Der SchlüsselWächter SW4 bietet Ihnen mehr als nur eine einfache Schlüsselüberwachung.
Jeder Schlüssel hängt an einem Schlüsselträger, der in Verbindung mit dem Schlüsselwächter nur autorisierten Mitarbeitern die Entnahme ermöglicht.

Schlüsselwächter SW4 bieten die Möglichkeit im Netzwerkverbund zu arbeiten. Dadurch ist jederzeit ersichtlich, in welchem System sich die gesuchten Schlüsselträger befinden. Je nach Konfiguration ist es möglich die Schlüsselträger in den Verbundsystemen zu platzieren. Zugriff zum System erhält der Benutzer über ID und PIN, optional über Kartenleser oder durch biometrische Erkennung.

Der SchlüsselWächter erstellt für jeden Schlüssel und Benutzer Einträge in ein Protokoll, so dass man in Sekundenschnelle nachvollziehen kann, wo sich die Schlüssel befinden und wer ihn entnommen hat.

All diese Punkte verbindet der SchlüsselWächter mit dem Vorteil des verhältnismäßig geringen Platzbedarfes durch Unterbringung der Schlüssel in einem stabilen Edelstahlschrank.

Alternative Gehäusevarianten erlauben die optimale Ausnutzung der gegebenen Platzverhältnisse. Kundenspezifische Systeme können auf Anfrage realisiert werden.

GEHÄUSE

Das Gehäuse des SW 4 besteht aus 2 mm dickem geschliffenem Edelstahl.

Die Außentür ist softwareseitig Alarmüberwacht gegen unberechtigte Öffnung und Benutzung.

BENUTZERFÜHRUNG

Erfolgt intuitiv über das TFT / Touch Bedienfeld.

Der freizugebende Schlüssel wird über das TFT-Display sowie blau leuchtenden Steckplatz identifiziert. Jeder Schlüssel ist elektromechanisch in seinem Steckplatz verriegelt und kann nur von einem autorisierten Benutzer freigegeben werden.

KRUSE Sicherheitssysteme GmbH & Co. KG • Duvendahl 92 • 21435 Stelle • Tel.: 04174 592-22 • vertrieb@kruse-sicherheit.de

SYSTEMSPRACHE	Deutsch und Englisch, andere Sprachen können optional implementiert werden.
LOGIN	ID und PIN, optional Kartenleser oder biometrische Erkennung.
BENUTZERSPRACHE	Beim Login wählbar oder wird vom Administrator dem Benutzer zugewiesen.
BENUTZERZAHL	Unbegrenzt
BENUTZERGRUPPEN	Unbegrenzt
SCHLÜSSELGRUPPEN	Begrenzt durch die Anzahl der Schlüsselträger
BERECHTIGUNGEN	Werden durch Addition über Schlüssel- und Benutzergruppen, Schlüssel-Benutzer- und Direktzuweisungen zwischen Benutzer und Schlüssel vergeben.
VIER-AUGENPRINZIP	Für Benutzer und / oder Schlüssel. Zwei Benutzercodes müssen eingegeben werden. Die Bestätigung erfolgt über einen Benutzer oder Gruppenmitglied.
BEDROHUNG / PANIK-ALARM	Bei Bedrohung kann jeder berechtigte Benutzer einen stillen Alarm auslösen.
ALARME	Werden erzeugt für Netzausfall, überfällige Schlüssel, illegale Entnahme von Schlüsseln, Tür noch offen, Tür unberechtigt geöffnet usw. Diese Alarmmeldungen werden über das Netzwerk zur Auswertung weitergeleitet, optional per SMS (GSM-Modem) oder E-Mail.
NOTFALLFREIGABE	Berechtigte Benutzer können eine Notfallfreigabe aller im System befindlichen Schlüssel durchführen.
SCHLÜSSELKAPAZITÄT	Verwaltung von maximal 1000 Schlüsselträgern pro System, max. 40 / 60 / 80 / 120 je Gehäusetyp, erweiterbar durch Zusatzgehäuse. Im Verbund besteht keine Begrenzung der Schlüsselträger.
SCHLÜSSEL- VERWAHRUNG	Der Schlüsselträger wird im Steckplatz verriegelt. Die Verriegelung wird nur durch berechtigten Zugriff aufgehoben.
VERZÖGERTE SCHLÜSSELAUSGABE	Für erhöhte Sicherheitsanforderungen bei einzelnen Schlüsseln.
SCHLÜSSELRÜCKGABE	Wahlfreier Steckplatz - fester Steckplatz in einem bestimmten System.

KRUSE Sicherheitssysteme GmbH & Co. KG • Duvendahl 92 • 21435 Stelle • Tel.: 04174 592-22 • vertrieb@kruse-sicherheit.de

SCHLÜSSEL/ SCHLÜSSELTRÄGER

Die zu überwachenden Schlüssel werden an dem Schlüsselträger mit einem 3mm starken Ring aus Edelstahl befestigt. Es können mehrere Schlüssel an einem Schlüsselträger befestigt werden.

Bis zu 3-mal können die Ringe bei Schlüsselauswechselungen erneuert werden.

Schlüsselträger sind erhältlich in 4 Farben: rot, blau, grün, gelb.

BENUTZER-BERECHTIGUNG

Zugriffscode: alphanumerisch – numerisch als globale Einstellung durch den Administrator, ID und PIN min. 4 - max. 256 Zeichen.

DATENSICHERHEIT

Gegen Störungen durch Stromausfall wurde eine USV-Funktion integriert. Unterschreitet die Akkuspannung nach dem Stromausfall einen Schwellwert, wird das Gerät heruntergefahren.

Durch Speicherung der Daten auf einer mSATA-Festplatte ist ein Datenverlust bei Stromausfall nicht möglich.

Nachdem die Stromzufuhr wieder besteht, startet das Gerät selbständig und steht nach kurzer Zeit zur Schlüsselausgabe bereit

AUTOMATISCHE DATENSICHERUNG

Sicherung wahlweise auf ein Netzlaufwerk oder einen USB-Stick möglich.

ZEITEINSTELLUNGEN

Es besteht die Möglichkeit über das Netzwerk die Zeit mit einem internen oder externen Zeitserver zu synchronisieren (wichtig bei mehreren SW4 im Netzwerk, damit bei allen Systemen im Verbund die Zeit synchron ist).

SCHNITTSTELLEN

1 freie RS232 serielle Schnittstellen zum Anschluss von z.B. Kartenleser, GSM-Modem oder biometrischer Erkennung.

4 USB 2.0 Ports stehen zur Verfügung.

Kundeneigene Kartenleser anzuschließen erfordert unter Umständen eine kostenpflichtige Anpassung an die bestehende Software.

Die Netzwerkanbindung wird ermöglicht durch eine Ethernet Netzwerkkarte mit RJ45 Schnittstellen zur Anbindung an bestehende 10 / 100 / 1000 Mbit Netzwerke.

Verwendetes Protokoll TCP/IP v4 und TCP/IP v6.

REMOTEZUGRIFF

Im Netzwerk für Administratoren möglich.

WEBSCHNITTSTELLE

Die Schlüsselwächter 4 Applikation ist über die Webschnittstelle per Webbrowser konfigurierbar. Je nach Einstellung kann der Zugriff über HTTP oder HTTPS erfolgen.

DATENERFASSUNG BEI RÜCKGABE

Bei der Schlüsselrückgabe muss der Benutzer vordefinierte Felder, wie den Kilometerstand oder ähnlich ausfüllen. Die Datenerfassung kann als CSV-Datei gespeichert oder weiterbearbeitet werden.
Die Datenerfassung ist optional zu bestellen.

SCHLÜSSEL-RESERVIERUNG

Hier kann der Administrator für bestimmte Schlüssel eine Reservierung nach von ihm festzulegenden Parametern vornehmen.
Die Reservierung ist optional zu bestellen.

ALARMAUSGANG

Auf einer internen Alarmrelais-Platine befinden sich 5 Relais mit separaten Kontakten für eine externe Alarmauswertung.

Alarmweiterleitungen sind per Relais an Zutrittskontrollsysteme möglich.

ALARME

Erzeugte Alarme werden am SW4 PC-Client dargestellt und können per Mail im Netzwerk versandt werden.

Eine Alarmweiterleitung per GSM-Modem ist optional möglich.

AKTIONEN

Alle Aktionen werden in einem Log-File bzw. Report-File registriert. Eine Speicherung der Daten kann im CSV Format (Excel) erfolgen.

Die Anzahl der gespeicherten Aktionen ist von den Einstellungen abhängig.

BERICHTE

Können am PC über den Webbrowser an einem Drucker ausgegeben werden.

HARDWARE-VORAUSSETZUNG

Die Mindestanforderung an Ihre PC-Hardware ist Pentium 4 mit VGA Monitor und CD-ROM Laufwerk.

Ihr PC muss über einen 512 MB Speicher und mind. 700 MB freien Speicherplatz auf der Festplatte verfügen.

PC, Drucker usw. gehören nicht zum Lieferumfang.

KRUSE Sicherheitssysteme GmbH & Co. KG • Duvendahl 92 • 21435 Stelle • Tel.: 04174 592-22 • vertrieb@kruse-sicherheit.de

OPTIONALE- KOMPONENTEN

Implementierung eines kundenspezifischen RS232 Kartenlesers, biometrischer Erkennung (Fingerprint oder IrisScan), SMS-Alarmierung per GSM-Modem

Zusätzliche Systemsprachen nach Absprache und Programmierung.

Individuelle Änderung der Reports oder Sonderprogrammierungen sowie Hardwareimplementierung (USB-Direktdrucker) sind möglich – sprechen Sie uns an!

OPC XML-DA SCHNITTSTELLE

In den SW4 wurde die OPC XML-DA-Schnittstelle implementiert. Hierdurch kann eine teilweise Verwaltung des SchlüsselWächter 4 durch eine Managementsoftware erreicht werden.
Die OPC XML-DA Schnittstelle ist optional zu bestellen.

SOAP – SCHNITTSTELLE

Der SW4 hat eine SOAP-Schnittstelle integriert, welche ermöglicht umfangreiche, integrierte Kundenlösungen zu realisieren.

Die Entwicklung/Anpassung der Kundensoftware erfolgt dabei grundsätzlich durch den Kunden
Die SOAP Schnittstelle ist optional zu bestellen.

KRUSE Sicherheitssysteme GmbH & Co. KG • Duvendahl 92 • 21435 Stelle • Tel.: 04174 592-22 • vertrieb@kruse-sicherheit.de