Connexion Bluetooth® sécurisée Endress+Hauser

Une technologie sûre et à faible consommation pour les process

Avantages de la connexion Bluetooth® sécurisée Low Energy d'Endress+Hauser avec le protocole CPace :

- Meilleure sécurité de votre installation lors de l'utilisation de dispositifs Bluetooth® grâce au protocole CPace.
- Utilisation sécurisée des mots de passe dans les installations industrielles indépendamment de la longueur du mot de passe et de la disponibilité d'une infrastructure PKI complexe en utilisant les protocoles PAKE
- Utilisation indépendante du type de dispositif et des spécifications de puissance grâce à la vérification d'une seule procédure.
- Prévention des attaques de type "phishing" et "man-in-the-middle" par l'utilisation de la cryptographie asymétrique
- Sécurité plus forte que les autres solutions utilisées couramment (par exemple, la clé pré-partagée) – La solution Endress+Hauser est recommandée par l'IETF

Surmonter les pièges de la sécurité Bluetooth®

L'accès sans fil aux instruments de terrain présente un intérêt croissant pour les opérateurs dans tous les secteurs des industries de process. Toutefois, des risques de sécurité importants apparaissent avec la multiplication des accès à distance aux appareils.
En outre, les avancées dans l'Internet industriel des objets (IIoT) conduisent à des instruments de plus en plus interconnectés entre eux. Ces instruments de terrain doivent être installés, surveillés ou entretenus régulièrement par du personnel interne ou externe. L'authentification sécurisée des utilisateurs à l'aide d'un mot de passe joue aujourd'hui un rôle particulier, notamment lorsqu'il s'agit d'appareils dotés de communications sans fil telles que le Bluetooth® et lorsque les exploitants d'installations n'ont pas encore mis en place leurs propres services de sécurité pour gérer ces communications.
L'environnement industriel exige une protection nettement plus élevée que les applications du quotidien, c'est pourquoi Endress+Hauser a développé une couche de sécurité supplémentaire qui protège les mots de passe, en utilisant un protocole appelé CPace comme composant de base. Avec CPace, les attaques usuelles visant l'étape d'appairage Bluetooth® sont évitées.
Comme il est extrêmement difficile de protéger les mots de passe, le CPace d'Endress+Hauser utilise une une fonction PAKE ultra puissante dérivée de la méthode PACE utilisée dans les cartes d'identité allemandes.

Mot de passe trop simple ? La sécurité est maintenue

Pour les solutions de sécurité conventionnelles, il faut obligatoirement utiliser des certificats et des clés assez longues et difficiles à retenir telles que "X4RTQ 4KPKM PTWXS 3BP4Z C66D5 RRJ26". Avec CPace, les connexions Bluetooth® aux instruments de mesure sont toujours sécurisées, même dans les cas où les utilisateurs ont attribué des mots de passe relativement courts, car les attaques critiques par mot de passe

Endress+Hauser
People for Process Automation

hors ligne sont évitées. Grâce à la cryptographie asymétrique utilisée dans les protocoles PAKE, le niveau de sécurité peut être largement découplé de la longueur du mot de passe. De plus, en raison des ressources limitées des appareils de terrain, la vérification du mot de passe avec des protocoles comparables comme SRP ou PACE aurait entraîné un délai de connexion d'une minute ou plus. Avec le protocole CPace d'Endress+Hauser, la latence maximale de connexion pendant la vérification du mot de passe est maintenue en dessous de deux secondes - sans sacrifice du niveau de sécurité.
Comme il est désormais possible d'assurer la sécurité sans infrastructure de sécurité complexe et sans mots de passe d'accès longs et cryptiques, on obtient une meilleure sécurité dans le monde réel et une meilleure convivialité de l'environnement connecté.

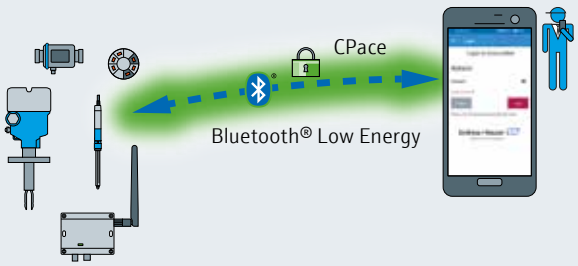
CPace a convaincu l'organisme de normalisation de l'Internet

La nécessité d'améliorer la sécurité des logins basés sur des mots de passe a été identifiée de manière indépendante par l'organisme de normalisation de l'Internet IETF en 2018. En 2019, il a mis en place une analyse de sécurité correspondante et un concours de processus de sélection au sein du groupe d'experts en cryptographie de l'IETF, le CFRG. En 2020, le CFRG a choisi la solution interne CPace d'Endress+Hauser comme lauréate ("Recommandée pour une utilisation dans les protocoles Internet"), à la suite d'une analyse de sécurité complète impliquant également plusieurs autres protocoles candidats.
Indépendamment, en 2016, l'Institut Fraunhofer AISEC, basé à Munich, a classé le niveau de protection de l'extension de sécurité Bluetooth® d'Endress+Hauser comme "élevé".

Concrètement cela signifie que des hackers ne réussiront pas à pirater la communication même si :

- Ils passent plusieurs semaines sur site à essayer de le faire
- Ils disposent de compétences élevée en cryptographie
- Ils possèdent des connaissances internes sur l'ensemble du système Endress+Hauser

Secure connection with Bluetooth® Low Energy and CPace



Actuellement tous les instruments Endress+Hauser avec connexion Bluetooth® sont supportés

Qu'est-ce que PAKE et IETF ?

L'échange de clés authentifié par mot de passe (PAKE) fait référence à un groupe de protocoles qui vérifient l'authentification de l'accès par des mots de passe sans permettre aux pirates de monter des attaques dites hors ligne (force brute) contre eux avec des outils de piratage (par exemple, dans un appareil de terrain avec interface Bluetooth®).
L'IETF (Internet Engineering Task Force) et son groupe de travail associé, l'IRTF (Internet Research Task Force), sont les organismes qui organisent les normes pour l'Internet, par exemple les protocoles tels que TCP/IP, TLS et IPSEC utilisés dans les dorsales internet, les infrastructures de réseaux locaux et les applications telles que les navigateurs Internet. Au sein de l'IETF, la responsabilité de l'analyse de la sécurité de la cryptographie dans les normes est confiée au groupe de recherche CFRG du Forum Crypto de l'IRTF.

France

Endress+Hauser France
3 rue du Rhin
68330 Huningue
info.fr.sc@endress.com
www.fr.endress.com

Agence Export
3 rue du Rhin
68330 Huningue
Tél. (33) 3 89 69 67 38
Fax (33) 3 89 69 67 17

Agence Paris-Nord
91300 Massy

Agence Ouest
33700 Mérignac

Agence Est
69800 Saint-Priest

Tél. 0 825 888 001 Service 0,15 € / min + prix appel

Fax 0 825 888 009 Service 0,15 € / min + prix appel

Canada

Endress+Hauser Canada
6800 Côte de Liesse
St Laurent, Québec
Tél. (514) 733-0254
Fax (514) 733-2924

Endress+Hauser Canada Ltd
1075 Sutton Drive
Burlington, Ontario
Tél. (905) 681-9292
Fax (905) 681-9444
info.ca.sc@endress.com
www.ca.endress.com

Belgique/Luxembourg

Endress+Hauser Belgium
17-19 Rue Carli
B-1140 Bruxelles
Tél. (02) 248 06 00
Fax (02) 248 05 53
info.be.sc@endress.com
www.be.endress.com

Suisse

Endress+Hauser Switzerland
Kägenstrasse 2
CH-4153 Reinach
Tél. (061) 715 75 75
Fax (061) 715 27 75
info.ch.sc@endress.com
www.ch.endress.com

IN01194S/14/FR/01.21

Endress+Hauser
People for Process Automation