CryptoTec Cipherbook
Light Paper

Introduction
As a technology enterprise, CryptoTec AG provides high-security solutions for connecting decentralized computer systems. In doing so, it is irrelevant whether communication takes place between people or machines. CryptoTec's customers expect highest security.

Background
CryptoTec AG has its roots in the payment and sports betting industry — a business environment with multi-billion turnovers that is constantly exposed to external and internal manipulation.

A high level of decentralization for input devices, associated with central odds management, requires the highest possible degree of security, particularly for M2M communication (machine-to-machine) that is protected against manipulation and wiretapping.

Within this industry, the founders of CryptoTec AG are considered as the system-relevant providers for implementing such security solutions.

Range of Services
The range of services can be described best using the example of the sports betting industry. It includes, for example, the generation of software for checkout systems that are connected to the internet, creation of automated systems including customer and administration interfaces, as well as the integration of money acceptance units.

Furthermore, the service portfolio comprises statistical fraud analysis and development of high-security systems for storing credit card information.

Expertise from Daily Practice
As a provider of security concepts and encryption solutions, the founders of CryptoTec AG can revert to 25 years of expertise particularly for developing and implementing security measures between decentralized, computerized systems.

This expertise which is applied on a daily basis and successes in combating thousands of system attacks has resulted in a major competitive edge.

Based on this know-how, it was obvious for CryptoTec AG to expand its business to other industries too.

CryptoTec Cipherbook
In 2016, CryptoTec AG launched CryptoTec Cipherbook which is a high-performance solution that allows enterprise employees to communicate in real time, transfer large amounts of data without any limits, and synchronize files in virtual Ledgers. A high level of encryption and an authenticated group of users protect against unauthorized access by third parties.

The authentication of the users additionally prevents intentional or unintentional transfer of data to unauthorized parties.

Internet of Things (IoT)

The continuously advancing connection of different devices to the internet presents manufacturers from different industries with new and major challenges for developing appropriate protective measures against manipulation and illegal access to connected devices and systems.

Here it is possible to revert to know-how and solutions across industries which have been developed in recent decades to find feasible and secure solutions more rapidly.

Summary

CryptoTec has an excellent know-how that has proven itself countless times in practical use. Digital signatures, end-to-end encryption, and an automated Public-Key-Infrastructure are the starting point for developing closed user group concepts.

Communication among people and machines, encrypted symetrically and asymmetrically and connected according to highest security standards, user-friendly implementation.

Assessment

CryptoTec AG invests a lot of money in the validation of its software modules that is carried out by external auditing firms. In this context, all auditing firms confirmed that they did not find any weak points via which the system can be accessed.

In the context of the CryptoTec Cipherbook launch, several globally known white-hat hackers have examined the CryptoTec Cipherbook modules for any weaknesses. Here as well, full security was certified for CryptoTec AG. CryptoTec AG also cooperates with the University of Erlangen, Germany. Prof. Freiling should be mentioned specifically here who is member of the board and checks security logs of CryptoTec in his department.

Location Germany

All modules are developed in Germany. As a result, CryptoTec AG is not subject to any restrictions by public institutions. Indeed, „Made in Germany" proves as a real attribute.
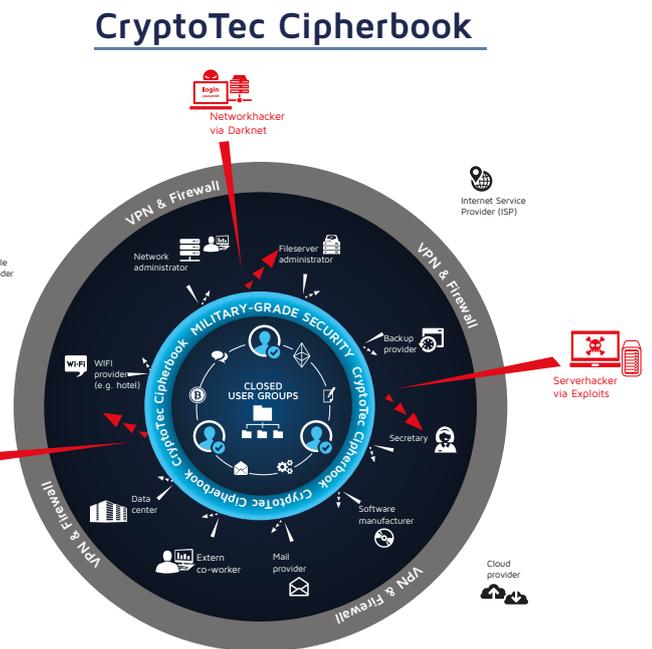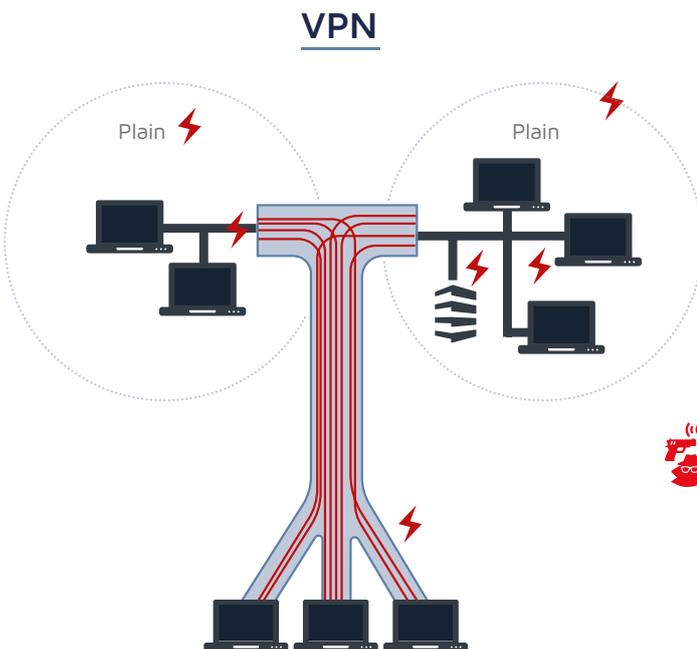
Cipherbook

CryptoTec Cipherbook

CryptoTec Cipherbook summarizes a series of user-friendly communication and co-operation tools that are all characterized by highly secure end-to-end encryption.

Security

Using traditional high-performance encryption technology in communication media has suffered from its own complexity and the associated difficulties for the user.

In more than ten years of research work, we developed a ground-breaking portfolio that can easily withstand even most severe attacks of well-equipped organizations and is also unrivalled in terms of ergonomics and user-friendliness.

Functioning compared to VPN

VPN



CryptoTec Cipherbook

Secure Tunnel from every end to every end
Called: **CryptoTec Cipherbook crypto framework**
Automated PKI

Benefits

Thanks to the encryption technology deployed and the digital signatures, CryptoTec Cipherbook protects against undesired wiretapping and data corruption (integrity) and validates all system participants (authenticity) based on a fully automated Public-Key-Infrastructure. All system participants receive an address that is labeled with a double @ character, for instance,

"bob@@Cipherbook.com." Manipulated content and sender data is detected automatically - this ensures that communication takes place with a limited participant group that consists of authenticated persons only.

Blockchain Technologie
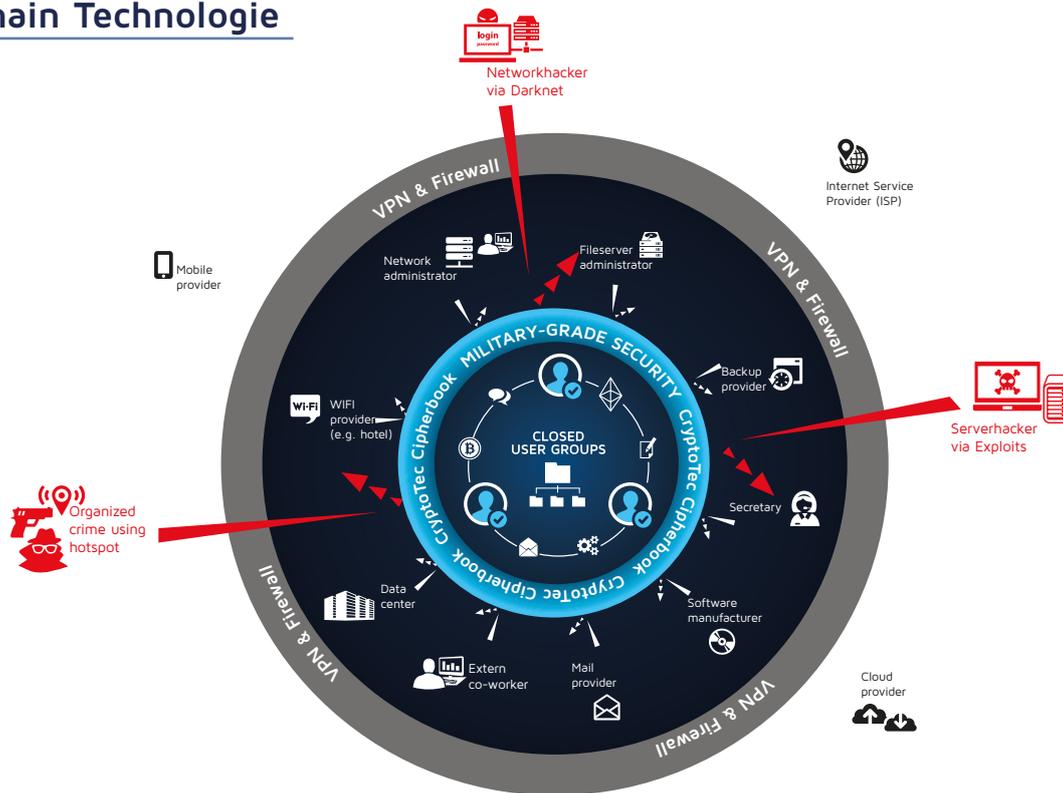
Portfolio

Our portfolio currently comprises the following functions:

- Real-time communication
- Filetransfer
- Online cooperation

Modules in detail

Cipherbook Messenger

- Fastest way of communication
- Perfect for quick exchange

Cipherbook Transfer

- Easy drag-and-drop
- Both peer-to-peer and via servers
- Files of any size can be dispatched (quota control)
- High-speed transfer through optimized protocol
- Ideal for worldwide dispatch of large data

Cipherbook Ledger

A virtual working space
- Shared processing of documents
- Authenticated protocol of all changes
- Free creation of folders and subfolders
- Access and processing using known programs
- Perfect for location-independent teamwork involving confidential documents

These modules are combined in the following packages depending on the intended use and scope:

Cipherbook Free

Own Ledgers: 5
Storage: 500 MB

CryptoTec Cipherbook Base

Own Ledgers: 10
Speicher: 3 GB

CryptoTec Cipherbook Pro

Own Ledgers: 20
Storage: 10 GB

For larger teams, companies and enterprises we developed the following bundles:

CryptoTec Cipherbook Business

Own Ledgers: 150
Storage: 1500 GB
User: 10

CryptoTec Cipherbook Enterprise

Own Ledgers: unbegrenzt
Ledger-Storage: customized
User: unlimited

Enterprise customers will receive their own dedicated

server. The Enterprise package is available through the partner network of the CryptoTec AG.

Reason Why

Today, information and data records constitute the backbone of most enterprises. While the protection options with traditional technologies can be considered as sufficient within your „own four walls," communication and decentralized distribution of data records are still a weak point.

This is where CryptoTec's Cipherbook is deployed as a data-based communication and collaboration solution for highly confidential data.

Background

CryptoLib is the cryptographic high-level library that was specifically developed by the founders of CryptoTec AG. It is the core of CryptoTec AG's cryptographic work. Experts of this matter confirm that the incorrect implementation of cryptographic standards constitutes the biggest source of error when developing security software. By deploying CryptoLib, the development of secure solutions is freed from this most complex and error-prone element.

- RSA-4096
- AES-256
- SHA-512

Appendix

What holds true for the communication among people also applies to the communication among machines and between people and machines. The portfolio of CryptoTec Cipherbook thus forms the basis for secure machine communication. Authenticated communication with integrity and sophisticated encryption is the most critical point in the era of "Internet of Things."

FAQ

What is CryptoTec Cipherbook?

While CryptoLib is the core, the distributed systems platform (DSP) contained therein represents the brain. The DSP not only comprises a Public-Key-Infrastructure (PKI) that ensures fully automated distribution of cryptographic keys. It also automates DNS integration, data distribution, and a variety of user-friendly functions such as notification of contacts if names or addresses change. In terms of encryption, CryptoTec AG relies on cryptographic procedures that are acknowledged around the world:
CryptoTec Cipherbook is a software solution which you can use to share information with a high level of security.

What does CryptoTec Cipherbook offer?

CryptoTec Cipherbook provides the option to send large files and messages easily and securely. Beyond that, CryptoTec Cipherbook offers the option to set up virtual file storages which several people can access in parallel. CryptoTec Cipherbook enables bug-proof exchange of information for each user without any previous knowledge and intensive training.

In concrete terms, CryptoTec Cipherbook comprises the following functions:
- File-based online cooperation
- Real-time communication
- Filetransfer

How does CryptoTec Cipherbook work?

CryptoTec Cipherbook is easy to install and operate and offers a highly secure end-to-end encryption. The distinct feature of CryptoTec Cipherbook is that private and public keys are generated fully automatically through a PKI (Public-Key-Infrastructure). Thanks to the encryption technology deployed and the digital signatures, CryptoTec Cipherbook protects against undesired wiretapping (secrecy) and data corruption (integrity) and validates all system participants (authenticity). Manipulated content and sender data is detected and removed automatically. For this purpose, CryptoTec Cipherbook uses the most renowned asymmetrical and symmetrical procedures for data encryption. These include the following:

- RSA-4096
- AES-256
- SHA-512

How do you register for CryptoTec Cipherbook?

After you have downloaded CryptoTec Cipherbook (PC, Mac, or Linux), you are guided through the individual installation steps. In this process, a personal address, similar to an email address, is generated for you. Contrary to a traditional email address, this personal address features a double @ character, for instance, „bob@@Cipherbook.com.“ You may use this address free of charge on a lifelong basis. Here, CryptoTec Cipherbook assumes the complex handling of the digital signature and the private key fully automatically.

A personal recovery code is generated during installation. The program then prompts you to print this document and store it in a safe location. This recovery code enables you to restore your digital identity if a reinstallation is required.

How do you contact other persons using CryptoTec Cipherbook?

After CryptoTec Cipherbook has been installed, position the cursor on the empty contact field and right-click it. This opens a dialog window. When you go to "Add Contact," a new window opens where you must enter the CryptoTec Cipherbook address of the other participant. After you have entered the information, the system checks the authenticity. If the address is known, the other participant is automatically informed about your contact request. Private and public keys are automatically exchanged by the system through forgery-proof certificates. Once the invitation has been accepted, the two participants are connected and can communicate authentically and with protection against wiretapping and forgery, transfer files, and share common file storages and folders.

How do you use real-time communication?

Position the cursor on the contact field. Double-click a contact to open a two-part communication field. Enter your message and click on the "Send" button. The messages sent by you and all answers sent by your contact are displayed in the upper area.

How does data transfer work?

To transfer a file from one participant to another, simply drag-and-drop the desired file to the desired contact in the communication field and confirm the correctness of the selected recipient and the file to be transferred. Your contact then immediately receives a message and confirms that he/she wants to accept the file. All files transferred are automatically stored in the central CryptoTec Cipherbook folder which is located under "Documents" (for Mac) or "My Files" (for PC) on your hard disk.

How does the online cooperation work?

Below your contact fields you can find the "Ledgers."
Right-click the Ledger area and choose "Create Ledger." Enter a name for the new storage and then invite the desired participants from your contacts.

When you double-click a group, a window opens in which you can store the files and documents that are to be processed jointly. Any changes to the documents are synchronized automatically and are visible to all participants.

Case studies

Different fields of application are available for CryptoTec Cipherbook ranging from simple private usage to deployment in internationally operating enterprises with subsidiaries around the globe. CryptoTec Cipherbook is also increasingly used in the university environment. There are countless application examples, some of which we want to mention here.

Biogas plants in China

A Germany-based enterprise builds biogas plants in China. Construction plans are the core of this enterprise. For cooperating with the engineers in Germany, the enterprise uses CryptoTec Cipherbook's online cooperation module (Ledger). This enables the engineers in Europe to exchange technical drawings and other know-how with their colleagues in China without having to fear wiretapping. But also during the construction phase, the construction engineers that operate on site utilize the data via Windows tablets to communicate with the headquarters. Here, particularly real-time communication takes effect (Messenger).

Universities

Some universities already utilize CryptoTec Cipherbook, both for communication among students and also in the research environment. As a result, research projects can be processed by several scientists at the same time independent of time and place - CryptoTec Cipherbook supports universities by providing the online cooperation module (Ledger).

Offices

Particularly larger offices with international customers are increasingly interested in CryptoTec Cipherbook. The confidentiality of conversations with the clients is ensured on a global scale using the real-time real-time communication module (Messenger) and the fully secure transfer of large amounts of files no longer poses a problem thanks to the filetransfer module (Transfer). For this reason, large offices rely on CryptoTec Cipherbook's solutions.

Civil rights organizations

People who stand for human rights, even under most difficult conditions, are true heroes of the modern age. For this reason, they can fully count on CryptoTec Cipherbook's support. They can use the entire CryptoTec Cipherbook enterprise package (Messenger, Transfer, Ledger) free of charge.

CryptoTec AG

Habsburgerring 2
50674 Köln
Germany
Tel: +49 221 2228383 0
Fax: +49 221 2228383 20
www.cryptotec.com
info@cryptotec.com

Represented by the board:

Michael Mertens (chairman)
Dr. Michael Raumann
Albrecht von Creytz

Supervisory board:

Robert A. Depner (Vorsitzender)
Prof. Dr. Felix Freiling
Peter Schlingloff