ActivID® ActivClient® for Windows Overview

DOCUMENT REFERENCE: AC_WIN_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

List of Tables **6**

List of Figures **6**

1.0 Introduction **7**

1.1 Product Overview 7
1.2 Document Scope and Audience 7
1.3 Supported Standards and Certifications 8

2.0 ActivClient Services **9**

2.1 PKI Services 9
2.2 Remote Access and One-Time Password Services 12
2.2.1 Log On to Applications Using an OTP 12
2.3 Remote Session Services 12
2.3.1 Citrix XenApp Support 12
2.3.1.1 Supported Citrix Versions 12
2.3.1.2 Supported Services in a Citrix Environment 13
2.3.2 Microsoft Remote Desktop Protocol (RDP) Support 13
2.3.2.1 Supported Environments 13
2.3.2.2 Supported Services 14
2.4 Management Services for End Users 14
2.4.1 ActivClient User Console 14
2.4.2 Digital Certificates 14
2.4.3 One-Time Passwords 14
2.4.4 Personal Information 15
2.4.5 Smart Card PIN 15
2.4.6 Smart Card Initialization 15
2.4.7 Smart Card Lock/Unlock 15
2.4.8 Remote/Centralized Management 16
2.4.9 ActivClient Agent 16
2.4.10 Advanced Diagnostics 16
2.4.11 Log Files 16
2.5 Management Services for Administrators 17
2.5.1 Installation and Deployment 17
2.5.2 Upgrading 17
2.5.3 Policy Management 17
2.5.4 Smart Card Automatic Registration 18
2.5.5 Branding 18
2.5.6 Notifications 18
2.6 ActivClient Software Development Kit (SDK) 19
2.7 Smart Card Services and Profiles 19
2.7.1 Standalone/Mini Mode 19
2.7.2 Standalone Mode 20
2.7.3 AAA Server-Managed Mode 21

2.7.4 ActivID CMS-Managed Mode 21
2.7.5 US Department of Defense Common Access Card (CAC) Mode 22
2.7.6 US Government PIV Mode 22

3.0 ActivClient Components 24

3.1 ActivClient Agent 24
3.1.1 ActivClient Agent Icons in the Notification Area 24
3.1.2 ActivClient Agent Shortcut Menu Commands 24
3.2 User Console 25
3.2.1 Shortcut Menu Commands 28
3.2.2 Menu Toolbar 29
3.2.3 Standard Toolbar 30
3.3 PIN Initialization Tool 31
3.4 Advanced Diagnostics 32

4.0 Operational Environment 34

4.1 ActivID Solutions 34
4.2 System Requirements 35
4.3 Operating Systems 35
4.4 Virtualization Environments 35
4.5 Smart Cards and USB Tokens 35
4.6 Smart Card Readers 39
4.6.1 HID Global Smart Card Readers 39
4.6.2 Third-Party Readers 39

Appendix A: Terms and Acronyms 40

A.1. Terms 40
A.2. Acronyms 42

List of Tables

Table 1: Supported Standards....8
Table 2: ActivClient PKI Services....9
Table 3: ActivClient Agent Shortcut Commands 24
Table 4: User Console Left and Right Panes 26
Table 5: Menu Toolbar.... 29
Table 6: Standard Toolbar Commands 30

List of Figures

Figure 1: Tasks View 27
Figure 2: Tree View 28
Figure 3: User Certificate Right-Click Menu 28
Figure 4: Menu Toolbar 29
Figure 5: Standard Toolbar.... 30
Figure 6: PIN Initialization Tool.... 32
Figure 7: Advanced Diagnostics Tool – Report Window.... 33

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)

For complete details of these services, see 2.0 ActivClient Services on page 9.

1.2 Document Scope and Audience

This guide provides an overview of ActivClient features and capabilities:

- ActivClient authentication, digital signature, encryption and associated card and credential management services.
- ActivClient components that enable you to use these services.
- Operational environment including the supported operating systems and authentication devices.

1.3 Supported Standards and Certifications

ActivClient supports the latest security algorithms and standards.

Table 1: Supported Standards

Feature	Standards
Smart cards	ISO 7816
Smart card operating system	Java Card 2.1 and 2.2
Smart card reader architecture	PC/SC
Public Key Mechanisms	1024 and 2048-bit RSA, X509 certificates
Public Key Cryptography (PKI)	• PKCS#7, 10, 11, 11 v2.2, and 12 • Microsoft Mini Driver specifications 7.0 (compatibility with Microsoft Base Smart Card CSP, Microsoft CAPI and CNG)
Symmetric Key Cryptography (one-time passwords)	Triple DES, AES, ANSI x9.9
US Government	• U.S Government Smart Card Interoperability Specifications GSC-IS 2.1 • GSA Basic Services Interface (BSI) versions 1.8, 2.0 and 2.1 • FIPS 201, PIV certified by NIST • NIST Special Publication 800-73-3-4 • NISTIR 7863 • U.S DoD CAC Middleware Requirements Release 4.0 • FDCC/SCAP 1.1
Smart card management	GlobalPlatform 2.0.1, 2.1 and 2.1.1
Setup	Windows Installer (MSI)
Product accessibility	Section 508 compliant

2.0 ActivClient Services

This chapter describes the authentication, digital signature, encryption and associated card and credential management services provided by ActivClient.

2.1 PKI Services

The following table lists the PKI services. ActivClient provides digital certificate services using RSA key pairs stored on a smart card.

Table 2: ActivClient PKI Services

Feature	Description

Windows logon	• Provides a digital certificate-based mechanism to log on to the domain on:
	  • Microsoft Windows 7 SP1, 8, 8.1 and 10
	  • Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2 and 2016
	• Provides the ability to log off users or lock the workstation on smart card removal.
	• Supports smart card logon with Fast User Switching.

Remote access (PKI)	• Microsoft Windows dialer on Microsoft Windows 7, 8, 8.1 and 10 • Microsoft Windows VPN on Microsoft Windows 7, 8, 8.1 and 10 • Check Point Endpoint Security VPN for Windows E80.51 • Cisco AnyConnect VPN Client 4 • Arkoon® SecurityBox (Stormshield® Data Security) • Other VPN clients supporting smart cards via Microsoft CAPI/CNG or PKCS#11 either in native 64-bit or 32-bit mode
Secure web access **Note**: The ActivClient PKCS#11 library is automatically registered in Firefox and Thunderbird during ActivClient installation and on application startup.	Access to any web server with SSL v3 or TLS and a smart card-based digital certificate with the following browsers: • Microsoft Internet Explorer 9, 10 and 11 • Microsoft Edge • Mozilla Firefox 38 ESR, 45 ESR and later • Google Chrome

Feature	Description

Secure email	• Email signature, encryption/decryption:
	  • Microsoft Outlook 2007 SP3 (Office 2007)
	  • Microsoft Outlook 2010 SP2 (Office 2010)
	  • Microsoft Outlook 2013 SP1 (Office 2013)
	  • Microsoft Outlook 2016
	  With Microsoft Exchange 2007 SP3, 2010 SP3, 2013 SP1 and 2016
	  • Mozilla Thunderbird (latest version)
	• Microsoft Outlook usability enhancements – Automatic configuration of the Microsoft Outlook security profile, including:
	  • Automatic selection of the latest signature and encryption certificates on the user smart card.
	  • Selection of the hash algorithm (for example, SHA-1, SHA-256, SHA-512).
	  • Selection of the encryption algorithm (for example, 3DES, AES, RC2).
	• Additional usability services:
	  • Automatic publication of users' smart card-based certificates to the Global Address List (GAL).
	  • Automatic addition of email senders' certificates to users' Microsoft Outlook Contacts.
	  • Automatic decryption of encrypted emails (saving in decrypted form).

Encrypting file system	• ActivClient supports the Encrypting File System (EFS) feature of Microsoft Windows 7, 8, 8.1 and 10. With a smart card-based certificate, users can encrypt/decrypt files. • BitLocker (disk encryption) bundled with Microsoft Windows 7, 8, 8.1 and 10
Entrust client software	ActivClient supports the following Entrust products: • Entrust Entelligence™ Security Provider for Windows 9.2 • Entrust Authority™ Administration Services 8.3 • Entrust Authority Security Manager 8.1

Feature	Description
	• Entrust Authority Security Manager Administration 8.1
Examples of other PKI enabled clients	ActivClient also supports other applications that provide PKI services with smart cards using the Microsoft CAPI/CNG interface (via the ActivClient Mini Driver) or PKCS #11 interface (via the ActivClient PKCS#11 library). For example: • Microsoft Office (2007 SP2, 2010 SP2, 2013 SP1 and 2016) and Microsoft XPS Viewer (bundled with Microsoft Windows 7, 8, 8.1 and 10) that provide file signing capability. • Adobe Acrobat 10 and 11 (Standard and Professional)

2.2 Remote Access and One-Time Password Services

ActivClient generates a one-time password (OTP) on the smart card and allows users to use the generated OTPs to log on to applications requiring strong authentication via dialup, VPN or web. These OTP services require an ActivID authentication server, such as the ActivID AAA Server for Remote Access.

2.2.1 Log On to Applications Using an OTP

Users have several options to log on to an application using an OTP:

- **Log on with an OTP in one-click** – From the 'Get One-Time Password' option in the ActivClient Agent (in the Windows notification area), ActivClient generates an OTP and copies it to the clipboard.
- **Log on manually with an OTP** – From the ActivClient User Console, ActivClient can generate OTPs in both synchronous and challenge/response modes.

Users then simply paste the generated OTP into any application.

2.3 Remote Session Services

ActivClient supports the following remote session environments:

- Citrix® XenApp™
- Microsoft Remote Desktop Connection

In these environments, ActivClient for Windows is installed on the remote server or workstation (typically hosting Citrix XenApp or Microsoft Windows Terminal Server / Remote Desktop Services).

On the local workstation (Windows or other), only a smart card reader and PC/SC smart card reader driver are required.

2.3.1 Citrix XenApp Support

2.3.1.1 Supported Citrix Versions

ActivClient supports the following versions of Citrix XenApp, Citrix clients and Web Interface:

- Citrix XenApp server:
  - Citrix XenApp 6.5 FP3 (32 and 64-bit editions)
  - Citrix XenApp 7.6 FP3 (32 and 64-bit editions)
- Citrix clients:
  - Citrix Receiver for Windows v4.3.100 (on Microsoft Windows7, 8, 8.1 and 10)
  - For other platforms (such as terminals with MacOS or Linux, or thin clients), use a Citrix client that supports smart card redirection.

- Citrix XenDesktop 7.6 FP3

Note: If your Citrix configuration requires local authentication, then smart card middleware is required on the client.

Otherwise, ActivClient is required only on the server.

2.3.1.2 Supported Services in a Citrix Environment

- The user can remotely log on to the Citrix Server machine with their smart card.
- Smart card operations are supported within a Citrix session. Software such as Microsoft Outlook is running on a remote machine, while the smart card reader is connected on a client machine.
- The client machine can access multiple Citrix servers in the same session (with ActivClient running on each Citrix server).

2.3.2 Microsoft Remote Desktop Protocol (RDP) Support

2.3.2.1 Supported Environments

ActivClient supports the following Remote Desktop Protocol (RDP) environments:

- Server:
  - Remote Desktop Services included in Windows Server 2008 R2
  - Remote Desktop Services included in Windows Server 2012
  - Remote Desktop Services included in Windows Server 2012 R2
  - Remote Desktop Services included in Windows Server 2016
- Client:
  - Remote Desktop Connection v6.1 on Microsoft Windows 7
  - Remote Desktop Connection on Microsoft Windows 8 and 8.1
  - Remote Desktop Connection on Microsoft Windows 10
  - For other platforms (such as thin clients), use a remote desktop client that supports smart card redirection

Note: If your Remote Desktop configuration requires local authentication, then smart card middleware is required on the client.

Otherwise, ActivClient is required only on the server.

2.3.2.2 Supported Services

- The user can log on with RDP client to a remote machine with their smart card.
- Smart card operations are supported within a RDP session. Software such as Microsoft Outlook is running on the remote machine but the smart card reader driver is on the client.
- One client accessing multiple Terminal Servers in the same session (with ActivClient running on each Terminal Server).

2.4 Management Services for End Users

The following management services are available to end users.

2.4.1 ActivClient User Console

The User Console allows users to view and manage smart cards and credentials, including digital certificates. For further information, see section 3.2 User Console on page 25.

2.4.2 Digital Certificates

Digital certificates can be Root CA certificates or User certificates.

They can be displayed by ActivClient User Console in a user-friendly way and can also be deleted by users if the smart card policy allows it.

- Root CA certificates can be imported on smart cards and exported from smart cards.
- User certificates can be imported on smart cards (PKCS #12 files).

2.4.3 One-Time Passwords

The following services are provided in the ActivClient User Console to use and manage OTP credentials:

- Generate automatic OTPs (also known as synchronous mode)
- Generate challenge/response OTPs
- Synchronize counters for OTPs
- Configure user name for remote access with OTP

2.4.4 Personal Information

The ActivClient User Console allows users to view personal information stored on their smart card.

Available for:

- PIV (Personal Identity Verification) cards issued to US Federal Employees and Contractors
- CAC (Common Access Card) issued by the US Department of Defense

2.4.5 Smart Card PIN

The smart card PIN is controlled by end users.

At any time, users can change their PIN using the Windows **Change a password** menu.

2.4.6 Smart Card Initialization

ActivClient allows users to initialize smart cards before they can be used. Depending on the smart card configuration, users can:

- Initialize a blank smart card including setting the PIN code (the blank smart card might already contain smart card applets or not).
- Reset a smart card (that is, erase the smart card content) and define a new PIN code.

For further information, see section 31 PIN Initialization Tool on page 31.

Note: ActivClient also supports smart cards initialized by ActivID Credential Management System (CMS) and the ActivID Device Initialization Tool.

2.4.7 Smart Card Lock/Unlock

If users enter several incorrect PINs on the smart card, the smart card locks, preventing any further unauthorized use.

If the smart card is locked, users can unlock their card using:

- Static unlock code owned by users (stand-alone mode).
- Challenge/response-based unlock code provided by the help desk (requires ActivID CMS, ActivID Authentication Server or ActivID AAA Server).
- Online and seamless unlock method through the ActivID CMS My Digital ID Card interface.

Note: Depending on the smart card configuration, users can use the PIN Initialization Tool to re-initialize a card without following an unlock process.

2.4.8 Remote/Centralized Management

- Provides support for My Digital ID Card, the self-service support interface of ActivID CMS.
- Allows you to securely update your organization's smart cards.
- ActivClient automatically checks if smart card updates are available in ActivID CMS and prompts users to update the smart card.

2.4.9 ActivClient Agent

- Provides access to common ActivClient operations and shows smart card activity.
- Is displayed as an icon in the Windows notification area.

For further information, see section 3.1 ActivClient Agent on page 24.

2.4.10 Advanced Diagnostics

- Helps advanced users and help desk personnel perform a thorough examination of the ActivClient environment (software and smart card).
- Sends an email of the diagnostic report to the help desk.

For further information, see section 3.4 Advanced Diagnostics on page 32.

2.4.11 Log Files

- Generates log traces to be analyzed by HID Global technical support. No confidential or personally identifiable information is displayed in the log files.
- Is activated from the ActivClient User Console.

2.5 Management Services for Administrators

In addition to the end-user services, administrators can also use the additional services provided by the ActivID management products.

2.5.1 Installation and Deployment

The ActivClient setup uses MSI (Microsoft Windows Installer) technology, as well as advanced capabilities to facilitate product installation in large deployments. Administrators can:

- Predefine user options and customize the master installation image.
- Customize the setup, such as make it silent (all options are already configured, no further intervention is required).
- Customize the configuration and choose options through Microsoft Transform files (MST) by using standard msiexec.exe Windows Installer command line options.
- Configure CA certificate installation during ActivClient installation.

ActivClient can be deployed using software deployment technology:

- Microsoft System Center Configuration Manager 2012 R2
- Microsoft Active Directory push (with Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016)

ActivClient also provides software Auto-Update feature that allows administrators without software deployment technology to automatically install ActivClient software updates.

2.5.2 Upgrading

You can upgrade to ActivClient 7.1 from versions 6.2, 7.0, 7.0.1 and 7.0.2.

2.5.3 Policy Management

ActivClient offers a wide range of policies enabling organizations to optimize ActivClient to meet their usability and security requirements.

These policies can be:

- Managed centrally from Active Directory using Administrative Templates and Group Policies.
- Managed locally using Administrative Templates.
- Viewed locally using the Microsoft Resultant Set of Policy console, accessed from the ActivClient User Console.

2.5.4 Smart Card Automatic Registration

Without any product update, ActivClient supports new types of smart cards that are PIV-compliant (including DoD CAC).

2.5.5 Branding

The User Console can be customized with customer-specific graphics.

2.5.6 Notifications

ActivClient displays notification messages to help resolve common issues:

- The 'No Smart Card Reader' notification message is displayed above the Windows notification area at logon when there is no smart card reader connected to the PC or if it is inadvertently unplugged.
- The 'Unattended Smart Card' notification is an audio notification to remind users to take their smart card with them when leaving the workstation. It is triggered only if the smart card has not been removed from the smart card reader and if users attempt to:
  - Log off
  - Lock the workstation
  - Shutdown the workstation
  - Restart the workstation

  You can customize the notification by configuring the sound file (*.wav*) (for example, a voice message or custom music). By default, the audio notification is three beeps.
- The Expiration Warning message notifies users that their smart card or one of their smart card certificates has expired or will expire soon. It is displayed at:
  - Smart card insertion
  - Start of the user session if the smart card is inserted when logging on
- The ActivClient tools and notification features have been adapted to the new Microsoft Windows 'modern' interface available on Microsoft Windows 8 and later.
  - The ActivClient Agent and tools are displayed as tiles in the Start page.
  - ActivClient notifications are displayed as 'toast' notifications, sliding in from the top right corner of the interface. They are visible for 24 seconds before they disappear.
  - Some operations require that you manually switch to the Desktop, by clicking on the Desktop tile, in order to access the necessary window or tool (for example, Initialize Smart Card).

2.6 ActivClient Software Development Kit (SDK)

ActivClient comes with a Software Development Kit (SDK), enabling integrators to build applications leveraging the ActivClient smart card middleware. It provides documentation, header files/libraries and code samples for the following APIs:

- Microsoft cryptography APIs (CAPI/CNG)
- PKCS#11 v2.20
- Personal Identity Verification (PIV) Middleware API as per National Institute of Standard and Technology (NIST) SP800-73-4 specifications
- Basic Services Interface (BSI) API, defined by the U.S. Government Smart Card Interoperability specifications GSC-IS 2.1

These APIs provide access to ActivClient services: card management services, PKI services, OTP services and data storage services.

They are available with C and Java interfaces.

2.7 Smart Card Services and Profiles

This section describes how the services offered by ActivClient (initialization, unlock and reset) vary depending on the smart card profile. ActivClient supports the following smart card initialization and management modes.

2.7.1 Standalone/Mini Mode

In this mode:

- Smart cards are delivered without applets.
- Smart cards are initialized (including applets loading and PIN definition) using ActivClient PIN Initialization Tool.
- If the smart card becomes locked with too many incorrect PIN codes, users can reset the smart card completely using the PIN Initialization Tool – no need to know any PIN or Unlock code to reset the card. When the card is reset, new credentials can be downloaded onto the card.

Supported with the following cards:

- ActivID Smart Card 64 V2 (same as Oberthur CosmopolIC 64K V5.2)
- ActivID Smart Card 64K V2c (same as Axalto Cyberflex Access 64K v2c)
- ActivID Smart Card 80K v3.2 (same as Giesecke & Devrient SmartCafe Expert 80K DI v3.2)
- ActivID Smart Card 144K v3.2 (same as Giesecke & Devrient SmartCafe Expert 144K DI v3.2)
- ActivID ActivKey V2 64k (same as Axalto Cyberflex Access 64K V1 SM 2.1)
- ActivID ActivKey SIM 64K (3 options: Axalto Cyberflex Access 64K v2c, Oberthur CosmopolIC 64K V5.2 and Giesecke & Devrient SmartCafe Expert 64K FIPS-1024)

- Gemalto Cyberflex Access 64K v2c
- Giesecke & Devrient SmartCafe Expert 144K DI v3.2
- Giesecke & Devrient SmartCafe Expert 80K DI v3.2
- HID Global Crescendo C1100
- Oberthur CosmopolIC 64K V5.2

Notes:

- For all 64K (or later) cards that support 2048-bit RSA, the profile combines 1024 and 2048.
- The standalone / mini mode is supported only with ActivID v1 applets.

2.7.2 Standalone Mode

In this mode:

- Smart cards are delivered with applets configured with a default 'standalone' profile.
- Smart cards are initialized (that is, PIN definition) using the ActivClient PIN Initialization Tool, or simply on smart card insertion. A (static) unlock code is displayed to users at the end of the initialization process.
- If the smart card becomes locked with too many incorrect PIN codes, users can (via the User Console or on smart card insertion) unlock their smart card with a static unlock code. This allows users to define a new PIN code while their credentials are preserved on the smart card.
- Users reset their smart card completely (from the User Console) if they know the PIN or unlock code.

Supported with the following cards:

- ActivID Smart Card 64 V2 – ActivClient Profile (based on Oberthur CosmopolIC 64K V5.2)
- ActivID Smart Card 64K V2c – ActivClient Profile (based on Axalto Cyberflex Access 64K v2c)
- ActivID Smart Card 80K v3.2 – ActivClient Profile (based on Giesecke & Devrient SmartCafe Expert 80K DI v3.2)
- ActivID Smart Card 144K v3.2 – ActivClient Profile (based on Giesecke & Devrient SmartCafe Expert 144K DI v3.2)
- ActivID ActivKey V2 64k – ActivClient Profile (based on Axalto Cyberflex Access 64K V1 SM 2.1)
- ActivID ActivKey SIM 64K – ActivClient Profile (3 options: Axalto Cyberflex Access 64K v2c, Oberthur CosmopolIC 64K V5.2 and Giesecke & Devrient SmartCafe Expert 64K FIPS-1024)
- HID Global Crescendo C1150

2.7.3 AAA Server-Managed Mode

When the AAA Server is used for OTP services:

- Smart cards are delivered with applets configured with a default ‘standalone’ profile.
- Smart cards are initialized (PIN code and OTP credentials) using the AAA Server Administrator Console or the ActivID Device Initialization Tool.
- If the smart card becomes locked with too many incorrect PIN codes, users can unlock the smart card with a challenge/response mechanism (from the User Console – users have access to the unlock response either on the phone, or online with the AAA Server Self Help Desk). This allows users to define a new PIN code while their credentials are preserved on the smart card.
- Users can reset the smart card completely (from the User Console) if they know the PIN or unlock code (challenge/response).

2.7.4 ActivID CMS-Managed Mode

In this mode:

- Smart cards are delivered without applets.
- Smart cards are initialized and managed by ActivID CMS (including applet loading and loading of user credentials such as certificates).
- If the smart card becomes locked with too many incorrect PIN codes, users can unlock the smart card either with the ActivClient User Console (using a challenge/response mechanism – users have access to the unlock response provided via telephone by their help desk) or online with the ActivID CMS My Digital ID Card portal. This allows users to define a new PIN code while their credentials are preserved on the smart card.
- Users can securely update the smart card content (applets and credentials) using the ActivID CMS My Digital ID Card portal.
- Users can reset the smart card completely using ActivID CMS.

2.7.5 US Department of Defense Common Access Card (CAC) Mode

In this mode:

- ActivClient uses the DOD Common Access Card in read-only mode for usage operations (PKI services and demographic data), in compliance with the DOD middleware requirements. The Change PIN function is supported.
- Issuance, card unlock and card update (update of certificate or demographic data) are services provided by the DOD.

Supported with the following CAC models:

- CAC v2
- CAC Next Generation NG
- CAC PIV Endpoint, with the PIV Authentication certificate 'activated' or not for the GSC-IS interface

For the list of supported card platforms, see 4.5 Smart Cards and USB Tokens on page 35.

Note: Most current CAC models are compatible with both GSC-IS and PIV FIPS 201.

When the US Department of Defense configuration feature is installed, ActivClient uses the cards in GSC-IS compliant mode; otherwise, ActivClient uses the cards in PIV-compliant mode.

2.7.6 US Government PIV Mode

This mode refers to:

- PIV and PIV-I (PIV interoperable) cards compliant with NIST Special Publication 800-73-4
- CIV (Commercial Identity Verification) and PIV-like cards (PIV interface, with additional flexibility in terms of card content and policies)

In addition:

- Smart cards can be issued by ActivID CMS (PIV-compliant) or by other smart card management systems.
- ActivClient uses the PIV smart card in read-only mode for usage operations (PKI services and demographic data), in compliance with the PIV specifications. The Change PIN function is supported.
- By FIPS 201 specification, smart card unlock (as known as PIN Reset) needs to be in the presence of an Issuance Officer with cardholder biometric verification. The smart card unlock functionality is not available for PIV smart cards in ActivClient, but can be performed with ActivID CMS.
- ActivClient also supports PIV extensions (also known as PIV-like or PIV+). In this configuration, ActivClient enables using the card following the card profile and policies used during the ActivID CMS-based card issuance. For example, the PIN can be unlocked using a challenge/response model, the PIN might not be required for signature operations (leveraging the ActivClient PIN Caching service), or additional credentials (certificates or one-time passwords) might be available.

Supported with the following cards:

- Cards with the ActivID PIV applet suite
- Athena IDProtect Duo PIV
- CardLogix Credentsys-J PIV
- Gemalto GemCombi'Xpresso R4 E72 PK Standard
- Gemalto TOP DL GX4 v2 144K FIPS with Gemalto PIV 1.55 applet
- HID Global pivCLASS
- HID Global Crescendo 144K FIPS
- Keycorp MULTOS 64K with StepNexus PIV Application v4.2.1
- Oberthur ID-One Cosmo 64K v5.2D Fast ATR with PIV application
- Oberthur ID-One Cosmo 64K v5.2D Fast ATR with PIV application SDK
- Oberthur ID-One Cosmo v7.0 with Oberthur PIV Applet v2.3.2
- Oberthur ID-One Cosmo v8 with Oberthur PIV Applet v2.3.5 / 2.4.0
- Safenet 400 PIV
- Sagem Orga J-ID Mark 64 PIV with Sagem PIV Applet version 01

3.0 ActivClient Components

This chapter describes the ActivClient components.

3.1 ActivClient Agent

The ActivClient Agent 'watches' for smart card activity (insertion, activity, and removal), and starts the ActivClient User Console and other ActivClient tools.

3.1.1 ActivClient Agent Icons in the Notification Area

The ActivClient Agent icons display in the Windows notification area:

 A smart card is inserted in the smart card reader

 Smart card is being used. Do not remove the card until the icon turns green!

 Smart card reader is empty

 No smart card reader is detected

 ActivClient is starting up

3.1.2 ActivClient Agent Shortcut Menu Commands

To display the following commands, left or right-click on the ActivClient Agent icon in the Windows notification area.

Table 3: ActivClient Agent Shortcut Commands

Command	Description
Open	Opens the ActivClient User Console
Get One-Time Password	Generates an OTP and copies it to the clipboard. OTP support must be installed and the card must be configured for OTP.
PIN Initialization Tool	Opens the PIN Initialization Tool to initialize and choose a PIN code while erasing the content of the smart card.

Command	Description
Advanced Diagnostics	Opens the Advanced Diagnostics wizard to thoroughly examine of the environment and send information in an email to the help desk.
About	Opens the About ActivClient window which displays information about ActivClient and the system.

3.2 User Console

The User Console helps manage logon credentials and certificates. For further information, refer to the *ActivID ActivClient for Windows User Guide*.

You can …	Action
Manage your digital certificates	• Import a CA or User certificate • Export a certificate • View a certificate's attributes • Delete a certificate • Set as default • Add your certificates to the Global Address List (GAL)
Manage your one-time passwords	• Generate an OTP • Resynchronize an OTP • Configure a user name for OTP-based remote access
View your personal information	Available for the US Department of Defense on Common Access Cards (CAC) or Personal Identity Verification (PIV) cards only.
Manage your smart card	• View your smart card's properties • Unlock your smart card • View your unlock code • Initialize your new smart card • Reset your smart card • Select a smart card reader

Users can access the User Console either:

- From the ActivClient Agent icon located in the Microsoft Windows notification area:
  - Double-click the ActivClient Agent icon  .
  - Left or right-click on the ActivClient Agent icon  and select **Open**.
- From the Start menu, go to the programs or apps directory, and select **User Console** under **ActivID ActivClient**.
- In the Start page of the Microsoft Windows 'modern' interface, click on the **User Console** tile .

The User Console interface consists of secondary windows, menus, toolbars and of a right and left pane.

Table 4: User Console Left and Right Panes

Pane	Description
Left pane or Tasks pane	The Tasks pane (the default pane on the left) lists common tasks associated with the information in the right pane. Users can switch between the Tasks and the Tree view by clicking the right and left arrows at the top of the pane.
Right pane	The right pane displays the content of the smart card. It provides access to: • Smart Card Info • My Certificates • CA Certificates • One-time passwords • My Personal Info

Figure 1: Tasks View

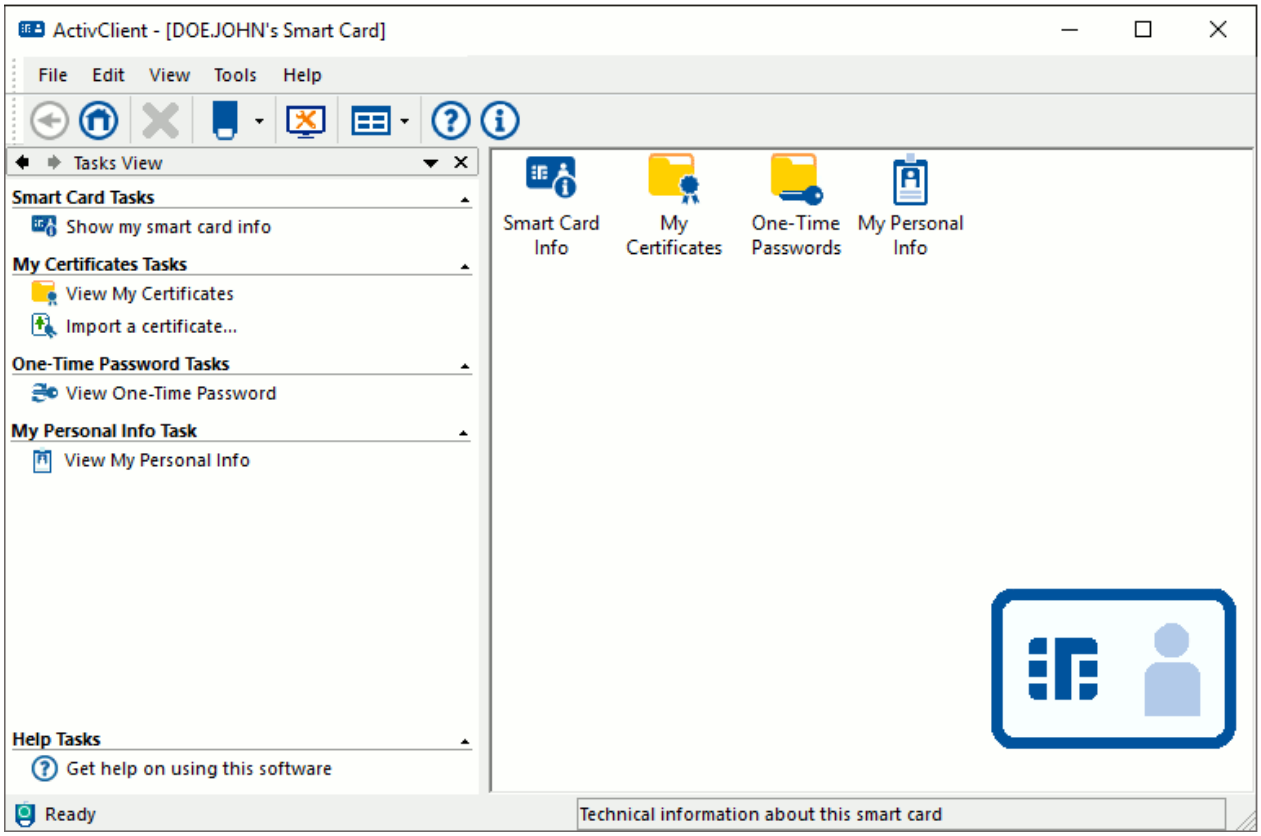
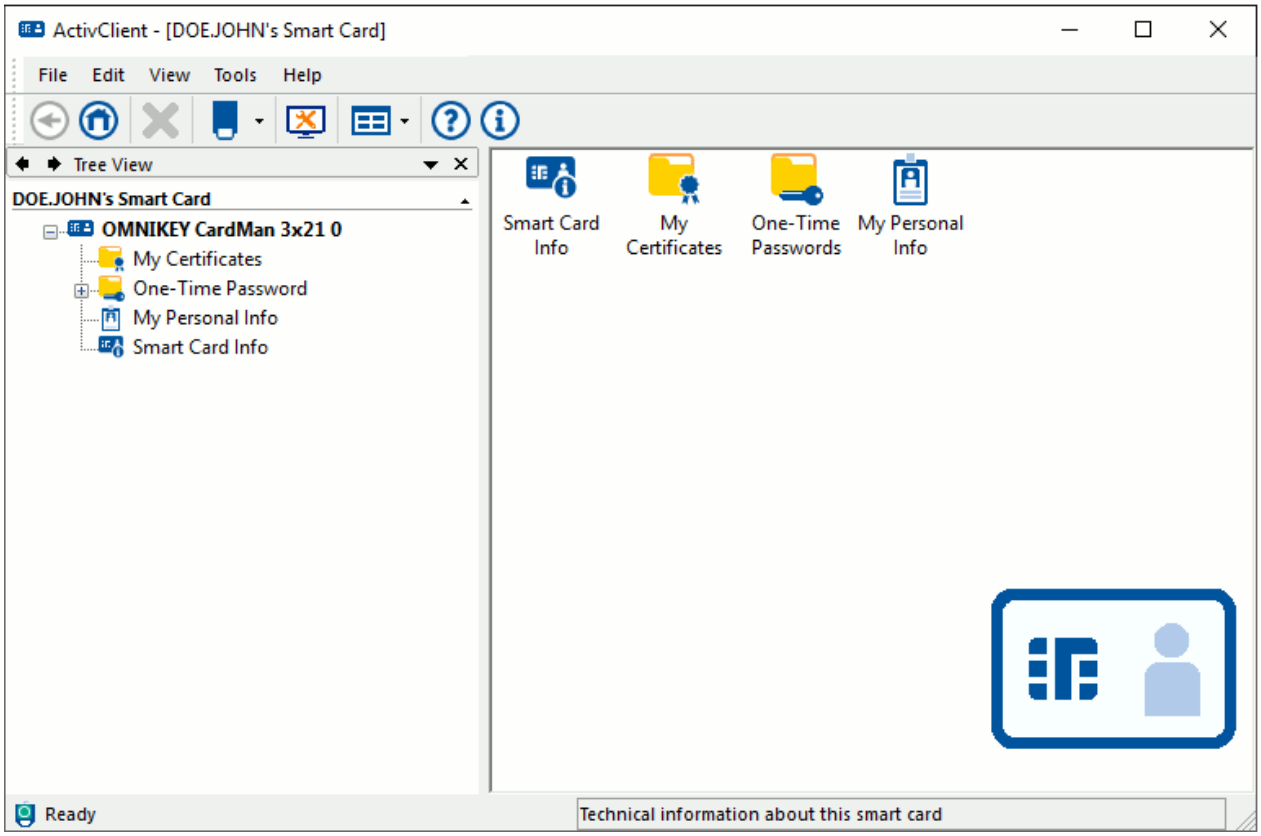


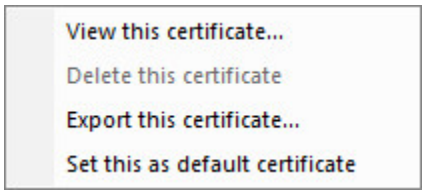
Figure 2: Tree View



3.2.1 Shortcut Menu Commands

When the users right-clicks on a credential, a command menu is displayed.

Figure 3: User Certificate Right-Click Menu



Note about Shortcut Menus:

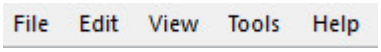
Right-clicking some elements in the User Console will display a shortcut menu that provides support for the most common tasks.

The displayed commands are different for each element.

3.2.2 Menu Toolbar

The Menu toolbar appears above the Standard toolbar in the User Console. It can be used to select ActivClient menus and commands.

Figure 4: Menu Toolbar



Note: Depending on the ActivClient components you installed, some menus might not be available.

Table 5: Menu Toolbar

Menu	Command	Function	Keyboard shortcuts
File	Open	Opens selected object	ENTER
	Delete	Deletes selected object	DEL
	Import	Imports a certificate	None
	Export	Exports a certificate	None
	Use Reader	Specifies what smart card reader to use	None
	Exit	Closes User Console session	None
Edit	Paste	Inserts text from the clipboard	SHIFT+INS
	Cut	Cuts selected text and places it on the Clipboard	SHIFT+DEL
	Copy	Copies selected text to the Clipboard	CTRL+C
	Select All	Selects all objects	CTRL+A
View	Toolbars	Toggles which toolbars are displayed	None
	Status Bar	Toggles status bar	None
	Explorer Bar	Toggles between Tasks pane and Tree View pane	None
	Large Icons	Displays large format icons	None
	Small Icons	Displays small format icons	None
	List	Displays objects in List format	None
	Details	Displays objects in Detail format	None
	Arrange Icons	Rearranges icons by name or type	None
	Go to	Goes to specified page	None
	Refresh	Refreshes current page	F5

Menu	Command	Function	Keyboard shortcuts
Tools	New Card	Sets PIN on a new smart card	None
	Unlock Card	Allows to enter unlock code to unlock a locked smart card	None
	Reset Card	Removes everything stored on the smart card, including certificates	None
	View Unlock Code	Allows to view and save an unlock code. Available after card is initialized with ActivClient	None
	Advanced	Accesses the advanced features: • View Policy Settings • Publish to GAL • Check for Card Update • Enable logging • Reset optimization cache	None
Help	ActivClient Help	Provides user access to ActivClient Online Help	F1
	Diagnose	Starts the Diagnostics Tool	None
	About ActivClient	Displays information about ActivClient and the system	None

3.2.3 Standard Toolbar

The Standard toolbar provides quick access to common functions in the User Console.

Figure 5: Standard Toolbar



The following commands are available on the Standard toolbar:

Table 6: Standard Toolbar Commands

Button	Command	Function
	Back	Goes back to previous page
	Home	Goes to home page

Button	Command	Function
	Delete	Deletes currently selected object
	Reader List	Displays list of attached smart card readers
	Run Diagnostics Tool	Starts the Diagnostics Tool
	Views	Displays large or small format icons, or List or Detail format lists
	Help	Launches the end user online help
	About	Displays information about ActivClient and the system

For further information about the User Console tasks, see the *ActivID ActivClient for Windows User Guide*.

3.3 PIN Initialization Tool

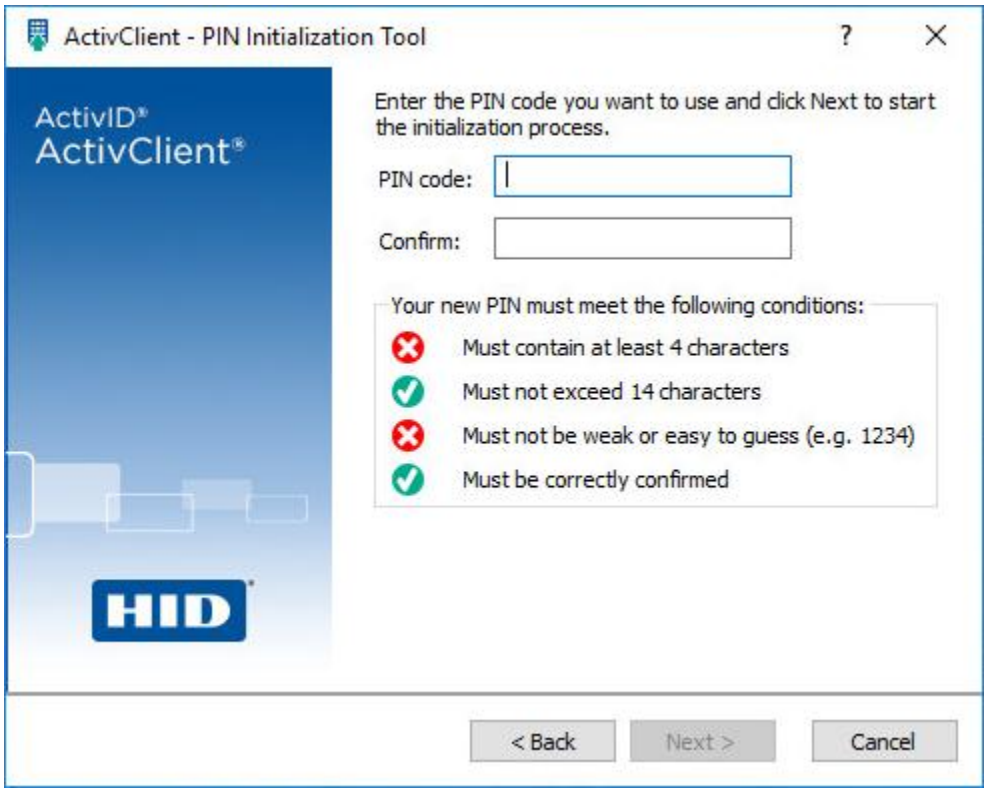
The PIN Initialization Tool allows users to initialize smart cards, including setting a new PIN code.

- If the smart card is used in a standalone / Mini mode (see 2.7.1 Standalone/Mini Mode on page 19), re-initialize the smart card at any time. The card content is erased, and the user can define a new PIN.
- If the smart card is used in a standalone mode (see 2.7.2 Standalone Mode on page 20), then:
  - If this is the first time the card is initialized, define the PIN. An unlock code is displayed for future use (in case the user locks the smart card).
  - If the card has already been used, enter the PIN code or unlock code (when appropriate) in order to set a new PIN. The smart card content is erased.

Users can access the PIN Initialization Tool either:

- From the ActivClient Agent's left or right-click menu, select **PIN Initialization Tool**.
- From the **Tools** menu of the User Console, select **New Card**.
- From the Start menu, go to the programs or apps directory, and select **PIN Initialization Tool** under **ActivID ActivClient**.
- In the Start page of the Microsoft Windows 'modern' interface, click on the **PIN Initialization Tool** tile .

Figure 6: PIN Initialization Tool



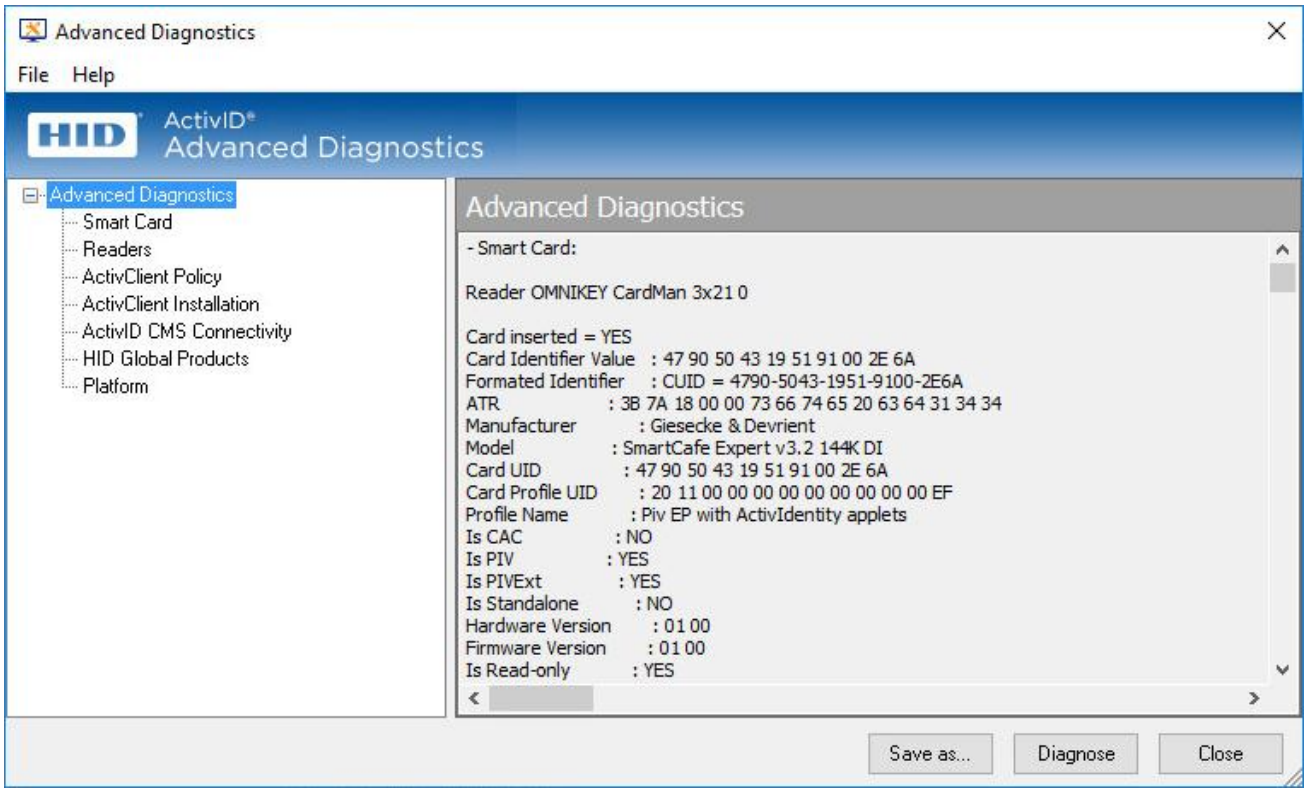
3.4 Advanced Diagnostics

Users can use the Advanced Diagnostics tool to diagnose a problem. If required, the tool can be configured to send the results to the help desk by email.

Users can access the Advanced Diagnostics Tool either:

- From ActivClient Agent's left or right-click menu, select **Advanced Diagnostics**.
- From the User Console Standard toolbar, select **Advanced Diagnostics** .
- From the User Console **Help** menu, select **Diagnose**.
- From the Start menu, go to the programs or apps directory, and select **Advanced Diagnostics** under **ActivID ActivClient**.

Figure 7: Advanced Diagnostics Tool – Report Window



4.0 Operational Environment

This chapter details the ActivClient operational environment.

4.1 ActivID Solutions

ActivClient can be deployed in standalone mode. Combined with additional HID Global ActivID products, it provides a fully comprehensive solution – the Identity Assurance solutions for Enterprise and for Government.

The following table lists the compatible ActivID products and their purpose.

Identity Assurance Components	Purpose
ActivClient	Smart card security client
ActivID Credential Management System 4.2 (SP3 and later) and 4.3	Credential Management System for smart card issuance and management services
ActivID AAA Server for Remote Access 6.7 and 6.8	Authentication server and smart card management services
ActivID Device Initialization Tool 3.0	Smart card initialization (compatible with ActivID AAA Server)
Desktop Validation Client 3.1	Plug-in for a Microsoft Windows-based computer to perform secure validation of digital certificates
• ActivID Validation Authority 5.6 (OCSP support) • ActivID Path Builder 2.1 (SCVP support) • ActivID Responder Appliance 3.2 (OCSP support)	Secure certificate validation solution

4.2 System Requirements

The minimum system requirements for ActivClient installation are:

- One of the support Operating Systems listed below
- 64 MB of RAM
- 32 MB (ActivClient x86) to 55 MB (ActivClient x64) of free disk space

4.3 Operating Systems

The following are the operating systems on which ActivClient can be run:

- Microsoft Windows 7 SP1 (32 and 64-bit editions)
- Microsoft Windows 8 (32 and 64-bit editions)
- Microsoft Windows 8.1 Update 1 and later (32 and 64-bit editions)
- Microsoft Windows 10 (32 and 64-bit editions)
- Microsoft Windows Server 2008 R2 SP1 (64-bit edition) including Server Core
- Microsoft Windows Server 2012 (64-bit edition) including Server Core
- Microsoft Windows Server 2012 R2 (64-bit edition) including Server Core
- Microsoft Windows Server 2016 (64-bit edition)

4.4 Virtualization Environments

ActivClient is supported in the following virtual environment when ActivClient is run on one of the supported operating systems:

- VMware® Workstation 12
- VMware Horizon View 6

4.5 Smart Cards and USB Tokens

The list below presents the smart cards and USB tokens supported by ActivClient.

For information on which cards are supported in the different ActivClient deployment modes (configuration), see 2.7 Smart Card Services and Profiles on page 19.

- HID Global/ActivID:
  - Smart Card 64K v1 (same as Gemalto Cyberflex Access 64K V1 SM 2.1)
  - Smart Card 64K v2 (same as Oberthur CosmopolIC 64K V5.2)
  - Smart Card 64K v2c (same as Gemalto Cyberflex Access 64K v2c)
  - Smart Card 80K v3.2 (same as Giesecke & Devrient SmartCafe Expert 80K DI v3.2)

- Smart Card 144K v3.2 (same as Giesecke & Devrient SmartCafe Expert 144K DI v3.2)
- ActivKey 32K v2 (same as Atmel 6464C Pro 64k)
- ActivKey 64K v2 (same as Axalto Cyberflex Access 64K V1 SM 2.1)
- ActivKey SIM
- ActivKey Display v2

  ActivClient Support for ActivKey Display v2 with SIM

  - When ActivKey Display is connected, ActivClient uses the SIM for all credentials (PIN, PKI and OTP).
  - When ActivKey Display is not connected, the user can read the OTP on the display (this is a different credential than managed on the SIM).
- Crescendo C800
- Crescendo C11xx (C1100 and C1150)
- Crescendo C1300
- Crescendo JCOP 21 v2.4.1 R2 64K
- Crescendo JCOP 21 v2.4.1 R2 64K #2
- Crescendo JCOP v2.4.2 R2 80K
- Crescendo JCOP v2.4.2 R2 144K
- Crescendo 144K FIPS
- pivCLASS v1.0

- Athena IDProtect Duo PIV
- Atmel 6464C Pro 64k
- CardLogix Credentsys-J PIV
- Gemalto:
  - Cyberflex Access 32K V2 #1
  - Cyberflex Access 32K V2 SM 7.2
  - Cyberflex Access 32K V4 SM 1.3
  - Cyberflex Access e-gate 32K
  - Cyberflex Access 64K V1 SM 2.1
  - Cyberflex Access 64K V1 Bio SM 3.1
  - Cyberflex Access 64K V1 SM 4.1
  - Cyberflex Access 64K v2a SM 2.3

- Cyberflex Access 64K v2b SM 1.1
- Cyberflex Access 64K v2c
- Cyberflex Access 128K
- GemXpresso 32K
- GemXpresso PRO 64K FIPS v1 Dual ATR
- GemXpresso PRO 64K R3 v1 Dual ATR
- GemXpresso PRO 64K R3 FIPS V2
- GemXpresso PRO R3 E64 PK – Standard Version
- TOP DM GX4 72K (FIPS)
- TOP DM GX4 72K (FIPS) Standard #1
- TOP DM GX4 72K (FIPS) Standard #2
- TOP IM GX4 72K (FIPS) Standard
- TOP IM GX4 72K (FIPS) Standard Rev B
- TOP DL GX4 144K FIPS
- TOP DL GX4 v2 144K FIPS
- TOP DL v2.1
- TOP WL 128K v2 with Gemalto PIV 1.55 applet

- Giesecke & Devrient:
  - SmartCafe 32K v1
  - SmartCafe Expert 32K v2.0
  - SmartCafe Expert 64K Non-FIPS
  - SmartCafe Expert 64K FIPS-1024
  - SmartCafe Expert 64K FIPS-2048
  - SmartCafe Expert 72K DI v3.2
  - SmartCafe Expert 80K DI v3.2
  - SmartCafe Expert 80K DI v5.0
  - SmartCafe Expert 80K DI v6.0
  - SmartCafe Expert 144K DI v3.2
  - SmartCafe Expert 144K DI v3.2 non-FIPS
  - SmartCafe Expert 144K DI v5.0
  - SmartCafe Expert 144K DI v6.0

  - SmartCafe Expert 144K DI v7.0
  - Secure Flash Solutions Mobile Security Card
- Keycorp MULTOS 64K with StepNexus PIV Application v4.2.1
- NXP JCOP31 v2.4.1 80K
- Oberthur:
  - Galactic 32K #1
  - Galactic 32K #2
  - CosmopolIC 32K V4
  - CosmopolIC 32K V4 Fast ATR
  - CosmopolIC 64K v5
  - CosmopolIC 64K V5.2
  - CosmopolIC 64K V5.2 Fast ATR
  - ID-One Cosmo 64K v5.2D Fast ATR with PIV application
  - ID-One Cosmo 64K v5.2D Fast ATR with PIV application SDK
  - ID-One Cosmo 64K v5.4
  - ID-One Cosmo 128K v5.5
  - ID-One Cosmo v7.0 80K
  - ID-One Cosmo v7.0 Type A Standard 80K Dual
  - ID-One Cosmo v7.0 128K
  - ID-One Cosmo v7.0 Type A Large 128K Dual
  - ID-One Cosmo v8.0 128K
  - ID-One PIV
  - ID-One Cosmo v8.0 with PIV 2.3.5 / 2.4.0
- Safenet 400 PIV
- Sagem Orga J-ID Mark 64 PIV with Sagem PIV Applet version 01
- Sharp JCOP 31 ID

4.6 Smart Card Readers

ActivClient supports any PC/SC certified smart card reader, from HID Global and third-party vendors.

4.6.1 HID Global Smart Card Readers

- OMNIKEY® contact readers:
  - 2061 Bluetooth
  - 3021 USB
  - 3121 USB
  - 5325 (contact and Prox contactless)
  - 6121 Mobile USB (SIM-size contact)
  - 6321 USB (SIM-size contact and contactless)
  - ActivKey SIM
  - ActivKey Display
- OMNIKEY contactless readers:
  - 5021 CL (contactless only)
  - 5022 CL (contactless only)
  - 5321 CR USB (contactless only, for clean room environments)
  - 5326 DFR (contactless dual frequency)
  - 5427 CK (contactless only)
  - 6321 USB (SIM-size contact and contactless)

4.6.2 Third-Party Readers

ActivClient supports any third-party PC/SC certified smart card reader. Make sure you install the latest firmware and driver for your smart card reader. Check Windows Update and your vendor's web site for the latest available version.

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

