public discussions is the refrigerator, which is connected to the Internet and can autonomously order fresh food if necessary. But the Internet of Things is far more: Based on the rapidly decreasing costs of high-performance sensors literally everything can be equipped with a sensor and get connected.

In this world of total interconnection of everyone and everything, "Cyber-security" becomes a main driver

Cyber-Security has many facets. It plays a crucial role in all kinds of contexts.

- When many employees use their smart phones from work for private purposes as well, who can make sure that confidential information is truly secure?
- When large corporations collecting vast amounts of data start working together, who can guarantee that they do not become too powerful and use their knowledge to exploit or blackmail consumers?
- When factories and power plants with all their highly sensitive and confidential data get connected to the Internet of Things, who will make sure that the competition or criminals do not get access?

[1] Megatrends and market drivers 2025, Z punkt – The Foresight Company 2014
[2]Definition of the Internet of Things, found at: http://www.businessinsider.de/what-is-the-internet-of-things-definition-2016-8?r=US&IR=T

A study conducted by the American Company Raytheon outlines, that 2/3 of all enterprises are not ready to protect billions of cyber-vulnerable devices[3].The different purposes of cyber-security in an interconnected world will occupy researchers and entrepreneurs for years to come.

In this whitepaper, we will focus on the specific security issues in communications networks and how they can be solved.

We will discuss the main risks, but also the opportunities of cyber-security, especially before the background of the game-changing technological revolution of Blockchain. What is the blockchain and what does it do?

According to the Oxford Dictionaries, the blockchain is "A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly."[4] It provides a secure way of "making and recording transactions, agreements and contracts – anything that needs to be recorded and verified as having taken place.

But the blockchain is not kept in one place only, it is distributed across a network of computers. It could be a dozen, a hundred or even thousands of people. The digital ledger becomes an extensive list of transactions, getting bigger and bigger.

How can this technology be used for cyber-security purposes?

The blockchain automatically distributes information among the entire network. Nobody can make alterations to the information without being noticed and "stopped" by the network. This means that external attackers would have to gain access to every computer in the network that hosts the blockchain database at the same time to manipulate it, which is regarded as practically impossible.

[3]Raytheon, Cyber Security Trends Infographic 2015, found at: http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233812.pdf

[4]Definition of "Blockchain", found at: https://en.oxforddictionaries.com/definition/blockchain

A market assessment estimated that $1 bln. has been invested in blockchain technology in 2016 alone[1].

Blockchain technology has become known to a wider public in 2008 because of the crypto-currency Bitcoin. But the use-cases for this technology do not only include financial transactions, but a wide range of interesting fields of business.

In this whitepaper, we will outline our vision of more secure interaction in communication networks and beyond based on blockchain technology and our specific approach to cyber-security and confidentiality.

Waldemar Konradi, CEO of Crypviser

2. Executive Summary

The key take-aways of this whitepaper are the following:

A) Our societies and economies are facing a technological revolution.

In an interconnected world, cyber-security becomes crucial both to individuals as well as to enterprises. As of now, most individuals and companies are not prepared to provide sufficient security regarding their communication. Crypviser intends to change that.

B) The Blockchain can revolutionize many businesses and markets.

It has an enormous potential regarding cyber security. Crypviser uses blockchain technology to develop bullet-proof solutions for B2C and B2B markets. By providing genuine encryptions key identification, Crypviser can prevent any kind of manipulation, interceptions and "man-in-the-middle" (MITM) attacks on all communication levels.

C) Crypviser products and solutions are based on the underlying thought of creating an eco-system of safe interaction for consumers as well as business customers.

The business opportunities today are diverse. Crypviser intends to be positioned as a pioneer and thought leader regarding blockchain usage for cyber-security purposes for instant communication networks.

3. The idea: Introduction to the world of encrypted interaction

3.1. How can encryption be easier and at the same time strong and professional?

Ever since the emergence of Bitcoin, the crypto-community has been growing. Nonetheless, the crypto-community is only a small target group of technically highly competent people with a strong web-affinity. Crypviser has developed an unbeatable security model, which is professionally designed to meet the highest standards of cryptography for securely exchanging and storing all kinds of data.

The vision of Crypviser is to make encrypted interaction understandable for the public and available for the mass market

To make our vision come true, we are committed to two major pillars of our ideology:

- The development of easy-to-use, user-centric products and solutions interesting for a wide range of markets and purposes
- The approach of thought leadership (including publications like this whitepaper but also participation at notable events), informing the public and investors about the potential of our technology

3.2. What are the main benefits of a more secure interaction?

The advantages of a more secure interaction are diverse. There are all kinds of crucial information that should be kept confidential. Here are some examples:

- **Consumers** want their personal information to be safe, for example their address, credit card number or car key frequency.
- **Government institutions** are dealing with all kinds of sensitive information daily, for instance tax information.

- **Insurances and attorneys** have gathered vast amounts of confidential data, for example regarding the financial or legal issues of their customers.

- **Medical institutions** need to protect and securely exchange all confidential information related to the patients according to the laws of most countries.

- **Financial organizations** mostly dealing and exchanging with top - secret financial and brokerage data related to their customers and partners. Leakage of this kind of data could cause serious financial damage and is a reputational risk.

- **Businesses** have a strong demand in keeping technical specifications of their most important products and services confidential, because the success of their business depends on this information.

3.3. Who needs confidential interaction?

As indicated above, confidential interaction may benefit a large variety of different target groups. The following scenarios are helpful to outline the benefits of encrypted communication for different stakeholders:

- **A casual user**
  Imagine an average person, who is annoyed of the lack of security in the contemporary popular social networks. Someone who would appreciate it a lot if their information, for example private pictures at the beach, are protected properly.

- **A wealthy businessman**
  He wants to communicate safely with his children who are currently studying abroad. Since he has had threats of kidnapping before, he needs an easy-to-use communication solution, which keeps sensitive information like the whereabouts of his children confidential.

- **A middle-class business owner**
  He works hard to create highly complex technical products for specialized B2B purposes. Due to industrial espionage, his company has already suffered devastating economic losses. A highly secure communication solution is needed immediately. It should be easy to implement (e.g. cloud service).

- **A CEO/CTO at a large corporation**
  This gentleman runs large `factories that produce state-of-the-art batteries. The products are dangerous themselves and should never fall into the wrong hands. Therefore, this person needs a

solution for highly encrypted communication and data exchange which can be integrated into already available systems.

- **A government official**
  This lady is responsible for the management of highly sensitive data, for example regarding military international affairs. She needs a partner with a proven track record of excellence in creating encrypted communication solutions.

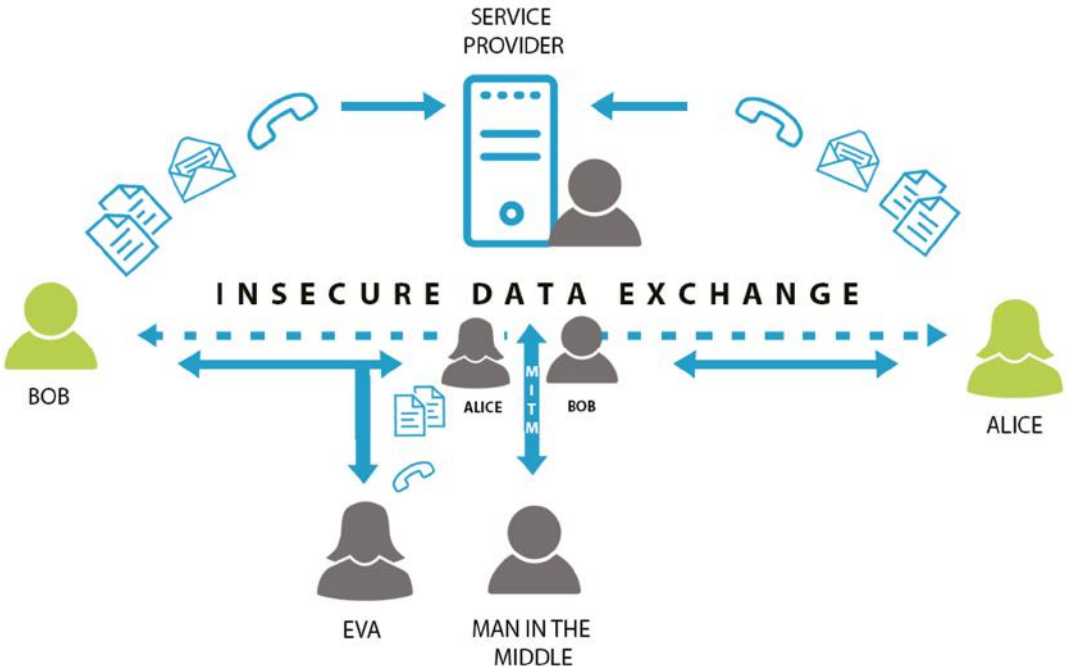
4. Security challenges in communication networks

4.1. Current security issues in communication networks

Today, the most popular communication networks for instant data exchange, such as GSM, Skype, WeChat, Slack, Google Talk, Facebook etc., do not provide an adequate level of protection and privacy. Classical schemes of such systems mainly mean data exchange between parties in an unprotected way.

Such communication models are a serious threat to safety, integrity and privacy of the transmitted information

Figure 1: Security challenges in an unprotected network



As shown in **Figure 1**, an open unprotected system is subject to three main types of attacks:

1.) Leakage of user's data to third parties voluntarily or accidentally due to the provider.

2.) Threat of unauthorized interception of data exchange between parties (Alice and Bob) from the intruder EVA.

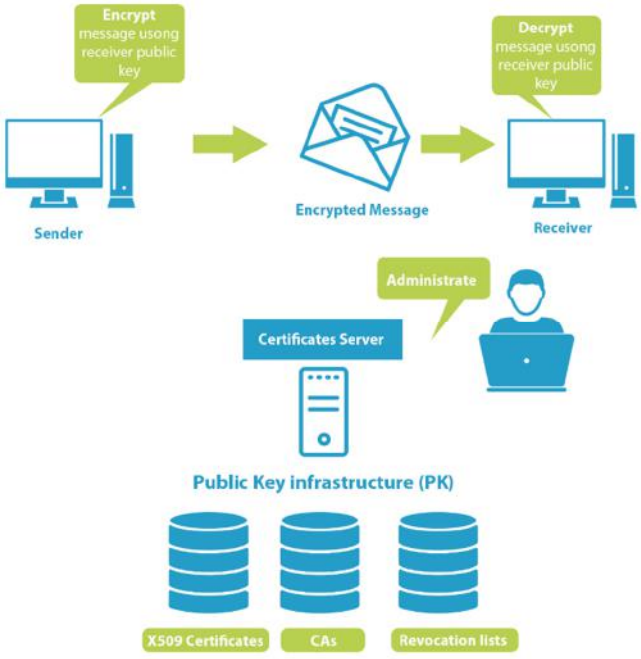
3.) The "man-in-the-middle" is an attack, during which an intruder intercepts and substitutes information, transmitted between Alice and Bob. As a result, Bob thinks that he talks with Alice, and Alice thinks that she shares data with Bob, but in fact data could be intercepted and replaced by the "man-in-the-middle", who can act on the behalf of Bob and Alice accordingly.

4.2. Classic model of an encrypted network

To protect against the above types of threats in communication networks, classic cryptographic protocols and technologies are mainly used (such as SSL, VPN, PPTP, SRTP etc.,) based on asymmetric data encryption standards and keys exchange.

In such models the data exchange is performed in an encrypted form, which eliminates the possibility of data interception. It also eliminates the threat from the intruder EVA. Even if the encrypted data is intercepted, it cannot be decrypted without the keys.

Figure 2: PKI security model



However, the main types of threats, such as "deliberate leakage of data" and "man-in-the-middle attack" remain in effort, as encryption is performed on the Provider's server side

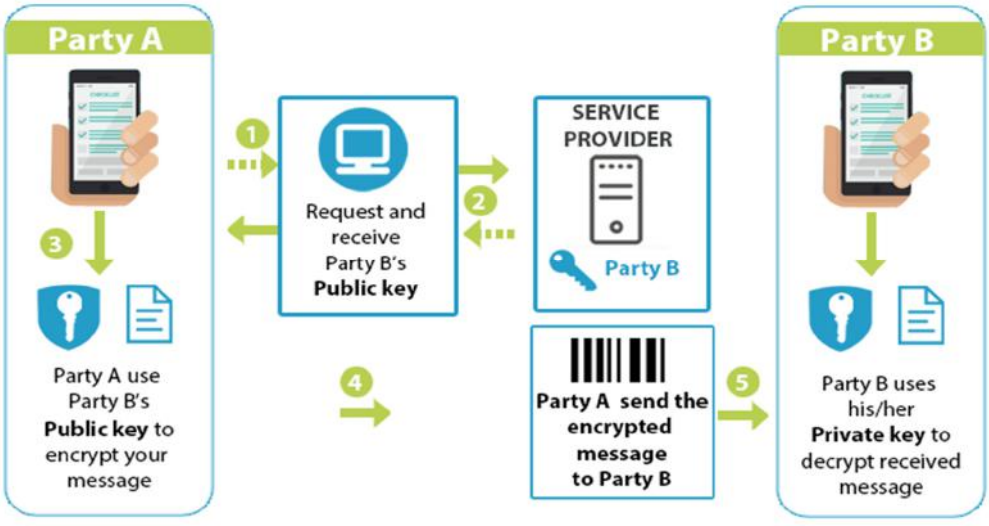
It follows that classical server-based peer-to-peer encryption models are suitable for use only in corporate networks, by using internal CAs (Certificate Authorities), but not in public or cloud-based (untrusted) networks. Although using of CA servers prevents man-in-the-middle attacks, but the servers itself are vulnerable for different kind of attacks.[5]

Public-key cryptography may be vulnerable to impersonation, even if users' private keys are not available. A successful attack on a certification authority will allow an adversary to impersonate whomever he or she chooses by using a public-key certificate from the compromised authority to bind a key of the adversary's choice to the name of another user.

4.3 End-to-End user-side encryption technology

To eliminate the threat from the provider's side and to exclude it from the encryption process, today many platforms use the popular end-to-end user-side encryption based on asymmetric encryption protocols. The technology involves generating a secret and a public key on a local device for each user. In this case, all types of data transmitted are encrypted by two keys at the same time — a secret and a public one. The public key is used for data encryption and it can be freely transmitted over the network between users. For data decryption, the secret key is used, which is always kept on the user side and never leaves its device. The pair of secret and public keys has a stiff mathematical relation, so that data can be decrypted only if the both keys are available. Since the secret key is never transmitted and is kept on the user's device only, the data can be decrypted only by the recipient whose public key was used for data encryption.

Figure 3: End - to – End encryption scheme



However, since the provider's server acts as a trusted party of data and public keys exchange between the users Alice and Bob, there is still the threat of "man-in-the-middle" attack. In this case, the server can intercept public keys and replace them with its own and start acting on behalf of one of the users, thereby manipulating data between them.

The major drawback of this scheme is the lack of ability to identify user's public keys and confirm their authenticity, which allows the "man in the middle" attacks on the provider side

Such models are mostly used in enterprise and cloud-public networks, for instance SIMSme messenger by Deutsche Post, which has such vulnerability.

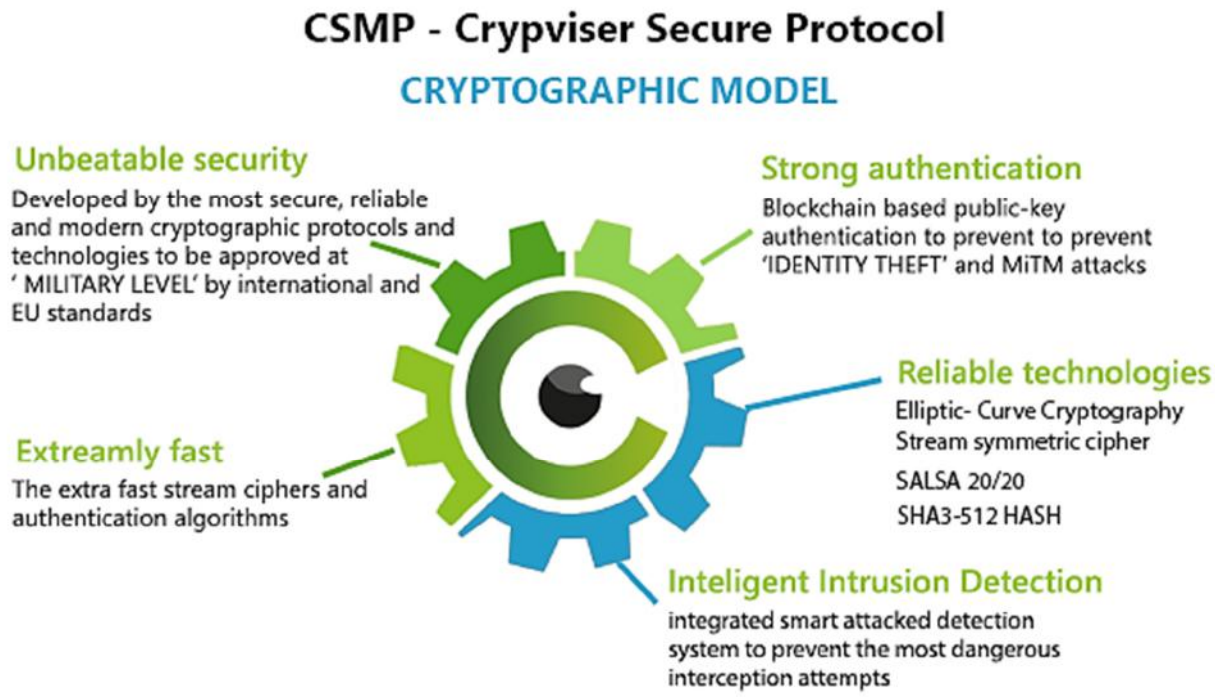
5. The technology: CSMP blockchain-based security protocol

5.1. Cryptography model

Crypviser has developed a unified secure instant communication network with real end-to-end encryption and unique blockchain based authentication. It is a comprehensive new generation communication platform, which meets modern challenges for information security and increased demand for data privacy and protection in instant data exchange networks. It features reliable protection at all layers.

The main technological solution is the genuine user-side encryption and blockchain-based public key authentication mechanism provided by the CSMP protocol

Figure 4: CSMP protocol



5.2. Blockchain-authentication method

The encryption keys exchange, distribution and management algorithms (authentication process) is the most important phase in any cryptographic model. Without a properly designed authentication model, the encryption looks like a house with a strong armored front door, but with open windows. It's hard to get inside the house through the front door, but easy to climb through unprotected windows. So, the security model of the most popular instant exchange networks looks like this house.

Crypviser introduces the solution of the biggest historical challenge of asymmetric cryptography: Public-keys decentralized distribution based on Blockchain technologies

A blockchain-based authentication model allows users to truly identify and confirm each other's public keys. This eliminates the MITM threat and any kind of manipulation attempts from the server and third parties' sides.

The algorithm: The idea is based on the Blockchain features of decentralized distribution and management of the public keys.

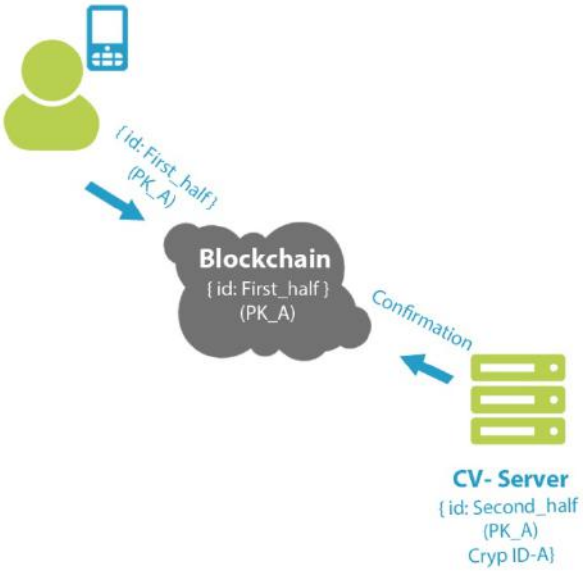
Since the Blockchain is decentralized database, it contains information on the correspondence of the unique identifier of each user and the first half of his public key (*id: first_half (PK)*). Crypviser's server (CV-server) contains information about the correspondence between the unique user ID and the value of the second half of its public key (*id: second_half (PK)*).

Initial authentication: During the account registration process, the Crypviser app generates a unique ID value and initial secret SK (Shared Key) on the user's local device. The public key is derived from the SK. These keys are permanently used for initial authentication purposes only. The CV-server, which operates as a node of Blockchain, has its own key pair.

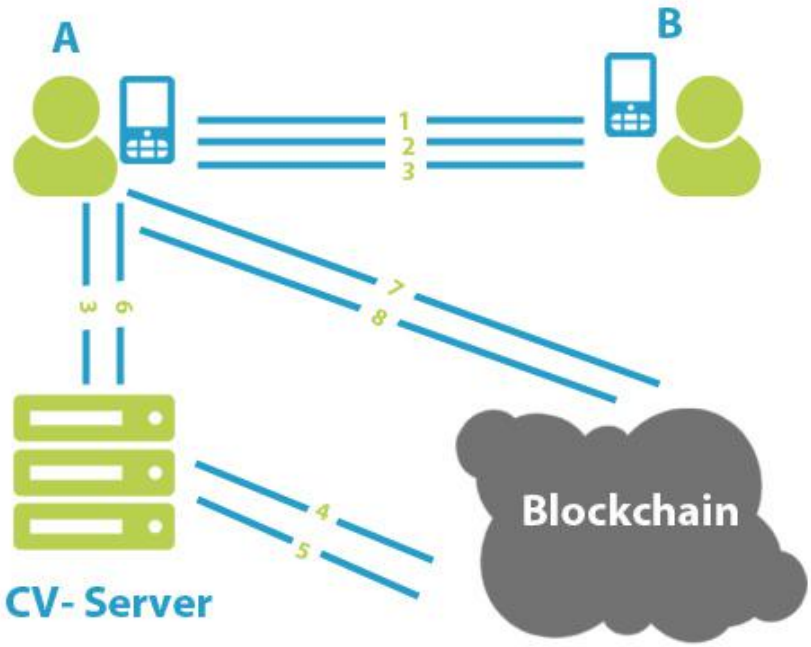
Account registration: After completion of the registration process a new key-pair is generated on the user's device related to the account. At the same time, a unique hash of CrypID is generated based on the different sources of entropy, such as partial hashes of symmetric key used for local database protection and user's passphrase. The second part of the public key, CrypID and User ID (*id: second_half (PK):CrypID*) are transmitted to the CV-server using the established secure connection.
The User ID which was generated during the initial authentication phase, is intended for providing anonymity on the CV-server side.

Blockchain integration: To record the first half of the initial public key to Blockchain, the user executes a transaction (sends authentication tokens) in favor of the CV-Server. The transaction contains meta-data with value of the first_half (PK) which is recorded in Blockchain ledger. Afterward the recorded part of the user PK must be verified on the CV-server and user sides to eliminate any MITM attack attempts during the transmitting the half-part of the PK through the network. Only the owner of the secret key can "spend" the tokens by solving the special cryptographic "problem" related to the complex calculations with CrypID. This means that CV-Server proves the validity of the first part of the user PK recorded into the Blockchain. To prove and validate the first part of PK recorded in Blockchain on the user side, CV-Server similarly sends authentication tokens to the user. The Crypviser app performs the same algorithms to validate the authenticity of the recorded part of its PK. In this way, the CV-server and user verify the authenticity of ledger, ensured by other nodes through the data distribution feature the half-part of user's initial PK at the same time in the ledger, ensured by other nodes through the data distribution feature.

Figure 6: Public-key distribution through Blockchain



Public-key authentication: The algorithm of the public-key distribution and validation between parties is shortly described below:



1. Party A wants to initiate a new encrypted session and sends a message containing:

$$(Nonce\_A,\ timestamp\_A)$$

2. Party *B* sends the following response:

$$(Nonce\_B,\ timestamp\_B, E[(timestamp\_A,\ Nonce\_A,\ id\_B,\ hash(id{:}PK\_B))_{SK\_B}]_{CrypID\_B})_{SK\_B},$$

Where, $E[(timestamp\_A,\ Nonce\_A, id\_B,\ hash(id{:}PK\_B))_{SK\_B}]_{CrypID\_B}$ is the output of the encrypted data with CrypID belonging to Party B. It is important to note that the data is first signed by Party B's key and then encrypted.

3. User A receives the message and forwards it as a request to the CV-Server through the secured TLS channel

$$E[(timestamp\_A,\ Nonce\_A, id\_B,\ hash(id:\ PK\_B))_{SK\_B}]_{CrypID\_B}),$$

4. The CV-server with the CrypID of Party B, decrypts the ciphertext and verifies that Party B's ID stored locally matches the its ID derived from the decrypted data;

5. Then it receives the first part of PK from the Blockchain ledger by the ID of Party B and combines it with the second-part of PK stored in local database, as well as checks the digital signature of the received data.

6.The CV-server signs the message with its secret key, encrypts it with the A Party's CrypID and sends the following data to the Party A:

$$E[(\text{'}OK\text{'}, timestamp\_A, Nonce\_A, id\_B, hash(id: PK\_B), second\_half(PK\_B))_{SK\_S}]_{CrypID\_A}.$$

7. Once it receives the message, Party A performs the following actions:

- decrypts the data received from the CV-server and checks the digital signature;

- compares the values of timestamp_A and Nonce_A with those previously sent to the Party B. The value of timestamp_A should be in the allowable timeframe but the Nonce_A value should match.

8. Party A requests the Blockchain and gets the first part of PK which belongs to Party B.

- derive the whole public Key of Party B by combining the received part of PK from Blockchain and from the CV-server

- checks the digital signature of the entire package received from user B earlier;

- calculates hash $(id:PK\_B)$) and compares it with the hash value of data received from the CV-server.

9. In case of successful completion of all validations, Party A considers that PK_B originally belongs to Party B. Then Party A sends to party B the following message

$$E[(timestamp\_B, Nonce\_B, id\_A, hash(id:PK\_A))_{SK\_A}]_{CrypID\_A}$$

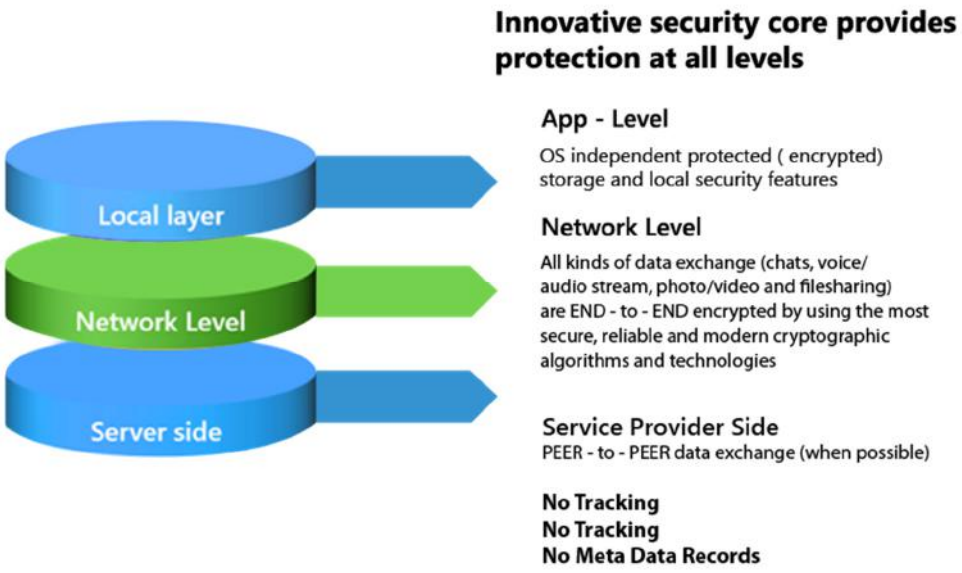
Party B follows the same algorithm to obtain and authenticate the public key of party A.

Secure communication:

All further transactions of encryption keys derivation required for the CSMP protocol to establish a secure communication channel between parties is held through Blockchain. It allows to keep permanent automated control of the security model through integrated smart intrusion detection system or having manually transparent access to any transaction for investigation purposes.

5.3. Security core

Figure 7: Security levels



5.4. Blockchain-based server authorization

As is known, in security issues all details matter and play an important role. This is the reason that the classic client-server authorization technologies became unsuitable and do not meet current security requirements. Crypviser cares of its users in a professional manner and introduces a patent-pending complex authorization solution to prevent any possibility of the user's meta-data manipulation on the service provider side.

Unlike conventional user authentication algorithms used in most of the known networks, the unique user identifier in the Crypviser Network - *CrypID* is generated locally on the user side, and then transmitted to the Blockchain. *CrypID* is generated using an innovative cryptographic algorithm, by using various sources of entropy, which provides the highest degree of uniqueness and avoids mathematical collisions. Moreover, for every user connection, a one-time session authorization token is generated based on *CrypID,* which is used and compared locally, to identify the user on the server. The session authorization token is destroyed after the session termination. This measure eliminates any possibility of manipulation with unique user *CrypID* on the Crypviser servers.

5.5. Local security

All kind of data is stored on the user device in a standalone encrypted storage, independent from the base OS such as Android or iOS. Crypviser's data storage is protected by a symmetric 256 bit encryption key, generated based on the user’s finger-motions, during the application installation. In the same time,

the symmetric key is protected with a passphrase defined by user. Thereby, even in case of physical leakage of protected database or the loss of control over the device, all sensitive data will be kept safe and untouchable.

However, to provide the highest level of usability, Crypviser's users can securely save the local storage's password through the patent-pending multi-level HASH encryption method. Which means, that some part of cryptographic hash isn't stored locally, but calculated automatically based on a unique algorithm for each device.

5.6. The key advantages of our technology at a glance

Crypviser has essential advantages and is the first to introduce a range of disruptive solutions:

Blockchain authentication - automated Blockchain based authentication and verification to prevent all kinds of MITM attacks

Intelligent intrusion detection - allows timely detection and prevention from the most dangerous third party interception attack attempts

Multi-device support - the first secure network with multi-device support that enables you to run the same Crypviser account on different devices

Secure Sync - secure multi-device synchronization in encrypted mode

6. The possibilities: Creating a secure multi-purpose ecosystem

6.1. CV Private Community

Crypviser aims at providing the best secure interaction products for consumer as well as business target groups. The product family will be continuously growing.

For consumers, Crypviser developed its flagship solution called CV Private Community.

The CV Private Community offers a wide range of features. The following table indicates the available plans and features.

Figure 8: Features and Plans of CV Private Community

Features	CV Free	CV Best	CV Max
Encrypted unlimited instant messaging (chats) and voice messages exchange	✓	✓	✓
Secure unlimited voice calls	✓	✓	✓
Encrypted video calls		✓	✓
Secure photo/video/file sharing	Limited by size	Unlimited	Unlimited
Auto-destruction feature	✓	✓	✓
CVPay exchange (fund transfers)	✓	✓	✓
Encrypted local storage	✓	✓	✓
Blockchain-based authentication (protection against MiTM attacks)		✓	✓
Manual authentication (MiTM protection)	✓		
Intrusion detection system	✓	✓	✓
Multi-device support	+1 device	+3 devices	+5 devices
Encrypted sync between multi – devices	✓	✓	✓
Group calls		✓	✓
Local security features		✓	✓
1 incoming international number (for choose)			✓
FREE minutes package for secure international calls (for choose)			✓

6.2 CV Secure Business

The CV Secure Business network is a cloud-based secure solution for enterprises, containing a wide range of features allowing to build own encrypted online communication and instant data exchange

infrastructure. It's a SaaS subscription based solution available for easy deployment and maintenance, without investment in expensive equipment and security audit for small and medium size companies.

The following table indicates the available plans and features.

Figure 9: Features and Plans of CV Secure Business

Features	CV Start	CV Pro	CV Ultimate
Incoming business numbers	**1**	**3**	**5**
Encrypted unlimited instant messaging (chats)and voice messages	✓	✓	✓
Unlimited Full HD audio and video calls	✓	✓	✓
Group calls	✓	✓	✓
Local security features	✓	✓	✓
Secure photo/video/file sharing (unlimited)	✓	✓	✓
Auto-destruction feature	✓	✓	✓
Encrypted local storages	✓	✓	✓
Automated BLOCKCHAIN – based authentication (protection against MiTM attacks)	✓	✓	✓
Intrusion detection system	✓	✓	✓
Cross-platform multi-device support	**3**	**5**	**10**
Encrypted sync between multi-devices	✓	✓	✓
Network and user's management through a single Management system	✓	✓	✓
User licenses included	**3**	**15**	**25**

6.3. CVCore

For larger corporations and enterprises, Crypviser is developing a powerful solution -CVCore. CVCore comprises the cryptographic secure technology and allows larger companies and E-commerce platforms to integrate the core cryptography and security model to any existing infrastructure regardless of its complexity.

All essential benefits of Crypviser's core technologies are based on Blockchain and can be obtained without having to invest in expensive equipment or to conduct serious technical updates

It is a completely hassle-free solution, providing companies with unbeatable cyber-security for all kinds of secure data exchange and storage purposes.

6.4. CVCoin and CVPay

To ensure the highest-level of confidentiality Crypviser has issued a unique authentication crypto token: CVCoin. The main purpose of CVCoin is covering charges of Blockchain transactions for authentication purposes, to authorize and identify the users' public encryption keys and to provide the highest level of security within the Crypviser Network.

CVCoin will serve as a unified network currency to simplify and secure blockchain authentication transactions

Another purpose of CVCoin usage is simple and anonymous money transfers between Crypviser users by using an integrated money exchange system: CVPay.

6.5. Crypviser OpenWorld

OpenWorld technology is a part of the Crypviser Network to provide the ability of secure communication with the external world. It includes a rich set of features.

Features include:

- International virtual DID numbers for accepting incoming calls from any external network regardless of the location (ROAMING free)
- Cost - effective wholesale minute packages for international calls to different countries
- International calls via VoIP to external phone numbers (mobile and landline) at cheap rates (20-30% cheaper than competitors) worldwide
- Profitable Partner (distribution) programs for increasing a business area or starting a new successful partnership with Crypviser
- Attractive Bonus promotions for Crypviser users to invite friends and earn real profit
- Powerful and multifunctional Web Account designed to take full control over Crypviser OpenWorld

These types of services can be obtained from the system-integrated online store. Additional services can be managed through the user's Web Account.

6.6. Future Work: Crypviser Blockchain

Figure 10: CSMP protocol based on Crypviser Blockchain

The next generation of Crypviser 2.0 will be based on the new kind of Blockchain especially designed for the reliable encryption keys exchange and authentication purposes in instant communication networks.

Crypviser Blockchain will be represented as a first mobile Blockchain, where every device will operate as a node to serve transactions of encryption keys exchange and validation.

The main benefits of Crypviser Blockchain are the following:

- **Specialized Blockchain** - for genuine authentication and encryption keys exchange
- **Designed for encrypted instant communication networks** - significantly faster confirmation of transactions
- **Mobile friendly** - the first full-fledged Blockchain for mobile devices

- **Affordable for everyone**- no more necessity to invest in expensive equipment to become a part of Blockchain network, just install the app!
- **Easy maintenance** - user-friendly way to control resources consumption, such as battery or network bandwidth
- **Extra earnings** - opportunity to get tokens for every mobile user operating as a key-exchange node

7.Conclusion

The need for a more secure interaction and encrypted communication both in private as well as business contexts is imminent. Blockchain technology will have a significant impact on a variety of markets and it most certainly will influence cyber-security applications.

By incorporating blockchain technologies into an already strong security protocol, Crypviser aims to revolutionize the level of security available both to the public as well as businesses in terms of secure data exchange and storage purposes

The technology behind the Crypviser is powerful and offers almost limitless possibilities. At the same time, it is of the upmost importance to simplify secure interactions and to develop solutions that have what it needs excite target groups. Therefore, a user-centric approach in the development of new products is crucial.

Crypviser – a game changing technologies provider of secure encrypted communication networks

About the author

The Crypviser Research Team is lead by Mr. Vadim Andryan. Mr Andryan has been awarded the CCNA and CCNP degrees of IT security and cryptography. The Founder has broad experience and knowledge in computer security and data encryption fields. He has worked in government and military projects focusing on cyber-security and social engineering. Since 2007 he has founded several telecommunication companies that are still successfully operating in several countries.

In 2013, Mr. Andryan decided to bundle his extensive technical and business expertise, which he has accumulated over more than 10 years, in the development of the innovative Crypviser project. Today, he is Chief Architect of Crypviser's cryptographic and security models.

References

- Megatrends and market drivers 2025, Z punkt – The Foresight Company 2014
- Definition of the Internet of Things, found at: http://www.businessinsider.de/what-is-the-internet-of-things-definition-2016-8?r=US&IR=T
- Raytheon, Cyber Security Trends Infographic 2015, found at:http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233812.pdf
- Definition of "Blockchain", found at: https://en.oxforddictionaries.com/definition/blockchain
- The Guardian, January 2017, found at: https://www.theguardian.com/global-development-professionals-network/2017/jan/17/blockchain-digital-technology-development-money
- RSA Laboratories Research, found at: https://germany.emc.com/emc-plus/rsa-labs/standards-initiatives/advantages-and-disadvantages.htm

Is not an alternative, it's better!

https://www.crypviser.net

Coming soon in

Crypviser GmbH
Alt-Pempelfort 15, 40211 Düsseldorf

Email: info@crypviser.net