

Anlagenbeschreibung

Allgemeines

cryptin® unterstützt alle Anwendungen im Bereich der Zutrittskontrolle, angefangen vom Hochsicherheitszugang über Standardanwendungen wie Innen- und Außenabsicherung bis hin zur elektronischen Schließanlage. Das Zutrittskontrollsystem **cryptin®** erfüllt als ganzheitliches System durchgängig die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nach TL 03402 (vormals BSI 7550). Darüber hinaus ist das System konform mit den Regelungen der VdS Schadenverhütung GmbH für Zutrittskontrollanlagen.

Ein wesentliches Merkmal von **cryptin®** Zutrittskontrollsystemen ist die Skalierbarkeit. So können Anlagen von einem Zugang bis theoretisch unendlich vielen Zugängen sowohl in einem Gebäude als auch weltweit vernetzt realisiert werden. Es können beliebig viele Personen angefangen von 1 Benutzer bis hin zur halben Menschheit administriert werden. Wohlbemerkt, wenn es sein muss, auch alle an einen Zugang. Die Sicherheit kann beliebig im Bereich zwischen Daueröffnung und beispielsweise einem 4 Augen- Zugang mit Echtheitsprüfung des Ausweises und PIN Eingabe bei Bereichswechselkontrolle gewählt werden.

Die Systeme unterstützen viele sowohl berührungslose als auch kontaktbehaftete Ausweismedien, die bei Bedarf auch parallel im System eingesetzt werden können. Neben den Ausweistypen Hitag, Mifare und Legic für Standardanwendungen unterstützen **cryptin®** Zutrittssysteme die Kartentypen TCOS Dual Interface sowie Mifare DESFire EV1 für den Hochsicherheitsbereich. Die Palette an Schlosstypen, die von den Systemen gehandelt werden können, reicht vom einfachen E-Öffner über Motorschlösser bis hin zu Vereinzelungsschleusen.

Anlagenbeschreibung

Auf der administrativen Seite ist das System ebenfalls skalierbar. Buchungen etwa, sind derart parametrierbar, dass sie wahlweise erst gar nicht erzeugt werden, anonym erzeugt werden, oder personalisiert erzeugt werden. Der Datenbankserver, die Dienste und die Administration kann auf einem PC unter Windows-NT oder höher installiert werden. Alternativ können beliebig viele Arbeitsplätze eingerichtet werden. **cryptin**[®] kennt also keine Systemgrenzen

cryptin[®] Systeme setzen an verschiedenen Stellen harte Verschlüsselungs-methoden (Kryptologie) ein. Als Verschlüsselungsverfahren können dabei je nach Anforderung und Ausweismedium die Verfahren DES/3DES (Data Encryption Standard) sowie AES (Advanced Encryption Standard) verwendet werden. Zum einen werden damit Ausweise auf Echtheit geprüft, zum anderen können die Systeme Ihre Daten problemlos über firmeninterne Netze oder gar öffentliche Netze (Internet) verschicken. Selbstverständlich werden dann auch sensible Daten so abgelegt (z. B. Buchungen). Diese Verschlüsselungsmethoden sind so ausgelegt, dass selbst wir als Systementwickler außerhalb der regulären Zugriffsverfahren keine Einsicht in Ihre Daten erlangen können.

Anlagenbeschreibung

Vernetzung

cryptin® Systeme sind Netzwerksysteme. Sie verwenden das Protokoll TCP/IP. Die Systeme sprechen quasi die Sprache des Internets und deren Standards. Dies ermöglicht die einfache Vernetzung der Systeme untereinander. Die Weltweite Standardisierung hat zu preiswerten Komponenten zur Vernetzung von Systemen geführt. **cryptin**® Systeme lassen sich dort mühelos integrieren und ermöglichen eine einfache Vernetzung der Systeme untereinander. Dabei können alle Übertragungsmedien der Netzwerktechnik genutzt werden. TCP-IP kann mühelos über das Ethernet- Netzwerkkabel als auch über eine ISDN-, Modem-, GSM-, oder Funk- LAN Verbindung übertragen werden. Weitere Teilnehmer werden wie PC's im Netzwerk eingebunden. Unterhalb der Zutrittskontrollzentralen werden mit herkömmlichen Verkabelungsmethoden die Zugänge in Stern- oder Bustopologie angeschlossen.

Anlagenbeschreibung

Leitebene (ÜZKZ)

Die zentrale Leitinstanz des Systemverbundes ist der **cryptin®** - Application- Server (CAS). Es findet auch häufig der DIN Begriff „ÜZKZ“ (Übergeordnete Zutritts-Kontrollzentrale) Verwendung. Dieser Serverdienst verwaltet die Anmeldungen der Bedien-Arbeitsplätze (Control- Clients), definiert die Zugangsrechte für die verwendete SQL- Datenbank und regelt die Kommunikation der angeschlossenen Anlagenteile. Dieser Application – Server wird als sogenannter Dienst auf einem Windows PC gestartet.

cryptin® verwendet zur Datenhaltung eine SQL- Datenbank. SQL – Datenbanken verwenden eine Beschreibungssprache für den Zugriff auf Daten, der sich zum internationalen Standard sowohl für kleine als auch für große Anwendungen durchgesetzt hat. Standardmäßig wird eine Interbase SQL Datenbank unterstützt. Bei der Softwareentwicklung wurde streng auf die Einhaltung des ANSI Standards (Internationale Norm) geachtet, so dass auch andere SQL- Datenbanken wie Oracle oder Microsoft- SQL angebunden werden können.

Ein weiterer Dienst der Leitebene ist der Meldungsdienst **cryptin®** - Message- Server (CMS). Er ist die Zentrale Kontrollinstanz und regelt das Handling von Buchungen und Meldungen der Zutritts-kontrollzentralen (ACU's) sowie die Verteilung an angeschlossene Überwachungsarbeitsplätze.

Die Softwaremodule der Leitebene müssen nicht zwingend auf einem PC (SERVER) installiert werden. Sie können aus organisatorischen Gründen auch im Netzwerk verteilt installiert werden. Die Leitebene erfordert nach Installation außer bei Systemwartung keine Bedienereingaben.

Anlagenbeschreibung

Bediener Ebene

Die Bediener Ebene des **cryptin®** Systemverbundes setzt sich modular aus verschiedenen Softwareelementen zusammen, die den Aufgaben einzelner Arbeitsplätze entsprechen. Die Arbeitsplätze können auch beliebig kombiniert auf einem Arbeitsplatz gemeinsam betrieben werden. Ein umfangreiches Rechtssystem regelt den Zugriff auf die einzelnen Funktionen. Folgende Arbeitsplätze (Clients) stehen derzeit zur Verfügung:

- ▶ Administrations-Arbeitsplatz **cryptin®**-Admin-Client (CAC)
- ▶ An diesem Arbeitsplatz werden die Rechte der einzelnen Benutzer verwaltet. Mit Gruppenmodellen können mit wenigen Arbeitsschritten umfangreiche Administrationen durchgeführt werden. Das Softwaremodul **cryptin@web** ermöglicht es diese Tätigkeiten auf Wunsch von jedem beliebigen Arbeitsplatz auszuführen.
- ▶ Pförtner-Arbeitsplatz **cryptin®**-(Building)-Control-Client (CCC)
- ▶ Dieser Arbeitsplatz ist auf die Belange von Pförtnern zugeschnitten. Alle Systemmeldungen, die seinen Zuständigkeitsbereich betreffen, werden hier angezeigt und verwaltet. (Das klassische Pförtnertableau)
- ▶ Sicherheitsdienst-Arbeitsplatz **cryptin®**-Control-Client (CCC)
- ▶ Der Sicherheitsdienst Arbeitsplatz ist die Übergeordnete Instanz des Pörtner-Arbeitsplatzes.
- ▶ Empfangs-Arbeitsplatz **cryptin®**-Visitor-Client (CVC)
- ▶ Dieser Arbeitsplatz dient zur Ausgabe von Besucherausweisen. Ein elektronisches Besucherbuch kann hier geführt werden.

Jeder dieser Arbeitsplätze ist mit einem Ausweisleser versehen, mit dem die Berechtigung für den Arbeitsplatz geprüft wird. Administrationsschritte und Alarmbestätigungen werden mit entsprechender Ausweisnummer gebucht.

Anlagenbeschreibung

Systemverbund

Bei **cryptin®** stehen verschiedene Zutritts- Kontrollzentralen (ACU's) zur Verfügung. Jede der Zentralen ist für Ihren Anwendungsfall optimiert. Diese sind:

- ▶ **ACU – TRUST**
Zutritts- Kontrollzentrale für Hochsicherheitsanwendungen, alle Standard-Anwendungen sowie Anwendungen für besonders viele Berechtigte. Die ACU-TRUST kann bis zu 8 Zugänge verwalten.
- ▶ **ACU – NET**
Zutritts- Kontrollzentrale für alle Standardanwendungen mit herausragenden Netzwerkfunktionalitäten. Die ACU-NET kann bis zu 8 Zugänge verwalten.
- ▶ **Multi – ACU 32**
Zutritts-Kontrollzentrale auf Basis von 4 ACU-NET Systemen für bis zu 32 Zugänge. Sie ist für elektronische Schließanlagen konzipiert.
- ▶ **ACU – RACK**
Zutritts- Kontrollzentrale und Fernwirkssystem für IT- Schaltschränke. Sie bietet unter anderem eine Fernüberwachung per Internet-Browser.