ActivID® ActivClient® SDK Overview

DOCUMENT REFERENCE: AC_SDK_7.1_OVR_07.2016

PRODUCT VERSION: 7.1

JULY 2016



Copyright

© 2008-2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved. This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID, HID Global, the HID Blue Brick logo, the Chain Design and 4TRESS, ActivIdentity and ActivID are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Revision History

Date	Description	Document Version
July 2016	Initial release of rebranded document and major technical updates.	1.0

Contacts

Americas		Asia Pacific
United States: +1 510.574.0100	U.S. Federal: +1 571.522.1000	+61 (0) 3.9809.2892
Europe		**Corporate**
+33 (0) 1.42.04.84.00		+1 800.237.7769

Technical Support

If you purchased your product from a third party, then please contact that third party for Technical Support. For products purchased directly from HID Global, please go to http://www.hidglobal.com/support

Typographic and Document Conventions

Typography	Description
blue	Cross-references within the document.
blue, underline	References to external web addresses.
bold	Action steps (paths, buttons, options); field and drop-down list labels; emphasis.
italic	File names, document titles, and file extensions.
`Code snippets`	Highlights `code snippets` within regular content.
Code samples	Highlights code samples
	**WARNING**: This symbol indicates a critical warning. It applies to actions that if taken or not taken will break the system. Read the warning carefully and follow it.
	**Important**: This symbol indicates something very important to the reader. Ignore this symbol at your own risk.
	**Note**: This symbol indicates a note that should be of interest to the reader. It is not critical. Nevertheless, the reader should pay attention.

Table of Contents

1.0 Introduction 5

1.1 Product Overview 5
1.2 Document Scope and Audience 5

2.0 About ActivClient SDK 6

2.1 ActivClient SDK Benefits 6
2.2 ActivClient SDK Use Examples 6
2.3 ActivClient SDK Components 7
2.3.1 Basic Services Interface (BSI) API 7
2.3.2 Microsoft Cryptography APIs 8
2.3.3 PIV API 9
2.3.4 PKCS#11 API 9
2.4 64 and 32-bit Versions 10
2.5 Interoperability 10

3.0 Installation 11

3.1 Distribution Content 11
3.1.1 BSI Content 11
3.1.2 Microsoft Cryptography Content 12
3.1.3 PIV Content 12
3.1.4 PKCS#11 Content 12
3.1.5 Miscellaneous Content 13
3.2 Installation Steps 13

Appendix A: Terms and Acronyms 14

A.1. Terms 14
A.2. Acronyms 16

1.0 Introduction



ActivID® ActivClient® guards against an ever-changing threat landscape by providing organizations with risk-appropriate and secure access to corporate IT assets.

1.1 Product Overview

HID Global's ActivID ActivClient is the latest smart card and USB token middleware from that allows enterprise and government customers to easily use smart cards and USB tokens to protect workstations and networks.

ActivClient enables the use of PKI certificates and keys and one-time passwords and static password credentials on a smart card or USB token to secure:

- Desktop applications
- Network logon
- Remote access
- Web logon
- E-mail
- Electronic transactions

ActivClient provides the following range of services:

- PKI services
- Remote access and One-Time Password (OTP) services
- Remote session services
- Management services (for end users and administrators)
- Development services with a Software Development Kit (SDK)

1.2 Document Scope and Audience

This document describes the ActivClient SDK (Software Development Kit).

Readers of this document are assumed to be experienced programmers who:

- Are accustomed to reading and writing in C/C++ or Java.
- Have a fair understanding of PKI and/or SKI.
- Intend to develop custom applications based on ActivClient middleware.

2.0 About ActivClient SDK

The ActivClient SDK provided as part of ActivID ActivClient for Windows. This SDK enables an integrator to customize and expand the standard ActivClient features.

Companies that want to use some of the standard features in ActivClient and also create their own smart card-based applications should use the ActivClient SDK.

2.1 ActivClient SDK Benefits

- Provides high-level APIs – the ActivClient SDK allows you to develop smart card applications without any previous knowledge about smart card technology.

  By encapsulating low-level commands (reader management, smart card structure management, smart card insertion and removal, and so on), the ActivClient SDK lets you focus on the security services that you need to develop.

- Compatible with standards – the ActivClient SDK is based on and leverages several smart card-based standards:
  - Microsoft Cryptography APIs – providing compatibility with Microsoft applications and a wide range of PKI-enabled Windows applications from third-party vendors.
  - PKCS#11 (from RSA Labs) – providing compatibility with a wide range of PKI-enabled applications from third-party vendors; also supports non-PKI services, such as data storage.
  - Smart Card Basic Services Interface (BSI) – defined by the U.S. Government as part of the Government Smart Card - Interoperability Specifications (GSC-IS). For more information, see http://csrc.nist.gov/groups/SNS/smartcard/index.html
  - PIV is the Personal Identity Verification of US Federal Employees and Contractors. For more information, see http://csrc.nist.gov/groups/SNS/piv/index.html.

- Feature-rich – the ActivClient SDK provides access to multiple security technologies – static passwords, one-time passwords (HID Global-patented mechanism or ANSI X9.9 standard), or a certificate (public key cryptography).

2.2 ActivClient SDK Use Examples

Following are examples of ways of using the ActivClient SDK:

- Create a smart card PKI application based on PKCS#11.
- Use the smart card to store private information (confidential records, keys, and so on).
- Automate the use of ActivID one-time passwords (for user authentication) by integrating communication with the smart card directly inside your application.

2.3 ActivClient SDK Components

The ActivClient SDK:

- Offers a generic and high-end approach to smart card applications.
- Provides all information and definitions for integrating ActivClient APIs.
- Allows to access and use ActivClient smart cards.

To provide choices to application developers and comply with all applicable API standards, the ActivClient SDK supports a variety of APIs:

- Basic Services Interface (BSI) API
- Microsoft cryptography APIs (CryptoAPI, Cryptography Next Generation…)
- PIV API
- PKCS#11 API

Note about the ActivClient ACOMX API

The ActivClient ACOMX API provided in ActivClient 6.x as a public API is now deprecated with ActivClient 7.x. The One-Time Password services previously available in ACOMX are now available in the PKCS#11 API. For further information, refer to the *ActivID ActivClient SDK PKCS#11 API Reference Guide*.

2.3.1 Basic Services Interface (BSI) API

Use the BSI API if you are developing a multi-credential application.

Supports: PKI and static data such as personal information data. The BSI API and the PKCS#11 API are similar in functionality and scope. They differ in that PKCS#11 is a standard developed by RSA whereas BSI is a standard developed by the US government/NIST. PKCS#11 implements a higher level of abstraction of card objects and services than BSI, which is much lower level than PKCS#11. In addition, BSI supports SKI.

Languages: C, Java; HID Global provides samples in C and Java.

Description: ActivClient SDK's BSI API component is an implementation of the Basic Services Interface (BSI) included in the U.S. Government Smart Card - Interoperability Specifications (GSC-IS). The library included in ActivClient SDK implements a subset of BSI API v2.1. This API provides cryptographic, data storage, and utility services.

The BSI API:

- Provides support for:
  - Smart card cryptographic and data storage operations.
  - Smart card state and reader state management.
  - Data storage.
  - PIN management.

- Is recommended for developers who want to perform smart card cryptographic operations and/or some data storage. While the BSI API hides most of the complexity of working with smart cards, it requires more knowledge of smart cards than other ActivClient APIs require.

For more information, refer to the *ActivID ActivClient SDK BSI API Reference Guide*.

2.3.2 Microsoft Cryptography APIs

Use Microsoft cryptography APIs for Microsoft PKI-based applications.

Supports: PKI

Languages: C++; HID Global provides a sample in C++ in a Universal Windows application (compatible Windows 10) with Windows::Security::Cryptography namespace.

Description: HID Global's ActivClient MiniDriver library is compliant with Microsoft Cryptographic APIs. It is used by the ActivClient product for secure Windows PKI logon, for secure email (S/MIME with Outlook and Outlook Express), and for secure Web access (SSL in Internet Explorer).

Microsoft Cryptography APIs:

- Abstracts the smart card data model and is primarily focused on cryptographic operations.
- Is recommended for:
  - Developers who want to create PKI-enabled applications but do not need to manage the smart card state (card insertion and removal, PIN change).
  - Use with applications dedicated to the Microsoft Windows environment and that leverage the Microsoft Cryptography APIs infrastructure.

Supported Microsoft cryptography APIs are:

- Smart Card MiniDriver API
- Microsoft Cryptography APIs: CryptoAPI (CAPI) using Microsoft Base Smart Card Crypto Provider (CSP).
- Microsoft Cryptography Next Generation (CNG) API using Microsoft Smart Card Key Storage Provider (KSP)
- Universal Windows Cryptography API (Windows::Security::Cryptography namespace)
- .Net Framework API (System.Security.Cryptography namespace)

For more information, refer to the Microsoft API documentation.

2.3.3 PIV API

Use this API for PKI based application using PIV End Point card or PIV data retrieval.

Supports: PKI and PIV data access, as well as mutual authentication and external authentication.

Languages: C, Java; HID Global provides samples in C and Java.

Description: ActivClient SDK's PIV API is an implementation of Personal Identity Verification (PIV) Middleware API as per National Institute of Standard and Technology (NIST) SP800-73-4 specifications. This API provides cryptographic, data storage, and utility services for FIPS 201 PIV-compliant cards.

The ActivClient PIV API:

- Provides support for
  - Smart card cryptographic and data storage operation
  - Client-based management on smart cards and smart card readers
- Is recommended for developers who want to perform smart card cryptographic and data retrieval operations specifically on FIPS 201 PIV-compliant cards.

For more information, refer to the *ActivID ActivClient SDK PIV API Reference Guide*.

2.3.4 PKCS#11 API

Use this API to create generic PKI-based applications.

Supports: PKI and static passwords

Languages: C, Java; HID Global provides samples in C and Java.

Description: ActivClient SDK's PKCS#11 API is a generic implementation of the PKCS#11 v2.20 standard.

The PKCS#11 API:

- Provides support for:
  - Smart card cryptographic operations.
  - Client-based management of smart cards and smart card readers.
- Is recommended for developers who want to:
  - Perform smart card cryptographic operations, use data storage, or have close control of the smart card state (card insertion and removal and PIN entry and change).
  - Reuse their code on a non-Windows platform.

For more information, refer to the *ActivID ActivClient SDK PKCS#11 API Reference Guide*.

2.4 64 and 32-bit Versions

ActivClient 7.1 x86 provides 32-bit editions of ActivClient Mini Driver, PKCS#11, BSI, and PIV as public APIs.

ActivClient 7.1 x64 provides 64-bit editions of these APIs and also supports 32-bit editions of the APIs for compatibility with 32-bit applications that rely on the 32-bit APIs.

The ActivClient SDK provides support for integrators implementing applications that rely on ActivClient APIs on 32 and 64-bit platforms. The SDK package provides API documentation and dependency files (header, lib).

Samples are available in Java, C++ and C language (source code and compiled binary).

For each API, the SDK provides:

- Dependency files (header, lib).
- C or C++ 32-bit sample: source code and binaries, can be run on 32 and 64-bit platforms.
- C or C++ 64-bit sample: source code and binaries; functional only on 64-bit platforms.
- Documentation: PDF versions of the reference guides are available for all APIs (except the Microsoft Cryptography APIs for which you should refer to the Microsoft documentation instead). Javadoc is available for BSI and PIV.
- Additional samples provided – For PIV, BSI, and PKCS#11 only, a Java wrapper sample and binaries which can be run on 32 and 64-bit platforms.

2.5 Interoperability

The ActivClient SDK focuses on providing card usage services for cards that have already been issued. The ActivClient SDK interoperates with other tools that provide other capabilities:

Goal…	**Tool…**
Issue smart cards	ActivID Credential Management System (CMS)
Customize ActivClient setup or configure ActivClient options	For more information, see the *ActivID ActivClient for Windows Administration Guide* which provides customization, deployment and configuration instructions.
Create new Java Card applets	Java Card Development Kit (available from Oracle at http://www.oracle.com and from card vendors)

3.0 Installation

3.1 Distribution Content

The ActivClient SDK is located in the **\SDK** folder of the ActivClient distribution. The SDK is organized per API with one sub-folder for each supported API. Code samples are included with each API.

In each API folder, the content of the distribution is organized by supported language with one folder for each language (Java, C, C++).

Each language folder in turn contains the necessary set of binaries, source files, and samples for that particular language.

C\Headers	Header file repository
C\Libraries	Dynamic library repository
C\Sample	Sample repository
C\Sample\Binaries	Folders contain the compiled versions of each sample
Java\javadoc	Java documentation
Java\Sample	Java sample repository
Documentation	API Reference Guide

3.1.1 BSI Content

\BSI

\BSI\C

\BSI\C\Headers

\BSI\C\Libraries\x86

\BSI\C\Libraries\x64

\BSI\C\Sample

\BSI\C\Sample\Binaries\x86\Release

\BSI\C\Sample\Binaries\x64\Release

\BSI\C\Sample\Headers

\BSI\C\Sample\Resources

\BSI\C\Sample\Sources

\BSI\Documentation

\BSI\Java\Sample\Binaries

\BSI\Java\Sample\bsi

\BSI\Java\Sample\ui

3.1.2 Microsoft Cryptography Content

\Microsoft Cryptography

\Microsoft Cryptography\C++

\Microsoft Cryptography\C++\Sample

\Microsoft Cryptography\C++\Sample\mscrypto.cppUWPsample

3.1.3 PIV Content

\PIV

\PIV\C

\PIV\C\Headers

\PIV\C\Libraries\x86

\PIV\C\Libraries\x64

\PIV\C\Sample

\PIV\C\Sample\Binaries\x86\Release

\PIV\C\Sample\Binaries\x64\Release

\PIV\C\Sample\Headers

\PIV\C\Sample\Resources

\PIV\C\Sample\Sources

\PIV\Documentation

\PIV\Java\Sample\Binaries

\PIV\Java\Sample\piv

\PIV\Java\Sample\ui

3.1.4 PKCS#11 Content

\PKCS #11

\PKCS #11\C

\PKCS #11\C\Headers

\PKCS #11\C\Libraries\x86

\PKCS #11\C\Libraries\x64

\PKCS #11\C\Sample

\PKCS #11\C\Sample\Binaries\x86\Release

\PKCS #11\C\Sample\Binaries\x64\Release

\PKCS #11\C\Sample\Headers

\PKCS #11\C\Sample\Resources

\PKCS #11\C\Sample\Sources

\PKCS #11\Documentation

\PKCS #11\Java\Sample\Binaries

\PKCS #11\Java\Sample\pkcs

\PKCS #11\Java\Sample\ui

3.1.5 Miscellaneous Content

\ActivClient SDK Overview.pdf

3.2 Installation Steps

Use the content of the ActivClient SDK distribution (samples, header files, and so on) on the developer workstation. You do not need to distribute it to end-user environments.

ActivClient is also required on the developer station and provides the smart card middleware required for the ActivClient SDK; in the ActivClient setup, install the ActivClient Common Services (for PIV and BSI APIs) and Digital Certificate Services (for Microsoft Cryptography and PKCS#11 APIs). You can install additional components as desired.

For end-user environments, ActivClient installation is required and sufficient.

Appendix A: Terms and Acronyms

This appendix lists terms and acronyms used throughout the full set of the set of technical publications for this product. Not all terms and acronyms appear in all documents in the set.

A.1. Terms

Certificate Authority (CA)	The CA issues and manages security credentials and public keys for message encryption in a networked environment. As part of a Public Key Infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA issues a certificate.
ActivID Credential Management System (CMS)	Formally known as ActivID Card Management System, ActivID CMS is a web-based, smart card, credential and application lifecycle management system. ActivID CMS augments and works in concert with an enterprise's primary identity management infrastructure components, including popular directory, database, and PKI components.
Challenge	Random number generated by the server API for authentication of a user in the asynchronous (challenge/response) mode.
Cryptographic Service Provider (CSP)	An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.
Discovery mode	Discovery mode enables a calling application to find out the size of the data that will be returned to by making a preliminary discovery call and then making a second call after it allocates a buffer large enough to accommodate the data that will be returned.
End-point card	The PIV standard defines two interfaces for communicating with PIV cards: • The PIV transitional interface. • The PIV end-point interface. A PIV end-point card is a card that implements the second of these interfaces. **Note:** The PIV transitional interface is not supported by the PIV API.
Federal Information Processing Standard (FIPS 140-2)	FIPS 140-2 is the standard for crypto-module security. FIPS 140-2 level 3 adds additional requirements to FIPS 140-2 level 2. These requirements concern physical security and a trusted path for entering a Cryptographic Service Provider, such as a PIN. FIPS 140-2 level 3 uses local ports and the key pad to enforce such security.
Federal Information Processing Standard 201 (FIPS 201)	FIPS 201 is the standard for Personal Identity Verification (PIV) cards defined for US Government employees and contractors.
Force change PIN flag	Flag which indicates whether the user must change the PIN on first use of the card.

Integrated circuit chip (ICC)	The chip on the smart card.
Mini Driver	Smart card middleware for the Microsoft platform that works with the Microsoft Base Smart Card CSP (Cryptographic Service Provider). The ActivClient Mini Driver replaces the ActivClient CSP available in previous versions. The Mini Driver architecture provides stronger cryptographic services.
My Digital ID Card (MDIDC)	This CMS component allows end users to access the self-service CMS functions, which includes card and credential management.
One-Time Password (OTP)	A one-time password is a password used only once to authenticate to remote applications. One-Time Passwords are only present on smart cards issued with SKI credentials.
Personal Identification Number (PIN)	The Personal Identification Number (PIN) code used to access an HID Global device's services such as Windows PKI logon, remote access and email signature. HID Global devices can only be used after a correct PIN is entered.
Public Key Infrastructure (PKI)	PKI describes the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys.
Registration Authority (RA)	RA is an authority in a network that verifies user requests for a digital certificate and instructs the CA to issue it. An RA is part of a PKI, a networked system that enables companies and users to exchange information safely and securely.
Symmetric Key Infrastructure (SKI)	SKI keys are used to perform strong authentication on remote applications. SKI keys encrypt passwords in: • Synchronous mode (generates 1 password without any challenge. The server uses the same method to create a password than the smart card) • Asynchronous: encrypts a challenge
Standalone smart card	Smart card with pre-loaded applets issued by the manufacturer.
Unlock code	Value that the card holder needs to provide in order to unlock a locked smart card. Depending upon the smart card unlock mechanism, the unlock code may or may not be different from the unlock key.
Verification	Process in which a signature that was produced by the signing operation is verified.
Weak PIN	A weak PIN is a PIN in which: • The length is less than three characters or digits, or • The difference between each character or digit and the following one is a constant. For example, a PIN that is a sequence of the same number (1111) or an increasing/decreasing sequence of numbers (1234, 4321) is a weak PIN.

A.2. Acronyms

CA Certificate Authority

CAC Common Access Card (for the United States Department of Defense)

CSP Cryptographic Service Provider

CUID Card Unique Identifier

CUID is a number that uniquely identifies a card.

FIPS Federal Information Processing Standard

GAL Global Address List

GP GlobalPlatform

Replaces OpenPlatform (OP).

OTP One-Time Password

PKI Public Key Infrastructure

PIV Personal Identity Verification.

Smart card issued by the United States government to federal employees and contractors.

RA Registration Authority

SKI Symmetric Key Infrastructure

