

# Endress+Hauser establishes internet security standards

IETF recommends the SmartBlue CPace protocol for password-protected access to instruments

**The cryptography working group within the IETF standards organization (Internet Engineering Task Force) has chosen the Endress+Hauser-developed CPace protocol as a recommended method for use in internet standards. After undergoing extensive security analyses, the CPace protocol emerged as the winner in a competition among submissions from developers at several well-known companies.**

Secure access to field instruments is of the highest priority for operators across all branches of the process industry. Modern plants contain hundreds or thousands of measurement and control instruments that must be accessed remotely with growing frequency. These field instruments also have to be installed, monitored or serviced on a regular basis. Secure password-based user authentication plays a special role today, especially when devices with digital interfaces are involved.

## **Security with user-friendly password lengths**

In order to utilize Bluetooth communications technology in industrial environments, security experts at Endress+Hauser identified a need for additional protection. The result was the development of a solution called CPace, which belongs to the class of PAKE (password-authenticated key exchange) methods. Among other things, PAKE technology is used with the German electronic ID cards as a means of largely decoupling the cryptographic security level from the length of the password. The advantage of CPace is that the processing power of even the smallest of field instruments is sufficient to provide devices, and thus the industrial systems, with the best level of protection against cyberattacks. At the same time CPace enjoys a high degree of acceptance among users given that the desired level of security can be achieved without relying on long passwords.

“We had to look internally to find a solution for establishing secure connections to the instruments. Previously available secure methods could not be used because of the limited processing power and storage capacity of field instruments. Password verification would have meant a login delay of two minutes or more,” explains Dr Björn Haase, head of the project at Endress+Hauser.

## **CPace makes life difficult for hackers**

The security of the PAKE-based solution with Bluetooth technology from Endress+Hauser was previously verified in 2016 as part of an analysis by the Fraunhofer Institute for Applied and Integrated Security (AISEC). The institute classified the protection level of the Endress+Hauser security layer, the core component of which is recommended for use in internet environments, as “high”.

## Glossary

### **PAKE**

Password-authenticated key exchange refers to a group of protocols that verify access authentication passwords without enabling hackers to mount so-called offline attacks against passwords with hacker tools.

### **PACE**

The PACE protocol (password-authenticated connection establishment) is a password-based authentication and encryption method developed by the German Federal Office for Information Security (BSI) for use with the new German ID card.

### **CPace**

Composable password-authenticated connection establishment refers to an Endress+Hauser-based enhancement of the BSI PACE protocol that adapts the PACE approach to the limited resources of small field instruments.

### **IETF**

The Internet Engineering Task Force is an open, international volunteer-based community of network engineers, manufacturers, network operators, researchers and engineers who develop and promote internet standards. The members of IETF create technical documents that have an impact on the utilization, further development and administration of the internet. In particular the IETF focuses on standardizing communications protocols and cryptography methods employed on the internet.



**EH\_CPace\_1.jpg**

Modern plants contain hundreds or thousands of measurement and control instruments. Secure password-based access to the instruments is thus becoming increasingly important.



**EH\_CPace\_2.jpg**

With the CPace protocol, Endress+Hauser ensures secure access to field instruments.



**EH\_CPace\_3.jpg**

Dr. Björn Haase, Senior Expert Electronics at Endress+Hauser Liquid Analysis.

### **The Endress+Hauser Group**

Endress+Hauser is a global leader in measurement and automation technology for process and laboratory applications. The family company, headquartered in Reinach, Switzerland, achieved net sales of over 2.6 billion euros in 2019 with a total workforce of 14,000.

Endress+Hauser devices, solutions and services are at home in many industries. Customers thus use them to gain valuable knowledge from their applications. This enables them to improve their products, work economically and at the same time protect people and the environment.

Endress+Hauser is a reliable partner worldwide. Its own sales companies in 50 countries as well as representatives in another 70 countries ensure competent support. Production facilities on four continents manufacture quickly and flexibly to the highest quality standards.

Endress+Hauser was founded in 1953 by Georg H Endress and Ludwig Hauser. Ever since, the company has been pushing ahead with the development and use of innovative technologies, now helping to shape the industry's digital transformation. 8,000 patents and applications protect the Group's intellectual property.

For further information, please visit [www.endress.com/media-center](http://www.endress.com/media-center) or [www.endress.com](http://www.endress.com)

### **Contact**

Martin Raab  
Group Media Spokesperson  
Endress+Hauser AG  
Kägenstrasse 2  
4153 Reinach BL  
Switzerland

Email [martin.raab@endress.com](mailto:martin.raab@endress.com)  
Phone +41 61 715 7722  
Fax +41 61 715 2888