

Terms of Use & Service description for Cryptshare on MS Azure

1. Introduction

Cryptshare on MS Azure is a combined offer of IT infrastructure, provided by Microsoft (hosting) and software, provided by Cryptshare AG.

Cryptshare is a software for the secure and encrypted transfer of large files and messages and needs to be activated with a license. This offer is designed for commercial customers with a minimum of 25 employees.

Cryptshare on MS Azure is operated from a Microsoft computing centre of the customer's choice and in accordance with the centre's respective terms and standards/certifications.

Our offer is for all registered users of the MS Azure cloud platform that are commercial customers (nonconsumers) unless the location of the customer must be excluded due to sanctions or country-specific reasons.

After registration, users can purchase the desired IT infrastructure in accordance with Microsoft's terms of use and for the prices determined by Microsoft. The software Cryptshare is subsequently installed on the infrastructure, provided (hosted) by Microsoft, free of charge. To activate the software, a separate license is necessary and can be purchased at Cryptshare AG or its resellers.

Cryptshare AG creates this separate license in the form of a *.txt file and transfers it to the customer electronically. By uploading the license to the respective (hosted) Cryptshare server via the software and by accepting the Cryptshare license agreement, the software is activated and can be used for the duration of the license term.

The customer determines the domain that is to be licensed (e.g. *@ACME.com) thereby generally licensing all employees using this domain. The minimum number of employees is 25.

For enterprises with fewer than 25 employees, Cryptshare.express is available as a hosted service provided by Cryptshare AG. More information can be found under the following link: <https://www.cryptshare.express>.

All email users stored on the Cryptshare server hosted by Microsoft can authenticate themselves with their stored email address via the Cryptshare Web application; given their respective license, they can also authenticate themselves via Office 365 & Outlook. Once authenticated, they can use the Cryptshare server as a sender and as a recipient.

2. Services

Cryptshare on MS Azure enables customers and their internal as well as external communication partners to exchange confidential messages and files bidirectionally in accordance with the terms of use as found in the system. Depending on the configuration, every user must accept the terms of use when sending data.

For providing and downloading data, a web application and, depending on the license, an integration for MS Outlook or for the customer's own communication solutions are available.

Data is transferred between the Cryptshare server and the systems of the sender or recipient(s) by using encryption that is determined by the customer (e.g. TLS v1.2 transportation encryption).

One-time passwords that are individually generated for each transfer are used for the encryption. Due to the nature of service (security by design), it is neither possible for Cryptshare AG nor Microsoft to decrypt the files on the server without knowing the password determined by the sender. This password is neither saved nor transferred by the system.

If the virus scan is activated, data that cannot clearly be classified as unsuspecting is removed from the transfer and the sender is notified.

Messages and files provided on the Cryptshare server for transfer purposes are only stored temporarily. The duration of the retention period can be freely configured by the administrator and is displayed to the sender once the transfer is ready for download. After the retention period has expired, the data is purged and can no longer be retrieved by the recipient. After the data has been sent, the sender no longer has access to it.

The total file size per transfer can be limited. Such limit can also be freely configured by the administrator.

For the purpose of restoring the system in the event of a catastrophe, regular backups of the entire system can be automatically created.

Cryptshare AG ensures that the provided software is operated on suitable hosted hardware (for the purpose of encrypted email and data transfers). The customer can choose from a preselection made by Cryptshare AG when placing their order.

3. Manufacturer support in case of malfunction

We reserve the right to perform manufacturer support exclusively for Cryptshare and its components. Disruption-free performance of service by the computing centre as well as the correct configuration of the network (which is required for the use of Cryptshare) are incumbent on Microsoft and the customer.

Generally, we perform support for malfunctions with Cryptshare products and its components that customers cannot solve with the provided handbooks and documents.

Tickets can be opened 24/7 in German and in English. For doing so, there are the following options:

- Via email: support@cryptshare.com
- Or via telephone: +49 761 38913 100

Events are processed according to their criticality:

- Critical events (malfunctions): Processed Monday to Friday, 8:00 a.m. to 5:00 p.m.(CET)
- Non-critical events: Processed Monday to Friday 9:00 a.m. to 4:00 p.m. (CET)

Cryptshare AG reserves the right to downgrade criticality if the software functions within the scope as described and the customer or MS Azure is responsible for the cause of the disruption.

Critical events are malfunctions that affect the availability of Cryptshare. All other disruptions are non-critical events.

- Response time: four hours for Monday to Friday, 8:00 a.m. to 5:00 p.m. (CET). If the response time exceeds 5:00 p.m., processing will be resumed on the following workday at 8:00 a.m.
- Resolution time: Best effort

4. Customer obligations

The customer assumes obligations that are necessary for duly delivering the service. The following describes but does not limit the activities that the customer needs to deliver free of charge, in a timely fashion, and to the necessary extent:

4.1 The customer is obligated to save their data in a form that is suitable for restoring with feasible effort. There is no right to having data restored by Cryptshare AG.

4.2 The customer is obligated to protect their operating systems and other applications against misuse and keep them free of malware (e.g. by applying up-to-date security patches, using virus scanners, and appropriate configuration of the firewall).

4.3 The customer ensures that they do not send or provide contents for retrieval via Cryptshare on MS Azure if the provision, publishing, transfer, or use of those contents violates applicable law or third-party rights. This is particularly the case for defamatory contents, incitement to hatred, pornographic, or right-wing extremist contents as well as "malicious codes" or other malware. If the customer violates this provision, Cryptshare AG reserves the right to terminate the license agreement for cause and without reimbursement for the purchase price in part or its entirety.

4.4 The customer agrees to written correspondence via email and will ensure that a current email address is always on file. The customer has been informed that essential product information is sent via email.

4.5 The customer is obligated to use and support the troubleshooting process.

4.6 The customer is responsible for adhering to all legal regulations, laws, provisions, and industry-specific rules that are relevant and applicable in the context of using Cryptshare on MS Azure and ensures compliance thereof. This includes, but is not limited to, compliance with confidentiality agreements, for example from employment. The customer assures that data relevant to confidentiality are only transferred if effective consent has been obtained.

4.7 The customer assures that their bidirectional use of Cryptshare on MS Azure takes place under suitable terms of use. These can be deposited and individually modified by the administrator. By depositing the terms of use it is possible to enable a mandatory acceptance of said terms by the users.

5. Pricing and advertising

Obtaining the Cryptshare software via the MS Azure cloud platform is free of charge from Cryptshare AG.

When purchasing the separate license for the respective license fee to activate the Cryptshare software, the customer can choose a license term of 12 or 36 months.

Valid prices are individually offered and agreed on, dependent on the extent of use.

Microsoft will determine and invoice costs for infrastructure etc. separately. The pricing from Microsoft is their sole responsibility.