POC: Jason R. Heiger, Jason.r.heiger.civ@mail.com around 10 August 2011

Windows 7 64x AGM and Dual Persona's Outlook 2007, and 32Bit Mail Client

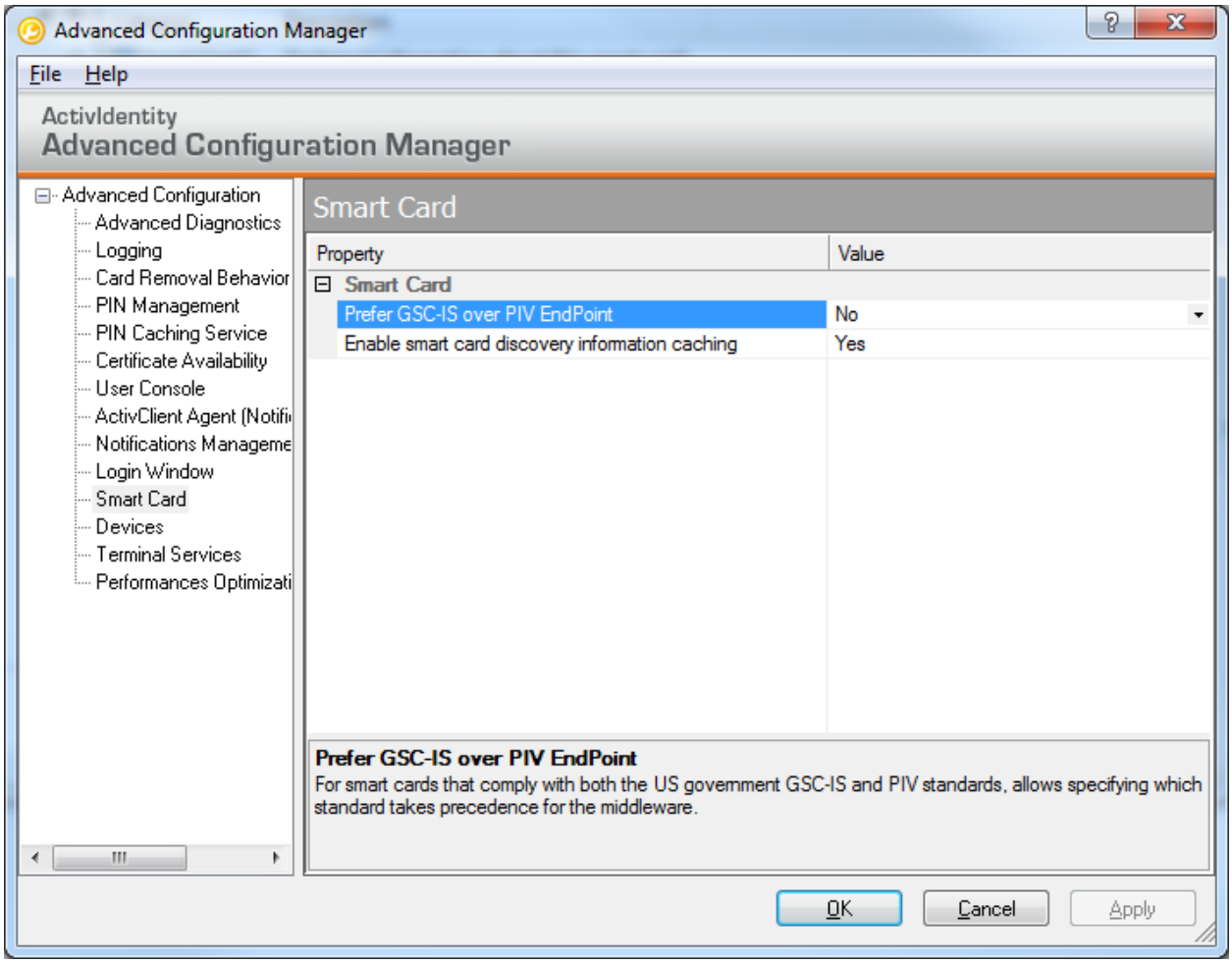
After much teeth gnashing, some articles on Militarycac.com, and some extra machines, It looks like I have found a fix for 64bit win 7 clients and dual persona's. This document assumes you have followed ALL DISA guidance and local DOIM guidance on patching Outlook, and extra registry entries for autodiscover, etc. It also assumes you have a dual persona, or your DISA mail account is registered the same as mine, which I assume is mapped to dual persona's since I had both a CTR and CIV account in mail.mil after I was migrated.

Active client has an update for 64 bit win 7 and vista clients that specifically addresses exchanging PIV certificates with 32 bit apps. A reference in the hotfix readme specifically addresses outlook and other programs using bult-in Microsoft cryptographic service providers.

See Addendum 1:

Identifier: #73641
Subject:
32bit application based on CSP fails to read all certificates on a x64 platform.
Technical Description:
A 32bit application based on CSP (such as Outlook 2007) fails to read all certificates on a x64 platform. The 32bit CSP wrapper was not managing properly PP_USER_CERTSTORE parameter of CPGetProvParam CSP function. PP_USER_CERTSTORE is now properly managed. This allows Outlook 2007 to retrieve read all certificates in the smartcard

Even with this update, outlook is still unable to connect. You will need administrative access, or a patch, to turn off the following setting in active client



Once this setting is changed from it's default of YES to NO, it will disable the implicit mapping of the smart card identity, and allow the user to specify the PIV cert properly. Once a restart is initied, make sure the user log's in with their std dod SCID (xxxxxxxxx@mil).

You should now be able to complete setup of the dual persona client without error.

Addendum 1:

ReadMe for ActivClient® Hot Fix FIXS1107012.msp

Version 6.2.0.124
Published on 2011-07-11

Table of Contents

1. Product

This Hot Fix applies to ActivClient 6.2 x64 and ActivClient CAC 6.2 x64. You can install it on top of ActivClient 6.2 (build number 50) or any later hot fix.

2. Hot Fix Information

This Hot Fix includes the following updated files:

- **N/A**

3. New Issues Corrected by this Hot Fix

Identifier: #75140
Subject:
Some settings are reset after hot-fix installation.
Technical Description:
Settings stored in HKLM\Software\Wow6342Node registry keys were not backuped/restored during hot-fix installation. These settings are now correctly backuped/restored.

4. Additional Issues Corrected by this Hot Fix

ActivClient Hot Fixes are cumulative.
This Hot Fix includes the following updated files that were included in previous Hot Fixes:

- **AcAdvCfm.exe** updated to version 8.2.0.30
- **ac.cardsync.dll** updated to version 6.2.1.30
- **acakd.dll** updated to version 3.2.0.19
- **acautoup.exe** updated to version 4.4.0.10
- **AcBcgPro.dll** updated to version 11.0.0.5
- **accrdsub.exe** updated to version 6.2.1.67
- **accrypto.dll** updated to version 3.1.0.15
- **accomacomx.exe** updated to version 5.1.0.6
- **accombsi21.exe** updated to version 5.1.0.9
- **accomcsp.exe** updated to version 5.1.0.12
- **accompiv.exe** updated to version 6.0.0.4
- **accompkcs.exe** updated to version 5.1.0.9
- **accsp.dll** updated to version 5.1.0.25
- **acevents.exe** updated to version 4.4.0.27
- **acexchex.dll** updated to version 6.2.1.8
- **acflex8.dll** updated to version 3.2.0.16

- **acflex16.dll** updated to version 3.2.0.16
- **acjavasc.dll** updated to version 3.2.0.27
- **acjscpiv.dll** updated to version 3.3.0.7
- **acjscpivext.dll** updated to version 3.3.0.8
- **acjsys.jar** updated to version 2.0.0.18
- **acjvscv2.dll** updated to version 3.3.0.6
- **ACMini-2011000000000000000000B9-HIDCrescendo80K.ini** new. version 6.2.1.5
- **ACMini-2011000000000000000000B9-GnD80K.ini** updated to version 6.2.1.4
- **ACMini-Blank- HIDCrescendo80K.ini** new. version 6.2.1.5
- **acpipint.jar** updated to version 1.10.64.9
- **acpivapi.dll** updated to version 6.0.0.2
- **acpkcs201.dll** updated to version 5.1.0.19
- **acpkcs201-en6.dll** updated to version 5.1.0.22
- **acpkcs201-ns.dll** updated to version 5.1.0.18
- **acpkcs211.dll** updated to version 5.2.0.4
- **ActivClient.chm** updated to version 6.2.0.5
- **Acuscons.exe** updated to version 6.2.1.76
- **acwpipint.dll** updated to version 1.10.64.9
- **aicfgreg.dll** updated to version 6.2.1.32
- **aiCOMMAPI.exe** updated to version 3.2.0.59
- **aijnipiv.dll** updated to version 5.1.0.5
- **aijnipiv.jar** updated to version 5.1.0.5
- **aipinch.exe** updated to version 6.2.1.27
- **aipinit.exe** updated to version 6.2.1.33
- **aipingui.dll** updated to version 6.2.1.41
- **aiwinext.dll** updated to version 1.5.0.19
- **aspcom.dll** updated to version 3.2.0.6
- **asphat32.dll** updated to version 3.3.0.7
- **bsi21classes.jar** updated to version 5.1.0.9
- **bsi21interf.jar** updated to version 5.1.0.9
- **jnibsi21.dll** updated to version 5.1.0.9
- **PersonalDataSnapin.dll** updated to version 6.2.1.24
- **xsi.jar** updated to version 4.4.0.6

Identifier: #73641
Subject:
32bit application based on CSP fails to read all certificates on a x64 platform.
Technical Description:
A 32bit application based on CSP (such as Outlook 2007) fails to read all certificates on a x64 platform. The 32bit CSP wrapper was not managing properly PP_USER_CERTSTORE parameter of CPGetProvParam CSP function. PP_USER_CERTSTORE is now properly managed. This allows Outlook 2007 to retrieve read all certificates in the smartcard.
Identifier: #74757
Subject:
Support of new card: HID Global Crescendo JCOP 21 v2.4.1 R2 64K.
Technical Description:
Card names and ATR have been added to the registry. These cards are now registered in the product. This card can be initialized with ActivClient.
Identifier: #74709
Subject:
Acpkcs211.dll reports version 5.2.0.4 while readme specifies 5.3.0.4 for build 120.
Technical Description:
There was a typo in hot-fix readme for build 120. Acpkcs211.dll version is 5.2.0.4. All files versions have been reviewed and checked.
Identifier: #74536
Subject:
Files created in RSA folder during a PKI login.

Technical Description:
For each ActivClient executable, a new entry is created in user's crypto folder at first card connection. ActivClient was using permanent keys. Now ActivClient used only ephemeral keys. This avoids creating unnecessary entries in user's crypto folder.
Identifier: #74528
Subject:
Need a custom BSI entry call to return change pin after first use flag value.
Technical Description:
gscXsiUtilGetForceChangePIN function has been added. This allows CMS to retrieve change pin after first use flag value.
Identifier: #74274
Subject:
NIST SP800-73-3 Retired Keys are not supported, which prevents issuance of a SP800-73-3 compatible profile with CMS 4.2 SP1.
Technical Description:
NIST SP800-73-3 Retired Keys has been implemented to allow issuance a SP800-73-3 compatible profile with CMS 4.2 SP1.
Remark:
Full support of NIST SP800-73-3 will be available in ActivClient 7.0.
Identifier: #74045
Subject:
Application like Cisco VPN may no more found certificates after extended hours of usage.
Technical Description:
ActivClient data cache distinguishes different connections to the smartcard by the application by using a random value computed at connection. The random was computed on a 0x7FFF value. If an application like Cisco VPN does a lot of connections, it may re-used a previously used value and does not retrieve correctly information in data cache. The random value is now computed with a UUID to avoid potential conflict.
Identifier: #73783
Subject:
PKCS C_DecryptInit failed with error CKR_KEY_FUNCTION_NOT_PERMITTED with some cards initialized by Entrust.
Technical Description:
Some versions of Entrust may initialize certificates with CKA_DECRYPT set to FALSE. This flag prevents ActivClient PKCS to use this certificate for decryption. To workaround Entrust behavior, ActivClient PKCS now ignores the flag CKA_DECRYPT set to FALSE if the certificate has PKI logon capabilities
Identifier: #74127
Subject:
ActivClient PKCS must retrieve PIV Objects present in the smartcard.
Technical Description:
ActivClient PKCS is now able to retrieve PIV Objects present in the smartcard. Updated header file and sample (exe and source code) are provided in this hot-fix.
Identifier: #73997
Subject:
Support of new card: Crescendo C800.
Technical Description:
Card names and ATR have been added to the registry. These cards are now registered in the product.
Identifier: #74005
Subject:
Auto-update does not work is installed build version is less than 100 and new build version is higher than 100.
Technical Description:
String comparison was performed instead of a number comparison; therefore build 115 was considered as less than 50 and no update was done. Comparison is now numerical.
Remark:

It is possible to install this hot-fix via ActivClient auto-update feature by setting version 6.2.0.99 in autoupdate.ini file on the server.

Identifier: #73972

Subject:

Unable to do a PKI logon with CAC cards V2 after installing version 6.2.0.114 or 115.

Technical Description:

Implementation of performance improvements (72706) engenders a regression with CAC cards V2: keyset is not properly recomputed at PKI logon. This regression has been corrected.

Identifier: #73756

Subject:

ActivClient jar files have expired signature.

Technical Description:

All jar files have been rebuild with new ActivIdentity certificate.

Identifier: #73544

Subject:

Unable to unlock workstation after updating PIV cards from 1024 to 2048bits certificates.

Technical Description:

For performance improvement, ActivClient stores information of the smartcard in registry. In this case, upgrade from 1024 to 2048bits certificate, ActivClient was trying to use 1024bits certificate instead of 2048 and this may generate unexpected behavior such as a crash of ActivClient at workstation unlock. ActivClient now reads certificate length in the certificate itself instead of registry to ensure using always the appropriate one.

Identifier: #72706

Subject:

Standard V2 and PIV+ smartcard have poor performance.

Technical Description:

At each insertion, ActivClient reads information in the card. The time needed to perform this operation is long with Standard V2 and PIV+ smartcard. Reading information process at card insertion has been improved by avoiding try to read unnecessary information (like content of empty PKI containers…) and read the full content of each certificate in one call instead of multiple calls reading only part of it. The performance improvement depends on the smartcard content; it can be up to 30% at each card insertion.

Identifier: #73406

Subject:

Smartcard Auto-Update failed with default CMS Synchronization Manager Timeout.

Technical Description:

The CCM API used to check if update is necessary is expecting timeout defined in milliseconds but ActivClient was using seconds. ActivClient now converts seconds in milliseconds before using CCM API.

Identifier: #73131

Subject:

PKCS#11 API creates 2 public keys for the same certificate.

Technical Description:

Using PKCS#11 API, 2 public key objects are created when creating first CKO_PUBLIC_KEY, then CKO_PRIVATE_KEY and CKO_CERTIFICATE objects (remark: There is no problem if private key object is created first). ActivClient PKCS has been modified to avoid creating twice the public key object in this case.

Identifier: #72879

Subject:

Automatic emails decryption fails with some E-mails.

Technical Description:

For some emails, the encrypted attachment is not formatted as expected by ActivClient automatic emails decryption. The algorithm has been modified to correctly detect such attachment.

Identifier: #73084

Subject:

Custom application based on ActivClient CSP fails with error ‘Not enough memory’.

Technical Description:

Due to Citrix corrections (see below issue #71737), connections to the card may be not freed and may engender errors in CSP based applications. In order to avoid such limitation, Citrix workaround can now be configured by registry key.
The new setting registry key is defined as below:

- Path = HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\CSP.
- Type = DWORD.
- Name = EnableCitrixOptimization.
- Value:
    - If value = 0 or registry key is not present, the Citrix optimization workaround is not used.
    - If value is not null, the Citrix optimization workaround is used.

Remarks:

- The registry key must be set to 1 only on Citrix server where issue #71737 occurs.
- The registry key is not set by the hot-fix.

Identifier: #72988
Subject:
Support of new cards: Giesecke & Devrient SmartCafe Expert 80K and 144K DI v5.0.
Technical Description:
Card names and ATR have been added to the registry. These cards are now registered in the product.
Identifier: #72546
Subject:
Hang during desktop's smart card unlock because another application is displaying PIN prompt dialog box.
Technical Description:
If a CSP-based application is prompting for PIN and workstation is or is being locked, it is not possible to unlock the workstation until card is removed. To avoid this hang, the PIN dialog box is now closed when workstation is locked.
Identifier: #72831
Subject:
Unable to initialize standalone V2 cards with PKCS#11 C_InitToken function.
Technical Description:
ActivClient was not reading properly standalone information when initializing a standalone V2 card. This was preventing to initialize such cards with PKCS#11 C_InitToken function. The flag is now properly retrieved.
Identifier: #72872
Subject:
Signature with a PIV card may fail if another application is accessing to the card at the same time.
Technical Description:
If another application is accessing to the PIV card just before a signature, the PIN is lost and signature fails. PIN is no more lost in this case.
Identifier: #72574
Subject:
OCS PIV 2.3.2 card with a PIN locked is not viewed as a PIN locked card.
Technical Description:
ActivClient now supports OSC 2.3.2 card which returns 63C0 instead of 6983 when card is locked.
Identifier: #72607
Subject:
PIV API: pivPutData fails if pivGetData was called on a PIN protected data since Admin authentication.
Technical Description:
To be compatible with SP 800-73-2, ActivClient no longer does internal logouts when called by PIV API, in order not to lose Admin authentication.
Identifier: #72552
Subject:
PIV API: pivCrypt function does not set output buffer length on success.
Technical Description:
To be compatible with SP 800-73-2, pivCrypt function now set output buffer length in all cases.

Identifier: #72553
Subject:
PIV API: pivCrypt fails with error 9B 03.
Technical Description:
To be compatible with SP 800-73-2, pivCrypt now distinguishes local and global PIN.
Identifier: #72508
Subject:
PIV API pivGetData: the middleware is expected not to strip 7E since it is a standard inter-industry tag as opposed to 53 which is a non standard tag.
Technical Description:
To be compatible with SP 800-73-2, pivGetData function no more strips 7E tag of DiscoveryObject.
Identifier: #72172
Subject:
32bit application crashes when unloading ActivClient PKCS dll on x64 machine.
Technical Description:
When an x86 application unloads the ActivClient PKCS dll on x64 machine, a thread was not correctly terminated. ActivClient x64 wrapper was crashing. The x64 wrappers have been corrected to properly terminate threads.
Identifier: #71737
Subject:
Citrix session freezes but releases upon smartcard removal.
Technical Description:
As Citrix wfica32.exe is mono-threaded for smartcard redirection, system may hang when reading smartcard with ActivClient. Workarounds have been implemented in ActivClient to avoid Citrix issue.
Identifier: #72016
Subject:
No more able to perform smart card logon - "Error: Impossible to get card properties" in ActivClient diagnostic.
Technical Description:
In rare conditions, removing the smartcard when ActivClient is using it may prevent to use the card. Removing the smartcard during some operations leaves ActivIdentity applets v2.x in an unstable state. A workaround has been implemented in ActivClient to restore correct state in applets.
Identifier: #64835
Subject:
Compliance with NIST SP 800-73-2.
Technical Description:
ActivClient PIV API has been updated to comply with NIST SP 800-73-2.
Identifier: #71808
Subject:
PIN Initialization Tool fails (unknown error) with G&D SmartCafe Expert 80K DI v3.2.
Technical Description:
G&D SmartCafe Expert 80K DI v3.2 have not the expected pre-issuance state. PIN Initialization Tool configuration files have been updated to be in concordance with manufacturer configuration.
Identifier: #71851
Subject:
Warning message for Smartcard Certificate/Outlook Account e-mail address mismatch dialog box title is confusing.
Technical Description:
Warning message for Smartcard Certificate/Outlook Account e-mail address mismatch has been improved (see #65307) but the title still refers only to publish to GAL. Title is now “ActivClient - Outlook Usability Enhancements”.
Identifier: #63286
Subject:
Outlook Security Profile configuration and publish to GAL does not work with Outlook 2010.
Technical Description:

Outlook Security Profile registry keys have been changed in Outlook 2010, this was preventing ActivClient to retrieve information for Outlook Security Profile configuration and publish to GAL. ActivClient is now able to retrieve Outlook Security Profile information for Outlook 2010 and previous versions.

Limitation:

“Automatically add sender’s certificate to Outlook Contacts” and “Automatically decrypt encrypted emails” are not operational with Outlook 2010.

Identifier: #71691

Subject:

When using the Mozilla Jarsigner tool, the certificate chain is not retrieved and is not added to the signature.

Technical Description:

Correction done on ActivClient 6.1 SP2 was not properly reported in 6.2. This has been corrected.

Identifier: #65307

Subject:

Unexpected Publish to GAL message received with AutoPublish to GAL disabled.

Technical Description:

“Allow Name Mismatch” setting is used for both “Publish to GAL” and “Setup Email Certs on Card Insertion”. To avoid asking the question twice to the user (1 for Outlook profile and 1 for Publish to GAL), there is only one message (message for Publish to GAL). Unfortunately, in some configuration (PublishtoGal=0, AutoRegOutlook=1 and AllowNameMismatch=1), the message may be confusing (Publish to GAL instead of Outlook Security profile). The message is now more generic: “ActivClient is about to use your smart card certificates to update your Outlook security profile and/or the Exchange Global Address List. However, your smart card certificates do not match your Outlook account…”.

Identifier: #65532

Subject:

Support of new cards: Gemalto TOP DL GX4 v2 144k FIPS with Gemalto PIV 1.51 applet and Oberthur ID-One Cosmo v7.0 with Oberthur PIV Applet Suite 2.3.2.

Technical Description:

Card names and ATR have been added to the registry. These cards are now registered in the product.

Identifier: #71580

Subject:

Unexpected PIN prompt when disconnecting user from SecurityBOX.

Technical Description:

With cards where CKO_DATA objects are not PIN protected except for the static unlock code, ActivClient may prompt for PIN when PKCS#11 C_FindObjectsInit is called. ActivClient PKCS#11 includes an optimization to avoid search of unlock code at each C_FindObjectsInit call. This optimization was not working if “Never display the Unlock Code again” option is checked. ActivClient has been improved to avoid read “Never display the Unlock Code again” option at each C_FindObjectsInit call if the option is checked.

Remark:

This avoid the issue as the card does not contain other PIN protected CKO_DATA object. If the card has other PIN protected CKO_DATA objects, ActivClient will prompt for PIN. In this case, SecurityBOX has to change its implementation to ensure PIN is presented to the card before calling C_FindObjectsInit.

Identifier: #64845/#65068

Subject:

Cisco AnyConnect client crashes when trying to get access to the certificate.

Technical Description:

When Cisco AnyConnect client (x86 process) tries to retrieve the certificate information, it used some NULL parameters. ActivClient x64 CSP wrapper was crashing with such data. The CSP wrapper now accepts NULL parameters.

Identifier: #65129

Subject:

SDK: potential deadlock if there was an error while opening a global transaction.

Technical Description:

After code review, a potential deadlock has been detected that occurs if there was an error while opening a global transaction. In case of error, the mutex is now always released.
Identifier: #65011
Subject:
Section 508 compliance: PIV information fields have no name.
Technical Description:
Microsoft Inspect Objects shows that PIV information fields have no name. Dynamically created windows now have names.
Identifier: #64820
Subject:
accrdsub.exe process hangs during the log off sequence.
Technical Description:
In order to empty the PIN cache, ActivClient retrieves the list of all present cards. To retrieve these cards, ActivClient reconnects to the cards. This operation may take time with Citrix/RDP remote sessions on slow networks (satellite, UMTS…). The algorithm to empty the PIN cache at logoff has been improved to avoid connecting to the card.
Identifier: #64812
Subject:
Enhancement Request: New Policy to have the option not to clear the PIN from the PIN cache when the screen locks. This is a Low Security policy.
Technical Description:
It is now possible to avoid ActivClient to clear the PIN from the PIN cache when the screen locks by adding manually the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\GlobalConfig\DisableClearPinAtWorkstationLock (DWORD) = 1.
Setting this policy to 1 reduces the security of the smart card deployment; ActivIdentity therefore recommends keeping the default policy to clear the PIN from the PIN cache when the screen locks.
Remarks:

- If the registry key is not present or equal to 0, the standard behavior occurs (PIN cleared from cache on workstation lock).
- It is necessary to reboot after modifying this setting.
- This setting is not compatible with lock on card removal.

Identifier: #64409
Subject:
Cannot access smart card with Broadcom contactless reader.
Technical Description:
The new setting to configure the T0 / T1 Communications Protocol (see #63961/# 63694) was not taken into account during the card discovery; T0 protocol was always tested first. This was preventing reading card information for a T1 protocol contactless card.
Identifier: #64693
Subject:
Section 508 compliance: Form fields for changing a user PIN do not expose the name, role and state of the fields.
Technical Description:
Using a tool like JAWS (http://www.freedomscientific.com/products/fs/jaws-product-page.asp), texts were not read on PIN Change Tool. The GUI of PIN Change Tool has been fully reviewed to be compatible with screen reader software.
Identifier: #64767
Subject:
Section 508 compliance: Tab order is not correct for PIV card holder info screen.
Technical Description:
PIV card holder fields are not read by screen reader software. The TAB key was not properly managed on this screen. TAB key order is now properly set.
Identifier: #64188
Subject:
Need ability to customize the PIN length max for PIV cards.

Technical Description:
ActivClient already has a policy (undocumented) to customize the PIV minimum PIN length: HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\PIVEPMinPinLen. In order to enforce a 6-digit PIV maximum PIN length, a similar key for the Max PIN length has been added: HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\ActivClient\ASPH\PIVEPMaxPinLen.
Remarks:

- If set to a value higher of 8, it is ignored and the default value 8 is used.
- If the card has been inserted before setting these registry keys, it is necessary to do a "Forget state for all cards" to force reading the new values.

Identifier: #64120
Subject:
ActivClient does not display the personal data from a Gemalto PIV card when no fingerprint information is stored on the card.
Technical Description:
ActivClient User Console was not displaying personal data if some information was missing on the card. User Console now displays PIV personal data even if incomplete.
Identifier: #63961/# 63694
Subject:
Enhancement Request: T0 / T1 Communications Protocol Test Order Configuration.
Technical Description:
See ActivClient readme: If you use smart cards supporting only the T=1 protocol (that is do not support the T=0 protocol), you will see error messages in the event viewer, such as "Smart Card Reader 'ActivCard ActivCard USB Reader C2 0' rejected IOCTL SET_PROTOCOL: The request is not supported." These errors are due to ActivClient attempting a T=0 connection before using a T=1 connection. Such errors can be ignored.
It is now possible to configure the default protocol by setting the following registry key: HKLM\Software\ActivCard\ActivClient\ASPH\DefaultCardProtocol (DWORD).

- If key not present (or value = 0), then ActivClient starts with T=0, then goes to T=1 if failure.
- If key present (value = 1), then ActivClient starts with T=1, then goes to T=0 if failure.

Remark: This key is not available in the Advanced Configuration Manager. This key is not set by the hot-fix, it is necessary to create it manually.
Identifier: #63890
Subject:
Differences in letter capitalization between the same email address are being recognized as different by ActivClient during Publish to GAL.
Technical Description:
Conforming to RFC 2821, ActivClient was treating the email address as case sensitive. As many systems allow case insensitive email addresses, ActivClient now makes the email address comparison case insensitive.
Identifier: #63940
Subject:
Roaming profile issues when using Citrix XenDesktop.
Technical Description:
In the customer configuration, Citrix smartcard redirection fails with SCARD_F_INTERNAL_ERROR error. This error was badly managed in ActivClient and the smartcard connection was badly reset when reconnecting the Citrix session.
Identifier: #63748
Subject:
SDK: BSI gscBsiPkiGetCertificate function returns compressed certificate with a PIV+ card.
Technical Description:
BSI gscBsiPkiGetCertificate function was returning the compressed certificate with a PIV+ card. The function now returns the uncompressed certificate.
Identifier: #63329
Subject:
PKCS: C_GetAttributeValue: ulValueLen contains value length instead of -1 when function returns CKR_BUFFER_TOO_SMALL.

Technical Description:
PKCS standard specifies that ulValueLen must be equal to -1 if buffer is too small. A correction to avoid issue with NULL pointer was introducing a regression.
Identifier: #62875
Subject:
ActivClient prompts for PIN even with isCKF_PROTECTED_AUTHENTICATION_PATHsupported = 0.
Technical Description:
For security reason, the PIN is cleared from cache when workstation is locked. After unlocking the workstation, a PKCS#11 call that requests a PIN protected operation (such as a digital signature) prompts for the PIN. If isCKF_PROTECTED_AUTHENTICATION_PATHsupported is set to 0, the ActivClient PIN prompt was displayed. This was not the expected behavior as the PIN prompt is supposed to be managed at the application level. After correction, the call to PKCS#11 function returns CKR_USER_NOT_LOGGED_IN and the calling application is in charge of calling the C_Login function.
Identifier: #62859
Subject:
Windows Smart card logon failing - ActivClient unable to locate the appropriate logon certificate on the smart card.
Technical Description:
A certificate can be automatically selected by default if it has one of the following key usages: smartcard logon, enrollment agent or EFS. If multiple certificates are electable, the first one found was used. Now, the selected certificate is chosen with the following priorities:

1. SmartcardLogon && Enrollment Agent && EFS
2. SmartcardLogon && Enrollment Agent
3. SmartcardLogon && EFS
4. SmartcardLogon
5. Enrollment Agent && EFS
6. Enrollment Agent
7. EFS

Identifier: #62671
Subject:
Selected view style in User Console is not persistent.
Technical Description:
When opening User Console, the view style was always “Large Icons”. Now, the last selected view is memorized and used when opening again the User Console.

The value is stored in registry key HKEY_CURRENT_USER\Software\ActivCard\Acuscons\ViewStyle (DWORD) with values:
1 = Large Icons
2 = Small Icons
3 = List
4 = Details
- If the value does not exist, the default value (1) is used.
- If the value exists, it is read at launch of User Console and appropriate view style is set.
- When the user changes the view (via menu), the registry key is updated with new value.
=> The view style is persistent.
Identifier: #62608
Subject:
SDK: C_Digest returns CKR_BUFFER_TOO_SMALL instead of CKR_OK if buffer is NULL.
Technical Description:
C_Digest function was not compliant with the PKCS#11 standard. C_Digest now uses the convention described in PKCS#11 Section 11.2 on producing output.

> **11.2 Conventions for functions returning output in a variable-length buffer**
> If *pBuf* is NULL_PTR, then all that the function does is return (in **pulBufLen*) a number of bytes which would suffice to hold the cryptographic output produced from the input to the function. This number may somewhat exceed the precise number of bytes needed, but should not exceed it by a large amount. CKR_OK is returned by the function.

Identifier: #62239
Subject:
Deadlock during a PKI logon with ActivIdentity Authentication Client and ActivIdentity SecureLogin Single Sign-On.
Technical Description:
In some rare conditions, ActivIdentity SecureLogin Single Sign-On may hang due to a hang in ActivClient: When a process accesses the card at the same time as another process using CAPI, there may be a deadlock between mutex when calling CAPI and smartcard transactions. Connection to the card is no more done during a transaction; this avoids a deadlock when CAPI is called.
Identifier: #62166
Subject:
Support of new cards: NXP JCOP31 V2.4.1 80K, Oberthur ID-One Cosmo v7.0-a Standard 80K Dual, Oberthur ID-One Cosmo v7.0-a Large 128K Dual, Gemalto TOP IM GX4 72K (FIPS) Standard and Oberthur ID-One Cosmo 128K v5.5 #2.
Technical Description:
Card names and ATR have been added to the registry. These cards are now registered in the product.
Identifier: #62089
Subject:
"Auto-request return receipt for outgoing emails" modifies also "Delivery Receipt".
Technical Description:
There was a confusion in Outlook settings and "Auto-request return receipt for outgoing emails" was modifying both "Request S/MIME receipt for all S/MIME signed messages" and "Tools-Options-Preferences-Email Options-Advanced Options-Delivery Delivery Receipt". ActivClient no longer changes "Delivery Receipt" setting.
Identifier: #62058
Subject:
Prompted twice for the PIN when making a VPN connection right after Windows logon.
Technical Description:
Using ActivIdentity Authentication Client and Cisco VPN, the user is prompted twice for the PIN when making a VPN connection right after Windows logon. If an application was checking if the PIN is already checked when PIN prompt dialog box is already opened, the checking function was returning immediately with “PIN not checked”; therefore the second application is asking again for the PIN. Now, the function that checks if the PIN is already verified waits until the PIN dialog box is closed.
Identifier: #61925
Subject:
SDK: PKCS C_SetAttributeValue function allows reverting CKA_SENSITIVE to FALSE and CKA_EXTRACTABLE to TRUE.
Technical Description:
ActivClient PKCS#11 was not compliant with PKCS#11 standard: a secret key object’s CKA_SENSITIVE attribute can be changed from CK_FALSE to CK_TRUE, but not the other way around. PKCS#11 now prevents reverting CKA_SENSITIVE to FALSE and CKA_EXTRACTABLE to TRUE for secret key objects.
Identifier: #61860
Subject:
ActivClient User Console does not display SHA-256 as the signature algorithm and instead still shows the numeric representation (1.2.840.113549.1.1.11).
Technical Description:
ActivClient User Console was not converting OID 1.2.840.113549.1.1.11 in text readable format. It is now done for SHA-256, SHA-384 and SHA-512 OID.
Identifier: #62049
Subject:
CMS 4.2 Card Issuance fails with V2 profiles.
Technical Description:
After checking access rights, a PKI applet was not explicitly selected. A signature may be done with an inappropriate applet. ActivClient now explicitly selects appropriate PKI applet after checking access rights.

Identifier: #61574
Subject:
Unable to see SHA256 algorithm when using an Entrust certificate signing a document with Entrust Entelligence Security Provider v8.
Technical Description:
A first version of ActivClient CSP supporting SHA256 was included in ActivClient 6.2. This implementation was not correct and has been improved to properly support the SHA256 algorithm.
Identifier: #61634
Subject:
Deadlock in ActivClient CSP when removing the card during CPAcquireContext.
Technical Description:
If the smart card is removed during a call of CSP CPAcquireContext, ActivClient may hang. A transaction in CSP may be released twice that was breaking low level transactions. Transactions in CSP are no more released twice.
Identifier: #61706
Subject:
Cannot use Digital Signing Certificate through ActivClient to sign PDF documents in Adobe Acrobat 9.2.0.
Technical Description:
Adobe Acrobat 9.2.0 is using the SHA256 algorithm for signature (as opposed to Adobe Acrobat 9.0.0 that uses SHA1). SHA256 is now properly supported (see #61574).
Identifier: #61783
Subject:
Error message when installing FIXS0911000 if Outlook is not installed.
Technical Description:
A new setting for Outlook was added in the previous hot-fix. Windows Installer determines that the Outlook feature has been changed and forces the installation even if Outlook is not installed. The hot-fix now forces REINSTALL=ALL REINSTALLMODE=omus to reinstall only the previously-installed features. Remark: if REINSTALL and/or REINSTALLMODE are set in a command line, the hot-fix uses the command line value instead of forcing the values.
Identifier: #60578
Subject:
When a certificate is being published to GAL, a PIN prompt may appear (depending on the use case and PIN cache policies); this PIN prompt is not explicit enough.
Technical Description:
When inserting a card, a PIN prompt may appear in order to publish certificate to GAL. The dialog box may surprise the user, who may cancel the PIN prompt, which will prevent the Publish to GAL to complete. The PIN prompt dialog box is now more explicit.
Identifier: #60691
Subject:
Outlook Profile Update does not support a configuration where the certificate email and the Exchange email do not match.
Technical Description:
ActivClient 6.2 performs a check to make sure that the smart card certificates used to configure the Outlook profile (and also published to the GAL) are associated to the current Outlook user. Specifically, the following check is performed (as described in ActivClient Administration Guide page 145):

> The certificate email address corresponds to the email address configured for the Exchange account. The comparison is performed by retrieving the email address in the certificate from the subjectaltName attribute, or if missing, from the “E=” value in the subject attribute. On the Exchange side, the comparison is performed by checking all email addresses defined in the Exchange account (prefixed by “SMTP:” or “smtp:”). This allows supporting email aliases.

This design does not address the scenario where some users have a legitimate email address (Outlook account) different from the address used on their smart card. Note that these scenarios require an Outlook configuration change (SuppressNameChecks), documented at http://support.microsoft.com/kb/276597.
To support this scenario, a new ActivClient policy is created: HKLM\Software\GSC\Cryptography\Certificate Registration\ActivCard\Outlook\AllowNameMismatch.

If this policy set to No = 0 (the default option) or does not exist, ActivClient performs the name check.

- If the email addresses match, it proceeds with updating the Outlook profile / publish to GAL.
- If they do not match, then ActivClient does not update the Outlook profile / does not publish to GAL.
- This configuration is recommended for most deployments (deployments where Outlook also performs a name check), to guarantee that only the certificates associated to the "correct" user are published in Outlook and the GAL.

If set to Yes = 1, ActivClient performs a name check. Then,

- If the email addresses match, it proceeds with updating the Outlook profile / publish to GAL.
- If they do not match, then ActivClient continues to check if Outlook / the GAL need to be updated.
    - If no update is needed (i.e. the card certificates are already used to configure Outlook / published to the GAL), then no action is performed.
    - If an update is needed, then ActivClient prompts the user by presenting the email addresses configured in Exchange and the email address used in the smart card certificate. The user then makes an informed decision on whether to proceed with updating the Outlook profile / publish to GAL.
- This model is applicable to customers who configure Outlook with SuppressNameChecks.

An updated ActivClient Administrative Template is also available with this new ActivClient policy.

Identifier: #61374

Subject:

SDK: Crash of the PKCS#11 library if multiple readers are plugged in.

Technical Description:

If multiple readers are plugged in and the calling application does multiple C_Initialize/C_Finalize PKCS#11 calls, the application may crash during the C_Finalize.

Identifier: #61286/#61421

Subject:

PKCS#11 fails to use a private key in CAC cards used in PIV Transitional mode. This leads to issues with applications using the PKCS#11 library, such as Firefox or Thunderbird.

Technical Description:

ActivClient attempts to read the content of the buffers referenced in the CCC (Card Capability Container), as defined in the GSC-IS v2.1 specifications. Some of these buffers are used for backwards compatibility and are in v1 format, instead of the expected v2 format – which led to the issue. ActivClient now ignores these buffers.

Identifier: #60182/#60183/#60200/#60201/#60202/#60203/#60282/#60283

Subject:

Accessibility (Section 508 compliance) improvements in User Console: Support of Task Pane.

Technical Description:

ActivClient has been rebuilt using an updated version of the user interface framework supporting accessibility for Task Pane.

Identifier: #60654

Subject:

Card slot number increments within Entrust Desktop Solutions.

Technical Description:

To solve an issue when a reader is unplugged then re-plugged, PKCS slot ID was incremented when re-creating slot list. The slot ID was also incremented when creating the list after a C_Finalize and C_Initialize. Slot ID is now reset to 0 during a C_Finalize but still incremented on a unplug/plug of reader before C_Finalize. This solves the issue and keeps behavior on reader unplug.

Identifier: #60739

Subject:

ActivClient locks the workstation after wakeup of Fargo Printer.

Technical Description:

Reader list is badly recomputed after Fargo Printer wakeup (readers information are not fully available when trying to find available readers). This has been corrected by trying again to re-compute the list when an error occurred on first building of the list.

Identifier: #60808

Subject:

User console crashes with Atmel 6464C Pro 64K.
Technical Description:
User Console and PIN initialization tool was accessing to non initialized memory when using profile defined for Atmel 6464C Pro 64K card. Buffer is now checked before accessing to memory.
Identifier: #60349
Subject:
Smart card removal may not be always detected.
Technical Description:
When a reader returns UNAVAILABLE and no device change event is sent by the system, ActivClient no longer monitors properly card change. The issue occurred only if multiple readers are connected to the machine. The issue is fixed by managing this as there is no more card in this reader (ie: locking the workstation if card was used for PKI logon).
Identifier: #60630
Subject:
RSA key pair may be set as default certificate.
Technical Description:
Default certificate flag was cleared only when the signing certificate was deleted (this must be the case with Entrust). Default certificate flag is now cleared when the default certificate is deleted without checking if it is the signing one.
Remark:
Cards that already have a RSA key pair set as default certificate, it is necessary to manually set the signing certificate as default using ActivClient User Console or recover the Entrust Profile.
Identifier: #60188
Subject:
Accessibility: AC User Console: View / Toolbars / Customize - For the "Mouse" tab, the two radio buttons are not in the tab order and are therefore inaccessible to the screen reader.
Technical Description:
Tab stop was not correctly set for this dialog box. This has been corrected.
Identifier: #60624
Subject:
Unable to access ActivKey Display with SIM.
Technical Description:
ActivClient 6.2 has been optimized to avoid duplicating same profiles with different card manager. ActivKey Display support was not changed to support such optimizations. This has been done in this fix.
Identifier: #60284/#60196/#60195/#60192/#60191/#60186/#60180
Subject:
Accessibility (Section 508 compliance) improvements in User Console, Advanced Configuration Manager and Help.
Technical Description:
ActivClient has been rebuilt using an updated version (11.0) of the user interface framework. Source code and help file have been reviewed for accessibility (section 508 compliance).
Identifier: #60425
Subject:
SDK: BSI gscBsiPkiGetCertificate function returns compressed certificate with a PIV card.
Technical Description:
BSI gscBsiPkiGetCertificate function was returning the compressed certificate with a PIV card. The function now returns the uncompressed certificate.
Identifier: #60399
Subject:
In case of upgrade from AC 6.1 to 6.2, ActivClient About dialog box's Credits button displays an error.
Technical Description:
The full path of Third Party Software Component License Terms documentation is stored in registry key. In case of upgrade from 6.1, the key was not set to the correct value; it is now correctly set.
Identifier: #60398
Subject:
Need support for GUID with binary values for PIV cards in the User Console.

Technical Description:
PIV GUID is stored in binary values. ActivClient was supposing that it is stored in ASCII format. PIV GUID is now displayed as binary.
Identifier: #60286
Subject:
Computer hangs after unlocking.
Technical Description:
In some rare conditions, the computer may hang after workstation unlock. The regression was due to a change recommended by Microsoft for Windows 7 Beta support. The change has been modified to avoid the issue.
Identifier: #60114
Subject:
The 2 docs installed inside C:\Program Files\ActivIdentity\ActivClient\Docs are incorrect.
Technical Description:
ActivIdentity End User License Agreement.pdf and Third Party Software Component License Terms.pdf were not correct. Correct versions are now installed.
Identifier: #60190
Subject:
Compliance 508: Advanced Configuration Manager: Third paragraph of splash screen beginning with “Do not change…” is not detected by the screen reader.
Technical Description:
Using tool like MAGIc 10.0, the third paragraph of Advanced Configuration Manager splash screen beginning with “Do not change…” is not detected by the screen reader. Tab order was preventing such tool to read all information. The tab order has been changed to solve the issue.

5. Installation Procedure

The following describes how to install this ActivClient Hot Fix.
Method 1: Interactive installation
Double click on the Hot Fix MSP file.
The ActivClient Patch InstallShield Wizard opens. Select “Update”.
Follow any additional instructions that may appear in the installation wizard.
If prompted to do so at the end of the installation, restart your computer for the changes to apply.
Method 2: Remote installation
To deploy software updates using Microsoft Active Directory push or Microsoft SMS, refer to the ActivClient Customization and Deployment Guide (available in the ActivClient Resource Kit).
Method 3: Automatic update
To deploy software updates from your company’s internal web site using the ActivClient automatic update feature, refer to the ActivClient Customization and Deployment Guide (available in the ActivClient Resource Kit).

6. Support Services

ActivIdentity provides technical support to its partners and customers that have purchased a Premium Support contract.
Contracted customers may contact us at one of the numbers below.
Please contact your ActivIdentity reseller if you have purchased your products through one of our partners.
ActivIdentity North America
Corporate Headquarters
6623 Dumbarton Circle
Fremont, CA 94555 USA
TEL: (1) (800) 670-6892
TEL: (1) (510) 745-6010
ActivIdentity Europe
European Corporate Headquarters

24-28 Avenue du General de Gaulle
92156 SURESNES Cedex FRANCE
TEL: (33) (0) 1-42-04-84-00
FAX: (33) (0) 1-42-04-84-84
ActivIdentity Australia
Asia/Pacific Corporate Headquarters
7 Phipps Close, Deakin
Deakin, ACT, 2600 AUSTRALIA
TEL: (61) (2) 6208-4891
FAX: (61) (2) 2681-7460
Or contact us by email at: support@actividentity.com