IN SITU
New generation security

RKD® - Radiosignal Key Distribution

Quantum-computer-resistant key generation based on physical cryptography

1. About Insitu

Insitu develops long-term security solutions for companies, government agencies and organizations with the highest information security requirements for data processing and collaboration.

Our RKD® (Radiosignal Key Distribution) product is based on a groundbreaking physical method for generating and distributing cryptographic keys to provide maximum security. RKD® uses the inherent randomness and reciprocity of radio channels to generate random numbers, enabling the creation and exchange of truly unpredictable keys.

Developed by Insitu, RKD® is the first product of its kind worldwide and is particularly suitable for generating keys for data associated with moving objects and vehicles.

2. RKD® - Scientific/Technical Background

With RKD®, radio signals at the same frequencies above 100 MHz are transmitted in both directions (from A to B and from B to A). The received signals are measured at both ends, usually in terms of signal strength, phase angle and/or propagation time. Because transmission is reciprocal in both directions, almost identical measurements can be obtained at both ends. Software developed by Insitu then derives cryptographic keys from these measurements. The keys are random and identical at both ends. Their randomness arises from the radio signal propagation path (its inherent unpredictability) and cannot be measured by a third party (attacker). Changes in the measurements primarily result from the dynamics of the propagation path (reflections, antenna position, etc.) and movement at least at one end (changes in distance). No additional non-deterministic random number generator is required, as randomness is derived from the random measurements.

3. Delivery Format - RKD® Illustration (Demonstration Unit/Development Prototype)



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.

Alternatively, RKD® can also be supplied as a complete device with a USB interface if required. As of November 2026, the device is approved for pilot projects; certification has not yet been obtained.

4. Applications

RKD® was developed for highly secure, long-term resilient data encryption for wireless data exchange between moving objects/vehicles. RKD uses the LoRa standard for its radio technology. In practice, the average range between communicating objects is approximately 10 km.

In practical use, the range may vary depending on the environmental conditions required for reliable operation of this radio technology.

RKD® is particularly suitable for the following industry segments:







5. Support and Consulting

Upon request, we are happy to assist customers in integrating our software into their own IT infrastructure/encryption solution.

6. Unique Selling Points of RKD®



Secure – PLKG: long-term resilience and maximum security through physical cryptography for key generation



Innovative – Wireless technology particularly suitable for moving objects



Cost-effective – Significantly more affordable than the better-known QKD method



Robust – Easy integration into common PC operating systems and seamless extensibility with new encryption algorithms in the future

7. Contact

insitu software GmbH

Heinrich Schneidmadel Strasse 15

A-3100 St. Pölten

Mail: office@insitu.software

Web: https://insitu.software

Tel.: 0043-(0)676-4337123