HID on the Desktop™ Security Overview

Executive Summary

HID on the Desktop™ (HOTD) is a suite of solutions designed to strengthen the overall security of a desktop log-on by using Two-Factor Authentication, combining something the user has (their ID card), and something that the user knows (the PIN associated with that card) as a substitute for the username/password that is usually used.

This document describes some of the risks and issues associated with password-based authentication, and explains how they can be mitigated using HID on the Desktop.

The Case for Two-Factor Authentication

Usernames and their associated passwords remain the most widely deployed logical access authentication method within most organizations

The deficiencies of password-based authentication are well known:

- Most users select passwords that are weak (easily guessable), thus offering virtually no protection against malicious attackers
- Passwords can be stolen, via shoulder-surfing, the use of keyboard loggers or through social engineering
- Passwords are easily shared, hence there is little assurance that the user of a given application is whom he/she asserts to be
- If an IT department institutes a strong password policy (for example: requiring long, complex passwords, and enforcing password changes every 90 days) users become more likely to write down their passwords near their workstations, increasing the chance of accidental disclosure and hence unauthorized access.
- The costs (in terms of lost productivity, and administrative overhead) associated with password management are significant. Independent studies estimate these costs between $65 and $125 per user per year

Given the high percentage of mobile users in today's workforce, and the large number of laptops reported lost or stolen each year, the need to increase the strength of the primary desktop authentication has never been clearer.

Because the type of two-factor authentication promoted by HID on the Desktop requires that the user provides a hardware token in addition to a secret (such as a PIN code), any of the risks associated with single-factor (password) authentication are mitigated:

- The PIN is only half of the set of authentication credentials provided. Even if the PIN is compromised, without the other factor, authentication is impossible
- Through the appropriate selection of two-factor technology components, Windows® passwords can be significantly strengthened – resulting in a level of security that is essentially resistant to both brute-force and dictionary-based systematic attack
- Because world-class two-factor authentication systems include self-service tools to allow users to manage their own authentication credentials, ongoing administrative overheads can be significantly reduced

An ASSA ABLOY Group brand   ASSA ABLOY   **HID**

HID on the Desktop™

HID on the Desktop™ is a suite of authentication products that leverages an organization's use of existing physical access credentials to secure access to computer workstations.

Recognizing that businesses have a wide variety of authentication needs, HID's solution allows the use of a variety of technologies to securely identify the user.

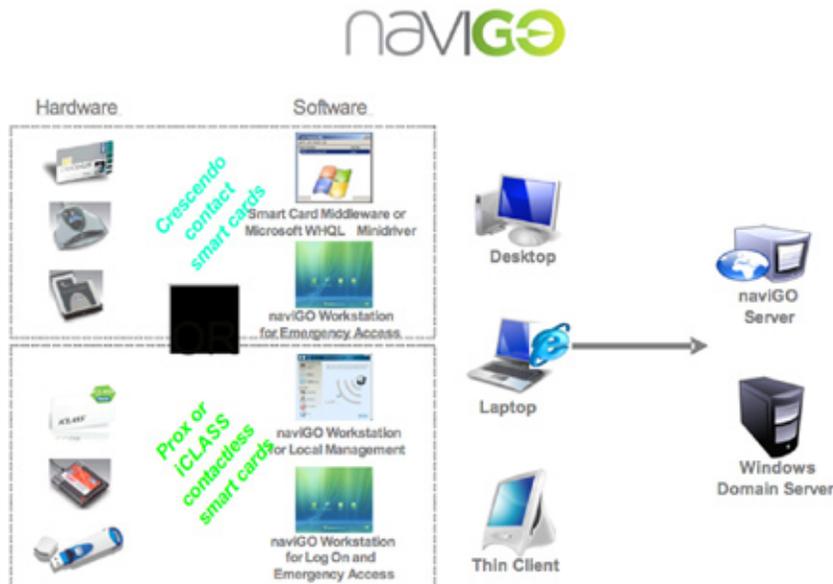Regardless of the specific authentication method used, the workflow in each case is identical:

1. The user introduces his/her card into the system (using a contact or contactless card reader as appropriate)
2. The user is presented with a dialog box and is prompted to input the PIN that he/she selected during initial enrollment
3. If the PIN is valid, data contained within ¡the card is combined with other system data and the authentication process completes

The actual authentication process varies significantly depending on the technology being presented. The following sections describe the concepts followed in each case.

Security Rating	Log-on Method	What happens at log-on?	Security Details
Least Secure	Username & Password	User provides a username and password to default Windows® interface	Method: One-Factor Password: Native to Windows®. Subject to replay attacks, social engineering, and brute force attacks.
	Prox	User presents a Prox card and enters a PIN Card broadcasts a static, unencrypted card number to the reader. naviGO™ validates the card number and PIN against its secure local cache. If valid, it logs the user on using Windows® log-on credentials.	Method: Two-Factor Card: A read-only card and static card number; possible to-intercept transmission; susceptible to replay attacks. PIN: PIN policy is enforced by software
	iCLASS®	User presents an iCLASS® card and enters a PIN Card validates mutual key and securely transmits three credentials – a serial number, token data, and a token hash value – to the application. naviGO validates these credentials, along with the PIN, against the secure local cache. If valid, it logs the user on using Windows® log-on credentials.	Method: Two-Factor Card: Mutual authentication between the card and the application. Difficult to intercept. Extremely difficult to reproduce. PIN: PIN policy is enforced by software.
Most Secure	Crescendo™	User inserts a smart card and enters a PIN Card securely transmits a digital certificate from a trusted certificate authority and also validates the PIN (on the card). Windows® validates the digital certificate against the trusted certificate authority and if valid, logs the user on using key exchange.	Method: Two-Factor Card: Mutual authentication between the card and the application. Difficult to intercept. Extremely difficult to reproduce. Requires a trusted PKI infrastructure. PIN: PIN policy is enforced on the card.

An ASSA ABLOY Group brand   ASSA ABLOY   **HID**

Solution Overview

naviGO™ Software

naviGO Workstation
This is a client-side software application that resides on the user's PC and manages the authentication of contactless credentials (Prox or iCLASS cards). Additionally, it allows Emergency Access under certain conditions in the event that a user does not have access to their card and requires access to their PC.

naviGO Server
This is used to support the issuance and lifecycle management of HID on the Desktop credentials. It provides users with a web portal that they can use to manage their cards; additionally it provides the system administrator with the ability to define security policies associated with logical access using HID products.

An ASSA ABLOY Group brand   ASSA ABLOY   **HID**

Prox on the Desktop™

Functional Overview
During registration, the user authenticates using their legacy Windows® password. Upon successful validation, the user is able to enroll his/her prox card.

During enrollment, the user registers their Prox card, along with his/her system username, password and domain, and selects an associated PIN.

naviGO Workstation encrypts the user PIN and places it within its local credential store, along with the username, password, the domain and data that links the user's card and the associated network identity.

In normal usage, at the Windows® log-on screen, it is now possible to supply log-on credentials via Prox card. Upon presentation to the Prox reader attached to the user's PC, card data is extracted from the card and validated by naviGO Workstation, along with the PIN supplied by the user.

If a successful match takes place, naviGO Workstation extracts the associated username, password and domain from its local credential store and presents them for validation by Windows®.

Access is only granted when a valid card and its associated PIN are presented.

Security Assessment

Uniqueness of Prox Authentication Credentials
Depending on the format encoded during card manufacture, the card number may not be unique. Thus there is a (relatively low) risk that the card number of a random Prox card presented to the system might match the card number of the valid card already registered. However, the risk of two users with the same card encoding accessing the same machine with the same PIN is so remote the level of risk is considered acceptable.

Note that if the card was issued under HID's Corporate 1000 program, uniqueness is assured.

Cloning / Replay Attack of Prox Credentials
It should be noted that as there is no encryption between the card and the reader, a malicious attacker could capture, and subsequently replay, a valid card number.

In this case, the PIN defends against system compromise. As mentioned earlier, an appropriately strong PIN policy is the best mitigation of this risk.

Brute-force Attack of the Card PIN
A security policy exists to control the number of invalid PIN attempts (typically, 3) that are permitted before a card is placed in a locked state. Once in a locked state, a credential cannot be used for authentication purposes.

In order to unblock a card, an "unblock" operation must be performed, either by an authorized security officer or by a user in a self-service transaction, which requires additional authorization factors (typically, Knowledge-Based Authentication) prior to the unblock operation.

Thus, the card is strongly resistant to brute-force attack.

iCLASS on the Desktop

In this case, naviGO Workstation uses iCLASS cards as the primary authentication mechanism.

Functional Overview

This method takes advantage of the higher levels of security offered by HID's iCLASS® technology.

During user enrollment, the user validates their identity to Windows using their password. Assuming that this validation completes successfully, the user then registers their username, password and domain with naviGO™ Workstation, and chooses a PIN which will be used to secure future log-ons.

naviGO Workstation encrypts the user PIN and places it within its local credential store, along with the username, password, and the domain.

Additionally, naviGO Workstation writes a secure data object within one of the application pages of the user's iCLASS® card.

- Included within the data object is a hash (message digest) of the unique card serial number ("CSN") and user PIN. This binds together the user and the physical credential (card). This is used to prevent "skimming" of user data from one credential to another.
- Additionally, the start and expiry dates of the credential are stored within the data object. Credentials that are used prior to the start of their validity period, or after the end of their validity period, will be rejected by naviGO Workstation.

Included within the data object is a hash (message digest) of the CSN and user PIN. This binds together the user and the physical credential (card). This is used to prevent "skimming" of user data from one credential to another.

When a valid iCLASS card is presented to naviGO Workstation, the following steps occur:

1. Mutual authentication takes place between the card and its reader. A challenge-response sequence is initiated to ensure that the card contains a valid issuer key
2. naviGO Workstation reads the CSN from the card, along with the secure data object from its data store
3. The user inputs his/her PIN using the naviGO Workstation login screen
4. The user encpted PIN and the CSN are hashed by naviGO Workstation, and compared with the hashed value retrieved from the card. If the two values match, the credential is known to be valid.
5. naviGO extracts the username, password and domain from its store and presents them to Windows® for validation

Security Assessment

iCLASS has a richer set of security features; thus the strength of the authentication is significantly increased:

Uniqueness of iCLASS Authentication Credentials

The CSN of the iCLASS card, by design, is assured to be unique.

Cloning / Replay Attack of iCLASS

Data exchanged between the card and its reader is encrypted. Given that the keys used for a transaction change every time, capturing and replay of card data does not yield a suitable attack.

Brute-force Attack of the Card PIN

A security policy exists to control the number of invalid PIN attempts (typically, 3) that are permitted before a card is placed in a locked state. Once in a locked state a credential cannot be used for authentication purposes.

In order to unblock a card, an "unblock" operation must be performed, either by an authorized security officer or by a user in a self-service transaction, which requires additional authorization factors (typically, Knowledge-Based Authentication) prior to the unblock operation.

Thus, the card is strongly resistant to brute-force attack.
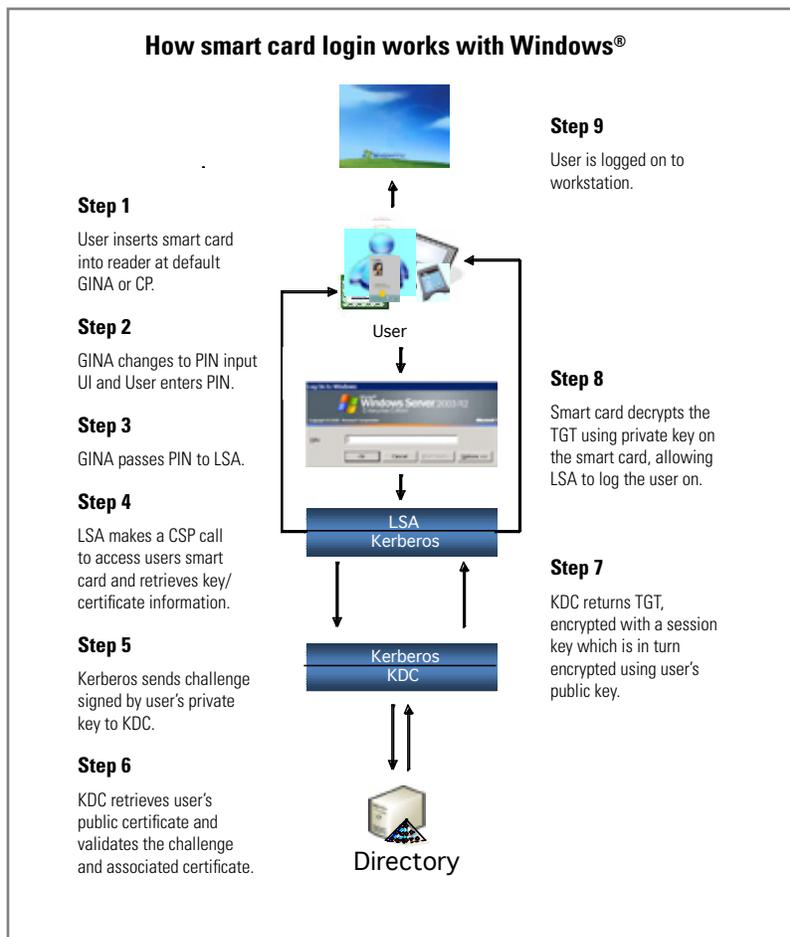
Crescendo on the Desktop

Crescendo is designed to use contact smart cards to perform smart card log-on in the manner defined by Microsoft's "Windows Smart Card Infrastructure" specifications.

Functional Overview

During initial enrollment, the user accesses naviGO Server and uses it to select a PIN that will be used to restrict access to their smart card. At the same time, user-specific security information (in particular, a private / public key pair and associated digital certificate) is generated and securely contained within the smart card. This data will be used whenever a smart card based login to Windows® takes place.

The sequence of operations is as follows:

1. The user inserts his/her smart card into a PC/SC compatible smart card reader
2. The user is prompted to input the PIN associated with his/her smart card
3. Windows® sends the PIN to the smart card for validation. If the PIN matches the value stored within the smart card, the smart card provides the certificate associated with the cardholder to Windows®, which then packages the certificate and other authentication data, signs it using the cardholder's private key, and sends it upstream for validation.
4. The domain controller looks up the user, and uses the associated certificate to check the integrity of the signature supplied with the log-on request.
5. If everything matches, standard Windows® processes are used to log the user on to his/her desktop/domain.

How smart card login works with Windows®

Step 1
User inserts smart card into reader at default GINA or CP.

Step 2
GINA changes to PIN input UI and User enters PIN.

Step 3
GINA passes PIN to LSA.

Step 4
LSA makes a CSP call to access users smart card and retrieves key/ certificate information.

Step 5
Kerberos sends challenge signed by user's private key to KDC.

Step 6
KDC retrieves user's public certificate and validates the challenge and associated certificate.

Step 9
User is logged on to workstation.

Step 8
Smart card decrypts the TGT using private key on the smart card, allowing LSA to log the user on.

Step 7
KDC returns TGT, encrypted with a session key which is in turn encrypted using user's public key.

User

LSA
Kerberos

Kerberos
KDC

Directory

Security Assessment

Uniqueness of Authentication Credentials
Windows® relies on standard Public Key Infrastructure (PKI) components to perform user authentication. Specifically, in order for a card to be valid, it must contain a valid private/public key pair and an associated log-in certificate.

Given that the key pair is generated on-card during user enrollment, and the private element of the log-in key, is, by design, non-exportable from the smart card, the uniqueness of the card/certificate is guaranteed.

Cloning / Replay Attack
Cloning of a given card, while technically feasible, requires such a significant investment of time and materials by a malicious attacker that it can be considered out of scope for a typical enterprise.

An ASSA ABLOY Group brand   ASSA ABLOY   **HID**

Emergency Access

HID on the Desktop's Emergency Access function uses Knowledge-Based Authentication (KBA) to allow a user access their workstation in the event that their card is lost, forgotten or blocked.

Functional Overview

During the enrollment process, the user is presented with a set of questions (for example: What was the name of your first pet?). By design, these questions require the user to supply information that is obvious to the user but not readily known by someone who is impersonating them.

The user selects a defined number of these questions, and provides appropriate answers, which are stored by the system and associated with that user.

Having done so, "Emergency Access" becomes one of the authentication methods available to the user at Windows® log-on.

If "Emergency Access" is selected, naviGO™ Workstation will present the user with a screen containing a list of questions to be answered, randomly selected from the set of questions/answers supplied by the user during enrollment.

The user then answers the questions supplied; provided that the user answers all of the presented questions correctly, naviGO workstation will proceed with the desired Emergency Access action.

The size of the initial list of questions, the number of answers required to be supplied by the user during enrollment and the number of correct answers required to allow Emergency Access are all configurable by the system administrator.

Additionally, after a defined number of unsuccessful Emergency Access attempts, the user's account becomes locked, preventing a brute-force attack.

Security Overview

Single Authentication Factor

Removing the requirement to supply two separate authentication factors degrades the overall security of the solution Accordingly, Emergency Access should not be seen as a day-to-day authentication mechanism.

The system administrator should carefully consider the following discretionary parameters:

- The size of the list of potential questions available to the user during enrollment
- The number of questions to be presented to the user during emergency access
- The number of correct answers to be supplied during the emergency access process

Obscurity of Authentication Questions

It is important that the questions being asked do not rely on information that can be easily guessed or inferred by a potential attacker (Example: the home telephone number of a given user could be established through an internet search)

General Security Issues

Security of User Data

Local data is secured against the two primary means of attack – decrypting data and copying encrypted data.

First, all authentication data is encrypted using a diversified key. The entire XML database residing on the machine is encrypted by a second unique application key. Therefore, sensitive data is essentially encrypted twice by two unrelated keys.

Second, local data is secured from copying encrypted data. Keys to encrypted authentication data are also 'salted'. In the 'salting' process, extra data is fed as input into the algorithm to ensure that although the same key is used to encrypt different items, each encryption result will look unique from the others when it is stored in the database. For example, if the same PIN is assigned to two different cards, each encrypted string will look different in the stored form.

Therefore, a potential hacker cannot copy the encrypted string from the first card and gain access with the second card.

PIN Policy

In order to gain access, a valid PIN is required in addition to the card. Assuming that a 4-digit numeric PIN is selected, and given that after thee invalid PINs are presented the card becomes blocked (inoperable), there is a 1-in-3333 chance that a PIN will be guessed. To increase the overall security of the solution, the system administrator can require that longer PINs be used.

For example, requiring a 5-digit PIN, consisting of upper and lower case letters and the digits 0-9, and allowing three invalid attempts before blocking the card, lowers the risk of PIN compromise to approximately 1-in-3.2 million.

Note that as a configuration setting, it is possible to suppress the input of a PIN using either Prox or iCLASS® on the Desktop, in which case authentication becomes one-factor (something that the user has).

This setting should only be applied in situations where the system administrator can be sure that only valid users have access to the card/workstation, and where the primary purpose of the solution is to streamline access to a PC (for example, in a shared workstation environment within a hospital)

Increased Password Strength

It is possible to configure the naviGO™ Workstation client so that the user's Windows® password is replaced by a "strong password" – that is, one whose length and complexity ensure that brute-force attack is impossible.

Normally, such a password is so opaque to the user that remembering/supplying when needed becomes a major operational difficulty.

Given that naviGO Workstation becomes the agent to store and supply this password as required, the adoption of such a password policy greatly increases the overall security of the computing infrastructure, while simplifying the user's day-to-day experience.

NaviGO Workstation manages the generation and presentation of this enhanced password in a manner that is transparent to the user. Should the user elect to revert to a weaker password at some future time, naviGO Workstation allows the user to do so.

Conclusion

Two-factor authentication significantly increases the security of a businesses IT infrastructure. HID on the Desktop™ effectively balances the security needs of a business with those of its users, and of its administrators.

Further Information

Email: sales@hidglobal.com
Web: http://www.hidglobal.com