Cybersecurity with encrypted authentication

Aside from the many advantages they offer, the Internet of Things and the rapidly emerging area of Artificial Intelligence are making companies increasingly vulnerable to cybercrime. This makes an encrypted authentication solution all the more important.

AI increases the risk of cyberattacks

According to the World Economic Forum, cyberattacks pose the fifth biggest risk worldwide in 2024. AI is a key driver of this development, as criminals turn increasingly to generative AI tools for social engineering or phishing attacks. And these are “only” the current risks. Recently, a quantum computer was integrated into a supercomputer in Munich for the first time – the resulting hybrid computer and its successor models will pose completely new challenges for cybersecurity, since they could easily decipher known encryption methods.

Authentication is at the heart of cybersecurity

As security threats increase, ongoing development of cybersecurity solutions is crucial. At the heart of this is powerful authentication with secure encryption, which is available

at various levels – from the older RSA (Rivest-Shamir-Adleman) to the very robust Elliptic Curve Cryptography (ECC) (see info box). The easiest way for companies to implement phishing-resistant authentication is to use an RFID (Radio Frequency Identification) card or a digital credential that is stored on the smartphone and transmitted via Near-Field Communication (NFC) or Bluetooth® Low Energy (BLE). For even greater security, the RFID/NFC login can be combined with a user PIN or a biometric factor to enable multi-factor authentication (MFA), as is also required by NIS2.

Minimizing risks

When using authentication solutions, it is important to minimize potential vulnerabilities. For example, cards or mobile credentials must not be easily cloned or manipulated and it should not be possible to intercept or read the signals exchanged between the RFID card and/or smartphone and reader. In addition, there should be no risk of the RFID reader being compromised or the configuration of the RFID reader being read, which would enable reverse engineering of the encryption keys. It is equally important to select card formats and readers that support advanced encryption algorithms such as AES, DES, and 3DES.

Best possible protection against cybercrime

Modern authentication solutions are capable of minimizing the risks described above. For example, readers can act as mini-computers that map advanced encryption algorithms, such as AES, DES, and 3DES, using multiple or hierarchical keys and symmetric cryptographic methods. Readers also enable secure MFA by being equipped with a keypad for PIN entry or with a device operating system or interface for logging on to devices. When using digital credentials, it is possible to use biometric data integrated into the smartphone as an alternative to a user PIN. If additional SAM slots (Secure Access Modules) are available, the readers perform cryptographic computations with SAM and facilitate key management in a secure manner. The ability to program customer-specific security applications offers particular added value. ELATEC's readers meet all of these requirements, providing the best possible protection against current cybersecurity threats.

More info

Elliptic Curve Cryptography (ECC) – the next level of cybersecurity
ECC is a robust public key cryptographic algorithm that enables essential security capabilities such as encryption, key exchange, and digital signatures. Compared to older algorithms, such as RSA (Rivest-Shamir-Adleman), ECC offers a higher level of security, since RSA is based on the factorization of large numbers, while ECC is based on the problem of the discrete logarithm, which is much more difficult to solve. ECC keys are also much shorter than RSA keys, resulting in reduced consumption of

computing power, battery resources, and storage space. ELATEC enables companies to update all TWN4 readers to ECC support via the proven TWN4DevPack.