FAQs

Crescendo® Temporary Access Card

What is the relationship between NIST FIPS 201-2 and the Crescendo Temporary Access Card (TAC)?	NIST FIPS 201-2 is the federal standard that describes how the data model that the PIV, CAC and PIV-I (interoperable) credential should be formatted to meet the HSPD-12 directive. TAC uses the same NIST FIPS 201-2 data model when HID Global provisions the credential in our Austin facility.
Why is the TAC formatted as a PIV-I card?	In 2013, the US Federal government updated the NIST FIPS 201 standard to FIPS 201-2. As a result of that revision, a new GSA Approved Products List was created. To be listed on the new GSA APL, the entire Physical Access Control System (PACS) from the head end to the wall reader needed to be able to authenticate the PIV/CAC/PIV-I using the PKI authentication methods described in FIPS 201-2. It also required the system to recognize and discern the PIV-I card from the other two cards. Using a format closer to PIV-I than PIV or CAC enables HID to provide TAC the same way regardless of which Federal agency will use the TAC card, which simplifies the ordering and fulfillment process and enables HID to make TAC more affordable to its customers.
What is the difference between a PIV/CAC and a PIV-I?	The PIV/CAC and PIV-I have the same elements with slight differences. The PIV/CAC/PIV-I contains a 200-bit Federal Agency Security Card Number (FASC_N) and a 128-bit Global Unique Identifier (GUID). When a PIV-I card is formatted, the first 14 digits of the FASC_N are 9's.
How does the Physical Access Control System (PACS) and wall readers discern a PIV-I card from a PIV or CAC?	The PACS uses the FACS_N to identity the PIV/CAC credential, while the PACS uses the GUID to identity the PIV-I credential. When the wall reader checks the FASC_N and "sees" the fourteen 9's, the reader's firmware recognizes the card as a PIV-I card and sends the 128-bit GUID to the PACS. This is the reason that after 2013, all PACS installed as FIPS 201-2 compliant systems must be able to manage at least 128 bits of either the FASC_N or GUID.
I have a PACS system that is reading the GSA 75-Bit format. Can I use the TAC on my system?	Not without making sure the PACS and readers can recognize 128-bits. To support a migration strategy from legacy cards to PIV/CACs, HID Global's pivCLASS readers can be formatted to read 48-bits, 75-bits, or 128-bits. If the PACS can manage 128-bits, but is only sending 75-bits of the FACS_N from the reader, the reader will need to be re-configured.
My wall readers are HID Global 6000 series G3.0 readers. Can I use the TAC?	No, the G3.0 readers cannot recognize a PIV-I card, therefore it cannot recognize a TAC.

How would a TAC card be added to the PACS?	As long as the PACS meets the FIPS 201-2 requirements outlined above, whatever process being used to add the PIV/CAC to the PACS can be used. HID Global provides a GSA APL PIV/CAC registration software solution that could be used to register the TAC into the PACS.
Do I need to use pivCLASS readers to use the TAC?	No, any PACS and reader that can recognize a PIV-I card, as described above, will be able to recognize the TAC.
Does the TAC use certificates issued from a Certification Authority (CA) that is cross certified with the Federal Bridge Certificate Authority (FBCA)?	The TAC uses certificates from a CA that is part of the CA/Browser Forum, which means that the certificate's identity will be trusted by default on most PC, laptop and mobile OSes. However the certificates are not issued from a CA that is cross certified by the FBCA. This is to enable simpler ordering and fulfillment process which in turn makes the TAC more cost effective for HID's customers. The reason the TAC was developed was to be able for a PACS to be meet the FIPS 201-2 requirements and also use a secondary card for visitors. GSA testing laboratories will fail a PACS if the system recognizes a low frequency proximity card, or high frequency iCLASS, MIfare or DESFIRE formatted cards. The only type of card that should be recognized by the system is a FIPS 201-2 formatted credential. If a cross certified federated credential is required, then a PIV-I solution should be deployed.
But if the TAC isn't being checked by the Federal Bridge, how can it be revoked?	The TAC is designed to replace providing visitors with a proximity card. Just as with a proximity card, there is no Credential Revocation List that is required to remove a proximity card from the system. If a card is lost, or not turned in, then that card is merely removed from the access control system. Certificate revocation is important for PIV and CACs because these cards are designed to be trusted between agencies. A visitor card is only meant to allow access to a particular door or site for a limited about of time.
If the TAC is not meant to be a trusted federated card, why then does it contain two digital certificates from Identrust?	The digital certificates are required to perform two functions. The first is to register the card using a GSA approved PIV registration process. The second reason is to perform the same one or two factor PKI authentication at the wall reader. As there is no biometric signature on the card, the TAC cannot be used with a three factor PACS reader. Because the certificates on the card are issued by IdenTrust TrustID CA, they are recognized by default on most PCs, and as such in most cases does not require to trust a new CA into the PACS system.
Can the TAC be used for logical access?	With some high-level manipulation, the TAC could perform log-on authentication. HID Global does not have any published processes that can assist with this type of manipulation. However, HID Global would recommend a PIV-I credential for this use case.

What is the validity period of the TAC?	Like most PIV / PIV-I certificates, the validity of the TAC certificates is 3 years from its issuance date (i.e.: production at HID's facility). After the 3 years, the TAC is still functional at the card level, but relying system like PACS will see the card as expired and thus the card will need to be exchanged for a new one. HID does not keep a stock of finished TACs and instead issue the TACs when customer's orders are processed so as to maximize the active period of the certificates embedded in the TAC.
Does the TAC have a PIN code? Can it be changed or unlocked?	Like all PIV/CAC and PIV-I cards, the TAC has a PIN code. This PIN code is set at manufacturing and can be changed by end-users using any standard PIV middleware as long as the user knows the current PIN code. The PIN code will be blocked after a certain number of incorrect PIN tries. HID does not provide a way to unblock a blocked TAC; a new on TAC should be used instead.
Does the TAC have a FIPS certification?	Yes, the TAC has an FIPS 140-2 Level 2 security certification and a FIPS 201 interoperability certification.
Can any USB Smart Card reader or integrated reader be used with the TAC?	The Omnikey® 3021 and 3121 USB desktop reader will function with the TAC. Other readers should be tested, before using them. https://www.hidglobal.com/products/readers/omnikey/3021-usb https://www.hidglobal.com/products/readers/omnikey/3121

hidglobal.com