



# mailclad

**Microsoft Outlook® AddOn**

## Benutzerhandbuch

Lockzone®

Copyright

© 2002 - 2005 Lockzone GmbH, Brieffach 61, Hönower Str. 35, 10318 Berlin

Auflage 1

2005-09

Alle Rechte vorbehalten.

Alle im Programm, der Hilfe oder Dokumentation angegebenen Warenzeichen sind Eigentum der jeweiligen Besitzer.



## INHALTSVERZEICHNIS

1. ALLGEMEINES.....	4
1.1. Kundendienst.....	5
1.2. Auslieferungskomponenten .....	6
2. INSTALLATION .....	7
2.1. Systemvoraussetzungen .....	8
2.2. Installtion.....	9
3. FUNKTIONEN .....	11
3.1. E-Mail Verschlüsseln .....	12
3.2. Einschreiben.....	13
3.2.1. Der Ablauf .....	14
4. INDEX.....	22



## 1. ALLGEMEINES

Vielen Dank, dass Sie sich für das mailclad Microsoft Outlook® AddOn entschieden haben – der sicheren Verschlüsselungskomponente für Ihre e-Mail Kommunikation über Microsoft Outlook®.

Verschlüsseln Sie mit einem Klick Ihre e-Mail und senden Sie diese an Nutzer der mailclad – Produktreihe. Mailclad Microsoft Outlook® AddOn erlaubt Ihnen eine 4-Augen Kommunikation, die durch eine spezielle Sicherheitshardware geschützt wird.

Im Gegensatz zu herkömmlichen, softwarebasierten Lösungen ist der Kern der Sicherheit der mailclad Produktreihe (der sog. private Schlüssel) nur auf der Sicherheitshardware abgespeichert und ist durch ein komplexes Verfahren durch Zugriff Dritter geschützt.

Die verwendete Sicherheitshardware des mailclad Microsoft Outlook® AddOn wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der höchst-möglichen internationale Zertifizierung ausgezeichnet. (common criteria EAL 4+)

Im Besonderen zeichnet sich der Mailclad Microsoft Outlook® AddOn durch die Einfachheit in der Benutzung aus – nur ein Klick für eine Verschlüsselung – mehr know-how ist vom Benutzer nicht gefordert.

## 1.1. KUNDENDIENST

Unser Support beantwortet Ihnen gern weitere Fragen zum mailclad Microsoft Outlook® AddOn. Um eine möglichst rasche Bearbeitung Ihrer Anfrage zu gewährleisten, empfehlen wir Ihnen Ihre Kundennummer und die Seriennummer Ihrer Lizenz stets anzugeben. Die Seriennummer finden Sie auf dem im Paket enthaltenen Registrierungsformular.

Erreichbar ist unser Support über folgende Wege:

Web: [www.Lockzone.de](http://www.Lockzone.de) (updates / FAQ)

e-Mail: [support@Lockzone.de](mailto:support@Lockzone.de)

Tel.: +49 (0) 30 50 96 85 74

Fax: +49 (0) 30 50 96 85 75

Anregungen zu unseren Produkten und unserem Service sind stets willkommen.

Falls Sie einen Servicevertrag mit einem Lockzone Service - Partner oder Lockzone direkt abgeschlossen haben, stehen Ihnen weitere gesonderte Kontaktdaten zur Verfügung.

## 1.2. AUSLIEFERUNGSKOMPONENTEN

Im Lieferumfang des mailclad Microsoft Outlook® AddOn sind folgende Komponenten enthalten:

- CodeMeter USB Stick (CM-Stick/M) ohne Flash Disk
- CD mit Installationsdateien
- Hülle für den USB Stick
- Umhängeband
- Registrierungsformular
- Handbuch

Bitte überprüfen Sie die erwähnten Lieferbestandteile auf ihre Vollständigkeit. Sollten Einzelkomponenten fehlen, wenden Sie sich bitte an Ihren Lieferanten.

## 2. INSTALLATION

Auf der im Lieferumfang enthaltenen Programm-CD befindet sich neben diesem Handbuch die Datei „Setup\_OutlookAddOn.exe“. Die Setup-Routine installiert alle notwendigen Komponenten des mailclad Microsoft Outlook® AddOn. Nach der Installation stehen Ihnen die Funktionen zur Verschlüsselung von e-Mails und dem Senden von Einschreibern sofort zur Verfügung.

## 2.1. SYSTEMVORAUSSETZUNGEN

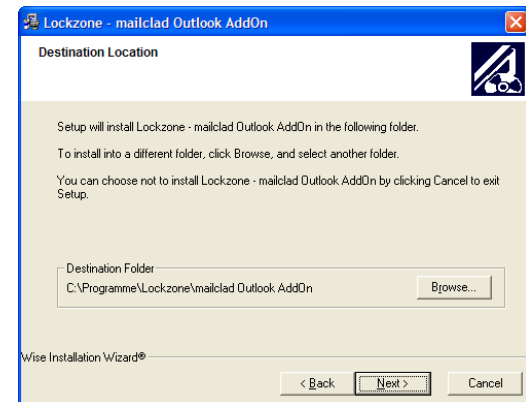
Die Mindestvoraussetzungen für den Betrieb sind:

<b>BETRIEBSSYSTEME</b>	Microsoft Windows 2000/ME/XP Home/XP Professional
<b>USB SCHNITTSTELLE</b>	USB Standard 1.1
<b>MIRCOSOFT OUTLOOK®</b>	Version 2000, 2002, XP, 2003

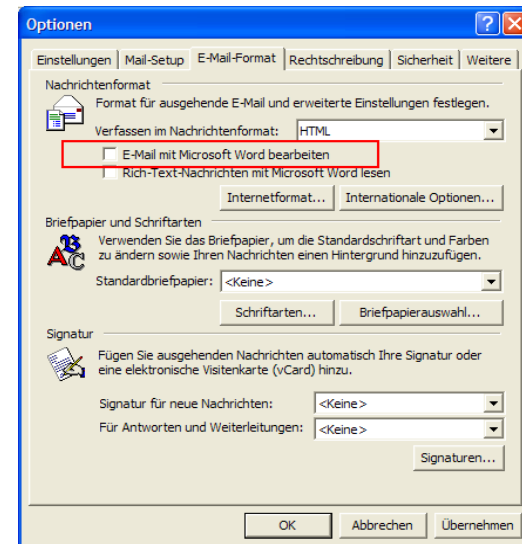
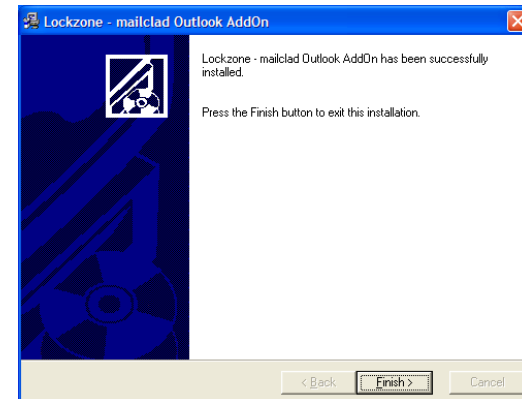


## 2.2. INSTALLTION

- Schritt 1.** Stecken Sie den CodeMeter USB - Stick in einen freien USB - Steckplatz. Der CodeMeter USB-Stick wird als neuer Massenspeicher erkannt.
- Schritt 2.** Legen Sie die Original-CD von mailclad Microsoft Outlook® AddOn in das CD-Fach ein. Das Setup startet automatisch.  
Sollten Sie die Autostartfunktion an Ihrem System deaktiviert haben, starten Sie das im Basisverzeichnis befindliche Programm „Setup.exe“.
- Schritt 3.** Wählen Sie zunächst die Installationsprache. Anhand dieser Auswahl wird ebenfalls die Installationsvariante des mailclad Microsoft Outlook® AddOn ausgewählt.
- Schritt 4.** Sie erhalten nun in mehreren Dialogen wichtige Hinweise zum Produkt. Lesen Sie bitte diese Hinweise gründlich durch und bestätigen Sie jeden Dialog mit einem Druck auf die [Next >] Schaltfläche.
- Schritt 5.** Im Dialog „Destination Location“ können Sie ein Zielverzeichnis festlegen in dem mailclad Microsoft Outlook® AddOn gespeichert wird. Drücken Sie hierzu die Schaltfläche [Browse...]. Es öffnet sich der Verzeichnisauswahldialog. Wählen Sie das Ziel aus und bestätigen Sie den Dialog mit der [Speichern] Schaltfläche.
- Schritt 6.** Die Setup-Routine besitzt nun alle Informationen und beginnt mit der Installation.



- Schritt 7.** Während der Installation werden notwendige Programmteile für den Betrieb des CodeMeter USB-Sticks kopiert. Hierzu werden ggf. weitere Informationen abgefragt.
- Schritt 8.** Der Abschluss der Installation wird mit dem Finish-Dialog angezeigt. Schließen Sie die Installation mit dem Druck auf die [Finish] Schaltfläche ab.
- Schritt 9.** Um mailclad Microsoft Outlook® AddOn nun verwenden zu können, starten Sie bitte Microsoft Outlook® neu.
- Schritt 10.** Die Funktionen von mailclad Microsoft Outlook® AddOn stehen nur dann zur Verfügung, wenn Sie den in Microsoft Outlook® integrierten e-Mail Editor verwenden. Schreiben Sie e-Mails in Word können Verschlüsselungsmethoden nicht verwendet werden. Prüfen Sie deshalb die Einstellungen im Optionsdialog von Microsoft Outlook® (Meüpunkt: Extras/Optionen).
- Schritt 11.** Deaktivieren Sie die Option „E-Mail mit Microsoft Word bearbeiten“.



### 3. FUNKTIONEN

Das derzeitige e-Mail Verfahren ähnelt dem Versenden einer Postkarte in Papierform. Jeder, der mit der Postkarte in Berührung kommt kann den Inhalt lesen und für sich verwenden.

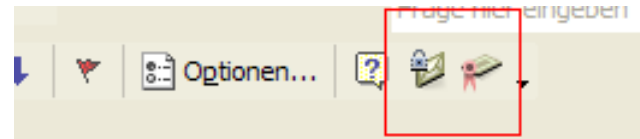
Eine versendete e-Mail wird über mehrere Stationen transportiert. Oft werden Kopien der e-Mail angelegt. Jeder, der Zugriff auf eine Kopie hat, kann auch den Inhalt der Mail lesen.

Versenden Sie in Zukunft Ihr e-Mail in einem gepanzertem Briefumschlag. Dieser elektronische, gepanzerte Briefumschlag wird Ihnen durch die Methode der sicheren Verschlüsselung von mailclad Microsoft Outlook® AddOn zur Verfügung gestellt.

In diesem Kapitel erfahren Sie wie Sie mit der One-Klick Methode Ihre e-Mails sicher verschlüsseln und so einen echten, elektronischen Brief versenden können, den nur der Empfänger lesen kann, für den er auch bestimmt ist.

### 3.1. E-MAIL VERSCHLÜSSELN

Erstellen Sie wie gewohnt eine neue e-Mail in Microsoft Outlook®. Sie finden im e-Mail Dialog zwei neue Icons in der Menüleiste.

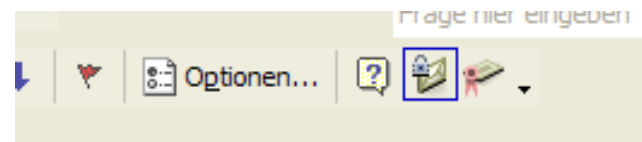


Durch einen Klick auf diese Icons schalten Sie die Funktion der Verschlüsselung und des in Kapitel () beschriebenen Einschreibevorgangs ein bzw. aus..

Damit Sie eine e-Mail (auch mit Anhang) verschlüsselt an einen Nutzer der mailclad - Produktfamilie senden können, müssen Sie sich gegenseitig sog. öffentliche Schlüssel austauschen, mit denen jeweils die Mails verschlüsselt werden.

Hierzu senden Sie eine unverschlüsselte e-Mail an den mailclad – Nutzer , mit dem sie in Zukunft gesichert kommunizieren möchten. An die e-Mail wird Ihr öffentlicher Schlüssel automatisch angehängt. Der Empfänger soll auf diese e-Mail eine beliebig Antwort schicken. Durch diese Antwort erhalten Sie von der Gegenseite den öffentlichen Schlüssel. Ab diesem Zeitpunkt können Sie verschlüsselt kommunizieren.

Senden Sie nun Ihre erste, verschlüsselte Nachricht in dem Sie wieder eine neue e-Mail verfassen. Tragen Sie als Empfänger einen (oder auch mehrere) Kontakte ein, mit dem Sie den öffentlichen Schlüssel ausgetauscht haben.



Klicken Sie das linke der neuen Icons (Nachricht verschlüsselt versenden) in Ihrer Menüleiste. mailclad Microsoft Outlook® AddOn verschlüsselt automatisch beim Senden Ihre Mail unter Verwendung der mitgelieferten Sicherheitshardware (USB Stick CodeMeter).

Der Nutzer eines mailclad Produkts als Empfänger Ihrer e-Mail muss keine weiteren Aktion ausführen um Ihre e-Mail lesen zu können. Die e-Mail wird automatisch entschlüsselt und lesbar dargestellt.

Im Gegenzug entschlüsselt mailclad Microsoft Outlook® AddOn automatisch eine an Sie gerichtete e-Mail.

**Hinweis:** Um eine e-Mail verschlüsselt versenden zu können muss von jedem Empfänger ein öffentlicher Schlüssel existieren. Ist ein Empfänger dabei, dessen öffentlicher Schlüssel nicht vorliegt, wird die e-Mail nicht versendet. Erst wenn in der Empfängerliste nur Empfänger mit bekanntem Schlüssel enthalten sind wird die e-Mail versendet.

### 3.2. EINSCHREIBEN

Das Einschreibeverfahren ist eine spezielle Form der Kommunikation zwischen Nutzern von e-Mail Produkten der mailclad – Reihe. Entsprechend dem Einschreibeverfahren der „Papier-Post“ versenden Sie eine e-Mail gekennzeichnet als Einschreiben. Der Empfänger muss zunächst den Empfang der e-Mail quittieren und bekommt diese dann erst ausgehändigt. Er kann aber auch den Empfang der e-Mail ablehnen, was dem Absender wiederum umgehend mitgeteilt wird. Wenn der Empfänger ablehnt kann er die e-Mail nicht lesen.

Sie garantieren durch dieses Verfahren die Zustellung der e-Mail beim Empfänger und haben so auch einen Nachweis über die Annahme der e-Mail.

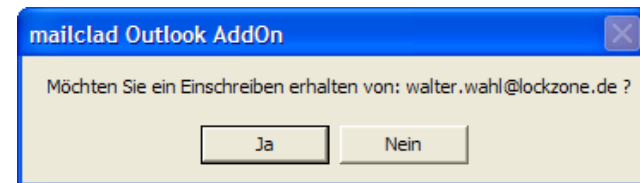
### 3.2.1. DER ABLAUF

Erstellen Sie eine neue e-Mail, die Sie im Einschreibeverfahren an einen Kontakt senden möchten. Tragen Sie als Empfänger einen Nutzer der mailclad Produktfamilie ein. Mit dem Empfänger müssen Sie bereits die öffentlichen Schlüssel ausgetauscht haben.

Starten Sie das Einschreibeverfahren mit dem selektieren des rechten Icons (Nachricht als Einschreiben versenden). Senden Sie nun die e-Mail ab.



Ihre e-Mail wird nun verschlüsselt an den Empfänger gesendet. Entgegen dem einfachen Verschlüsselungsverfahren, wird beim Empfänger die e-Mail zunächst nicht entschlüsselt. Der Empfänger erhält nur eine Meldung über den Eingang eines Einschreibens. Nimmt der Empfänger das Einschreiben durch Bestätigung der Nachricht mit der [Ja] Schaltfläche an, wird diese Antwort an Sie zurück gesendet. Beim Lesen dieser Antwort e-Mail sendet mailclad Microsoft Outlook® AddOn automatisch den Öffnungscode an den Einschreibeempfänger. Erst jetzt wird das Einschreiben beim Empfänger entschlüsselt und er kann die e-Mail lesen.



Lehnt der Empfänger das Einschreiben ab, wird Ihnen auch hierüber eine Antwort e-Mail zugesendet. Das Einschreiben wird in diesem Fall beim Empfänger automatisch gelöscht.

Entsprechend dieser Vorgehensweise können Sie auch selbst Einschreiben empfangen. Bestätigen Sie das Einschreiben mit dem Druck auf die [Ja] Schaltfläche. Nachdem der Sender Ihnen daraufhin den Freigabecode für das Einschreiben zugesendet hat, können Sie das empfangene Einschreiben lesen.



## 4. GLOSSAR

### **APOP**

Das APOP-Protokoll ist ein erweitertes POP-Protokoll mit verbesserten Sicherheitsmechanismen. APOP verschlüsselt die Authentifizierung kryptografisch, um sie so gegen unerlaubtes Mithören zu schützen.

### **CRAM-MD5**

CRAM-MD5 ist ein Mechanismus zur Authentifizierung von Benutzern an einem e-Mail Server. CRAM-MD5 verwendet zur Authentifizierung einen Frage-Antwort-Mechanismus (CRAM, Challenge-Response Authentication Mechanism) basierend auf dem Zeitstempel des Servers und dem Benutzer-Passwort unter Zuhilfenahme der kryptographischen Prüfsummen-Funktion MD5 (message digest 5). Die Einzelheiten werden in RFC 2195 beschrieben.

### **Digest-MD5**

“Digitaler Fingerabdruck” einer beliebigen Nachricht. Der MD5-Hashfunktion wird in RFC 1321 definiert.

### **ECC (Elliptic Curve Cryptography)**



Elliptische Kurven werden zwar seit geraumer Zeit in der Mathematik studiert, finden aber erst seit kurzem eine Anwendung in der Praxis. So werden sie heute zur Faktorisierung, bei Primzahlnachweisen und in der Public-Key-Kryptographie eingesetzt. Als Verfahren der Verschlüsselung sind sie geeignet, die etablierten Standards DES (Data Encryption Standard) und RSA (Rivest, Shamir, Adleman) abzulösen, weil es wesentlich kürzere Schlüssel benötigt. Ein 160 Bit langer ECC-Schlüssel bietet beispielsweise die gleiche Sicherheit wie ein 1024 Bit langer RSA-Schlüssel.

### **e-Mail Client**

Ein Programm Lesen und Schreiben von e-Mails. Bekannte Vertreter sind hier der mailclad Communicator PRO, Microsoft Outlook, oder

### **IMAP**

Internet Message Access Protocol nach RFC 1730. Spezifikation für die client-seitige Manipulation einer entfernten Mailbox. IMAP definiert Methoden zum Erstellen, Löschen und Umbenennen einer Mailbox sowie zum prüfen, ob neue Nachrichten vorhanden sind. Ferner erlaubt IMAP auszugsweises Laden (von Teilen) einer eMail.

### **Kryptographie**

Die Kryptografie beschäftigt sich mit der Entwicklung von Algorithmen zur Verschlüsselung von Informationen. Als Wissenschaft befasst sich die Kryptografie dazu mit der Entwicklung von Kryptosystemen bzw. den Verfahren zur Verschlüsselung und der (befugten) Entschlüsselung von Daten.

In der Anwendung geht es darum, vertrauliche Nachrichten über nicht vertrauenswürdigen Nachrichtenverbindungen auszutauschen. Zu diesem Zweck werden Nachrichten so umgewandelt (chiffriert), dass sie ohne Rückumwandlung (Dechiffrierung) nicht zu lesen sind.

### **MAPI (Messaging Application Program Interface)**

Von Microsoft definierte Schnittstelle, mit der Sie von jeder Windows-Software aus E-Mails verschicken können. Das Dokument, an dem Sie gerade arbeiten, wird als Attachment angehängt.

### **MP80**

mailclad MP80 ist ein Server der es ermöglicht über der http-Port 80 sichere e-Mails zu senden und zu empfangen.

### **POP3**

Das Post Office Protocol. Derzeit üblich ist die Version 3. Es beschreibt ein Verfahren zum TCP/IP-basierten Zugriff auf einen Mailbox-Server und zum übermitteln der dort vorhandenen Nachrichten an einen Mail User Agent. Das Protokoll ist in RFC 1939 definiert.

## Private/Public Key - Verfahren

Ermöglicht den verschlüsselten Datenaustausch zwischen Anwendern

- Jeder Anwender erzeugt ein Schlüsselpaar, das zur Ver- und Entschlüsselung von Nachrichten dient.
- Veröffentlichen des Public-Key. Dies kann auf einem öffentlichen Schlüssel-Server stattfinden, oder Sie übermitteln den Public Key direkt in einer Mail an den Empfänger, der den Key dann lokal speichert.
- Will man nun eine private Nachricht verschicken, so beschafft man sich zunächst den öffentlichen Schlüssel des Empfängers, oder liest diesen aus der lokalen Sicherung, verschlüsselt die Nachricht mit diesem und sendet sie ab. Gegebenenfalls wird die Nachricht zuvor mit dem eigenen, privaten Schlüssel signiert.
- Erhält man eine verschlüsselte Nachricht, entschlüsselt man sie mit dem eigenen, privaten Schlüssel. Kein anderer Empfänger kann diese Nachricht entschlüsseln. Gegebenenfalls prüft man die Signatur anhand des öffentlichen Schlüssels des Versenders, denn nur er kann mit dem privaten Schlüssel unterzeichnet haben.

## SSL (Secure Socket Layer)

Der Secure Socket Layer wurde von Netscape entwickelt. Es handelt sich hierbei um eine hybride Verschlüsselung der Daten zwischen der IP- und der TCP-Schicht, dadurch ist SSL nicht allein auf HTTP festgelegt: Wird auf eine geschützte Seite zugegriffen, wird zunächst der Public-Key der Website zum Client übertragen. Vom Client wird dann eine zufällige Zahl erzeugt, die als Sitzungsschlüssel für eine symmetrische Verschlüsselung der Datenübertragung benutzt wird. Dieser Schlüssel wird mit dem Public-Key der Website verschlüsselt und an den Server übertragen, so dass eine gesicherte

Kommunikation aufgebaut werden kann. SSL unterstützt eine Reihe von Verschlüsselungsverfahren, z.B. RC4, DES und Triple-DES, wobei primär RC4 verwendet wird, welches als sicher gilt, wenn ein 128-Bit Schlüssel verwendet wird

### **STLS (Start Transport Layer Security)**

StartTLS (Start Transport Layer Security) wie auch SSL (Secure Socket Layer) dienen der sicheren Übermittlung von Mail: Einerseits werden bei der Authentifizierung Benutzername und Passwort verschlüsselt übermittelt - so ist z.B. für den Zugriff auf das Postfach via POP oder IMAP die Eingabe des Benutzernamens und des Passworts notwendig - andererseits wird der Text des Briefes einschließlich der Anhänge verschlüsselt übertragen. SSL wie auch StartTLS werden sowohl vom POP- und IMAP-Protokoll beim Empfangen von Mails als auch von SMTP beim Versenden benutzt. StartTLS (das den normalen Port benutzt) ist etwas neuer im Vergleich zu SSL (das einen alternativen Port verwendet).

### **TCP/IP**

Transfer Control Protocol / Internet Protocol - ein Satz an Protokollen die für die Kommunikation zwischen Rechnern im Internet verwendet werden. Das Internet Protokoll (IP) ist der Kern der TCP/IP Suite. Das Internetprotokoll ist dafür verantwortlich, die Ursprungs- und Zieladresse in das Datenpaket einzutragen und dieses Paket dann an seinen Bestimmungsort zu schicken. Im Prinzip funktioniert das so: Ursprungs- und Zieladresse werden am Kopf des Datenpakets -packet header- "angeklebt", so dass die Pakete wissen, wohin die Reise geht. Der Teil des Packets der diese Informationen enthält wird deshalb auch -packet header- genannt. Das Paket wird dann im Netzwerk herumgeroutet und andere Rechner untersuchen den Paketkopf, um herauszufinden, ob das Paket vielleicht für sie bestimmt ist. In Verbindung mit dem TCP-Protokoll ist IP der Kern des Netzwerkprotokolls TCP/IP.

## **TLS (Transport Layer Security)**

TLS ist der designierte Nachfolger von SSL und baut auf diesem auf. Schon die Bezeichnung lässt erkennen, dass es sich um ein Protokoll der Transportschicht handelt. Auf dieser Schicht gewährleistet es eine zuverlässige und transparente Datenübertragung zwischen zwei Systemen. Zentrale Aufgabe von TLS ist der Verbindungsaufbau und die Koordination der Kommunikation zweier Prozesse. Das vordringlichste Ziel ist es jedoch, einen Mechanismus bereitzustellen, mit dem Privatheit und Datenintegrität zwischen zwei Anwendungen erlaubt werden. (RFC 2246)

## 5. INDEX

### A

Absender .....	13
Austausch .....	13

### C

CodeMeter .....	6, 9
-----------------	------

### E

Einschreiben .....	7, 13, 14
Einschreibeverfahren.....	13, 14
e-Mail	
Empfang.....	13

### K

Kommunikation .....	4, 13
Komponenten.....	6
Kundennummer .....	5

### L

Lieferumfang .....	6
--------------------	---

Lizenz.....	5
-------------	---

### M

Massenspeicher .....	9
Mindestvoraussetzungen .....	8

### P

Public Key.....	12, 13, 14
-----------------	------------

### S

Seriennummer.....	5
Support .....	5

### U

unverschlüsselt .....	13
USB	
Standard.....	8
Steckplatz.....	9

### V

Version .....	8
---------------	---

