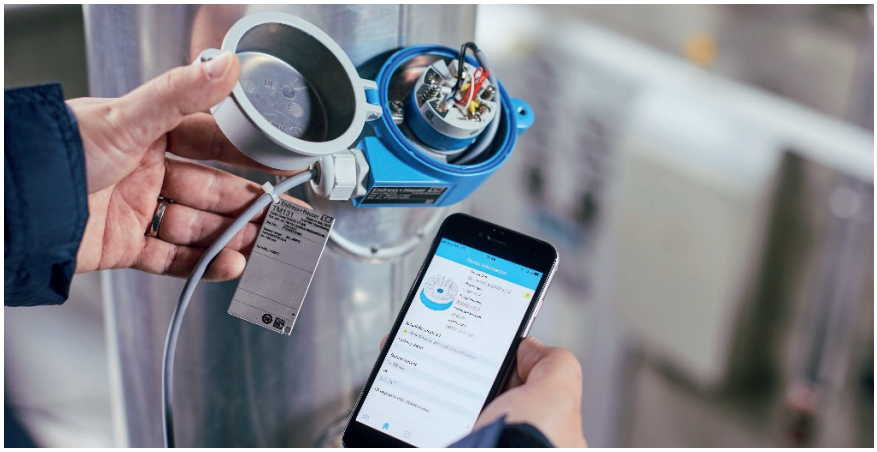
Veilige Bluetooth®-verbinding ontwikkeld door Endress+Hauser

Een veilige, energiezuinige technologie voor de procesindustrie

Voordelen voor de klant van Endress+Hauser's veilige Bluetooth® Low Energy verbinding met CPace protocol:

- Verhoogde gebruiksvriendelijkheid, tijdsefficiëntie en veiligheid van uw installatie bij Bluetooth®-apparaten dankzij CPace
- Veilig gebruik van wachtwoorden in industriële installaties onafhankelijk van de lengte van het wachtwoord en beschikbaarheid van een complexe PKI infrastructuur door gebruik te maken van PAKE protocollen
- Onafhankelijk van type apparaat en vermogensspecificaties door verificatie van slechts één procedure
- Voorkomen van phishing en man-in-the-middle aanvallen door gebruik van asymmetrische cryptografie
- Sterkere beveiliging dan andere oplossingen in standaardgebruik (b.v. pre-shared-key) – de oplossing van Endress+Hauser wordt aanbevolen door IETF



Bluetooth® beveiligingsvalkuilen overwinnen Comfortabele draadloze toegang tot instrumenten is van toenemend belang voor operators in alle sectoren van de procesindustrie. De toenemende frequentie waarmee instrumenten op afstand worden benaderd, brengt aanzienlijke veiligheidsrisico's met zich mee. Bovendien leiden ontwikkelingen in het Industrial Internet of Things (IIoT) tot steeds meer onderling verbonden procesbesturingscomponenten. Deze instrumenten moeten regelmatig worden geïnstalleerd, bewaakt of onderhouden door intern of extern personeel. Veilige gebruikersverificatie op basis van wachtwoorden speelt vandaag de dag een bijzondere rol, met name wanneer het apparaten met draadloze interfaces zoals Bluetooth® betreft en wanneer fabrieksoperators nog geen eigen beveiligingsafdelingen hebben opgezet voor het beheer van een complexe Public Key Infrastructure (PKI). Aangezien de industriële omgeving een aanzienlijk hogere bescherming vereist dan het consumentendomein dat door de ingebouwde mechanismen van Bluetooth® in aanmerking wordt genomen, heeft Endress+Hauser een extra beveiligingslaag ontwikkeld die de wachtwoorden beschermt, gebruikmakend van een oplossing genaamd CPace als kern-component. Met CPace, worden de beruchte aanvallen op de Bluetooth® pairing-step voorkomen. Omdat het extreem moeilijk is om wachtwoorden te beschermen, maakt Endress+Hauser's CPace gebruik van een krachtige PAKE techniek die is afgeleid van de PACE methode die wordt gebruikt in Duitse ID-kaarten.

Veiligheid met gebruiksvriendelijke wachtwoord lengtes Voor conventionele beveiligingsoplossingen zijn ofwel certificaten en PKI, ofwel lange en cryptische sleutels zoals 'X4RTQ 4KPKM PTWXS 3BP4Z C66D5 RRJ26' verplicht. Met CPace zijn Bluetooth®-verbindingen met meetinstrumenten

Endress+Hauser
People for Process Automation

altijd veilig, zelfs in gevallen waarin gebruikers relatief korte wachtwoorden hebben toegekend, aangezien de kritieke offline wachtwoordaanvallen worden voorkomen. Dankzij de asymmetrische cryptografie die in PAKE-protocollen wordt gebruikt, kan het niveau van beveiliging grotendeels losgekoppeld worden van de lengte van het wachtwoord.

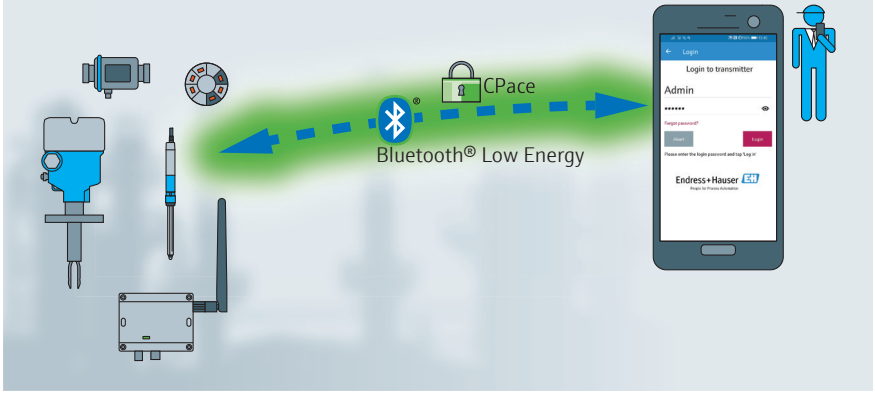
Bovendien zou wachtwoordverificatie met vergelijkbare protocollen als SRP of PACE, vanwege de beperkte middelen in instrumentatie, hebben geleid tot een inlogvertraging van een minuut of meer. Met Endress+Hauser's CPace ontwerp is de maximale login vertraging tijdens wachtwoord verificatie onder de twee seconden gehouden - zonder in te leveren op het niveau van beveiliging. Aangezien beveiliging nu kan worden bereikt zonder een complexe beveiligingsinfrastructuur en zonder lange en cryptische toegangswachtwoorden, wordt een betere beveiliging en een betere bruikbaarheid gerealiseerd.

CPace overtuigde het internetstandaardiseringsorgaan De behoefte aan betere beveiligingsoplossingen van op wachtwoorden gebaseerde logins, werd in 2018 onafhankelijk vastgesteld door het internetstandaardiseringsorgaan IETF. In 2019 zette het een overeenkomstige veiligheidsanalyse en selectieproceswedstrijd op in IETF's cryptografie-expertgroep CFRG. In 2020 koos de CFRG de Endress+Hauser in-house oplossing CPace als winnaar ("Recommended for use in internet protocols") als resultaat van een uitgebreide veiligheidsanalyse waarbij ook verschillende andere protocolkandidaten betrokken waren. Onafhankelijk daarvan heeft het in München gevestigde Fraunhofer-instituut AISEC in 2016 het beschermingsniveau van de Endress+Hauser Bluetooth®-beveiligingsuitbreiding als "hoog" geclassificeerd.

Potentiële hackers zijn niet succesvol, zelfs niet als ze...

- er meerdere weken aan spenderen
- deskundig zijn op het gebied van elektronica, cryptografie en nevenkanalen aanvallen
- interne kennis over het gehele systeem bezitten en
- volledige toegang kunnen krijgen tot alle draadloze interfaces

Veilige verbinding met Bluetooth Low Energy en CPace



Momenteel worden alle Endress+Hauser meetinstrumenten met Bluetooth® verbinding ondersteund.

Wat is PAKE en IETF?

Met «Password-Authenticated Key Exchange» (PAKE) wordt een groep protocollen bedoeld waarmee de toegangsauthenticatie via wachtwoorden wordt gecontroleerd, zonder dat hackers er zogenaamde offline-aanvallen tegen kunnen uitvoeren met hacker-tools (bv. binnen een instrument met Bluetooth®-interface). De Internet Engineering Task Force IETF en de daaraan verbonden Internet Research Task Force IRTF is het orgaan dat de normen voor het internet organiseert, bijvoorbeeld protocollen zoals TCP/IP, TLS en IPSEC die worden gebruikt in internet backbones, infrastructuur voor lokale netwerken en toepassingen zoals internetbrowsers. Binnen de IETF is de verantwoordelijkheid voor de veiligheidsanalyse van de cryptografie binnen de normen toegewezen aan de IRTF Crypto Forum Research Group CFRG.

Nederland

Endress+Hauser Nederland
Postbus 5102
1410 AC Naarden
Tel. +31 35 695 86 11
info.nl@endress.com
www.nl.endress.com

IN01199S/15/NL/01.21

Endress+Hauser
People for Process Automation