

ActivIdentity® ActivClient™ for Windows

Overview

Version 7.0.2 | Released | April 2, 2013

Table of Contents

Chapter 1: Introduction	6
About ActivClient	6
Services	6
Standards	7
Chapter 2: ActivClient Services	8
PKI Services	8
Remote Access and One-Time Password Services	9
Log On to Applications Using an OTP	10
Remote Session Services	10
Citrix XenApp Support	10
Supported Citrix Versions	10
Supported Services in a Citrix Environment	10
Microsoft Remote Desktop Protocol (RDP) Support	11
Supported Environments	11
Supported Services	11
Management Services for End Users	11
ActivClient User Console	11
Digital Certificates	11
One-Time Passwords	12
Personal Information	12
Smart Card PIN	12
Smart Card Initialization	12
Smart Card Lock/Unlock	12
Remote/Centralized Management	13
ActivClient Agent	13
Advanced Diagnostics	13
Log Files	13
Management Services for Administrators	13
Installation and Deployment	13
Upgrading	14
Policy Management	14
Smart Card Automatic Registration	14
Branding	14
Notification	14
Smart Card Services and Profiles	15
Standalone / Mini Mode	15
Standalone Mode	16

AAA Server-Managed Mode	16
ActivID CMS-Managed Mode	17
US Department of Defense Common Access Card Mode	17
US Government PIV Mode	17
Chapter 3: ActivClient Components	19
ActivClient Agent	19
ActivClient Agent Icons in the Notification Area	19
ActivClient Agent Shortcut Menu Commands.	19
User Console	20
Access Shortcut Menu Commands	22
Menu Toolbar	22
Standard Toolbar	23
PIN Initialization Tool	24
Access the PIN Initialization Tool	24
Advanced Diagnostics	25
Access the Advanced Diagnostics Tool	25
Chapter 4: Operational Environment	27
ActivIdentity Identity Assurance	27
System Requirements	27
Operating Systems.	27
Virtualization Environments	28
Smart Cards and USB Tokens.	28
Smart Card Readers	30
HID Global/ActivIdentity Smart Card Readers	30
ActivClient Support for ActivKey Display v2 with SIM	31
Third-Party Readers	31
Appendix A: Terms and Acronyms	33
Terms	33
Acronyms	34

List of Tables

Table 1.1: Supported Standards	7
Table 2.1: List of PKI Services	8
Table 2.2: Log On to Applications Using an OTP	10
Table 3.1: ActivClient Agent Shortcut Commands	19
Table 3.2: User Console Left and Right Panes	20
Table 3.3: Menus and Commands from the Menu Toolbar	22
Table 3.4: Standard Toolbar Commands	24
Table 4.1: ActivIdentity Products	27

List of Figures

Figure 3.1: Tasks View	21
Figure 3.2: Tree View	21
Figure 3.3: User Certificate Right-Click Menu	22
Figure 3.4: Menu Toolbar	22
Figure 3.5: Standard Toolbar	23
Figure 3.6: Advanced Diagnostics Tool - Report Window	26

Chapter 1: Introduction

Chapter Contents

- 6 [About ActivClient](#)
- 6 [Services](#)
- 7 [Standards](#)

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.

About ActivClient

ActivClient is the latest smart card and USB token middleware from ActivIdentity that allows enterprise and government customers to easily use smart cards and USB tokens for a wide variety of desktop, network security and productivity applications.

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

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

Services

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)
- Smart card services and profiles

For complete details of these services, see [Chapter 2, "ActivClient Services," on page 8](#).

This document is for:

- System administrators
- Operators/end users
- People with knowledge of Microsoft® Windows® operating systems as well as some understanding of Public Key Infrastructure

Standards

ActivClient supports the latest security algorithms and standards.

TABLE 1.1: Supported Standards

Feature	Description
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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 • 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

Chapter 2: ActivClient Services

Chapter Contents

- 8 [PKI Services](#)
- 9 [Remote Access and One-Time Password Services](#)
- 10 [Remote Session Services](#)
- 11 [Management Services for End Users](#)
- 13 [Management Services for Administrators](#)
- 15 [Smart Card Services and Profiles](#)

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

PKI Services

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

TABLE 2.1: List of PKI Services

Feature	Description
Windows logon	<ul style="list-style-type: none"> Provides a digital certificate-based mechanism to log on to the domain on: <ul style="list-style-type: none"> Microsoft Windows Vista SP2 Microsoft Windows 7 SP1 Microsoft Windows 8 Microsoft Windows Server 2008 SP2 (including Server Core) Microsoft Windows Server 2008 R2 SP1 (64-bit edition) (including Server Core) Microsoft Windows Server 2012 (64-bit edition) (including Server Core) 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)	<ul style="list-style-type: none"> Microsoft Windows dialer on Microsoft Windows Vista and Windows 7 Microsoft Windows VPN on Microsoft Windows Vista and Windows 7 Check Point Secure Platform R75 Check Point Endpoint Security VPN for Windows R75 Cisco VPN Client 5.0.06 Cisco AnyConnect VPN Client 2.4 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	<p>Access to any web server with SSL v3 and a smart card-based digital certificate with the following browsers:</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 8, 9 and 10 Mozilla Firefox 16 and later Google Chrome 22 and later

Note

The ActivClient PKCS#11 library is automatically registered in Firefox and Thunderbird during ActivClient installation and on application startup.

TABLE 2.1: List of PKI Services

Feature	Description
Secure email	<p>Email signature, encryption/decryption:</p> <ul style="list-style-type: none"> • Microsoft Outlook 2007 SP2 (Office 2007) (32-bit edition) • Microsoft Outlook 2010 (no SP and SP1) (Office 2010) • Microsoft Exchange 2007 SP1 • Microsoft Exchange 2010 (no SP and SP1) • Mozilla Thunderbird 3.0 <p>Microsoft Outlook usability enhancements: Automatic configuration of the Microsoft Outlook security profile, including:</p> <ul style="list-style-type: none"> • 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). <p>Additional usability services:</p> <ul style="list-style-type: none"> • 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	<p>ActivClient supports the Encrypting File System (EFS) feature of Microsoft Windows Vista, Windows 7 and Windows 8. With a smart card-based certificate, users can encrypt/decrypt files.</p>
Examples of other PKI enabled clients	<p>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:</p> <ul style="list-style-type: none"> • Microsoft Office 2007 SP2 and Office 2010 (no SP and SP1) and Microsoft XPS Viewer (bundled with Microsoft Windows 7) that provide file signing capability. • Windows BitLocker To Go (Microsoft Windows 7) to encrypt external drives. • Adobe Acrobat 10.0 (Standard and Professional) • IBM Lotus Notes • Novell Certificate Login

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 ActivIdentity 4TRESS™ authentication server, such as the ActivIdentity 4TRESS AAA Server for Remote Access.

Log On to Applications Using an OTP

Users have several options to log on to an application using an OTP as described in [Table 2.2](#):

TABLE 2.2: Log On to Applications Using an OTP

Feature	Description
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. Users simply paste it into any application.
Log on manually with an OTP	From the ActivClient User Console, ActivClient can generate OTPs in both synchronous and challenge/response modes. Users simply paste the OTP into any application.

Remote Session Services

ActivClient supports the following remote session environments:

- Citrix® XenApp™
- Microsoft Remote Desktop Connection

In both 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.

Citrix XenApp Support

Supported Citrix Versions

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

Citrix XenApp server:

- Citrix XenApp 5.0 (FP3 or later) (32 and 64-bit editions)
- Citrix XenApp 6.0 (32 and 64-bit editions)

Citrix clients:

- Citrix Online Plug-in - Full (version 11 or 12).
- Citrix Online Plug-in - Web (version 11 or 12).
- For other platforms (such as terminals with MacOS or Linux, or thin clients), use a Citrix client that supports smart card redirection.

Supported Services in a Citrix Environment

- The user can remotely log on to the Citrix Server machine with their smart card.

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.

Note

For Microsoft Windows Vista, apply the software update: <http://support.microsoft.com/kb/969084>

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.

- 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).

Microsoft Remote Desktop Protocol (RDP) Support

Supported Environments

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

- Server:
 - Terminal Server included in Windows Server 2008 (32 and 64-bit editions)
 - Remote Desktop Services included in Windows Server 2008 R2 (64-bit edition)
- Client:
 - Remote Desktop Connection v6.1 on Microsoft Windows Vista and Windows 7 (32 and 64-bit editions).
 - For other platforms (such as thin clients), use a remote desktop client that supports smart card redirection.

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).

Management Services for End Users

The following management services are available to end users.

ActivClient User Console

The User Console allows users to view and manage smart cards and credentials, including digital certificates.

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).

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

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

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.

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.

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)

Note

ActivClient also supports smart cards initialized by ActivID Card Management System (CMS).

Note

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

- Challenge/response-based unlock code provided by the help desk (requires ActivID™ CMS, 4TRESS Authentication Server or 4TRESS AAA Server)
- Online and seamless unlock method through the Self Service Portal (requires ActivID CMS)

Remote/Centralized Management

- Provides support for **My Digital ID Smart card**. ActivClient supports 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.

ActivClient Agent

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

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.

Log Files

- Generates log traces to be analyzed by ActivIdentity Customer Support. No confidential or personally identifiable information is displayed in the log files.
- Is activated from the ActivClient User Console.

Management Services for Administrators

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

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

- Configure CA certificates installation upon installation of ActivClient.

ActivClient can be deployed using software deployment technology:

- Microsoft System Center Configuration Manager 2007 SP1
- Microsoft Active Directory push (Windows Server 2008 and 2008 R2)

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

Upgrading

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

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.
- Can be managed locally using Administrative Templates.
- Can be viewed locally using the Microsoft Resultant Set of Policy console, accessed from the ActivClient User Console.

Smart Card Automatic Registration

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

Branding

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

Notification

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 (three beeps) 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
- The Expiration Warning message notifies users that their smart card or one of their smart card certificates is about to expire or has expired. 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 8 'modern' interface.
 - 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).

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.

Standalone / Mini Mode

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 ActivIdentity v1 applets.

- 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:

- ActivIdentity Smart Card 64 V2 (same as Oberthur CosmopolIC 64K V5.2)
- ActivIdentity Smart Card 64K V2c (same as Axalto Cyberflex Access 64K v2c)
- ActivIdentity Smart Card 80K v3.2 (same as Giesecke & Devrient SmartCafe Expert 80K DI v3.2)

- ActivIdentity Smart Card 144K v3.2 (same as Giesecke & Devrient SmartCafe Expert 144K DI v3.2)
- ActivIdentity ActivKey V2 64k (same as Axalto Cyberflex Access 64K V1 SM 2.1)
- ActivIdentity 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

Standalone 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:

- ActivIdentity Smart Card 64 V2 - ActivClient Profile (based on Oberthur CosmopolIC 64K V5.2)
- ActivIdentity Smart Card 64K V2c - ActivClient Profile (based on Axalto Cyberflex Access 64K v2c)
- ActivIdentity Smart Card 80K v3.2 - ActivClient Profile (based on Giesecke & Devrient SmartCafe Expert 80K DI v3.2)
- ActivIdentity Smart Card 144K v3.2 - ActivClient Profile (based on Giesecke & Devrient SmartCafe Expert 144K DI v3.2)
- ActivIdentity ActivKey V2 64k - ActivClient Profile (based on Axalto Cyberflex Access 64K V1 SM 2.1)
- ActivIdentity 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

AAA Server-Managed Mode

When 4TRESS 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 Administrator Console.
- 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 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).

Note

Smart card initialization requires ActivClient 6.2 on the machine hosting the 4TRESS AAA Server Administration Console.

ActivID CMS-Managed 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 Self Help Desk: My Digital ID Card. 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 Self Help Desk: My Digital ID Card.
- Users can reset the smart card completely using ActivID CMS.

Note

Some 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.

US Department of Defense Common Access Card 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 ["Smart Cards and USB Tokens" on page 28](#).

US Government PIV Mode

- Refers to PIV and PIV-I (PIV interoperable) cards compliant with NIST Special Publication 800-73-3
- Also refers to PIV-like cards: PIV interface, with additional flexibility in terms of card content and policies
- 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 ActivIdentity 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
- 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
- Safenet 400 PIV
- Sagem Orga J-ID Mark 64 PIV with Sagem PIV Applet version 01

Chapter 3: ActivClient Components

Chapter Contents

19	ActivClient Agent
20	User Console
24	PIN Initialization Tool
25	Advanced Diagnostics

This chapter describes the ActivClient components.

ActivClient Agent

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

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!



Smart card reader is empty



No smart card reader is present



ActivClient is starting up

ActivClient Agent Shortcut Menu Commands

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

TABLE 3.1: 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.
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.

User Console

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

You can	Action
Manage your digital certificates	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

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

TABLE 3.2: 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	<p>The right pane displays the content of the smart card. It provides access to:</p> <ul style="list-style-type: none"> • Smart Card Info • My Certificates • CA Certificates • One-time passwords • My Personal Info

FIGURE 3.1: Tasks View

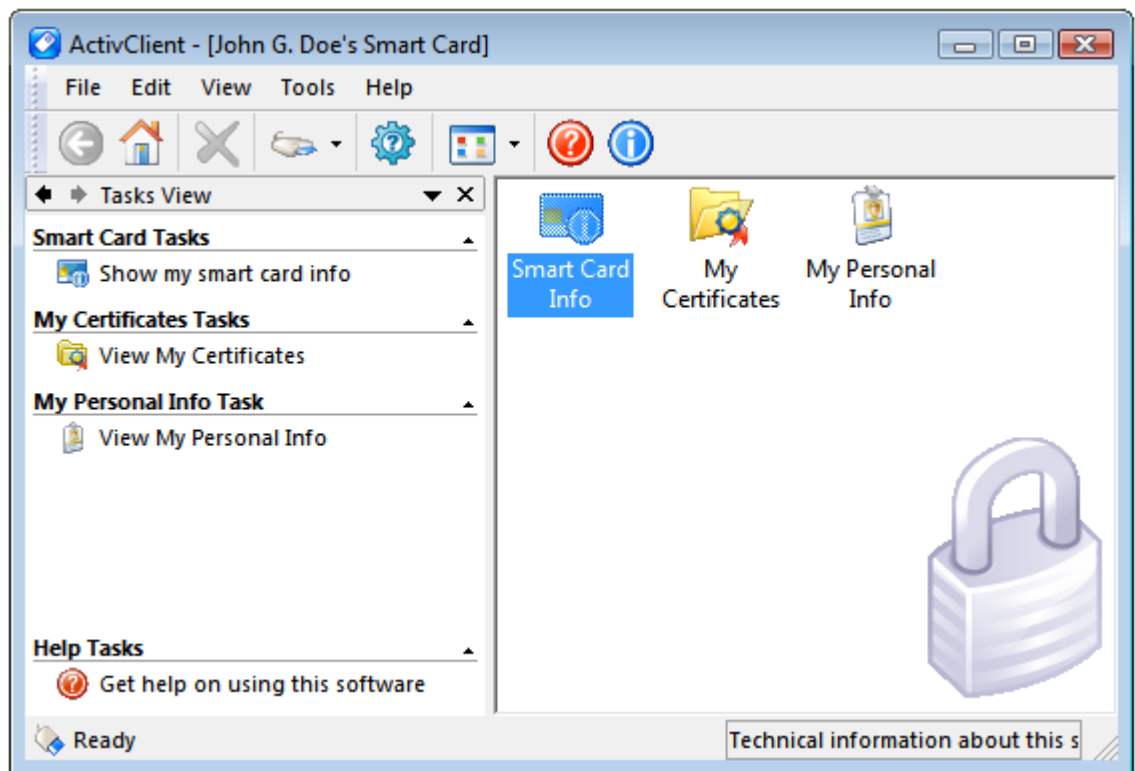
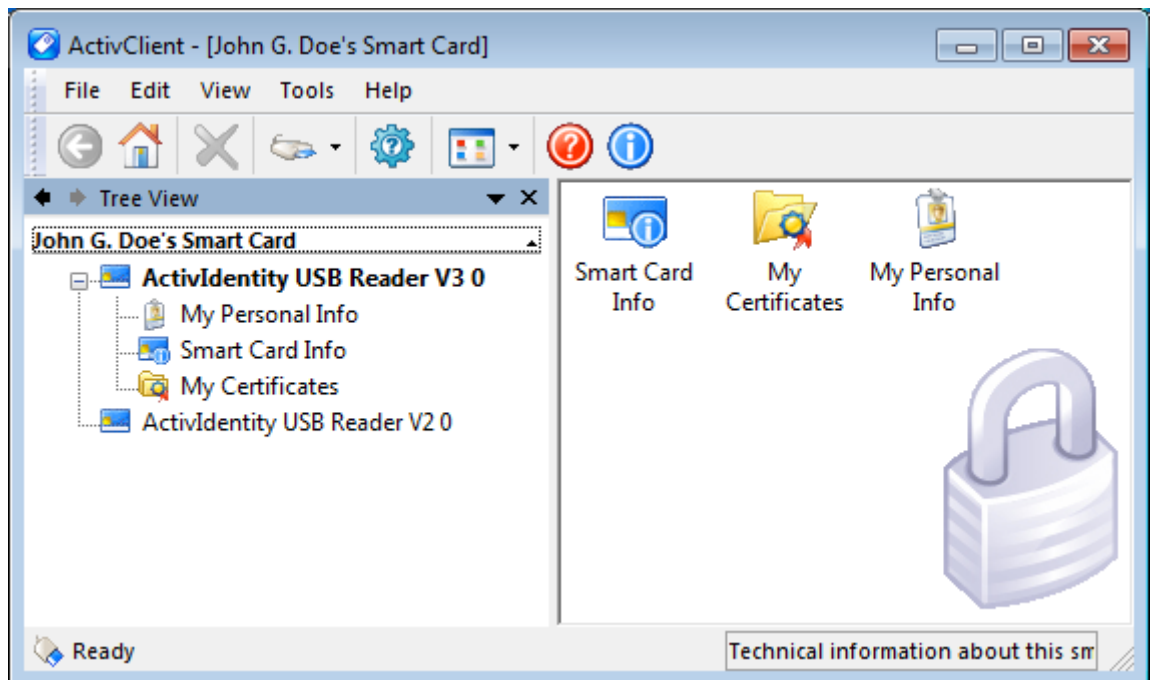


FIGURE 3.2: Tree View



Shortcut Menus

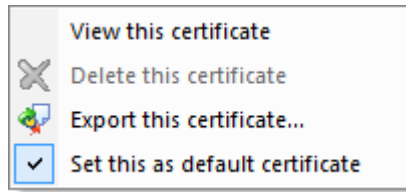
Right-clicking some elements in the User Console displays a shortcut menu that provides support for the most common tasks.

The displayed commands are different for each element.

Access Shortcut Menu Commands

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

FIGURE 3.3: User Certificate Right-Click Menu



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 3.4: Menu Toolbar

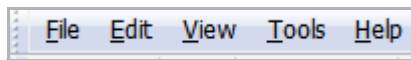


TABLE 3.3: Menus and Commands from the Menu Toolbar

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

Note

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

Menu	Command	Function	Keyboard shortcuts
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
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: <ul style="list-style-type: none"> 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

Standard Toolbar









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

FIGURE 3.5: Standard Toolbar



The following commands are available on the **Standard** toolbar:

TABLE 3.4: Standard Toolbar Commands

Button	Command	Function
	Back	Goes back to previous page
	Home	Goes to home page
	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	Provides user access to Online Help
	About	Displays information about ActivClient and the system

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

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 ["Standalone / Mini Mode" on page 15](#), 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 ["Standalone Mode" on page 16](#), 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.

Access the PIN Initialization Tool

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 Programs, ActivIdentity, ActivClient and select **PIN Initialization Tool**.

ActivClient - PIN Initialization Tool

ActivIdentity
ActivClient

Enter the PIN code you want to use and click Next to start the initialization process.

PIN code:

Confirm:

Your new PIN must meet the following conditions:

- ☒ Must contain at least 6 characters
- ☒ Must not exceed 25 characters
- ☒ Must not be weak or easy to guess (e.g. 1234)
- ☒ Must be correctly confirmed

ACTIV IDENTITY

< Back Next > Cancel

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.

Access the Advanced Diagnostics Tool

Users can access the Advanced Diagnostics Tool either:


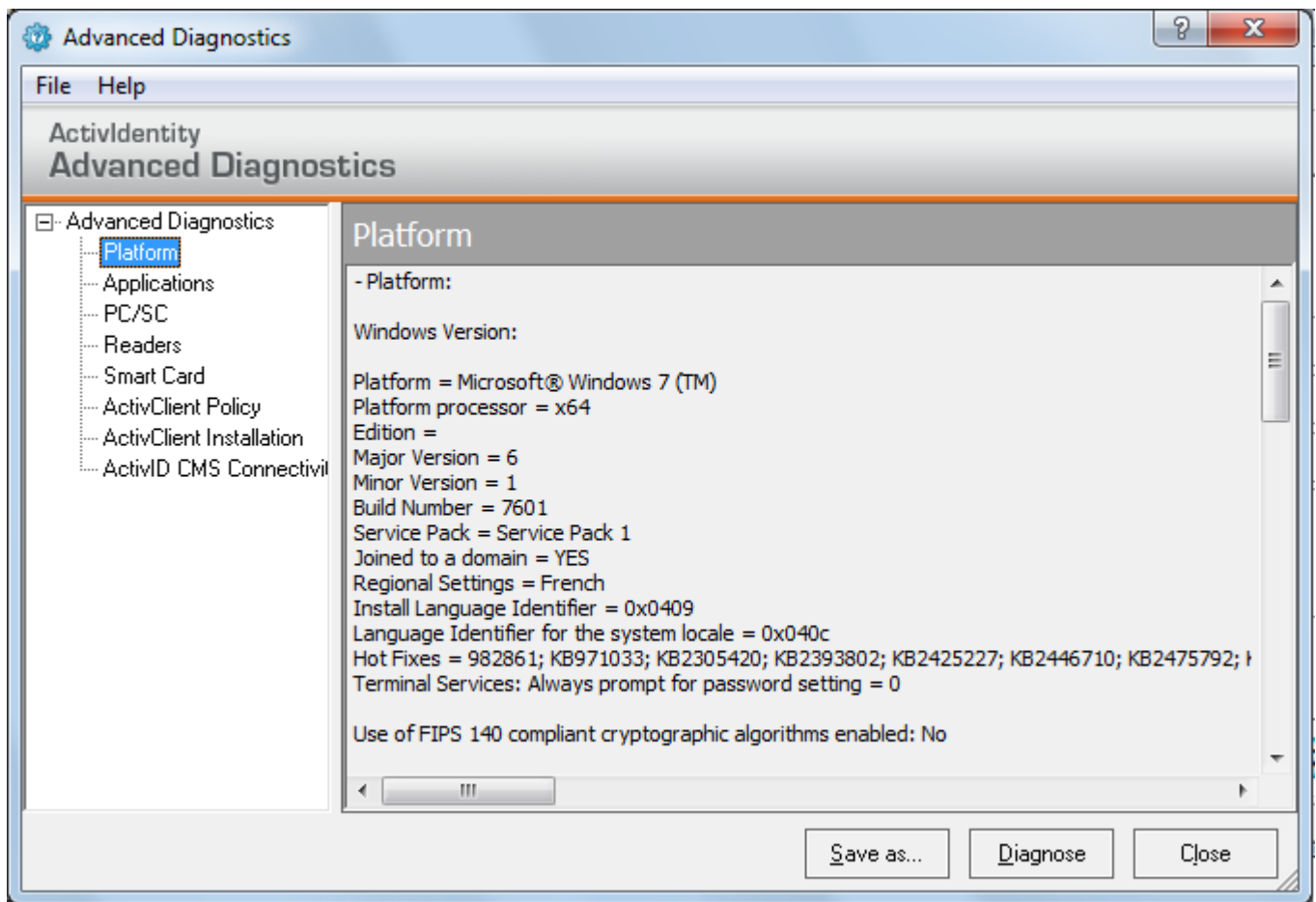
- From ActivClient Agent's left or right-click menu, select **Advanced Diagnostics**.
- From the User Console **Standard** toolbar, select **Advanced Diagnostics** .
- From the User Console **Help** menu, select **Diagnose**.
- From the **Start** menu, go to **Programs, ActivIdentity**, and select **Advanced Diagnostics Tool**.

FIGURE 3.6: Advanced Diagnostics Tool - Report Window


Chapter 4: Operational Environment

This chapter details the ActivClient operational environment.

Chapter Contents

27	ActivIdentity Identity Assurance
27	Operating Systems
28	Smart Cards and USB Tokens
30	Smart Card Readers

ActivIdentity Identity Assurance

ActivClient can be deployed in standalone mode. Combined with additional ActivIdentity products, it provides a fully comprehensive solution - the ActivIdentity's Identity Assurance solutions for Enterprise and for Government.

[Table 4.1](#) lists the compatible ActivIdentity products and their purpose.

TABLE 4.1: ActivIdentity Products

ActivIdentity Identity Assurance Components	Purpose
ActivClient	Smart card security client
ActivID Card Management System 4.1 SP1, 4.2, 4.2 SP1, SP2 and SP3 Note: On 64-bit platforms, the 'My Digital ID Card' component of ActivID CMS is only supported with version 4.2 and later.	Card Management System for smart card issuance and management services
4TRESS AAA Server for Remote Access 6.6 and 6.7	Authentication server
Desktop Validation Client 3.1	Plug-in for a Microsoft Windows-based computer to perform secure validation of digital certificates.
<ul style="list-style-type: none"> Validation Authority 5.5 (OCSP support) Path Builder 2.0 (OCSP support) Responder Appliance 3.1 (OCSP support) 	Secure certificate validation solution.

System Requirements

The minimum system requirements for ActivClient installation are:

- One of the supported [operating systems](#) listed below
- 64 MB of RAM
- 32 MB (ActivClient x86) to 55 MB (ActivClient x64) of free disk space

Operating Systems

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

- Microsoft Windows Vista SP2 (32 and 64-bit editions)
- Microsoft Windows 7 SP1 (32 and 64-bit editions)
- Microsoft Windows 8 (32 and 64-bit editions)

- Microsoft Windows Server 2008 including Server Core SP2 (32 and 64-bit editions)
- Microsoft Windows Server 2008 R2 including Server Core SP1 (64-bit edition)
- Microsoft Windows Server 2012 including Server Core (64-bit edition)

Virtualization Environments

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

- VMware® Workstation 6.5, 7.0 and 7.1
- VMware View v4

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 ["Smart Card Services and Profiles" on page 15](#).

Notes

- ActivID CMS supports several profiles per smart card type. For further information, see the ActivID CMS documentation.
- ActivID CMS supports smart card issuance with both ActivIdentity v1 applets and ActivIdentity v2 applets, including FIPS 140-2 Level 3 configuration with encrypted PIN.
- ActivClient supports 1024- and 2048-bit RSA keys on smart cards and USB tokens that support these cryptographic operations.
- Smart cards previously used with ActivCard Gold are supported with ActivClient - with the exception of ActivCard Gold profiles with the Match On Card functionality. Credentials not supported with ActivClient (that is, QuickFill/Single Sign On data) are ignored by ActivClient.

- ActivIdentity Smart Card 64K v1
- ActivIdentity Smart Card 64K v2
- ActivIdentity Smart Card 64K v2c
- ActivIdentity Smart Card 80 K v3.2
- ActivIdentity Smart Card 144K v3.2
- ActivIdentity ActivKey™ SIM
- ActivIdentity ActivKey 32K v2
- ActivIdentity ActivKey 64K v2
- ActivIdentity ActivKey Display v2
- Athena IDProtect Duo PIV
- Atmel 6464C Pro 64k
- CardLogix Credentsys-J PIV
- Gemalto Cyberflex Access 32K V2 #1
- Gemalto Cyberflex Access 32K V2 SM 7.2
- Gemalto Cyberflex Access 32K V4 SM 1.3
- Gemalto Cyberflex Access e-gate 32K
- Gemalto Cyberflex Access 64K V1 SM 2.1
- Gemalto Cyberflex Access 64K V1 Bio SM 3.1
- Gemalto Cyberflex Access 64K V1 SM 4.1
- Gemalto Cyberflex Access 64K v2a SM 2.3

- Gemalto Cyberflex Access 64K v2b SM 1.1
- Gemalto Cyberflex Access 64K v2c
- Gemalto Cyberflex Access 128K
- Gemalto GemXpresso 32K
- Gemalto GemXpresso PRO 64K FIPS v1 Dual ATR
- Gemalto GemXpresso PRO 64K R3 v1 Dual ATR
- Gemalto GemXpresso PRO 64K R3 FIPS V2
- Gemalto GemXpresso PRO R3 E64 PK - Standard Version
- Gemalto TOP DM GX4 72K (FIPS)
- Gemalto TOP DM GX4 72K (FIPS) Standard #1
- Gemalto TOP DM GX4 72K (FIPS) Standard #2
- Gemalto TOP IM GX4 72K (FIPS) Standard
- Gemalto TOP IM GX4 72K (FIPS) Standard Rev B
- Gemalto TOP DL GX4 144K FIPS
- Gemalto TOP DL GX4 v2 144K FIPS
- Gemalto TOP DL GX4 v2 144K FIPS with Gemalto PIV 1.55 applet
- Giesecke & Devrient SmartCafe 32K v1
- Giesecke & Devrient SmartCafe Expert 32K v2.0
- Giesecke & Devrient SmartCafe Expert 64K Non-FIPS
- Giesecke & Devrient SmartCafe Expert 64K FIPS-1024
- Giesecke & Devrient SmartCafe Expert 64K FIPS-2048
- Giesecke & Devrient SmartCafe Expert 80K DI v3.2
- Giesecke & Devrient SmartCafe Expert 80K DI v5.0
- Giesecke & Devrient SmartCafe Expert 144K DI v3.2
- Giesecke & Devrient SmartCafe Expert 144K DI v5.0
- Giesecke & Devrient Secure Flash Solutions Mobile Security Card
- HID Global Crescendo C800
- HID Global Crescendo C1100
- HID Global Crescendo C1150
- HID Global Crescendo JCOP 21 v2.4.1 R2 64K
- HID Global Crescendo JCOP 21 v2.4.1 R2 64K #2
- HID Global pivCLASS
- HID Global Secure MicroSD v2 80K – 1GB
- HID Global Secure MicroSD v2 80K – 4GB
- Keycorp MULTOS 64K with StepNexus PIV Application v4.2.1
- NXP JCOP31 v2.4.1 80K

- Oberthur Galactic 32K #1
- Oberthur Galactic 32K #2
- Oberthur CosmopolIC 32K V4
- Oberthur CosmopolIC 32K V4 Fast ATR
- Oberthur CosmopolIC 64K v5
- Oberthur CosmopolIC 64K V5.2
- Oberthur CosmopolIC 64K V5.2 Fast ATR
- 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 64K v5.4
- Oberthur ID-One Cosmo 128K v5.5
- Oberthur ID-One Cosmo v7.0 80K
- Oberthur ID-One Cosmo v7.0 Type A Standard 80K Dual
- Oberthur ID-One Cosmo v7.0 128K
- Oberthur ID-One Cosmo v7.0 Type A Large 128K Dual
- Oberthur ID-One PIV
- Safenet 400 PIV
- Sagem Orga J-ID Mark 64 PIV with Sagem PIV Applet version 01
- Sharp JCOP 31 ID

Smart Card Readers

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

HID Global/ActivIdentity Smart Card Readers

- USB Reader v2
- USB Reader v3
- PCMCIA Reader v1
- PCMCIA Reader v2
- ActivKey SIM and Display
- Serial Reader

Smart Card Reader Drivers

Drivers for the ActivIdentity and OMNIKEY readers are provided on the ActivClient distribution.

- Omnikey®:
 - 3021 USB
 - 3121 USB
 - 4040 Mobile PCMCIA
 - 4321 Mobile ExpressCard 54
 - 5121, supported in contact mode only
 - 5125 USB, supported in contact mode only
 - 5321 USB, supported in contact mode only
 - 6121 Mobile USB
 - 6321 USB

For Microsoft Windows platform compatibility and driver information, see the *ActivIdentity ActivClient for Windows Installation Guide*.

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).

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.

As an example, the following is a list of third-party readers compatible with ActivClient:

- Compaq® keyboard (with O2micro OZ773 rev A chip set)
- Dell®:
 - Inspiron 600m laptop with built-in reader (O2Micro O2711EC1 PCMCIA chip set)
 - Latitude D series laptop with built-in reader (O2Micro O2711EC1 PCMCIA chip set or O2Micro OZ77Cxx USB SmartCard Controller)
 - Latitude E series laptop with built-in reader (Broadcom controller)
 - Keyboard REV A03 with smart card reader
 - 104-Key USB Keyboard with smart card reader for Dell OptiPlex / Precision Workstations
- Gemplus®:
 - GemPC 430 (USB)
 - GemPC 432 (USB)
 - GemPC 433-SL, GemPC 433-SW (USB)
 - GemPC USB-SL reader
 - GemPC USB-SW reader

- Hewlett-Packard® keyboard (with SCM Microsystems SCR338-04 smart card reader)
- IBM® laptop with built in smart card reader
- KSI® 1451/ASC keyboard
- Precise™ Biometrics:
 - 100MC (USB)
 - 100MC BioKeyboard
 - 100 PC-Card MC (with SCM Microsystems SCR243 smart card reader)
 - 100XS swipe reader
 - 200MC (USB)
- Schlumberger® Reflex 20 PCMCIA reader
- SCM Microsystems:
 - SDI010 (dual interface) - supported in contact mode only
 - SCR331 (USB)
 - SCR3310 (USB)
 - SCR3311 (USB)
 - SCR3340 (ExpressCard)
 - SCR338-03 (bundled in keyboards)
 - SCR338-04 (bundled in keyboards)
 - SPR337 (with fingerprint sensor)

Appendix A: Terms and Acronyms

Appendix Contents

33	Terms
34	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.

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 Card Management System (CMS): Formally known as ActivCard Identity Management System (AIMS), CMS is a web-based, smart card, credential and application lifecycle management system. CMS augments and works in concert with an enterprise's primary identity management infrastructure components, including popular directory, database, and PKI components.

Cryptographic Service Provider (CSP): An independent software module that performs cryptography algorithms for authentication, encoding, and encryption.

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.

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): Is used to authenticate to your smart card in order to perform actions such as Windows PKI logon, remote access and email signature.

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.

Acronyms

CA: Certificate Authority

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

CSP: Cryptographic Service Provider

FIPS: Federal Information Processing Standard

GAL: Global Address List

GP: GlobalPlatform.
Replaces OpenPlatform (OP)

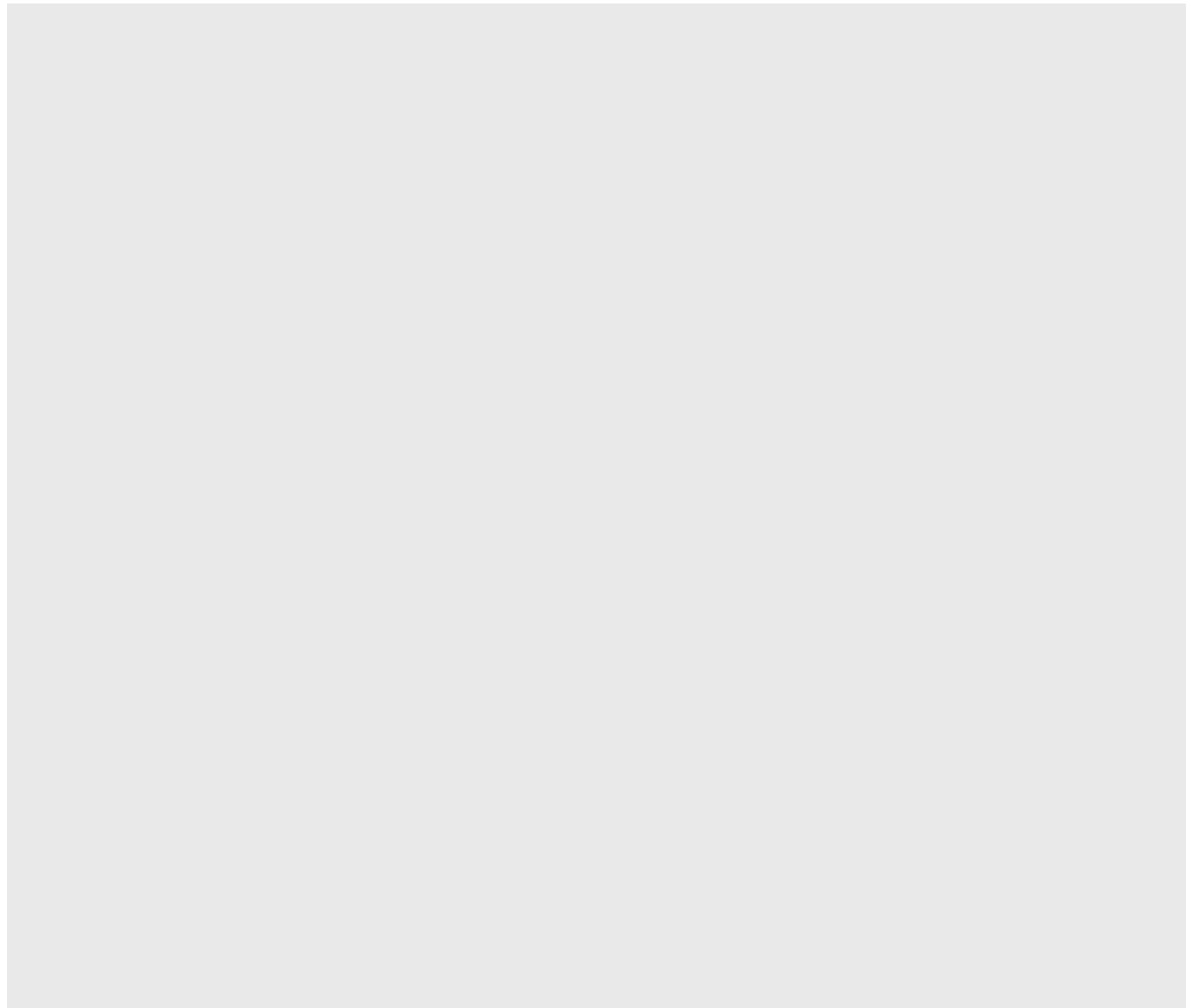
OTP: One-Time Password

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



Legal Disclaimer

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 3.9809.2892
Email info@actividentity.com
Web www.actividentity.com

Trademarks: ActivIdentity, ActivIdentity (logo), and/or other ActivIdentity products or marks referenced herein are either registered trademarks or trademarks of ActivIdentity in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of the ActivIdentity trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.