

Crypt4000 Produktkonzept und Basics

Produkteinführung Schritt für Schritt

Inhaltsverzeichnis

1. Einführung zu Crypt 4000	3
Was Sie zu Crypt4000 wissen sollten.....	4
2. Crypt4000 Stand Alone	5
Pre Boot Authentifizierung (PBA)	5
PBA Integration – WinLogon, Single Logon.....	6
Einführung von SmartCard – Marke vor Startup.....	6
Verschlüsselte und Closed Security Environments (CSE) ..	7
CSE, Definition und Hauptziele	7
Erstellen einer CSE, Verschlüsselungstypen	9
Verwaltung von Crypt4000	10
Verschlüsselte Devices	10
Crypt4000-Profiles für Anwender.....	11
3. Rechtshinweis.....	14

Dieses Dokument umfasst nur einen Überblick der Hauptgrundsätze von Crypt4000.

Eine ausführliche Beschreibung der Funktionen der verschiedenen Versionen dieses Produktes sowie Einzelheiten zu Updates finden Sie auf der beiliegenden Dokumentations-CD.

1. Einführung in Crypt 4000

Crypt4000 ist ein auf Verschlüsselung und Zugangskontrolle basierendes Datenschutzsystem

Verschlüsselung ist der Schritt, der unternommen wird um zu Verhindern, dass Firmendaten ohne entsprechenden Schutz die Firma verlassen, egal wo sie abgespeichert sind.

Crypt4000 bietet 2 Verschlüsselungsebenen:

- Die physikalische Verschlüsselung auf der Format- und Dateiebene für Festplatten und Speichergeräte wie Floppy disketten, CDs, DVDs, USB Sticks, FireWire und anderen Medien.
- Fixed Logic Verschlüsselung der Dateien: für Netzwerkressourcen die zur freien Verfügung mehreren Personen/Abteilungen zur Verfügung stehen und für BackUp.

Geräteschutz wird durch Pre Boot Authentifizierung (PBA) gewährt. Verifizierung des Anwenders ID als erster Schritt vor dem Hochfahren des Systems verhindert das Ausführen irgendwelcher Aktionen die die Information, die auf diesem Gerät und auch in der Infrastruktur zu dem es Zugang hat gespeichert sind, auf irgendeiner Weise gefährden können.

Hierzu gibt es drei verschiedene Möglichkeiten zur User Authentifizierung:

- Passwort für Anwender und Domain
- Eine Marke (SmartCard oder USB Marke)
- Digitale Zertifizierung innerhalb der Hardware

Was Sie über Crypt4000 wissen sollten

- Crypt4000 ist ein auf Verschlüsselung und Kontrolle des Datenzugangs basierendes Datenschutzprogramm.
- Durch die Schaffung von geschlossenen Sicherheitsumgebungen wird gewährleistet, dass Daten immer auf der gewünschten Ebene geschützt sind und für Unberechtigte unzugänglich. Weiterhin schützt dies vor dem Einbringen von unerwünschten Daten durch nicht autorisierte Anwender.
- Der Sicherheitsadministrator kann durch die Erstellung von Verschlüsselungscodes für die verschiedenen Geräte, Autorisierungsmechanismen und Anwender, festlegen welche Einschränkungen für die Nutzung dieser gelten und sichert den Schutz der Datenverschlüsselung ohne Eingriffe durch den Anwender.
- Hat der Sicherheitsadministrator einmal die Sicherheitsrichtlinien festgelegt und in das System eingespielt oder auf dem PC des einzelnen Anwenders installiert, werden diese das Gerät und die darauf gespeicherten Informationen sowie Daten zu dem das Gerät Zugang hat schützen.

2. Crypt4000 Stand Alone

Durch Crypt4000 ist Ihr PC mit einem auf Verschlüsselung und Zugangskontrolle basierendes Datenschutzsystem ausgestattet.

Die PC-Sicherheit ist durch Pre-Boot Authentifizierung gegeben. Verifizierung des Anwender IDs als erster Schritt vor dem Hochfahren des Betriebssystems verhindert die Ausführung von Vorgängen die die gespeicherten Informationen oder andere Infrastrukturen zu dem das Gerät Zugang hat, gefährden könnten.

Gleichermaßen wird die ungeschützte Entnahme von Firmendaten aus dem Firmenumfeld durch die Verschlüsselung verhindert. In anderen Worten wird die Information, ungeachtet der Art wie sie gespeichert wurde, verschlüsselt; dennoch haben autorisierte Anwender innerhalb der Firma ohne Schwierigkeiten ungehinderten Zugang zu der Information.

Folgend werden wir nun allgemein die Schritte erläutern, die zum Einsetzen der Crypt4000 Security innerhalb Ihrer Organisation notwendig sind. Eine detaillierte Anleitung befindet sich auf der dieser Beschreibung beiliegenden CD.

Dies ist eine allgemeine Zusammenfassung der Schritte zur Inbetriebnahme Ihrer Crypt4000 Security.

1. Der Administrator definiert folgendes für jeden Arbeitsplatz:
 - 1.1 Alle verschlüsselten Geräte auf denen Zugriff erfolgt und die Definition benötigen
 - 1.2 Diese Geräte werden dann Anwendern zugeteilt und die Autorisierungsebene wird für jeden Einzelfall festgelegt
2. Installation der Crypt4000 (des Kunden) auf die PCs der Anwender, durch remote Installation
3. Wenn Crypt4000 auf alle PCs installiert wurde:
 - 3.1. Anwender werden aufgefordert sich im neuen Autorisierungsprozess auszuweisen. Dies geschieht nur einmal, hier tritt eine höhere Sicherheitsebene ein um unberechtigten Zugriff zu verhindern.
 - 3.2. Hat der Anwender sich mit einer gültigen Autorisierung ausgewiesen, treten die vom Administrator vorgegebenen Sicherheitsparameter automatisch ein und können vom Anwender weder deaktiviert oder auf irgendeiner Weise verändert werden.

Pre-Boot Authentifizierung (PBA)

Crypt4000 Zugangskontrollen erfolgen durch Pre-Boot Autorisierung (PBA) im Betriebssystem.

Pre-boot Zugangskontrolle bietet zusätzliche Stufen der PC-Sicherheit, die gewährleisten, dass nur autorisierte Anwender den Arbeitsplatz hochfahren können.

Für PCs, die sich an öffentlichen Plätzen befinden (z.B. in einer Empfangshalle oder die zur allgemeiner Benutzung freigegeben sind) oder für mobile Geräte wie

Laptops, die leicht entwendet werden können, ist PBA das Mittel schlechthin um in allen Situationen außerhalb unseres Einflussbereiches den unbefugten Zugang zu Informationen zu verhindern, schon allein dadurch, dass der PC nicht hochfahren kann und seine Informationen deshalb nicht zugänglich sind.

Der Crypt4000 Start-Up Prozess ist allumfassend und erlaubt dem Gerät ohne Autorisierung durch ein gültiges Anwender ID sich weder hochzufahren noch verschlüsselte Informationen auf der Festplatte zu entschlüsseln. Die Chiffre für die Festplatte ist zusätzlich verschlüsselt durch die eingegebenen Identifizierungsausweise um die Dechiffrierung der geschützten Information zu verhindern.

Drei verschiedene Arten der Identifizierungsausweise können benutzt werden:

- A) Anwender/Passwort
An einem gültigen Systemaccount gekoppelt
- B) USB Token oder SmartCard ID
Mit einer Hardware Seriennummer
- C) Digitale Zertifizierung auf SmartCard oder Token. Vorlegen eines Passwortes aus einer Paarung von Passwörtern.

PBA Integration – WinLogon, Single Logon

PBA bietet vor dem Hochfahren des Betriebssystems ein Interface in dem eine autentifizierte Identifizierung vorgezeigt werden muss. Dieser Prozess ist in dem WinLogon Prozess integriert, welches bedeutet, dass das ID nur einmal eingegeben werden muss. Dem User bietet sich hier die Einfachheit des Single Logon.

In allen drei angegebenen Identifizierungsverifizierungsoptionen ist diese Integration sowohl vollständig wie auch dem Anwender klar.

Einsatz des SmartCard-Token vor Start-up

Diese Option steht nur einer SmartCard Installation zur Verfügung.

SECUWARE ist der einzige Hersteller der eine einwandfreie SmartCard Integration (mit USB Leser) und Token USB in der Windows Anwendung erreicht hat.

Die Karte erlaubt die Authentifizierung des Anwenders durch lesen der SmartCard nach Eingabe des verifiziertem Passwort. Dieser Teil wird zur Registrierung von SmartCards benutzt. Crypt4000 ermöglicht die Anwendung vielerlei Karten (Ceres, VISA, 4B, WG10, AMEX Blue, usw.) um das Gerät hochzufahren.

Ein USB Token bewirkt Anwender Authentifizierung durch Eingabe eines Verifizierungspasswortes. Dieser Teil wird zur Registrierung von USB Tokens benutzt. Crypt4000 kann ohne weiteres mit vielen verschiedenen Tokens (iKey, usw.) hochfahren.

Durch PBA-GINA Integration, ist ein Restart auch ohne erneutes Einbringen der Tokens oder Karte in den PC möglich, obwohl diese eingesetzt werden müssen um hochzufahren.

PBA liefert eine unverschlüsselte Karten-PIN die für den GINA Prozess notwendig ist, ob für Microsoft selber oder einen GINA Drittanbieter über den standardmäßigen GINA Prozess.

Verschlüsselte und Geschlossene Sicherheitsumfelder (CSE)

Crypt4000 bietet folgende zwei Ebenen:

- Physikalische Verschlüsselung, für alle Formate und Dateien: Anwendbar auf Festplatten und Aufbewahrungsgeräte, inklusive Floppy Disketten, CDs und USB Laufwerke.
- Statische Logische Verschlüsselung von Dateien: Eingesetzt bei gemeinsam genutzte Netzwerkressourcen und deren Back-up Kopien.

CSE, Definition und Hauptziele

Der komplexeste Teil eines jeden Verschlüsselungssystems ist es zu ermöglichen die verschlüsselte Information zu bearbeiten als sei sie nicht verschlüsselt. Mit anderen Worten, das Sicherheitssystem muss für den Anwender in der Anwendung transparent sein und trotzdem Fehlerquellen, die das System für Angriffe bloßstellen würden, ausschließen.

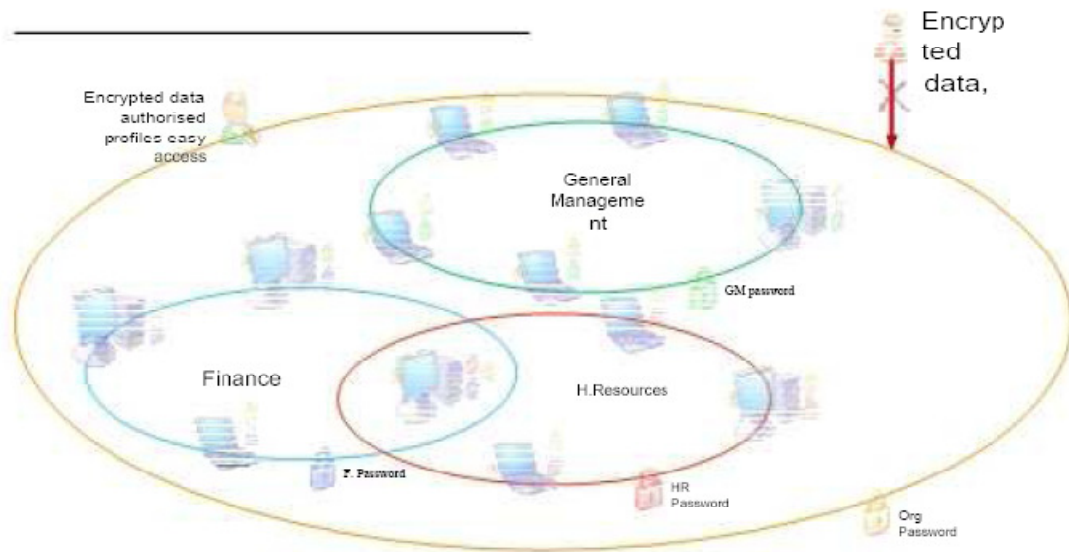
Die Anwendergruppe mit Anwenderprivilegien und Zugang zu den Informationen bildet das geschlossene Sicherheitsumfeld.

Hauptziele der geschlossenen Sicherheitsumfelder (CSE) sind deswegen die, die am besten diese Informationen schützen:

- Sie sind geschützt und vom Unternehmen kontrolliert.
- Zugang nur durch berechtigte Anwender aus autorisierten Systemen.
- Sie sind gesperrt für jeden Zugriff von Außen.

SECUWARE Crypt4000 stellt sicher, dass ein solches Umfeld auch wirklich ein integriertes Umfeld darstellt. Das heißt, es ist auf die größtmögliche Anzahl von Fällen im täglichen Arbeitsprozess jedes Anwenders anwendbar.

Der Gebrauch verschiedener Speichermedien ist ohne weiteres mit Crypt4000 machbar, da es möglich ist die meisten davon mit Hilfe der Anwender-transparenten Methode zu verschlüsseln. So ist der Gebrauch eines solchen verschlüsselten Mediums mit dem normalen, unverschlüsselten arbeiten damit fast identisch, so dass Anwender sogar nicht merken ob sie nun mit verschlüsselten oder unverschlüsselten Informationen arbeiten oder diese abspeichern.



Innerhalb dieser geschlossenen Sicherheitsumfelder, wie oben illustriert:

Haben alle Anwender innerhalb des Unternehmens Zugang zu verschlüsselten Daten über das Passwort: „ORG“.

Diese erste Ebene macht es:

- Unmöglich, dass jemand außerhalb des Unternehmens Zugang zu diesen verschlüsselten Informationen erlangt,
- möglich, dass diese Informationen von allen PCs innerhalb des Unternehmens erreichbar ist, und
- unmöglich verschlüsseltes Material in dieses Sicherheitsumfeld einzuschleusen. Sollte ein Zugang von Außen notwendig sein, werden autorisierte Profile erstellt, die die Quellen definieren, von denen externe Daten zugelassen werden.

Sicherheitsumfelder der zweiten Ebene setzen sich zusammen aus Anwendergruppen mit begrenztem Zugang über Passwörter ihrer einzelnen Abteilungen, wie z.B. Personalwesen, Buchhaltung oder Verwaltung.

Zugangscharakteristika der verschiedenen Passwörter die den einzelnen Anwenderprofile zugeordnet sind, erlaubt es ineinander verflochtene oder interoperative Umfelder zu entwickeln.

Erstellen eines Sicherheitsumfeldes, Arten der Verschlüsselung

Um ein echtes Sicherheitsumfeldes, die die Anwendung der gewöhnlichsten Methoden der Speicherung und Back-Up (u.a. Floppy Disketten, CDs, USB Laufwerke und Netzwerkdateien) zu unterstützen, werden zwei verschiedene Verschlüsselungsmethoden verwendet:

Physikalische Verschlüsselung

Integrierte Verschlüsselung, Festplatte (HD)

Die Verschlüsselung der Festplatte eines Systems als Sicherheitsmaßnahme hat zwei grundsätzliche Vorteile:

- Einen höheren Sicherheitsgrad, und
- Kein Zugriff auf Informationen der Festplatte, auch nicht über andere Zugriffsarten wie z.B. Floppy Disk oder durch die Installation einer anderen Festplatte in einem anderen System.

Wenn alle Informationen auf der Festplatte verschlüsselt sind, dann sind alle Daten die darauf gespeichert sind automatisch geschützt, auch die temporären Dateien und andere Daten die normalerweise von anderen Prozessen und Anwendungen ungeschützt sind. Somit ist das Risiko durch ungeschützte Daten vermieden.

Physisch verschlüsselte Festplatten Effizienz

Vielfach stellt sich die Frage nach dem Einfluss der integrierten Verschlüsselung der Festplatte auf die Arbeitseffizienz des Systems.

SECUWARE benutzt symmetrisch verschlüsselte Sektor Algorithmen (IDEA 128 bit oder AES 256 bit) die sich in ihren spezialisierten Märkten den Ruf hoher Sicherheit und Zuverlässigkeit erworben haben.

Die Festplatten Datenzugangszeiten sind physikalische Zeiten (T = Millisekunden), während Echtzeit Datenverschlüsselung/Dechiffrierung Prozessorzeiten (t = Microsekunden) sind. Daher stellt $T+t$ eine Steigerung der Auslastung von ca. 1,5 pro 1000 dar. Der Unterschied zwischen der Arbeitsleistung eines PC mit verschlüsselter Festplatte und einer standard Festplatte sind unbedeutend.

Wenn $T = 1\text{ms}$ und $t = 1,5\mu$, dann sind $T + t \approx 1,0015\text{ms}$.

Integrierte physikalische Verschlüsselung von tragbaren Geräten (FDD, CD, DVD, USB, usw.)

Die Verschlüsselung von tragbaren Geräten ist eine Sicherheitsmaßnahme die ein Format bietet, das nur für befugte Anwender innerhalb eines sicheren Umfeldes (CSE) lesbar ist. Hier wird die Offenlegung von Information, ob beabsichtigt oder nicht, für Anwender außerhalb der Gruppe, nach den Richtlinien wie eine Gruppe innerhalb des Unternehmens als Arbeitsbereich in der diese Daten berechtigterweise bearbeitet werden, definiert ist, verhindert.

Es ist für den Anwender nicht zu ersehen, dass die Information in irgendeiner Form geändert wurde. Die Daten erscheinen weiterhin transparent, d.h. die Arbeit sowohl innerhalb wie außerhalb der Organisation ist unbeeinträchtigt.

Sollte ein Anwender firmeninterne geschützte Informationen auf eine CD brennen, oder anderweitig kopieren, werden diese gespeichert, das Format und die Daten werden aber zur Sicherheit verschlüsselt unter Anwendung eines vorher eingerichteten Passworts, ohne besondere vorherige Bearbeitung der fraglichen Information um so menschliche Fehler zu minimieren und die Daten sicher zu schützen.

Statisch-Logische Verschlüsselung

Verschlüsselung von Netzwerkressourcen

Hinweis: Diese Option ist nur für Workstation und SmartCard Installationsvarianten verfügbar

Die statisch-logische Verschlüsselung arbeitet auf der Dateien-Ebene um die Nutzung der verschlüsselten Daten auf fast jedes physikalische Medium zu ermöglichen, ohne Rücksicht auf die Formatierung des Mediums.

Die statisch-logische Verschlüsselung eines Netzwerkes wird der Dateien-Ebene übertragen um zu ermöglichen, dass verschiedene verschlüsselte Netzwerkstandorte mit identischen oder unterschiedlichen zugeordneten Verschlüsselungsziffern auf demselben Server definiert werden können.

Back-Up Kopien von Netzwerkdaten, die in verschlüsselten Ordnern enthalten sind werden auch verschlüsselt; während das Back-Up System die Dateien kopiert und während die Originaldatei verschlüsselt wird, wird die Kopie ähnlich geschützt, wie auch das entsprechende Chiffre.

Crypt2000 Verwaltung

Die Anwendung von Crypt4000 basiert auf Zugangsautorisierung und Merkmale die einer Serie von Gegenständen zugewiesen wurden.

Verschlüsselte Geräte

Diese Kategorie umfasst die verschiedenen Geräte die verschlüsselt werden können.

- Die Verschlüsselung von physikalischen Geräten (Festplatten, Floppies, CD-ROM und USB Geräte) ist ein voll-integrierter physikalischer Verschlüsselungsvorgang (das heißt, dass das ganze Gerät mit einem entsprechenden Code verschlüsselt wird.)
- Die Verschlüsselung von Netzwerk Ordnern ist eine durchsichtige statisch-logische Verschlüsselung (das heißt, dass die Dateien vor dem speichern auf externe Ressourcen aber nach dem Lesen verschlüsselt werden).

Hinweis: Diese Option ist nur für Workstation und SmartCard Installationsvarianten verfügbar.

Die Handhabung der verschiedenen Geräte ist deswegen etwas unterschiedlich.

Definition der Verschlüsselungs-Codes für jedes Gerät

Der Administrator kann so viele verschlüsselte Geräte erstellen wie für die verschiedenen Medien benötigt werden, mit einer Kennzeichnung zu Namen des Gerätes, Beschreibung und Festlegung für welche Art von Medium es bestimmt ist.

Im speziellen Fall der Netzwerk Ordner muss die Definition der verschlüsselten Geräte für diese Art von Anwendung zusammen mit einer Liste der existierenden mit dieser Definition zu verschlüsselnden Netzwerk Ordnern fertiggestellt werden.

ES IST UNERLÄSSLICH, dass die Liste der Ordner, die dem verschlüsselten Netzwerkgerät zugeordnet wurde, die beiden möglichen Zugangspfade zu jeder Ressource enthalten:

*\\nombremaquina\recurso

*\\dirección.IP\recurso

Wichtig:

Verschlüsselte Netzwerk Ordner Geräte sollten zu leeren Netzwerk Ordnern zugeteilt werden, da wenn der Ordner unverschlüsselte Dateien enthält und einem verschlüsseltem Netzwerkgerät zugeteilt wird, diese Dateien unbrauchbar werden weil das Öffnen der Datei den Entschlüsselungsprozess beginnt (für unverschlüsselte Informationen unmöglich).

Crypt4000 Profile für Anwender

Die Crypt4000 Profile für Anwender erlauben es für jedes definierte verschlüsselte Gerät den Zugang entweder zuzulassen oder zu verhindern.

Durch Schaffung dieser Art von Anwenderprofile werden sowohl die Geräte zu dem der Anwender Zugang hat, so wie auch den Umfang seiner Autorisierung festgelegt. Je nach Gerätetyp stehen folgende Autorisierungsebenen zur Verfügung: Lesen (Read), Schreiben (Write) und Formattieren (Format).

Verschlüsselte Netzwerk Ordner Geräte als gemeinsam genutzte Ressourcen besitzen eine Nutzungsautorisierung die durch NTFS Erlaubnisse, die der Domain Administrator vergibt, kontrolliert werden.

- In physikalisch verschlüsselte Geräten wird die Zugangserlaubnis zum Gerät automatisch von der Einrichtung eines Leser (R) Autorisierung begleitet welches bedeutet, dass der Anwender

Zugang zum Inhalt der Dateien die auf dem verschlüsselten Gerät gespeichert sind. Die übertragenen Autorisierungsebenen sind kumulativ, in der Reihenfolge wie sie definiert wurden.

- Die „Schreiben“ Autorisierungsebene (W) erlaubt es dem Anwender neue Dateien hinzuzufügen indem er das gleiche verschlüsselte Gerät nutzt, welches vorher für dieses System formatiert wurde.
- Die „Format“ Autorisierungsebene (F) betrifft Floppies und USB Laufwerke so wie jedes andere Laufwerk/Geräte das vor der Inbetriebnahme formatiert werden muss. Ohne diese Autorisierung ist es nicht möglich ein neues Floppy Disk oder ein USB Laufwerk mit diesem verschlüsseltem Gerät zu erstellen und der Anwender ist darauf begrenzt nur die Medien nutzen zu können die ihm vorab freigegeben wurden.

WICHTIG:

Schnellformatierung der verschlüsselten Geräte ist ungültig! Da es sich um eine physikalische Verschlüsselung handelt, muss das gesamte Laufwerk/Gerät formatiert werden damit dadurch das Gerät/Laufwerk für die Speicherung der verschlüsselten Informationen vorbereitet wird.

Jedem Anwender wird auch eine Berechtigungsebene zur Änderung der Konfiguration des Produktes zugeteilt. Diese reicht von keine Änderungen vornehmen zu dürfen bis hin zur Kontrolle der Produktkonfiguration, dazwischen liegen weitere drei Ebenen die es den Anwendern erlauben, die ihn übertragenen Sicherheitsaufgaben innerhalb des vom Sicherheitsadministrator festgelegten Rahmen zu erledigen.

3. Haftungsausschluss

Alle hierin aufgeführten Namen sind gewerbliche Handelsnamen und geschützte Markenzeichen der dazugehörigen Firmen. Secuware hat keine Interesse an Rechte Dritter aus Handelsmarken oder Warenzeichen. Secuware hat alle Angaben nach besten Wissen und Gewissen geprüft, behält sich trotzdem vor, die vorgelegten Konditionen ohne vorherige Ankündigung jederzeit ändern zu dürfen.

Wenn nicht anders ausgewiesen, sind die Firmen, Namen und Daten die in diesem Dokument als Beispiele genannt wurden fiktiv.

Es ist weder erlaubt ohne die schriftliche Erlaubnis von Secuware dieses Dokument in irgendeiner Form zu reproduzieren , noch es aus irgendeinem Grund oder in irgendeiner Form, ob elektronisch oder mechanisch, weiterzuleiten .

© Copyright 2005-2009 Secuware. All rights reserved.

Secuware Deutschland GmbH
Eifelstraße 9
53119 Bonn

TEL.: 0228 962979 0
Fax: 0228 962979 29
Mail: sales@secuware.de

Internet: www.secuware.com