Cryptshare®

The company and the product

A success story

A success story.

In the year 2000, IT systems worldwide had survived the transition into the new millennium without the widely feared crash, and the 'dot-com bubble' had burst and shaken the New Economy. At the same time, the Bluetooth standard made its first appearance in consumer products, and Microsoft published Windows 2000. It was at this time the company that would later become Cryptshare AG was founded in Freiburg im Breisgau in Southern Germany.

First an idea. The team's experience in technology illuminated a universal problem in business: There was no easy way for companies to exchange messages and large files in a simple, fast, and secure way with suppliers, customers, or partners.

The starting point for securing the transfer of information was in-depth research of email, which had been well-established as the universal communication product in the business world. The goal was to find a way to enhance the technology of the email ecosystem, whilst getting rid of its known disadvantages in a cost-efficient, controlled, and secure way.

Cryptshare®

Cryptshare®

Email for the secure **transfer of information.**

Having identified a universal problem across all industries and in enterprises of all sizes, it was clear that email was and is a universally accepted standard for communications, easy to use and globally available. Every user with a computer, smartphone, or tablet PC could then as now communicate with any other regardless of the device, operating system, or email application.

Today's standards and demands, especially for the security of information in transfer, go far beyond the situation then and even email's current capabilities. Every company or authority must exchange confidential files electronically – and often even the written messages in emails are of a sensitive nature and need to be protected. Security concerns are high on, if not at the top of, the agenda for all as email systems are a prime target of attack for criminals, hackers, and industrial espionage. By far the most cyberattacks start with an email!

In addition, the sheer amount and size of email attachments unnecessarily strains the email systems of enterprises. Often attachments surpass manageable size, creating excessive cost, and are in many cases confidential.

Particularly large digital files, such as contracts or patient records, that can't be sent or received via email and are rejected by policy lead employees and other stakeholders to use other means to exchange files. Products like USB sticks, consumer grade file sharing solutions, or cloud services which they know from private use, are readily available. The result: the frequently invoked 'Shadow IT' – the unwanted use of non-authorised software and tools in companies to exchange data. So how can enterprises secure their information when it is in transfer and most vulnerable?

The key to succes **encryption?**

Enterprises are under increasing pressure to protect their data and their communication from unauthorised access by third parties. Taking measures for doing so is inevitable as they are imperative to safeguarding intellectual property as well as successfully meeting ever-growing compliance requirements and data protection regulations. Complex file transfer and email encryption solutions try to eliminate those risks. However, they often fail at striking a balance between security, usability, and cost. Even though there are effective and established encryption methods that can be used for email, they lack three basic demands:

- First, they usually involve complicated acquisition and set-up of public and private keys, and therefore cannot be used ad hoc between two communication partners. This leads to them being ignored or circumvented.
- Second, there is little focus on usability for the average office user or private customer. Many solutions are too complicated to use and therefore are not used at all.
- Finally, many solutions carry very high purchasing costs as well as maintenance costs.

Despite the many encryption methods available on the market, enterprises still need to find solutions for their communication that not only provide security for their data in transfer but that are also affordable and easy enough to use for their employees.

Cryptshare®

Cryptshare

The answer: **Cryptshare.**

Cryptshare is a digital communication solution for the secure exchange of information. With it, emails and files of any size can be exchanged ad hoc easily and securely, with auditability and at low cost. Cryptshare is easy to set up and is immediately available. The intuitive user interface and direct integration in existing applications makes it a workable and user-friendly solution.

The process is deliberately kept simple: the recipient is notified via email that a transfer is available for them. Separately by phone or SMS they receive a unique password from the sender with which they download the messages and files directly and securely from the server that is located in the sender's DMZ. Since the system works without user accounts there is no registration needed for either sender or recipient. Nor is it necessary to purchase, exchange, or manage time-consuming and costly certificates.

This has two advantages: The data is protected from unwanted external access, and it is possible to send much larger files than via common email. The system can handle messages and attachments of sizes of many gigabytes while most email systems are limited to just a few megabytes per transfer.

Cryptshare offers complete auditability across all in- and outgoing transfers. It offers clear and understandable notifications for the sender about when the email and files were sent and delivered to the intended recipient, and a new innovation eliminates the need for passwords entirely. With all this and further functions, it successfully helps companies meet compliance rules and regulations.

From the very start, Cryptshare has adapted to customers' ever-changing requirements and needs. Since the European General Data Protection Regulation (GDPR) took effect in May 2018, those affected are obligated to report violations of data protections. Industries such as healthcare, banking, insurance, or operators of critical infrastructures are under particular scrutiny by regulating authorities. To address enterprises' needs to act, in 2017 Cryptshare added a feature allowing IT staff in any industry to meet legal requirements and enact their company's own guidelines and policies in an easy and flexible way: email classification. Cryptshare protective email classification makes it possible to classify outgoing messages depending on the sensitivity of the contents and drive policy actions in different protection classes as defined by the enterprise.

Cryptshare has been continuously improved to secure customers' data in transit. Cryptshare.express, the Cryptshare cloud service for small enterprises that seek flexibility and minimal costs, was launched in early 2019. Starting in Germany, this SaaS solution is now available in numerous countries across Europe, and it supports small enterprises that do not have the same resources as big corporations. It secures communication in an easy, quick, and effective way.

The introduction of patent pending Cryptshare QUICK Technology in June 2019 represents a ground-breaking revolution for regular exchanges between communication partners. With QUICK, a secret key generates one-time passwords for all transfers between sender and recipient(s), thereby enabling permanent secure connections that are easy to use for employees without needing to involve IT administrators. This represents a meaningful addition, as it builds on the many possibilities Cryptshare already offers for the automated exchange of data with its API, which facilitates great potential for secure machine-to-machine communication between IoT devices.

The company today, geared for **growth.**

A great deal has happened at Cryptshare since the team started its project. At first it was meant to be a custom-made software for a single blue chip client. Today, Cryptshare is the central product of this German software house from the Black Forest.

Not only is the software an organic growth success, but also the company behind it is growing rapidly with currently over 70 employees and the number is increasing fast.

Since 2010 the company has been led by Dominik Lehr and joint CEO Mark Forrest and has recently expanded the leadership team to include the CMO Oliver Gäng, CFO Oliver Kenk and long-time technical leader and CTO Matthias Kess.

In May of 2019, befine Solutions AG became Cryptshare AG. This step places the communication solution Cryptshare centre stage and reflects its significance in the company name. Following this reasoning, a new tagline emerged, changing from: “Making email better” to “Secure all the way”, underscoring the fact that Cryptshare is a digital transport service protecting information when it is most at risk: in transit from senders to recipients.

Excellent perspectives awards and nternational **growth.**

Recent years have been very good for the software developer from Freiburg with being honoured the ‘Cybersecurity Excellence Award 2017’ in the category of ‘Email Security’. This annual award is given to companies, individuals, or products from all over the world that are contributing exceptionally to the field of data security.

2018 started fast with rapid international growth in the United States, UK, and the Netherlands. The regional sales teams in Boston and Arnhem bring Cryptshare as a ‘Made in Germany’ solution to the American and Dutch markets. A further branch office in the UK is steadily contributing to this international growth.

Due to Cryptshare’s success, the team in the USA and the UK continue to grow. Cryptshare AG’s success and sustainable economic management were again confirmed by the ratings of the company’s financial partners, once again underscoring Cryptshare AG’s status as a healthy and well-positioned enterprise.

Milestones.

- 2000: Founding of Connect Software AG by Dominik Lehr as a service provider for specialist bespoke software.
- 2007: Shipping of Cryptshare v1.0 to a small group of customers.
- 2010: Renamed befine Solutions AG, Start of a dedicated Cryptshare sales team, Cooperation with first distribution partners and with resellers.
- 2011: Opening of sales offices in the UK and the Netherlands, Market launch of Cryptshare for Outlook (now Cryptshare for Office 365 & Outlook) and Cryptshare for Notes.
- 2012: Cryptshare is in use in over 20 countries and available in numerous new languages.
- 2013: Cryptshare v3.0 is released with a wide array of new features and an enhanced administration interface enabling significant customisation.
- 2015: Launch of Cryptshare for Outlook v2.0 with new functionality and features and user-centred interface design.
- 2017: ‘Cybersecurity Excellence Award’ in the category of ‘Email-Security’, Launch of the protective email classification as well as an archiving and DMS interface, more than 2.5 million certified users, Founding of Cryptshare Inc. in the USA, Moving headquarters to a new, much larger office in Freiburg im Breisgau, Germany.
- 2018: Launch of SMS Gateway as a password transfer option for Office 365, Launch of cloud service Cryptshare.express in Germany, Cryptshare v4.0 is released with responsive design and new GDPR features, The Cryptshare team grows to more than 60 employees.
- 2019: Launch of cloud service Cryptshare.express in the Netherlands, UK, and 12 more countries, Renaming company to Cryptshare AG to reflect the product’s significance within the business, Launch of Cryptshare QUICK Technology – Save time, not passwords.

 Near the Headquater in Freiburg.

Cryptshare®

Cryptshare AG

Schwarzwaldstr. 151
79102 Freiburg
Germany

Phone: +49 761 / 38913-0
Fax: +49 761 / 38913-115
E-Mail: info@cryptshare.com
Web: www.cryptshare.com

Register Court Freiburg, HRB 6144

CEO: Mark Forrest, Dominik Lehr
Chairman: Thilo Braun

VAT-ID: DE812922179

- Keeping your e-mail private
- Removing file size limits
- Track and trace