EVIDEN

cryptovision SCalibur

eID middleware SDK

Cryptovision SCalibur is a Java® middleware SDK that enables the integration of smart cards and tokens into applications. It supports all common eID protocols and is also suitable for complex trust models. Thanks to cryptovision SCalibur, developers do not have to build up smart card know-how and can concentrate on their core tasks instead.

Management summary

eID cards and machine-readable travel documents (MRTDs) are currently experiencing a worldwide boom. The data stored on these cards must be protected with authentication and encryption. Only authorized parties may have access to the data on the chip in a clearly defined manner. In addition, it must not be possible to forge or copy a card with the data stored on it.

The authentication and encryption mechanisms required for eID cards and MRTDs are usually provided by standardized security protocols. These include for example BAC, EACv1, EACv2 and PACE. These protocols use modern cryptographic methods including digital certificates.

Cryptovision SCalibur by Eviden is a distributed smart card middleware SDK that supports all relevant eID protocols and enables their easy use. Cryptovision SCalibur provides the developer with powerful interfaces to control the protocol flow. Realized with Java, cryptovision SCalibur is platform-independent and can be integrated into existing applications on any device.

With cryptovision SCalibur, the customer does not have to worry about the details of the security protocols. Instead, developers can focus on business logic and user experience. The time to market is extremely short. Rapid prototyping is easy.

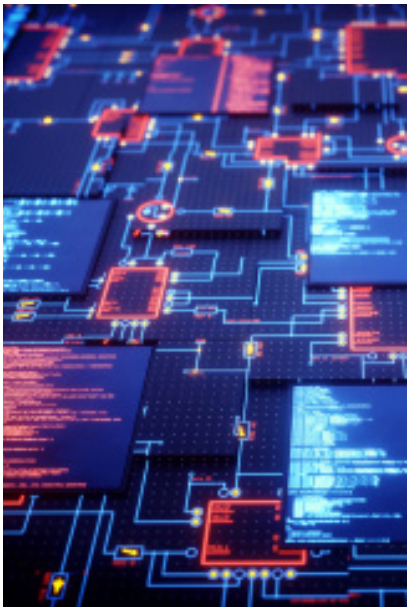
What is a distributed middleware?

If sensitive data is stored on smart cards or tokens, it must not be possible to use these or read them out without permission. Instead, access must be clearly regulated and secured with reliable authentication mechanisms such as a PIN or a fingerprint scan. This is especially important for cryptographic keys and personal information stored on electronic identity cards.

In order to put mechanisms of this kind into practice, a number of protocols have been developed, primarily by the International Civil Aviation Organisation (ICAO) and the German Federal Office for Information Security (BSI). Among the most important of this kind are the Basic Access Control (BAC) protocol, the Extended Access Control (EAC) protocol, and the Password Authenticated Connection Establishment (PACE). These protocols play an important role in the field of electronic identity cards.

Protocols of this kind are often realized in a distributed way. For instance, if a key can't be securely stored on the device itself, which is quite common, it is kept on a secure central server, and the protocol is carried out with the server as an additional component.

A software that implements these protocols and that provides its services to other components is referred to as a distributed middleware.



Basics

cryptovision SCalibur

Cryptovision SCalibur is an advanced distributed smart card middleware SDK supporting all relevant eID protocols and complex trust models.

Java-based

Cryptovision SCalibur is a Java® based software solution. This makes cryptovision SCalibur platform-independent and flexible.

Ease of use

Cryptovision SCalibur comes with numerous example applications. It is very easy to use, even for less experienced developpers. In addition, cryptovision SCalibur includes an extensive documentation.

Protocol support made easy

Depending on the applications, an eID document needs to apply different security protocols like BAC, EACv1, EACv2, SAC or PACE. A developer using cryptovision SCalibur does not need to know how the details of these protocols work. They can rather focus on the applications.

Integration of biometrics

In addition to using a personal identification number (PIN), it is possible to employ fingerprint authentication to protect the smart card access. For this purpose, cryptovision SCalibur supports ISO compliant Match-on-Card biometric technology.

Rapid deployment

Cryptovision SCalibur allows for minimizing the time to market of your own implementations. The modular design of cryptovision SCalibur easily allows you to integrate your own components. You can even extend cryptovision SCalibur's scope. Rapid prototyping is easily possible.

On all components of an eID system

Cryptovision SCalibur handles protocols on all clients and servers involved in a transaction. It's the one-stop-shop solution for all components of an eID system.

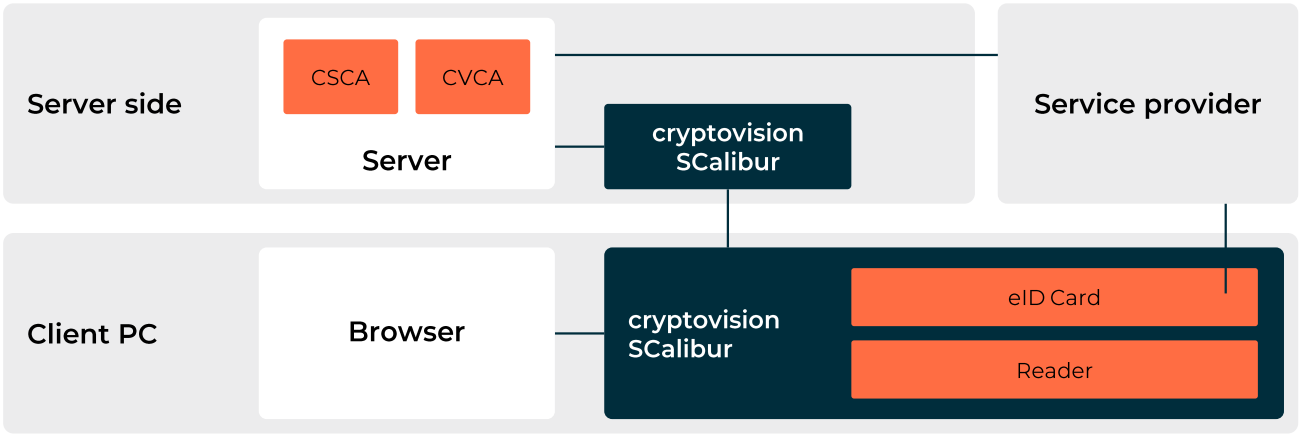
Integration of hardware modules

Cryptovision SCalibur supports contact-based as well as contactless card readers. In addition, card readers with or without PIN pad or fingerprint scanners can be used. MRZ scanners, HSMs and SAMs are supported as well.

Platforms

Cryptovision SCalibur is available for the operating systems Microsoft Windows, Linux and Apple macOS.

Product architecture



Cryptovision SCalibur consists of several modules. Client components offer secure messaging between the card and the terminal, while the server components deliver additional functionalities, such as establishing an authenticated and encrypted end-to-end connection between a server and the card.

Cryptovision SCalibur scope of supply

Low level interface

This interface can be used to achieve a higher degree of control for developing software that requires a direct interface to the hardware and the card profile

High level interface

This interface can be used to comfortably develop applications that utilize an abstraction level such as directaccess to datagroups.

Use cases

These are simple reference applications that help developers to build their own cryptovision SCalibur based applications.

Standalone terminal

This reference example application demonstrates a substantial usage of the middleware SDK functionality for non-distributed use-cases with a customizable HTML based graphical user interface.

Documentation

The documentation consists of three documents (Getting started, Manual and Offline Terminal), as well as a comprehensive JavaDoc documentation for developers.

Biometric support

Cryptovision SCalibur includes fingerprint recognition-with Match-on-Card (MoC) functionality and support for multiple fingerprint scanners.

eID data access

Can be used to read out data protected by EACv1 or EACv2. Further, it also allows to change/update data based on rights defined in access certificates.

PIN management

Provides functions for changing, unblocking and verifying PINs for various applications.

Reference Project

Credence ID is a California-based company with a long history in multi-modal biometric devices. Their solutions are used by US Federal, State and Local Governments, as well as in countries such as India, the Kingdom of Saudi Arabia, Indonesia, and Pakistan.

Credence ID has been licensing cryptovision SCalibur SDK for several years. They use cryptovision SCalibur as a part of their device software stack, a solution that allows the company‘s customers to develop their own applications. The cryptovision SCalibur licenses are separately counted by activation in the Credence app store.

Customers

Cryptovision SCalibur is used by the following customers:

- **Nigeria:** The Nigerian National Identity Management Commission (NIMC) uses cryptovision SCalibur for their National electronicidentity card, especially for (but not restricted to) quality control and card issuance.
- **Emerging market countries:** Several other countries with emerging markets use cryptovision SCalibur for national electronicidentity documents.
- **South American country:** A country in South America uses cryptovision SCalibur for a National electronic identity project.

Connect with us

eviden.com