

RKD® - Radio Key Distribution

Quantensichere Schlüsselgenerierung auf Basis physikalischer Kryptographie

1. Über Insitu

Insitu entwickelt long-term Security Lösungen für Unternehmen, Behörden und Organisationen mit höchsten Sicherheitsansprüchen an die Informationssicherheit bei Datenverarbeitung und Kollaboration.

Hinter unserem Produkt **RKD®** (Radio Key Distribution) steht eine bahnbrechende physikalische Methode zur Generierung und Verteilung von kryptografischen Schlüsseln für maximale Sicherheit. RKD® nutzt die inhärente Zufälligkeit und Gegenseitigkeit von Funkkanälen zur Erstellung von Zufallszahlen, um damit wirklich unvorhersehbare Schlüssel zu erstellen sowie auszutauschen.

Das von Insitu entwickelte RKD® Produkt ist weltweit das erste seiner Art und eignet sich besonders zur Schlüsselgenerierung von Daten bei bewegten Objekten und Vehikeln.

2. RKD® - Wissenschaftlich-/Technischer Hintergrund

Bei **RKD®** werden Funksignale mit gleichen Frequenzen über 100 MHz in beide Richtungen (von A nach B und von B nach A) gesendet, die empfangenen Signale auf beiden Seiten gemessen - meist die Signalstärke, der Phasenwinkel und/oder die Laufzeit - und weil die Übertragung in beide Richtungen reziprok ist, können auf beiden Seiten nahezu die gleichen Messwerte ermittelt werden. Aus diesen Messwerten werden dann durch eine von Insitu entwickelte Software kryptografische Schlüssel ermittelt, die zufällig und auf beiden Seiten gleich sind. Die Zufälligkeit der Schlüssel ergibt sich aus dem Übertragungsweg der Funksignale (der inhärenten Unvorhersehbarkeit) und kann von einem Dritten (Angreifer) nicht gemessen werden. Änderungen der Messungen entstehen vor allem durch die Dynamik des Übertragungsweges (Reflexionen etc.) und der Bewegung auf zumindest einer Seite (Entfernungsänderungen). Es ist kein zusätzlicher nicht-deterministischer Zufallszahlengenerator erforderlich, weil sich die Zufälligkeit aus den zufälligen Messwerten ergibt.

3. Lieferform - Schaubild RKD® (Ansichtsexemplar/Entwicklungsmuster)



Im Standard liefern wir dieses Produkt als „software-only“ Paket zur Integration in die kundeneigene Hardware/System Infrastruktur.

Dafür stellen wir eine Bauteile-Stückliste, einen Platinen-Plan sowie die RKD® Software in einem gesicherten Installationspaket zur Verfügung.

Aktuell unterstützt die RKD®-Software gängige, aktuelle Linux Betriebssysteme.

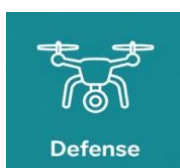
Alternativ, bei Bedarf, kann RKD® auch als fertiges Gerät inkl. USB Schnittstelle geliefert werden. Aktuell (Stand 06/2026) ist das Gerät für Pilotprojekte freigegeben; es existiert noch keine Zertifizierung.

4. Einsatzbereiche

RKD® wurde entwickelt zur hochsicheren und langfristig resilienten Datenverschlüsselung für kabellosen Datenaustausch zwischen bewegten Objekten/Vehikeln. RKD setzt für die eingesetzte Funktechnologie auf den LoRa Standard. Dabei liegt die durchschnittliche Reichweite in der Praxis zwischen den kommunizierenden Objekten bei ca. 10 km.

Im praktischen Einsatz kann es dabei zu Schwankungen kommen, die sich aus den Qualitätsanforderungen dieser Funktechnologie an die Umgebungsbedingungen ergeben.

RKD® eignet sich besonders für folgende Branchen Segmente:



5. Support und Beratung

Auf Kundenanfrage leisten wir gerne Unterstützung, unsere Software in die kundeneigene IT-Infrastruktur/Verschlüsselungslösung zu integrieren.

6. USPs von RKD®



Sicher – langfristig resiliente und maximale Sicherheit durch physikalische Kryptographie zur Schlüsselgenerierung



Innovativ – kann insbesondere für Bewegte Verwendung modernster mathematischer und physikalischer Kryptographie



kostengünstig – Wesentlich kostengünstiger als das bekanntere QKD Verfahren



robust - Einfache Integration in gängige PC-Betriebssysteme und *seamless* erweiterbar mit zukünftigen, neuen Verschlüsselungsalgorithmen

7. Kontakt

insitu software GmbH

Heinrich Schneidmadel Strasse 15

A-3100 St. Pölten

Mail: office@insitu.software

Web: <https://insitu.software>

Tel.: 0043-(0)676-4337123