Stadtsparkasse Düsseldorf

Berliner Allee 33
40212 Düsseldorf

Telefon: 0211 878-2211
Fax: 0211 878-1748
E-Mail: service@sskduesseldorf.de

Stadtsparkasse
Düsseldorf

Sicherheit mit System: CryptShare®

Ein System für die sichere Dateiübertragung.

Leitfaden und Nutzungsbedingungen.

Leitfaden zur Nutzung des Systems CryptShare®

Die Web-Anwendung CryptShare® ermöglicht den einfachen und sicheren Austausch vertraulicher Informationen durch die verschlüsselte (Verschlüsselung über 256 Bit AES) Ablage von Dateien auf dem CryptShare®-Server. Diese Dateien können mit einem Kennwort abgerufen werden. Der Server informiert Empfänger und Absender über die Vorgänge auf dem Server.

Bei der Ersteinrichtung erfolgt die Verifizierung des Benutzers über die Prüfung der E-Mail-Adresse. Diese Verifizierung ist für maximal 30 Tage gültig. Nach Ablauf dieser Zeit verlangt das System bei der Anmeldung wieder eine neue Verifizierung.

Eine neue Verifizierung ist auch bei Änderung der E-Mail-Adresse erforderlich.

Das für den Zugriff zu vergebende Kennwort muss aus mindestens 8 Zeichen bestehen.

Um Ihnen die Funktionsweise von CryptShare® zu verdeutlichen, ist nachfolgend zunächst der

- **Ablauf bei der Bereitstellung von Dateien**

und anschließend der

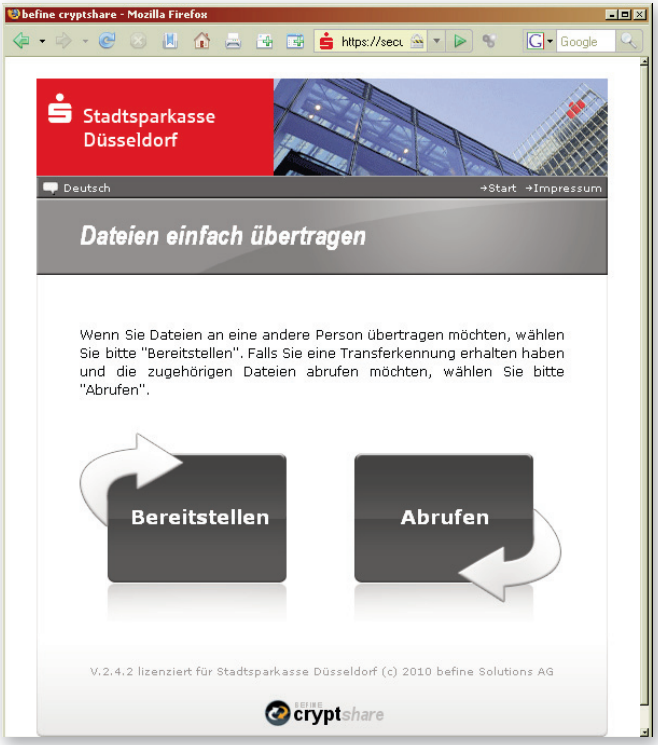
- **Ablauf beim Abruf von Dateien**

dargestellt.

Ablauf bei der Ablage (Bereitstellung) von Dateien

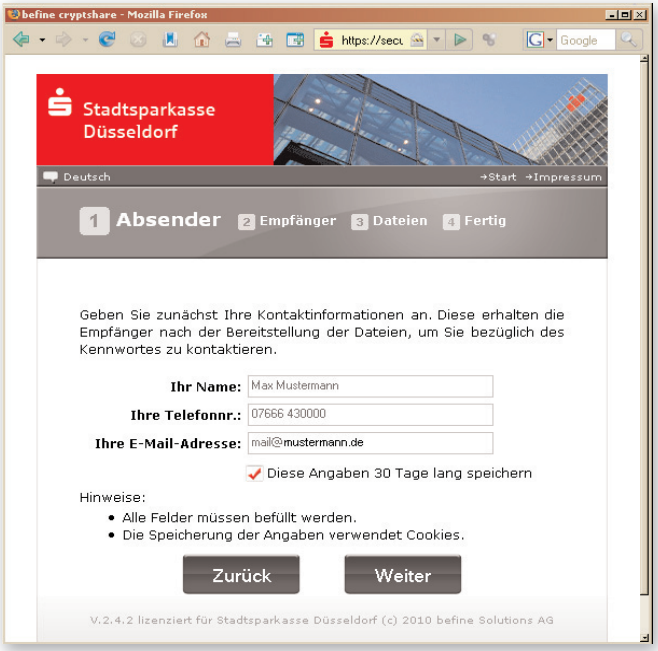
Die für den Informationsaustausch erforderlichen Schritte/ Handlungen sind in den jeweiligen Bildschirmmasken beschrieben.

Rufen Sie bitte im Browser die folgende Internetseite auf:
https://securebox.sskduesseldorf.de/
Es erscheint die folgende Startseite:



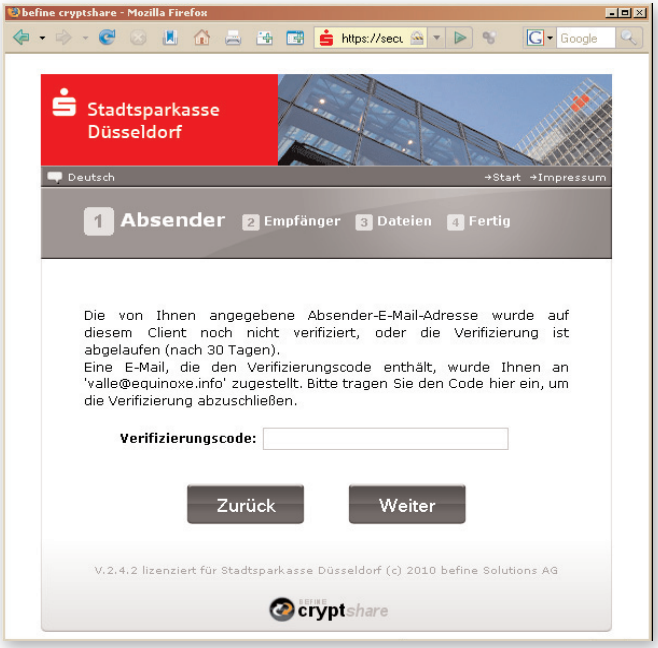
Schritt 1

Bestätigen Sie den Schalter „Bereitstellen“



Schritt 2

Tragen Sie hier Ihre Kontaktdaten ein.



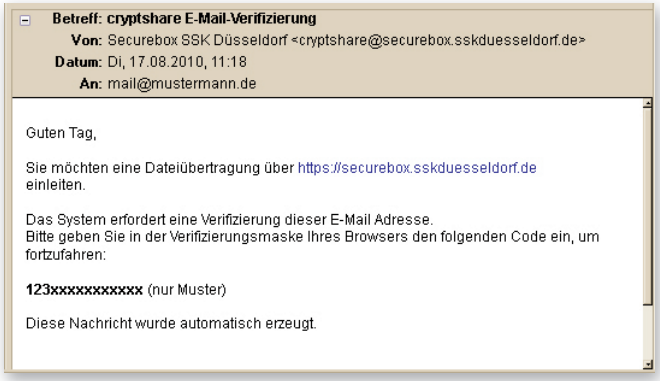
Schritt 3

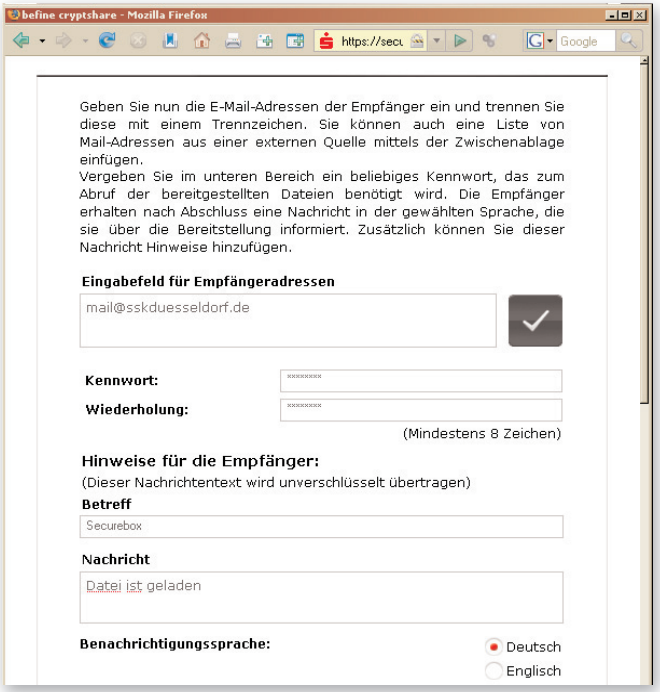
Verifizierungscode: Eine Verifizierung (Gültigkeitsprüfung) der E-Mail-Adresse ist bei der ersten Anmeldung am CryptShare®-System sowie immer spätestens nach Ablauf von 30 Tagen erforderlich.

Wechseln Sie in Ihren E-Mail-Eingang und tragen Sie den per Mail mitgeteilten Verifizierungscode hier ein.

Starten Sie ihre E-Mail-Anwendung. Wechseln Sie in Ihren E-Mail-Eingang, öffnen Sie das automatisch vom Absender **„cryptshare@securebox.sskduesseldorf.de“** zugestellte E-Mail und tragen Sie den darin mitgeteilten Verifizierungscode hier ein.

Muster einer automatisierten E-Mail mit dem Verifizierungscode der E-Mail-Adresse des Absenders.



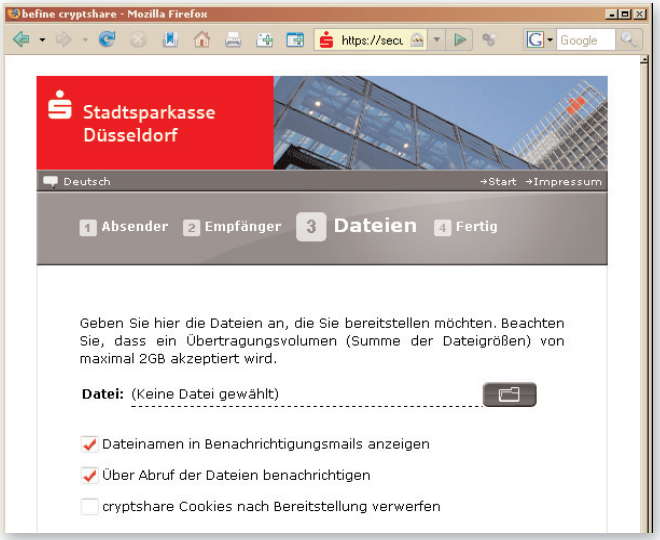


Schritt 4

E-Mail-Adresse Empfänger:
Geben Sie hier die E-mail-Adresse des Empfängers ein und klicken anschliessend auf den „Bestätigen“ Button rechts. Sie haben auch die Möglichkeit, mehrere Empfänger durch Komma getrennt anzugeben.

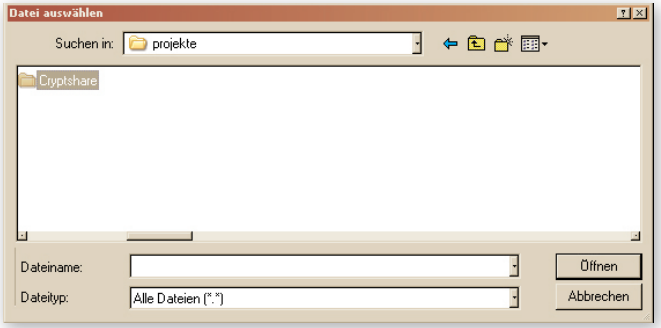
Kennwort:
Legen Sie für die Empfänger ein Kennwort fest, tragen Sie es hier ein und teilen Sie dieses den Empfängern z.B. telefonisch mit. Ohne die Kenntnis dieses Kennworts ist den Empfängern ein Zugriff auf die in CryptShare® eingestellten Dateien nicht möglich. Schreiben Sie das Kennwort niemals in das Nachrichtenfeld für den Empfänger.

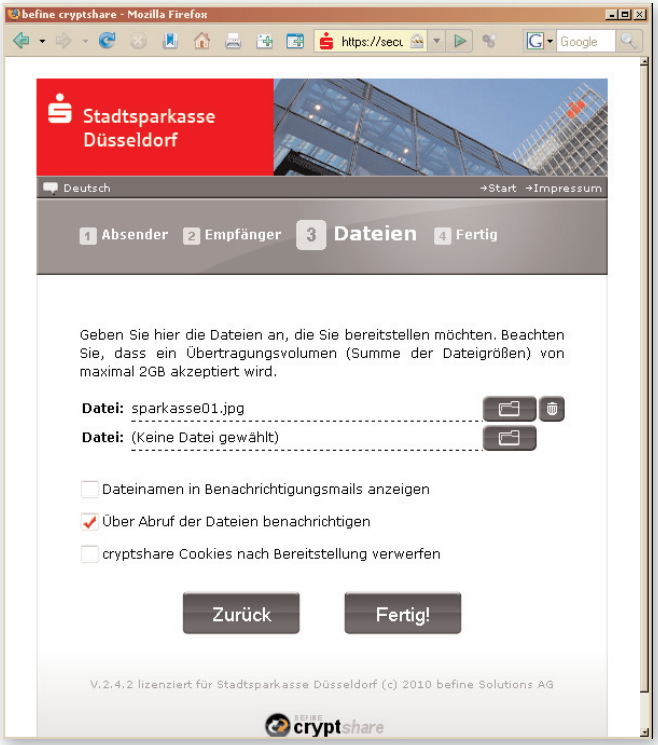
Hinweise für die Empfänger:
In dieses Feld können Sie für den Empfänger eine Kurznachricht einstellen. Bitte berücksichtigen Sie hierbei, dass der in dieses Feld eingetragene Text unverschlüsselt und somit ungeschützt an die Empfänger übertragen wird.



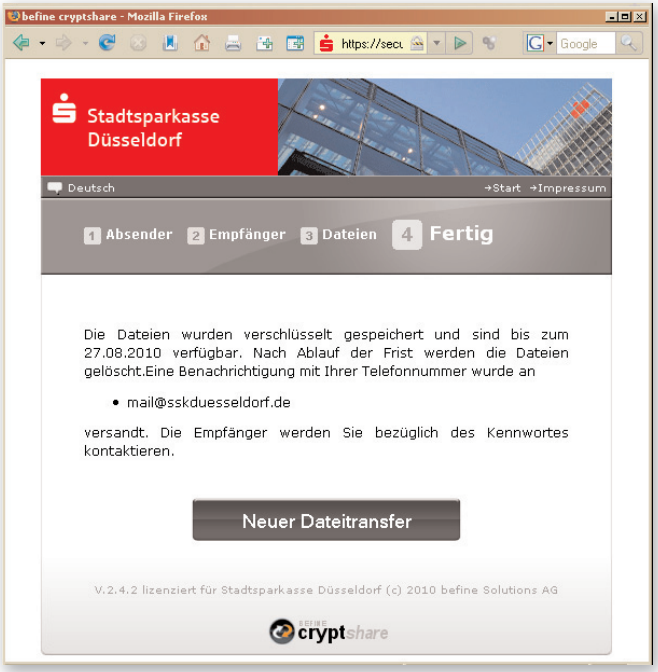
Schritt 5

Durchsuchen:
Mit der Bestätigung dieses Schalters öffnet sich ein Windows Fenster und ermöglicht analog dem Windows Explorer die Suche und Auswahl der zur Übermittlung bestimmten Datei.





Weitere Dateien anfügen:
Sie haben jederzeit die Möglichkeit, weitere Dateien anzuhängen oder über das Papierkorbsymbol zu löschen.



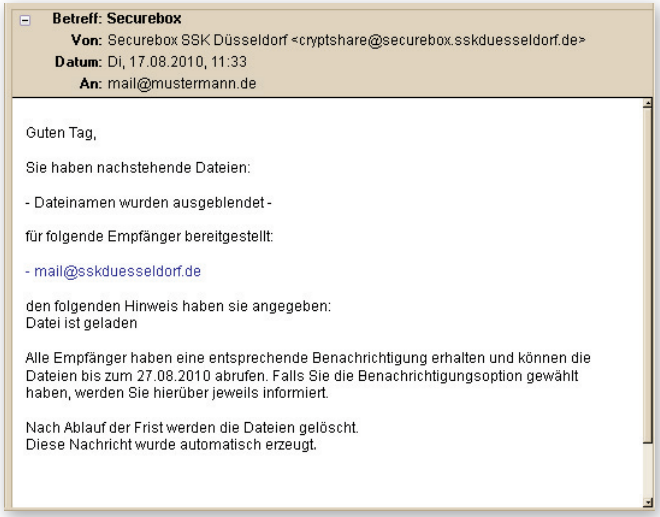
Schritt 6

Zum Abschluss der Bereitstellung betätigen Sie den Schalter „Fertig“ und es erscheint diese Maske.

Bitte beachten Sie die maximale Speicherdauer der Datei(en) von 10 Tagen.

Schritt 7

Mit der Schließung des Browserfensters wird der Zugriff geschlossen und die Verbindung zur CryptShare®-Anwendung getrennt.
Zur Bestätigung erhalten Sie vom System die folgende Nachricht per E-Mail zugestellt:



Betreff: Securebox
Von: Securebox SSK Düsseldorf <cryptshare@securebox.sskduesseldorf.de>
Datum: Di, 17.08.2010, 11:33
An: mail@mustermann.de

Guten Tag,

Sie haben nachstehende Dateien:

- Dateinamen wurden ausgeblendet -

für folgende Empfänger bereitgestellt:

- mail@sskduesseldorf.de

den folgenden Hinweis haben sie angegeben:
Datei ist geladen

Alle Empfänger haben eine entsprechende Benachrichtigung erhalten und können die Dateien bis zum 27.08.2010 abrufen. Falls Sie die Benachrichtigungsoption gewählt haben, werden Sie hierüber jeweils informiert.

Nach Ablauf der Frist werden die Dateien gelöscht.
Diese Nachricht wurde automatisch erzeugt.

Ablauf beim Abruf von Dateien

Schritt 1

Mailnachricht über die Bereitstellung von Dateien

Betreff: Dateien von Max Mustermann (1): sparkasse01.jpg
Von: Securebox SSK Düsseldorf <cryptshare@securebox.sskduesseldorf.de>
Datum: Di, 17.08.2010, 11:33
An: mail@skkduesseldorf.de

Guten Tag,

Max Mustermann hat Ihnen Dateien zur Verfügung gestellt. Sie können diese bis zum 27.08.2010 abrufen. Nach Ablauf der Frist werden die Dateien gelöscht.
Die Übertragung erfolgt verschlüsselt.

Das zur Entschlüsselung der Dateien notwendige Kennwort erhalten Sie vom Absender unter Tel.: 0761-12345 (Muster)

I. Direkter Abruf
Sie können Ihre Dateien durch Klick auf folgenden Link und Eingabe des Kennwortes abrufen:
https://securebox.sskduesseldorf.de/download1.php?id=UA8jP2f4F6&lg=de

II. Manueller Abruf
Öffnen Sie die Website https://www.securebox.sskduesseldorf-postfach.de in Ihrem Browser
Klicken Sie auf "Abrufen"
Geben Sie die Transferkennung 123xxxxxxx (Muster) sowie das Kennwort ein, um auf die bereitgestellten Dateien zuzugreifen.

Diese Nachricht wurde automatisch erzeugt.

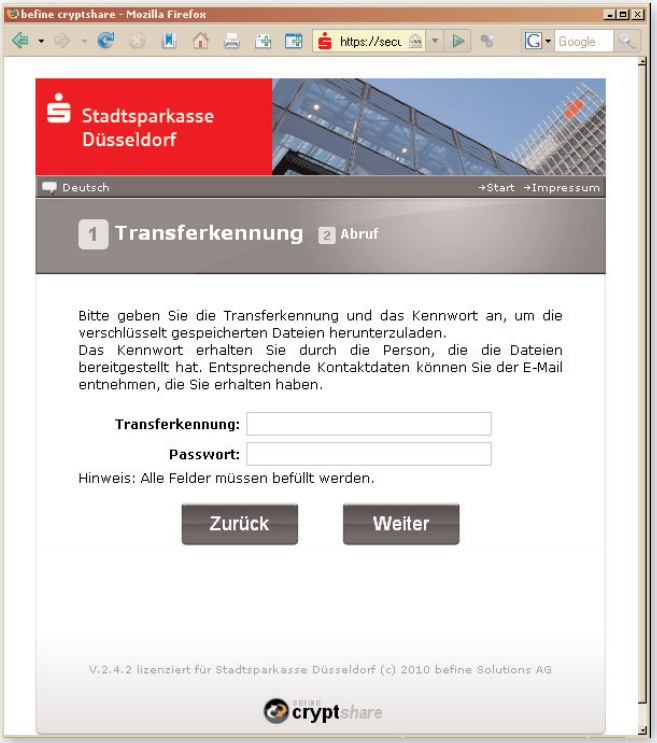
Am einfachsten ist der Abruf über den in der E-Mail angeführten Link.

Schritt 1a

Es erscheint das folgende Bild (Maske).
Bitte tragen Sie hier lediglich das vorab mitgeteilte Passwort ein.

Schritt 1b

Wenn Sie den Dateiabruf manuell durchführen, erscheint diese Maske.
Weiter mit Schritt 1c.



Schritt 1c

In diesem Fall, sind sowohl die Transferkennung als auch das Passwort manuell einzutragen.

Schritt 2

Sie können nun mit einem Klick auf den Dateinamen die Datei öffnen.

Je nach den von Ihnen in Ihrem Unternehmen getroffenen Sicherheitsvorgaben können Sie die Datei unmittelbar auf Ihrem PC-System speichern oder aus der zugrundeliegenden Anwendung öffnen:

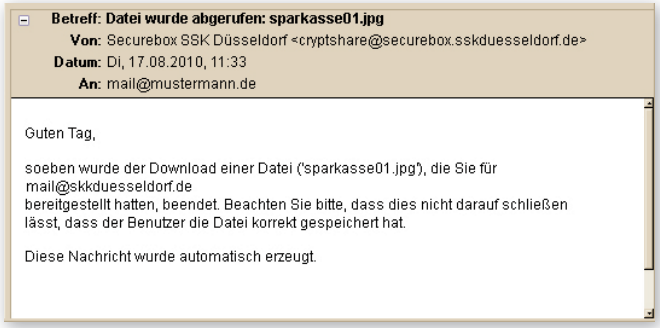
z.B. Microsoft Word, Excel oder Adobe Reader für PDF-Dateien.

Schritt 3

Mit Betätigung des Schalters „Beenden“ kommen Sie wieder in die Ausgangsmaske zurück.

Der Absender wird mit folgender Nachricht über den Abruf informiert:

Mailnachricht beim Dateiabruf an den Absender



Stadtsparkasse Düsseldorf

Nutzungsbedingungen für die Kommunikation mittels **CryptShare®**

1.
Zweck der Kommunikation mittels CryptShare®

Für den sicheren elektronischen Austausch von Informationen mit Dritten, insbesondere ihren Geschäftspartnern bedient sich die Stadtsparkasse Düsseldorf (nachfolgend: Sparkasse) der Web-Anwendung CryptShare®.

Bei der Web-Anwendung CryptShare handelt es sich nicht um ein E-Mail-System. Das System hat lediglich die Funktion eines elektronischen Postfachs.

Der jeweilige Absender stellt die Informationen zum Abruf auf dem System bereit. Der Empfänger wird systemgesteuert per E-Mail über für Ihn zum Abruf bereitgestellte Dateien informiert.

2.
Beschränkung der Kommunikationsinhalte

Die Kommunikation mittels Crypt-Share® dient nur dem Austausch vertraulicher Informationen.
Als vertraulich im Sinne dieser Regelung gelten Informationen, die dem
- Bankgeheimnis

oder
- Betriebsgeheimnis der Sparkasse

oder
- Berufs- oder Betriebsgeheimnis des/von Dritten unterliegen

oder
- es sich um schutzwürdige personenbezogene Daten im Sinne des § 3 Bundes-Datenschutzgesetz handelt.

Die Sparkasse gibt über CryptShare® keine rechtsgeschäftlichen Erklärungen ab

oder nimmt rechtsgeschäftliche Erklärungen oder Aufträge (z.B. Überweisungen, Wertpapierorders, Einwendungen gegen Rechnungsabschlüsse) entgegen.

3.
Vertraulichkeit/ Datensicherheit

Zum Schutz der Daten vor unberechtigter Kenntnisnahme und zur Wahrung der Vertraulichkeit

- erfolgen sowohl die Ablage der Daten auf dem Crypt-Share®-System als auch die Übertragung (Transfer bei der Einstellung und beim Abruf) in verschlüsselter Form.

- wird der Zugriff auf die im CryptShare®-System abgelegte Datei mit einem jeweils individuell vergebenen Passwort geschützt.

Das zur Verschlüsselung verwendete Verfahren entspricht dem anerkannten technischen Stand.

Mit dem Abruf der Daten werden diese auf dem CryptShare®-System nicht sofort gelöscht, sondern stehen bis zum mitgeteilten Ablaufdatum (Ziffer 4. Zugang der Informationen/ Rechtzeitiger Datenabruf) für weitere Abrufe zur Verfügung.

Der Adressat/Nutzer hat dafür Sorge zu tragen, dass keine unbefugten Personen von dem mitgeteilten Passwort Kenntnis erhalten.

4.
Zugang der Informationen/ Rechtzeitiger Datenabruf

Die in CryptShare® eingestellten Dateien gelten gegenüber dem Adressaten mit dem erfolgreichen Abruf (Download) als zugegangen. Es obliegt dem Adressaten, den rechtzeitigen Abruf der für ihn bereitgestellten Dateien sicherzustellen.

Die Sparkasse weist ausdrücklich darauf hin, dass die über CryptShare® bereitgestellten Dateien nur innerhalb eines Zeitraums von 10 Kalendertagen, beginnend mit dem Zeitpunkt der Bereitstellung der Dateien, abrufbar sind.

5.
Protokollierung

Im Rahmen der Kommunikation (Dateiaustausch) werden folgende Vorgänge protokolliert:

Absender:
- Datum und Uhrzeit der Dateiablage auf dem CryptShare®-System,
- die E-Mailadresse des Absenders und des Empfängers,
- der vollständige Dateiname der abgelegten Datei,
- die Dateigröße in Megabyte,
- eine vom System intern vergebene Datei-Identifikation.

Empfänger:
Unter seiner E-Mailadresse

- Datum und Uhrzeit des Dateiabrufs vom CryptShare®-System,
- der vollständige Dateiname der abgerufenen Datei,
- die bei der Dateiablage vom System intern automatisch vergebene Datei-Identifikation.

Diese Protokolldaten werden nach 90 Tagen gelöscht.

6.
Haftung

Die Sparkasse übernimmt keine Haftung für Störungen oder Probleme bei der Kommunikation über CryptShare®, die außerhalb ihres Verantwortungsbereichs liegen.

Im Übrigen haftet die Sparkasse nur bei Vorsatz oder grober Fahrlässigkeit oder bei der Verletzung von Leben, Körper oder Gesundheit. Im Falle einfacher Fahrlässigkeit haftet die Sparkasse nur bei der Verletzung von vertragswesentlichen Pflichten (Kardinalpflichten), wobei die Haftung auf die typischerweise bei Vertragsschluss vorhersehbaren Schäden begrenzt ist.

Die Haftung für entgangenen Gewinn oder unvorhersehbare Schäden ist auch im Falle einfacher Fahrlässigkeit ausgeschlossen.

7.
Veränderungen betreffend der Kommunikation mittels CryptShare®

Die Sparkasse ist gegenüber den Nutzern nicht verpflichtet, die Kommunikationsmöglichkeit über CryptShare® dauerhaft aufrecht zu erhalten. Veränderungen aufgrund geänderter rechtlicher, technischer oder sonstiger Rahmenbedingungen sind jederzeit möglich.

Technische Änderungen vorbehalten.
Stand: 15.08.2010
Stadtsparkasse Düsseldorf