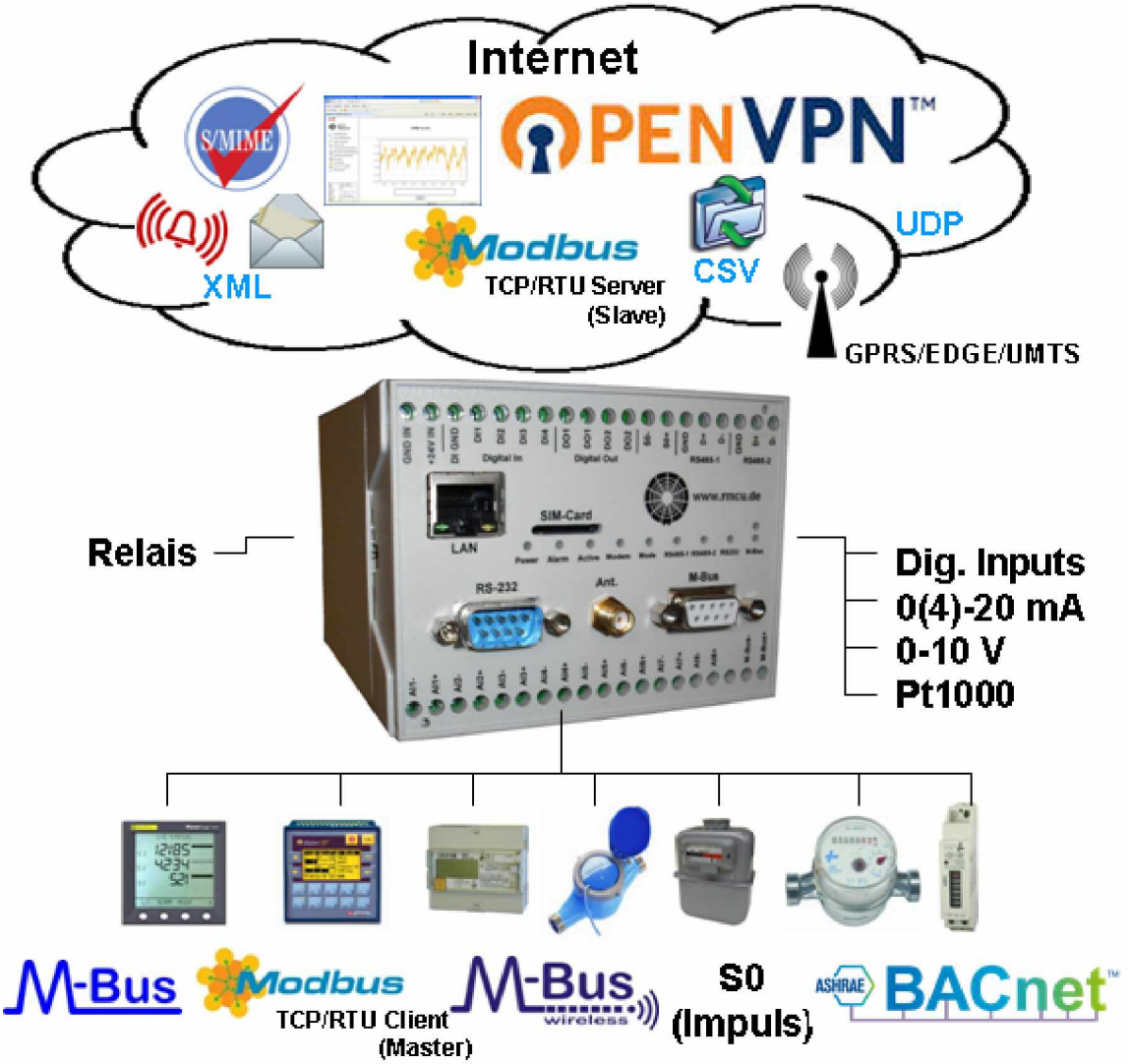
Ingenieurbüro H. Lertes GmbH & Co. KG
Georg Treber Strasse 27
D- 65428 Rüsselsheim

Tel.: +49 6142 945950
Fax: +49 6142 406873
Email: sales@lertes.de
www.RmCU.de

# RmCU V 4.0 DIN Rail
# RmCU V 3.4 DIN Rail / Compact

## IT- Sicherheitsgesetz / BSI IT- Grundschutz
## ISO 27001 Zertifizierung

August 2016, Draft V00




Member of OMS®

# Inhaltsverzeichnis

# 1 Einleitung

Das vorliegende Dokument befasst sich mit der Zertifizierungsfähigkeit des Datenloggers RmCU im Sinne des IT- Grundschutzes.

## *1.1 Anforderungen (Zitate)*

"Im Juni 2015 hat der Bundestag nun das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz) verabschiedet. Dadurch will er eine verbindliche Grundlage dafür schaffen, die Sicherheit von IT-Systemen in Deutschland zu erhöhen."

"Die Versorgung mit Wasser, Elektrizität, Gas, Mineralöl und Wärme ist sowohl für die Bevölkerung als auch für die Wirtschaft – und somit für das staatliche Gemeinwesen – essenziell. Deshalb unterliegen Unternehmen der Versorgungswirtschaft im Rahmen der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS) speziellen Auflagen."

"Als IT-Grundschutz bezeichnet die Bundesverwaltung eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik (IT). Das Ziel des Grundschutzes ist das Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme. Zum Erreichen des Ziels empfehlen die IT-Grundschutz-Kataloge technische Sicherheitsmaßnahmen und infrastrukturelle, organisatorische und personelle Schutzmaßnahmen."

"Seit Anfang des Jahres 2006 können daher auch ISO 27001-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden. Die Integration von ISO 27001, der aus der BS 7799-2 hervorgegangen ist, macht diese ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz besonders für international tätige Institutionen interessant."

"§ 8 Absatz 1 BSIG regelt die Befugnis des BSI, allgemeine technische Mindeststandards für die Sicherung der Informationstechnik des Bundes vorzugeben. Der Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um eine angemessene Sicherheit für einen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen."

# 2 Umfang der Zertifizierung

Zertifiziert werden keine Systemkomponenten einzelner Hersteller, sondern das von einer Firma betriebene Gesamtsystem, bestehend aus einzelnen Komponenten und der firmeninterne Umgang mit diesen Komponenten.
Die einzelnen Systemkomponenten unterstützen dabei die geforderten Mindeststandards im Sinne des BSI- Grundschutzes. Der Betreiber erbringt bei der Zertifierung den Nachweis, dass er mit diesen Standards verantwortungsvoll umgeht, benennt intern verantwortliche System- bzw. Gateway- Administratoren und definiert Prozesse wie z.B. das Erstellen, oder den zyklischen Austausch von Zertifikaten.

Unsere Produkte unterstützen diese Zertifizierung in dem sie die entsprechenden Mindeststandards unterstützen und Schnittstellen zur Administration zur Verfügung stellen.

# 3 zertifizierbare technische Mindeststandards

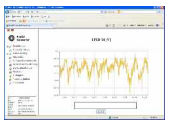
Im Sinne des BSI Grundschutz verfügt RmCU folgende zertifizierungswürdige "technische Mindeststandards".

## *3.1 OpenVPN*

OpenVPN ist ein Programm zum Aufbau eines Virtuellen Privaten Netzwerkes (VPN) über eine verschlüsselte TLS-Verbindung. Zur Verschlüsselung werden die Bibliotheken des Programmes OpenSSL benutzt. OpenVPN verwendet wahlweise UDP oder TCP zum Transport.

RmCU seitige Implementierung:
- Die Zertifikate können über den SSH Zugang, auch automatisiert, ausgetauscht werden
- Über eine in RmCU integrierte Firewall kann geregelt werden ob:
    - IP Pakete die LAN- seitig eingespeist werden in den VPN Tunnel gelangen können
    - IP- Pakete aus dem VPN Tunnel auf den LAN Port weitergereicht werden können
    - RmCU trotz aktivem VPN auf andere IP- Netze zugreifen kann
    - RmCU trotz aktivem VPN über andere Netze (LAN/Mobile-Internet) ansprechbar ist
    - Der SSH Zugang trotz aktivem VPN über Netze erreichbar ist
    - RmCU auf Ping Requests aus anderen Netzen (LAN/Mobile-Internet) reagiert wird

## 3.2 HTTPS



HyperText Transfer Protocol Secure (HTTPS, englisch für sicheres Hypertext-Übertragungsprotokoll) ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen. Es nutzt zur Transportverschlüsselung TLS(SSL).

RmCU seitige Implementierung:
- Das Zertifikat kann über den SSH Zugang, auch automatisiert, ausgetauscht werden
- Es ist einstellbar ob das Zertifikat über den WEB- Browser downloadbar ist

## 3.3 SFTP


Das SSH File Transfer Protocol oder Secure File Transfer Protocol (SFTP) ist eine für die Secure Shell (SSH) entworfene Alternative zum File Transfer Protocol (FTP), die Verschlüsselung ermöglicht.

RmCU seitige Implementierung:
- Ip- Adresse, Port, Uid und Pwd sind über das Webinterface editierbar und könnten auch direkt in der entsprechenden XML Datei verändert werden.

## 3.4 S/Mime


S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und das Signieren von MIME-gekapselter E-Mail durch ein hybrides Kryptosystem.

RmCU seitige Implementierung:
- Das Zertifikat kann über den SSH Zugang, auch automatisiert, ausgetauscht werden

### *3.5 SSH / SCP Zugang*

Secure Shell oder SSH bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann.

RmCU seitige Implementierung:
- Der Zugang erfolgt ausschliesslich über den User root.
  Die Uid´s und Pwd´s aller Userlevel liegen verschlüsselt (MD5) im Dateisystem.
  Diese Datei kann über das Webinterface editiert werden, sie kann aber komplett über den SSH Zugang ausgetauscht werden.

### *3.6 Uid´s und Pwd´s der Userlevel*

RmCU seitige Implementierung:
Die Uid´s und Pwd´s aller Userlevel liegen verschlüsselt (MD5) als Datei im Dateisystem vor.
Die User können über das Webinterface ihre und untergeordnete UID´s und Pwd´s ändern.
Die Datei kann über SSH Zugang aautomatisiert ausgetauscht werden.