Secure Bluetooth® connection developed by Endress+Hauser

A secure low power technology for the process industry

Customer advantages of Endress+Hauser's secure Bluetooth® Low Energy connection with CPace protocol:

- Increased usability, time efficiency and security of your plant when using Bluetooth® devices thanks to CPace
- Secure use of passwords in industrial plants independent of the password length and availability of a complex PKI infrastructure by utilizing PAKE protocols
- Usage independent of device type and power specifications due to verification of only one procedure
- Prevention of phishing and man-in-the-middle attacks by using asymmetric cryptography
- Stronger security than other solutions in standard use (e.g. pre-shared key) – Endress+Hauser solution recommended by IETF

Overcoming Bluetooth® security pitfalls Convenient wireless access to field instruments is of increasing interest for operators across all sectors of the process industry. Significant security risks emerge with the growing frequency with which instruments are accessed remotely.

Additionally, developments in the Industrial Internet of Things are leading to increasingly interconnected process control components. These field instruments have to be installed, monitored or serviced on a regular basis by internal or external personnel. Secure password-based user authentication plays a special role today, particularly when devices with wireless interfaces such as Bluetooth® are involved and when plant operators have not yet set up their own security departments for managing a complex Public Key Infrastructure (PKI).

As the industrial setting demands significantly higher protection than the consumer domain that is considered by Bluetooth®'s built-in mechanisms, Endress+Hauser has developed an additional security layer that protects the passwords, using a solution called CPace as its core-component. With CPace, the notorious attacks on the Bluetooth® pairing-step are prevented.

As it is extremely difficult to protect passwords, Endress+Hauser's CPace uses a powerful PAKE technique which was derived from the PACE method used in German ID cards.

Security with user-friendly password lengths For conventional security solutions, either certificates and PKI or long and cryptic keys such as "X4RTQ 4KPKM PTWXS 3BP4Z C66D5 RRJ26" are mandatory. With CPace, Bluetooth® connections to measuring instruments are always secure, even in cases where users have assigned relatively short passwords, as the critical offline password attacks are averted. Thanks to the asymmetric cryptography used in PAKE protocols, the level of security can be largely decoupled from the password length.

Endress+Hauser
People for Process Automation

Furthermore, due to the limited resources in field devices, password verification with comparable protocols like SRP or PACE would have resulted in a login delay of a minute or more. With Endress+Hauser's CPace design, the maximum login latency during password verification is kept below two seconds – with no sacrifice of the level of security.

As security can now be achieved without a complex security infrastructure and without long and cryptic access passwords, better real-world security and better usability is realized.

CPace convinced the Internet standardization body The need for improved security solutions of password based logins was independently identified by the Internet standardization body IETF in 2018. In 2019, it set up a corresponding security analysis and selection process competition in IETF's cryptography expert group CFRG. In 2020 CFRG chose the Endress+Hauser in-house solution CPace as winner ("Recommended for use in internet protocols") as the result of a comprehensive security analysis also involving several other protocol candidates.

Independently, in 2016, the Munich-based Fraunhofer Institute AISEC classified the protection level of the Endress+Hauser Bluetooth® security extension as "high".

Potential hackers will not be successful even if they ...

- expend several weeks of effort
- have expertise in the areas of electronics, cryptography and side-channel attacks
- possess internal knowledge about the entire system and
- can gain full access to all wireless interfaces

Secure connection with Bluetooth Low Energy and CPace

Currently all Endress+Hauser measuring instruments with Bluetooth® connection are supported

What is PAKE and IETF?

Password-authenticated key exchange (PAKE) refers to a group of protocols that verify access authentication via passwords without allowing hackers to mount so-called offline attacks against them with hacker tools (e.g. within a field device with Bluetooth® interface).

The Internet Engineering Task Force IETF and its associated Internet Research Task Force IRTF is the body organizing the standards for the internet, e.g. protocols such as TCP/IP, TLS and IPSEC used in internet backbones, local-area networking infrastructure and applications such as internet browsers. Within the IETF the responsibility for the security analysis for the cryptography within the standards is assigned to the IRTF Crypto Forum Research Group CFRG.

Eco-friendly produced and printed on paper from sustainable forestry.

www.addresses.endress.com

IN01194S/04/EN/01.21

Endress+Hauser

People for Process Automation