# Sichere Bluetooth®-Verbindung von Endress+Hauser

## Eine sichere Low-Power-Technologie für die Prozessindustrie

**Kundenvorteile der sicheren Bluetooth® Low Energy-Verbindung mit CPace-Protokoll von Endress+Hauser:**

- Bessere Nutzbarkeit, Zeiteinsparungen und erhöhte Anlagensicherheit bei der Verwendung von Bluetooth®-Geräten – dank CPace
- Sichere Verwendung von Passwörtern in industriellen Anlagen, unabhängig von der Passwortlänge und der Verfügbarkeit einer komplexen PKI-Infrastruktur dank Nutzung von PAKE-Protokollen
- Nutzung unabhängig von Gerätetyp und Leistungsspezifikationen, da nur ein Protokoll verifiziert werden muss
- Verhinderung von Phishing- und Man-in-the-Middle-Angriffen durch Nutzung einer asymmetrischen Kryptografie
- Deutlich mehr Sicherheit als andere Lösungen im Standardeinsatz (z. B. Pre-Shared Key), Endress+Hauser Lösung von der IETF empfohlen

**Schluss mit Bluetooth®-Sicherheitslücken** In allen Sektoren der Prozessindustrie sind Betreiber und Bediener zunehmend an dem komfortablen drahtlosen Zugriff auf ihre Feldgeräte interessiert. Doch mit dem immer häufigeren Fernzugriff auf die Geräte entstehen auch Sicherheitsrisiken.

Zudem führen Entwicklungen wie das Industrial Internet of Things zu einer zunehmenden Vernetzung der einzelnen Prozessregelungskomponenten. Diese Feldinstrumente müssen installiert, überwacht oder regelmäßig von internem oder externem Personal gewartet werden. Die sichere passwortbasierte Benutzerauthentifizierung spielt heutzutage eine entscheidende Rolle, insbesondere wenn es um Geräte mit drahtlosen Schnittstellen wie Bluetooth® geht und Anlagenbetreiber noch keine eigenen Sicherheitsabteilungen eingerichtet haben, um eine komplexe Public Key Infrastructure (PKI) zu verwalten.

Da industrielle Umgebungen einen bedeutend höheren Schutz verlangen als der Endverbraucherbereich, für den die in Bluetooth® integrierten Mechanismen gedacht sind, hat Endress+Hauser zum Schutz von Passwörtern eine zusätzliche Sicherheitsebene entwickelt, deren Kernkomponente eine Lösung mit der Bezeichnung CPace ist. Mit CPace werden Angriffe während des Bluetooth® Pairings verhindert.

Da es extrem schwierig ist, Passwörter zu schützen, nutzt Endress+Hauser's CPace eine leistungsstarke PAKE-Technik, die von der PACE-Methode abgeleitet wurde, wie sie in deutschen Personalausweisen zum Einsatz kommt.

**Sicherheit mit benutzerfreundlichen Passwortlängen** Für konventionelle Sicherheitslösungen sind entweder Zertifikate und PKI oder lange, kryptische Schlüssel wie „X4RTQ 4KPKM PTWXS 3BP4Z C66D5 RRJ26" zwingend vorgeschrieben. Mit CPace sind Bluetooth®-Verbindungen zu Messgeräten jederzeit sicher, auch dann, wenn Benutzer nur relativ kurze Passwörter vergeben haben, da kritische Offline-Angriffe auf Passwörter wirksam abgewehrt werden.

Endress+Hauser

People for Process Automation

Dank der in den PAKE-Protokollen eingesetzten asymmetrischen Kryptografie hängt die Sicherheit nicht mehr von der Passwortlänge ab.

Zudem würde eine Passwortverifizierung mit vergleichbaren Protokollen wie SRP oder PACE aufgrund der beschränkten Ressourcen in den Feldgeräten zu einer Verzögerung von einer Minute oder mehr bei der Anmeldung führen. Mit CPace von Endress+Hauser betragen die bei der Anmeldung durch die Passwortverifizierung hervorgerufenen Latenzen dagegen weniger als zwei Sekunden – und zwar ohne Kompromisse bei der Sicherheit einzugehen.

Da Sicherheit jetzt auch ohne eine komplexe Sicherheitsinfrastruktur und lange, kryptische Zugangspasswörter möglich ist, lassen sich eine deutlich höhere reale Sicherheit und eine bessere Nutzbarkeit erreichen.

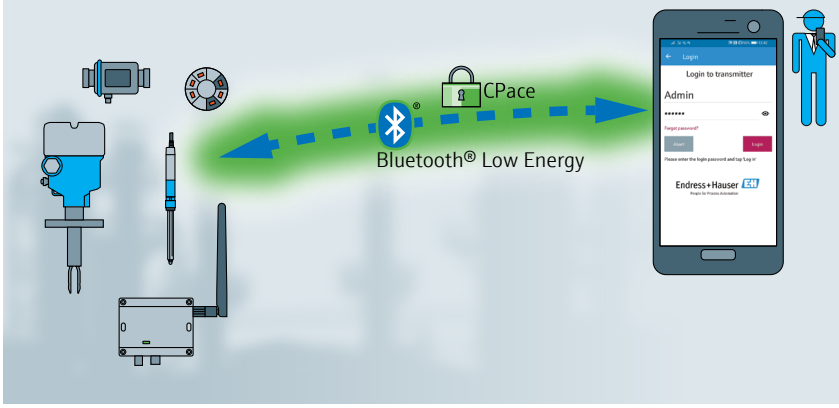
**CPace hat das Internet-Standardisierungsgremium überzeugt** Der Bedarf nach besseren Sicherheitslösungen für passwortbasierte Anmeldungen wurde bereits 2018 vom Internet-Standardisierungsgremium identifiziert. 2019 schrieb die CFRG, die kryptografische Expertengruppe der IETF, einen entsprechenden Wettbewerb für Sicherheitsanalyse und Auswahlprozesse aus. 2020 hat die CFRG die von Endress+Hauser entwickelte Lösung CPace nach einer umfassenden Sicherheitsanalyse, die auch verschiedene andere Protokolle umfasste, zum Gewinner des Wettbewerbs erklärt („Zur Verwendung in Internet-Protokollen empfohlen“).

Unabhängig davon wurde 2016 das Schutzniveau der Endress+Hauser Bluetooth®-Sicherheitserweiterung vom Münchner Fraunhofer Institut AISEC als „hoch“ eingestuft.

**Potenzielle Hacker haben keine Chance, selbst dann nicht, wenn sie …**

- mehrere Wochen mit großem Aufwand angreifen
- Erfahrung in den Bereichen Elektronik, Kryptografie und Seitenkanalangriffen haben
- über interne Kenntnisse zum gesamten System verfügen und
- Zugriff auf alle drahtlosen Schnittstellen erlangen

**Sichere Verbindung mit Bluetooth® Low Energy und CPace**




Derzeit werden alle Endress+Hauser Messgeräte mit Bluetooth®-Verbindung unterstützt

**Wofür stehen PAKE und IETF?**

Password-Authenticated Key Exchange (PAKE) bezieht sich auf eine Gruppe von Protokollen, die die Zugangsauthentifizierung anhand von Passwörtern prüfen, ohne es Hackern zu erlauben, so genannte Offline-Angriffe mit Hacker-Tools zu starten (z. B. bei einem Feldgerät mit Bluetooth®-Schnittstelle).

Die Internet Engineering Task Force, IETF, und die ihr angeschlossene Internet Research Task Force, IRTF, sind die Standardisierungsgremien für das Internet und somit z. B. für Protokolle wie TCP/IP, TLS und IPSEC zuständig, die in Internet-Backbones, LAN-Infrastrukturen und Anwendungen wie Internet-Browsern verwendet werden. Innerhalb der IETF liegt die Verantwortung für die Sicherheitsanalyse für die Kryptografie innerhalb der Standards bei der CFRG, der Crypto Forum Research Group.

Umweltfreundlich produziert und gedruckt auf Papier aus nachhaltiger Forstwirtschaft.

www.addresses.endress.com

IN01194S/04/DE/01.21

Endress+Hauser
People for Process Automation