cryptoVision
an atos company

Product Brief

SCalibur

eID middleware SDK

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 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.

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

With 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.

Version: 11/2021

BACKGROUND

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.

THE BASICS

SCalibur

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

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 SCalibur does not need to know how the details of these protocols work. They can rather focus on the applications.

On all components of an eID system

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.

Java-based

SCalibur is a Java® based software solution. This makes SCalibur platform-independent.

Integration of biometrics

In addition to using a PIN, it is possible to use fingerprint authentication to protect the smart card access. For this purpose, SCalibur supports ISO compliant Match-on-Card biometric technology.

Integration of hardware modules

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.

Ease of use

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

Rapid deployment

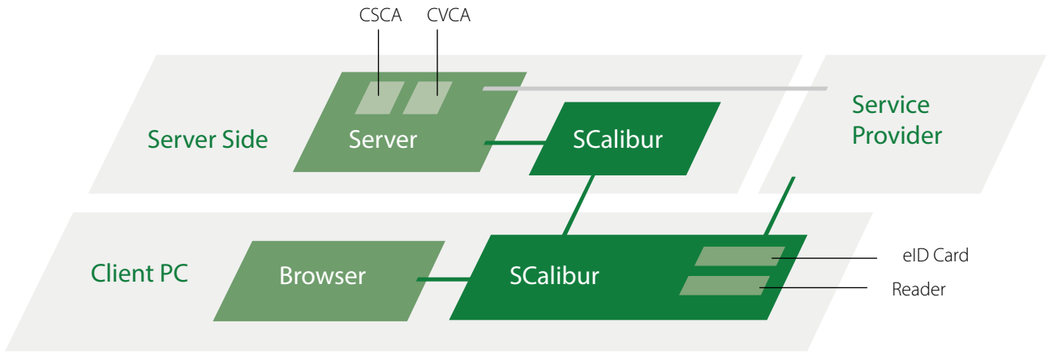
SCalibur allows for minimizing the time to market of your own implementations. The modular design of Scalibur easily allows you to integrate your own components. You can even extend SCalibur's scope. Rapid prototyping is easily possible.

Platforms

SCalibur is available for the operating systems Microsoft Windows, Linux and Apple OS X.

PRODUCT ARCHITECTURE

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.



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 direct access to datagroups.

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.

Use cases

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

Documentation

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

Biometric support

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.

SUPPORTED SYSTEMS

Windows 7/8.1/10

Linux Ubuntu 14.04 LTS,
RedHat 7, OpenSuse 13.2

OS X Yosemite 10.10.3,
El Capitan 10.11

Oracle JDK 1.8

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

CUSTOMERS

SCalibur is used by the following customers:

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

cryptovision

cv cryptovision GmbH is one of the leading specialists for modern, user-friendly cryptography and secure electronic identities. With its solutions, over 250 million people worldwide and a multitude of institutions in the digital world protect themselves against hacker attacks, manipulation, misuse of identities and espionage.

cryptovision addresses various industries such as public administration, health, automotive, finance & insurance, energy or IT. Its customers include countries such as Nigeria, Ghana and Ecuador, institutions such as the German Armed Forces, the German Federal Office for Information Security (BSI), the city of New York and companies such as E.ON, VW and Allianz. Since 31 August 2021, cryptovision is part of Atos.

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

CONTACT

cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

T: +49 209 16724-50
F: +49 209 16724-61
info@cryptovision.com

www.cryptovision.com