SCalibur

eID middleware SDK

SCalibur is a middleware SDK for Java that enables integration of eID smart cards and security tokens into applications. With a focus on security mechanisms used in eID documents, it provides methods for stand-alone client access and distributed use case where credentials are accessed via a remote server. SCalibur comes with reference applications which allow for rapid prototyping and effortless showcase setups.

MANAGEMENT SUMMARY

The rising demand for electronic identity verification requires much more than simple user names and passwords. Additional verification methods are a crucial, and digital certificates and cryptographic keys stored on smart card chips are ideal for this purpose. As a very mature solution, smart cards have been widely deployed for years on bank cards and more recently on electronic ID cards and passports. Sophisticated standardized hardware and software security mechanisms ensure that chips can't be cloned and data stored on the chip can't be read or altered by unauthorized devices.

Access to card data can be restricted to terminals by forcing them to authenticate before being able to read or even update the chip's data. This authentication is based on strong public key cryptography using a terminal private key and a corresponding digital certificate. With standalone (offline) terminals this key needs to be stored securely on the device requiring special security hardware.

To overcome this problem the read-out process and other card services can be split up into client and server components. In these scenarios the terminal initiates the communication to the card and then hands it over to the server component. This creates a secure end-to-end connection between the card's chip and the background server. This facilitates security management and allows for secure access by remote eGovernment and private enterprise services based on the trusted credentials stored on the card. Alternatively the terminal's authentication token can be computed centrally with the required private key stored on a secure server or hardware security module (HSM) and then locally used by the terminal.

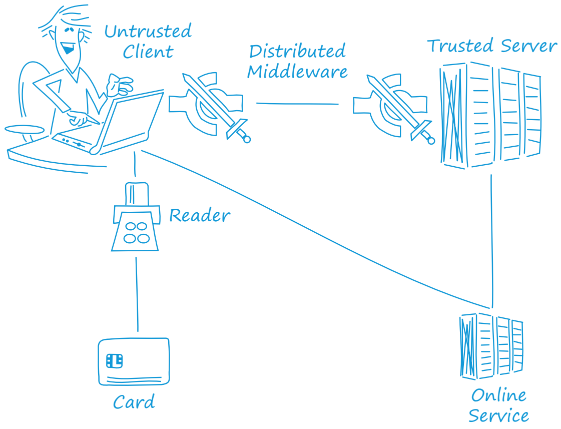
A distributed smart card middleware should be platform independent and support a broad number of applications across various devices. In addition, the middleware should utilize standardized protocols and advanced cryptographic methods.

BACKGROUND

What Is a Distributed Middleware?

Reading sensitive data from modern smart cards and eID documents requires sophisticated authentication mechanisms before access is granted. A distributed middleware allows these mechanisms to be performed in a server-client setting where the server is connected to the card via the client and some network. In this scenario the required credentials can be centrally verified in a high security environment and end-to-end secure channel can be established. These credentials cannot be extracted from the client which might have been compromised or stolen. In addition, the server verifies the authenticity of the card on its own, so it does not have to trust the client's verification process.

With SCalibur, a developer can easily realize a distributed (or local) execution of EACv2, a sophisticated authentication and verification mechanism augmenting the "Extended Access Control" protocol known from electronic Passports. In addition, SCalibur supports smart card readers with pin pads and the PACE protocol which prevents PINs from ever leaving the client. Therefore, developers are enabled to develop applications that do not need any additional credential stored on the client.



THE BASICS

SCalibur

SCalibur is an advanced smart card middleware, created to realize these distributed scenarios, but is not restricted to them.

Flexibility Based on Standards

When dealing with projects in the scope of millions of customers or citizens worldwide, broad platform support is crucial for user adoption and success. Leveraging SCalibur is the solution of choice, whenever smart cards or eID documents are to be used for secure web access. The flexibility SCalibur delivers allows for a single card eID document to become a multipurpose device.

For the Application You Need

With SCalibur you can consolidate physical and logical access applications together or secure web-site access with digital authentication needed for e-commerce or online government services.

Biometrics

In addition to PINs, it is possible to use fingerprints to protect a smart card. SCalibur supports Match-on-Card biometric technology.

Form Factors

SCalibur supports smart cards in several form factors, for instance ID-1 (credit card), ID-000 (SIM card), MicroSD, USB token, both via contact and contactless interfaces. ID-000 and MicroSD are mainly used on handheld devices, which are an attractive replacement for conventional smart cards.

Increased Security

Security of client devices and terminals cannot be controlled easily and in most eID settings these devices can neither be blacklisted nor can issued terminal certificates be revoked. The distributed architecture of SCalibur can help to increase the security by performing critical operations in a trusted environment remotely.

Server Integration

SCalibur can be integrated into web applications or enterprise grade application servers.

Platforms

SCalibur is available for Windows, Linux, and macOX. A separate mobile SDK for Android is also available. Users can leverage the same smart card across diverse platforms. Note that some supported external devices are not working across all platforms.

Smart Card Types

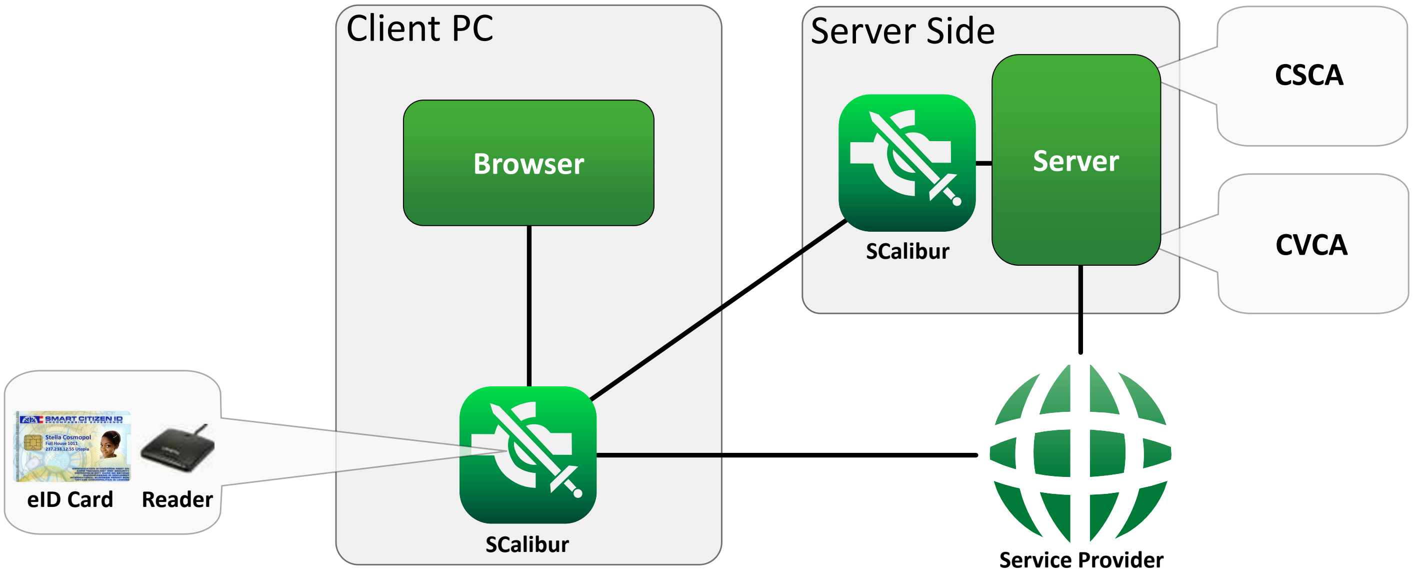
SCalibur supports many card types. Among others, cards supplied by NXP, Gemalto, G&D, Siemens and Austria Card can be used.

Modular Architecture

SCalibur consists of several modules. Client components offer secure messaging between card and terminal; server components deliver additional functionalities for authenticating against certified servers.

THE TECHNICAL PART

SCalibur consists of several modules. Client components offer secure messaging between the card and terminal while the server components deliver additional functionalities for authenticating against certified servers of a government or private enterprise.



THE MODULES

SCalibur is a Software Development Kit (SDK), which provides the following modules:

- **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 which utilizes an abstraction level (e.g. direct access to datagroups).
- **StandaloneTerminal:** 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 con¬sists of three documents (Getting started, Manual and Offline Terminal), as well as a comprehensive JavaDoc documentation for developers.
- **Biometric Support:** Includes fingerprint recognition with Match-on-Card (MoC) functionality and support for multiple fingerprint scanners.

FUNCTIONS

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.

MoC: Enables fingerprint checking directly on the smart card chip (Match-on-Card). This can be used as a PIN alternative.

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

SUPPORTED SYSTEMS

- Windows Vista, Windows 7, Windows 8.x, Windows 10, Windows Server 2003, 2008 and 2012 Linux Ubunutu 12.04 LTS, RedHat 6.5, OpenSuse 13.1, Debian 7.5 Mac OS X Lion (10.7), OS X Mountain Lion (10.8), OS X Mavericks (10.9), OS X Yosemite (10.10) macOS (in preparation)
- Tested with Oracle JDK 1.8

Success story

With 175 million citizens, Nigeria is Africa's most populous country. As part of an ambitious Presidential initiative, adult Nigerians and resident legal aliens will receive advanced multipurpose electronic identity cards. cryptovision plays a critical role in this mammoth project as the Gelsenkirchen-based company is responsible for the deployment of the Public Key Infrastructure (PKI) as well as system critical middleware components based on SCalibur. This middleware is for example used for card holder identification and card activation during card pickup. The unique and secure features of cryptovision's products enable a highly secure and convenient way to easily provide the required functionality to the government as well as to its citizens.

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 (but not restricted to) for 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.

About cryptovision

cryptovision is a leading supplier of innovative cryptographic IT security solutions. Based on its two decades of market experience and broad background in modern cryptographic techniques, such as Elliptic Curve Cryptography, all cryptovision products provide the most state-of-the-art and future-proof technologies. The company specializes in lean add-on components which can be integrated into nearly any IT system to gain more security in a both convenient and cost-effective way.

From small devices like citizen eID cards, all the way to large scale IT infrastructures, more than 500 million people worldwide make use of cryptovision products every day in such diverse sectors as defense, automotive, financial, government, retails and industry.

cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

T: +49 (209) 16724-50
F: +49 (209) 16724-61

cv cryptovision
100 Park Avenue / Suite 1600
New York City, NY 10017, USA

T: +1 (212) 984 0750
F: +1 (212) 880 6499

www.cryptovision.com