Smartcard Management: flexible and not tied to one supplier

Whitepaper

DriveLock

Smartcard Middleware - Your investment into an independent and secure future

What is the benefit of a multi-factor authentication?

Not just since the GDPR came into force, have companies been obliged to implement suitable technical and organizational measures to protect personal data. E.g. the German "Business Secrets Protection Act" implements Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of confidential know-how and business information (business secrets) against unlawful acquisition, use or disclosure and requires companies, that want to protect their secrets to establish a comprehensive protection concept. This absolutely includes the secure authentication of a user before he or she is able to gain access to these data records. The scope of such measures must also be based on the degree of secrecy: the more worthy the secret is of protection, the more effective and secure the protective measure must be. This could mean that a login with a password will longer be sufficient to access data for the new prototype, and that a multi-factor authentication with smart card or token, or even biometric identification must be considered instead.

The fact that passwords, as the only factor, are no longer secure and represent a weak point in any security concept is attributable to our continued attempts to achieve the highest degree of simplicity - especially for routine tasks such as the daily logon process to your own computer, or other access systems within the company. There are many tips for the secure use of passwords, however, in practice most of them are often ignored. This makes it easy for hackers to acquire third-party identities and gain access to illicitly targeted systems. Even the BSI (German IT security Ministry) has issued that passwords should have been replaced by multi-factor logins a long time ago.

With a 2F or 3F authentication, in addition to known factors (password, PIN), either a biometric feature (e.g. iris, fingerprint or vein scan) and/or a physically available item (smartcard or token) is used as an additional factor for the credible identification of a particular user. Thus, it is no longer sufficient for an attacker to only acquire the password, whereas the obstacle to also gain possession of the respective other factor is significantly higher. Through this, multi-factor authentication offers a significantly better level of protection or so-called strong authentication, as it is intended to be used in modern environments for an access to critical infrastructures or for securing financial transactions.

What is Smartcard Middleware?

Operating systems and an increasing number of applications provide a multi-factor authentication using smartcards (or tokens) in addition to the user name and password login. Smartcards store the secret key of a user that can be used for a log-in or data access. A smartcard middleware software is required which provides the application with a standardized interface and translates requests into the correct commands for the card, in order to enable the application to communicate with the smartcard. A manufacturer-independent Smartcard middleware enables a connection to many different card types through a respective Crypto-API. The core of the middleware is a driver for the operating system, which acts as a translator and provides the required cryptographic interfaces.

What advantages can a manufacturer-independent smartcard middleware offer me?

If a company uses a smartcard from a single vendor, it could also install and use the vendor's custom driver software. However, smartcards also have a life cycle and the technology is constantly evolving. Key lengths and algorithms that have been considered secure enough to date, should no longer be used in the future (1). Cards are lost or damaged, and approximately 10% of the smartcards used must be replaced each year. A change to more up-to-date smartcards is therefore inevitable. Since manufacturers often pay heavily for the support of older cards, this reduces the costs considerably, especially at the end of a card's life cycle.

In addition, there is a whole range of smartcards with different possible uses, from which companies often choose the card that covers the total number of requirements - at a correspondingly higher total price. These requirements include, for example, a simple login to the operating system, the encryption of data or e-mails, physical access to locked rooms or payments for lunch in the cafeteria. Thanks to a vendor-independent middleware that supports many different card systems simultaneously, customers are not bound to one card manufacturer and can therefore choose the proper card for the respective application and the company - if it's viable, even for cards from different manufacturers at the same time. Through this, it is possible to also implement and introduce different requirements and functions step by step. A later change to newer cards and other manufacturers is easily possible at any time.

In addition, a modern smartcard middleware should also be available for the most important operating system platforms Windows, macOS and Linux so that the same smartcard technology can also be used in heterogeneous environments.

For whom is a smartcard middleware suitable?

Every company with business-critical secrets should no longer rely on weak identification methods based on passwords, but should rather utilize at least a two-factor authentication for the logon process. In system environments that are based on a Microsoft architecture, the administrator has access to all the functions required to operate a public-key infrastructure (PKI). If this is available, there is nothing to prevent the use of smartcards for logging on to a computer. And a smartcard middleware, which is already installed on the computer when a new one is installed, simplifies the later selection of the right smartcard and reduces the costs for changing or replacing to newer hardware during the operation.

For manufacturers who want to offer additional smartcard authentication in their own solutions, a smartcard middleware is also an ideal solution to offer customers the greatest possible flexibility. No matter whether it's a new access control system for production or research areas, identification for a printer used throughout a department, authentication at important industrial control systems (ICS), or an integration into the new web application. For customers who already use cards, the support of existing hardware is always an effective sales argument.

Smartcard middleware also enables biometric identification solution providers to add value for customers by seamlessly integrating multiple authentication factors into a simple logon process. This enables convenient and above all very secure authentication processes, which are also accepted by customers and their users due to their simplicity.

What does DriveLock SmartCard Middleware offer?

The use of DriveLock SmartCard middleware makes it possible to perform a secure multi-factor authentication for a broad range of applications (web applications, e-mail or VPN clients, browsers, SSO, hard disk and file encryption) so that the use of insecure passwords can be omitted.

DriveLock SmartCard Middleware provides all relevant cryptographic interfaces for each major operating system: Microsoft CSP/KSP and CNG with Minidriver (for Windows), PKCS#11 (for Linux derivatives, Windows and macOS) and Apple TokenD (for macOS).

Over 100 different security tokens, smart card types (JCOP, CardOS, TCOS, SecCOS, ACOS and others) and profiles (e.g. PKCS#15, SSID, SigG, FINeID, CNS, PIV/CAC) are already supported by the DriveLock SmartCard Middleware, and newer card systems are constantly being added.

DriveLock SmartCard Middleware allows the use of RSA algorithms to generate keys up to 4096 bits in length and Elliptic Curve (ECC) cryptography up to 512 bits in length.

The support of biometric identification systems such as Fujitsu PalmSecure make it easy to use the SmartCard Middleware even in environments with very high requirements for a reliable and secure user authentication.

With the help of the additional management software "Security Token Configurator", cards can be easily personalized before they are issued to the user. A simple tool is available for the end user to adjust the card PIN afterwards or to unlock a card blocked by failed PIN entries, provided a super PIN has been set up beforehand.

Sources:

(1) BSI TR-02102-1 "Cryptographic methods: Recommendations and key lengths", version: 2019-01