AuthCryptor

Advanced protection for password and data
on all communication channels

SDT-Solutions

AuthCryptor stands for comprehensive data security

Nowadays every transmission of data requires a password for login purposes. Online banking, exchanging of or accessing important corporation data, controlling industrial facilities, retrieving confidential documents like electronic health records or managing a Smart Home – authentication via password in order to verify the identity of a user is the prevalent way to initiate communication between clients and servers. VPN-connections, certificates or security-apps currently protect these processes. Nevertheless the german Federal Office for Information Security (BSI) registers up to 39.000 infections of german IT-systems a day by botnets alone. These numbers indicate: Todays security standards are not sufficient.

Insider or Man-in-the-Middle: No prospects for unauthorised access

Common login-processes verify the identity of a server using a certificate. The identity of the user is confirmed through knowledge of a password. This approach is vulnerable to insider threats since the password can be intercepted in plaintext once the server has received it. Insider threats do not necessarily have to come about deliberately and may occur unintentionally through infected laptops, USB flash drives or mobile devices of employees.

Another threat for common methods is a so-called Man-in-the-Middle (MitM) that intrudes on or manipulates a communication session between user and server. Passwords are intercepted and used without authorisation. The user gains no knowledge of such an incident and the server accepts this unwarranted authentication as valid process. Both insider threats and MitM-attacks bear far-reaching consequences: Unauthorised persons obtain data access and are able to initiate processes. The level of exposure is tremendous and underestimated by many users.

Summary of AuthCryptor

- Insider threats – deliberate or unintentional – are eliminated
- Man-in-the-Middle attacks are detected and prevented
- Advanced password protection – No storage or transmission of passwords or equivalents to passwords
- Authentication and encryption are combined into one process
- Integrity, origin and confidentiality of all transmitted data is ensured through end-to-end encryption
- Highly secure, encrypted transmission of data even when using unsafe networks, while simultaneously staying independent from third parties such as the public key infrastructure (PKI)
- Several network services may be bundled into one connection. AuthCryptor handles the necessary internal routing. Therefore the number of open network ports can be reduced to a single one.
- AuthCryptor ensures perfect forward secrecy (PFS). A new and independent session key is generated for every connection
- No posting of false status messages through unauthorised third parties possible
- Customer friendly and easy handling on all end devices
- Adheres to guidelines and specifications of the Federal Office for Information Security (BSI, Germany) and the National Institute of Standards and Technology (NIST, U.S.)
- AuthCryptor can be integrated into existing processes

New approach for upcoming challenges

No password gets lost using AuthCryptor. It is simply not transmitted to the server when logging in and is therefore not exposed to the risk of getting stolen. Every time the password is entered a new and independent calculation of cryptographic keys is triggered. The functional principle is based on mathematical calculations that are conducted by client and server for every authentication process. Only corresponding counterparts and their combination are accepted as valid by the system. At no point of the process passwords or equivalents to passwords can be obtained by unauthorised third parties since no such data is stored or transmitted. Even a captured session key would leave no hint to expired or future keys. Altogether making AuthCryptor a reliable gatekeeper.

Usability and mobility

Authentication via AuthCryptor is easy for users: They enter their password as usual. Again, no password is transmitted when using mobile devices or the communication takes place in unsafe networks.

Data security at the highest level

AuthCryptor offers a secure and patent pending authentication method that adheres to guidelines and specifications of the Federal Office for Information Security (BSI, Germany) and the National Institute of Standards and Technology (NIST, U.S.), while simultaneously ensuring integrity, origin and confidentiality of transmitted data through end-to-end encryption. No sensitive data is saved or transmitted. The consequence: Insider threats and MitM-attacks are futile.

SDT-Solutions

SDT-Solutions GmbH
Erb 10 · 77876 Kappelrodeck · Germany
Phone: +49 7842 98856
E-Mail: info@sdt-solutions.de
www.sdt-solutions.de