

## ISK-CRASER

Der ISK-CRASER ist ein leistungsstarker OpenVPN-Server für die Internet-Fernwartung. Zusammen mit den IKOM-Routern LAN-WAN, GPRS und HSPA ermöglicht er Fernwartungslösungen mit sehr kurzen Inbetriebnahme Zeiten.

Im Unterschied zum CS200 nutzen Sie beim ISK-CRASER einen Virtual Server, der von uns über einen Hosting-Dienstleister betrieben wird. Das hat den Vorteil, dass Sie einschließlich der fixen public IP eine fertige Serverlösung vorfinden, die rund um die Uhr Online ist und von uns gewartet wird. Wir verwenden leistungsstarke Industrie-PCs

des Hosting-Dienstleisters, die eine redundante Stromversorgung und die nötige Breitbandanbindung ans Internet bereitstellen (100MBit/s). Dennoch können Sie diesen Server wie vom CS200 gewohnt, selbst konfigurieren. Wir bieten Ihnen dazu PC-Fernwartungs-Zertifikate an, mit denen Sie nicht nur den Datenaustausch mit Ihren Routern realisieren, sondern bei entsprechenden Konfigurationsrechten auch auf die Konfigurationsseiten des ISK-CRASERs geschützt zugreifen können. Je nach bestelltem Zertifikat, können Sie bis zu 128 weitere Routerzertifikate und 20 PC-Zertifikate selbst erzeugen. Auch ein Vollzugriff, bei dem Sie den gesamten Server benutzen ist möglich. Die Hauptaufgabe des ISK-CRASERs besteht darin, den VPN-Datenstrom so zu vermitteln, dass die Endgeräte und Router-Subnets untereinander kommunizieren können. Dabei werden konfigurierbare Zugriffsrechte beachtet. Das durchgängig angewandte Prinzip der Subnetkopplung ermöglicht neben der Fernwartung auch einen Einsatz für allgemeine Automatisierungsaufgaben mit weit verteilten Inputs/Outputs.



## Endgeräte am ISK-CRASER

Folgende Endgeräte können als OpenVPN-Clients am ISK-CRASER arbeiten

- IKOM-Router GPRS
- IKOM-Router HSPA
- IKOM-Router LAN-WAN mit DSL-Modem AM100
- IKOM-Router LAN-WAN mit Kopplung zu Ihrem vorhandenen DSL-Router
- Fernwartungs-PC (WIN-XP, WIN7, Linux, Mac OS X) ausgestattet mit OpenVPN GUI
- Industrie-PC (WIN-XP, WIN7, Linux, Mac OS X) mit OpenVPN-Client-Funktionalität
- beliebige OpenVPN-Router (OpenVPN-Client-Zertifikat muss als p12-Datei ladbar sein)



## Produktmerkmale des ISK-CRASERS

- Der ISK-CRASER löst das Problem der privaten IP-Adresse normaler SIM-Karten. Es können daher alle SIM-Karten verwendet werden, die für UMTS geeignet sind.
- Die Adressierung wird konsequent in globale und lokale Subnet-Bereiche eingeteilt. Dadurch sind identische Subnets auf der lokalen Seite möglich. Die Planung der lokalen Subnets ist somit unabhängig von später hinzukommenden Subnets.
- Zu jedem Fernwartungs-Subnet und zu jedem Fernwartungs-PC protokolliert der ISK-CRASER die Verbindungszeiten. Nach einer Verbindungstrennung wird auch das verbrauchte Datenvolumen des betreffenden Teilnehmers protokolliert.
- Der ISK-CRASER konfiguriert nach Ihren Anforderungen Zugriffsrechte für die Datenstrecken:
  - Subnet-Subnet
  - Subnet-FernwartungsPC
  - FernwartungsPC-IndustriePC
- Beim ISK-CRASER bekommen Sie zu jedem einzelnen Parameter einen ausführlichen Maschinenkommentar angezeigt, sobald Sie den Parameternamen mit dem Mauszeiger berühren.
- Zur Konfiguration eines Fernwartungs-subnets im IKOM-Router HSPA/GPRS/LAN-WAN müssen Sie lediglich eine Zertifikatdatei downloaden. Die Datei wird vorher vom ISK-CRASER generiert.
- Die OpenVPN-Keepalive-Funktion ist frei konfigurierbar. Dadurch ist eine bedarfsgerechte GPRS/UMTS-Traffic-Regulierung möglich.
- Die Konfigurationsseiten des ISK-CRASER können Sie über einen Fernwartungstunnel erreichen. Die Zugriffsrechte sind konfigurierbar.
- Der ISK-CRASER ist 24h am Tag Online, besitzt eine redundante Stromversorgung und stellt einen 100MBit/s-Internetanschluss mit fixer public IP zur Verfügung. Die Software wird auf dem neuesten Stand gehalten.



### Fernwartung mit dem ISK-CRASER



In diesem Beispiel werden 2 Subnetze und ein Fernwartungs-PC über den ISK-CRASER gekoppelt. Der Fernwartungs-PC kann sowohl auf das gesamte LAN1-Subnetz des HSPA-Router zugreifen als auch auf das gesamte LAN1-Subnetz des LAN/WAN-Router. Die Zugriffsrechte im ISK-CRASER lassen sich auch so konfigurieren, dass HSPA-Router und LAN/WAN-Router untereinander auf ihre LAN1-Subnetze zugreifen können. Somit sind neben Fernwartungsaufgaben auch allgemeine Automatisierungsaufgaben lösbar.



## Die Zertifikatetypen des ISK-CRASERs

Zur Nutzung unseres OpenVPN-Servers bieten wir Ihnen Zertifikatetypen mit unterschiedlichen Konfigurationsrechten an. Das bedeutet, dass unsere Fernwartungszertifikate nicht nur zum Datenaustausch zwischen den OpenVPN-Clients verwendbar sind, sondern darüber hinaus auch zum Konfigurieren des OpenVPN-Servers. Der Vorteil dieses Ansatzes besteht darin, dass jedes PC-Fernwartungs-Zertifikat bereits alle Adress- und Zugangsdaten enthält, um sicher über den CRASER mit den OpenVPN-Clients der jeweiligen Anwendung zu kommunizieren. Warum sollte man diese Adress- und Zugangsdaten nicht nutzen, um den OpenVPN-Server zu konfigurieren? Man spart unnötige Adress- und Passworttabellen und kommuniziert außerdem sicherer als bei Konfigurationszugriffen über einen separaten Konfigurationszugang über https. Der https-Port kann in der CRASER-Firewall deaktiviert werden. Somit ist das System besser gegen DDOS-Attacken geschützt. Der OpenVPN-UDP-Port 1194 ist nicht so einfach angreifbar wie der auf TCP beruhende Port 443 von https.

Wir bieten unsere PC-Fernwartungszertifikate mit einer Option zur CRASER-Konfiguration an. Dazu unterscheiden wir 4 Konfigurations-Level:

**L0-Zertifikatetyp:** L0 steht für Konfigurations-Level0. Mit diesem Typ können Sie lediglich Fernwartungsaufgaben über den ISK-CRASER realisieren und nicht auf die CRASER-Konfigurationsseiten zugreifen. Zur Fernwartung benötigen Sie ein oder mehrere PC-Zertifikate und ein Routerzertifikat für jeden Fernwartungsrouter Ihres Projektes. Je nach Bestellung bekommen Sie ein für Ihre Anwendung zugeschnittenes Zertifikatpaket. Die Zugriffsrechte für Ihre Anwendung sind bei Auslieferung des Zertifikatpaketes schon fertig eingerichtet.

**L1-Zertifikatetyp:** L1 steht für Konfigurations-Level1. Mit diesem Typ können Sie neben den eigentlichen Fernwartungsaufgaben auch auf die Konfigurationsseiten des ISKCRASERs zugreifen. Dieser Zugriff beschränkt sich bei L1 auf eine Visualisierung der Statusinformation aller an der VPN-Kopplung beteiligten Router und PCs. Sie können somit leicht überprüfen, ob Ihre Router am CRASER angemeldet sind oder nicht. Auch die Zugriffsrechte aller beteiligten VPN-Clients lassen sich im Konfigurationslevel 1 ändern.

**L2-Zertifikatetyp:** L2 steht für Konfigurations-Level2. Dieser Typ erlaubt Ihnen sogar eigene Router und PC-Zertifikate zu erzeugen, so dass Sie Ihr Projekt bei Bedarf selbständig erweitern können, ohne weitere Zertifikate zu erwerben.

**L3-Zertifikatetyp:** Mit dem L3-Konfigurations-Level haben Sie den vollen Zugriff auf unseren ISK-CRASER und konfigurieren zusätzlich zu allen vorgenannten Funktionen auch eigene Projekte. Somit können Sie mehrere unabhängige Anwendungen über den ISK-CRASER fahren. Zwischen verschiedenen Projekten ist jeglicher Zugriff gesperrt. Mit diesem Zertifikatetyp nutzen Sie alle Ressourcen des CRASERs. Damit verbunden ist ein Nutzungsvertrag beim Hosting-Dienstleister.

Die Systemgrenzen liegen bei

- 253 Subnetzen (253 Router)
- 40 Fernwartungs-PCs
- 16 Projekte
- 200 gleichzeitig aktive VPN-Tunnel

Im Folgenden werden die einzelnen Zertifikatetypen ausführlich vorgestellt:



ISK-CRASER-L0-PC OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Nach dem Start der OpenVPN-GUI arbeitet Ihr PC als Fernwartungs-PC. Sie haben freien Zugriff auf die Subnetze Ihrer Fernwartungs-Router. Für alle Fernwartungs-Router wird der hierzu passende Zertifikatetyp "ISK-CRASER-RT" benötigt. Die Zugriffsrechte werden nach Ihren Anforderungen eingestellt. Die Fernwartungsrouter können auch für Zugriffe untereinander freigeschaltet werden. ISK-CRASER-Konfigurationsseiten:

- Zugriff nicht möglich.

ISK-CRASER-L1-PC OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Nach dem Start der OpenVPN-GUI arbeitet Ihr PC als Fernwartungs-PC. Sie haben freien Zugriff auf die Subnets Ihrer Fernwartungs-Router. Für alle Fernwartungs-Router wird der hierzu passende Zertifikatetyp "ISK-CRASER-RT" benötigt. Die Zugriffsrechte werden nach Ihren Anforderungen eingestellt. Die Fernwartungsrouter können auch für Zugriffe untereinander freigeschaltet werden. ISK-

CRASER-Konfigurationsseiten (Aufruf: "<http://172.20.0.1>):

- Zugriff auf die Seiten „Subnet Table“ und „RW Table“:  
Der Status aller Fernwartungs-Router/Fernwartungs-PCs wird angezeigt.  
Es ist möglich die Zugriffsrechte zu ändern.

ISK-CRASER-RT OpenVPN-Zertifikat im gepackten p12-Format und Firewall als ShellScript (sh-Datei). Beide Dateien lassen sich in einen IKOM-Router laden. Nach Aufbau der OpenVPN-Verbindung ist das Fernwartungs-Subnet des Routers von Ihrem Fernwartungs-PC erreichbar. Sie benötigen den Typ "ISK-CRASER-RT" immer dann, wenn Sie Ihren Fernwartungs-PC mit den Zertifikatetypen "ISK-CRASER-L0-PC" oder "ISK-CRASER-L1-PC" ausstatten.

ISK-CRASER-L2-S16 OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Mit diesem Zertifikatetyp können Sie nicht nur auf die Subnetze Ihrer Fernwartungsrouter zugreifen, sondern auch Zertifikate für neue Subnets selbst generieren.

ISK-CRASER-Konfigurationsseiten (Aufruf: "<http://172.20.0.1>):

- Zugriff auf die Seite "Add New Subnet":  
Sie können die Zertifikate für max. 16 Fernwartungs-Subnets selbst erzeugen.
- Zugriff auf die Seite "Add new RW":  
Sie können die Zertifikate für maximal 10 Fernwartungs-PCs selbst erzeugen.
- Zugriff auf die Seiten „Subnet Table“ und „RW Table“:  
Der Status aller Fernwartungs-Router/Fernwartungs-PCs wird angezeigt.  
Es ist möglich, die Zugriffsrechte zu ändern.



ISK-CRASER-L2-S32 OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Mit diesem Zertifikatetyp können Sie nicht nur auf die Subnets Ihrer Fernwartungsrouten zugreifen, sondern auch Zertifikate für neue Subnets selbst generieren.

ISK-CRASER-Konfigurationsseiten (Aufruf: "<http://172.20.0.1>):

- Zugriff auf die Seite "Add New Subnet":  
Sie können die Zertifikate für max. 32 Fernwartungs-Subnets selbst erzeugen.
- Zugriff auf die Seite "Add new RW":  
Sie können die Zertifikate für max. 10 Fernwartungs-PCs selbst erzeugen.
- Zugriff auf die Seiten „Subnet Table“ und „RW Table“:  
Der Status aller Fernwartungs-Router/Fernwartungs-PCs wird angezeigt.  
Es ist möglich, die Zugriffsrechte zu ändern.

ISK-CRASER-L2-S64 OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Mit diesem Zertifikatetyp können Sie nicht nur auf die Subnets Ihrer Fernwartungsrouten zugreifen, sondern auch Zertifikate für neue Subnets selbst generieren.

ISK-CRASER-Konfigurationsseiten (Aufruf: "<http://172.20.0.1>):

- Zugriff auf die Seite "Add New Subnet":  
Sie können die Zertifikate für max. 64 Fernwartungs-Subnets selbst erzeugen.
- Zugriff auf die Seite "Add new RW":  
Sie können die Zertifikate für max. 20 Fernwartungs-PCs selbst erzeugen.
- Zugriff auf die Seiten „Subnet Table“ und „RW Table“:  
Der Status aller Fernwartungs-Router/Fernwartungs-PCs wird angezeigt.  
Es ist möglich, die Zugriffsrechte zu ändern.

ISK-CRASER-L2-S128 OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Mit diesem Zertifikatetyp können Sie nicht nur auf die Subnets Ihrer Fernwartungsrouten zugreifen, sondern auch Zertifikate für neue Subnets selbst generieren.

ISK-CRASER-Konfigurationsseiten (Aufruf: "<http://172.20.0.1>):

- Zugriff auf die Seite "Add New Subnet":  
Sie können die Zertifikate für max. 128 Fernwartungs-Subnets selbst erzeugen.
- Zugriff auf die Seite "Add new RW":  
Sie können die Zertifikate für max. 20 Fernwartungs-PCs selbst erzeugen.
- Zugriff auf die Seiten „Subnet Table“ und „RW Table“:  
Der Status aller Fernwartungs-Router/Fernwartungs-PCs wird angezeigt.  
Es ist möglich, die Zugriffsrechte zu ändern.



### ISK-CRASER-L3

OpenVPN-Zertifikat im gepackten p12-Format und OpenVPN-Konfiguration als cnf-Datei. Beide Dateien lassen sich direkt ins config-Verzeichnis der OpenVPN-GUI für PCs laden. Mit diesem Zertifikatetyp können Sie nicht nur auf die Subnets Ihrer Fernwartungsrouters zugreifen, sondern auch Zertifikate für neue Subnets selbst generieren und neue Projekte erzeugen. Mit diesem Zertifikatetyp nutzen Sie alle Ressourcen des CRASERs. Damit verbunden ist ein Nutzungsvertrag beim Hosting-Dienstleister.

ISK-CRASER-Konfigurationsseiten (Aufruf: "<http://172.20.0.1>"):

- Zugriff auf die Seite "Add New Subnet":  
Sie können die Zertifikate für max. 252 Fernwartungs-Subnets selbst erzeugen.
- Zugriff auf die Seite "Add new RW":  
Sie können die Zertifikate für max. 50 Fernwartungs-PCs selbst erzeugen.
- Zugriff auf Seite „Add Project“  
Sie können neue Projekte erzeugen.
- Zugriff auf die Seiten „Subnet Table“ und „RW Table“:  
Der Status aller Fernwartungs-Router/Fernwartungs-PCs wird angezeigt.  
Es ist möglich, die Zugriffsrechte zu ändern.

## Technische Daten

CPU Core	Intel XEON-CPU, Hardware-RAID
Speed	1,5GHz
Memory	1GByte RAM 2GByte dynamisches RAM 50GByte Festplatte
WAN-IP-Address	fix, public IP
Redundancy	redundancy of power supply
Operating System	Linux Debian 7.0
Firmware	CRASER V1.