Welcome

Introducing “On the Desktop”

HID Global
&
A3M
present
Speakers

Silvia Ocamica
Adrian Castillo
Steven Commander
Frédéric Sallandre
Summary

Introduction, the landscape and value proposition

“On the Desktop”, solution overview

The A3M / HID “On the Desktop” opportunity

Pricing model

Questions and answer
Technical introduction

Architecture

naviGO stand alone
GINA and local administration interface

naviGO Client - Server
Client interface and centralized administration

Try the software!
Demo machines available
You already know us
On the Desktop

One badge...
Open doors
Open Windows®
Why “On the Desktop”?
Information

is the most valuable asset for most companies today
Information

- Blueprints
- Financial Report
- Patient Information
- Code
- Customer information
- IPR
- Brand/Marketing
- Contract
The Question?

Do you really know who's accessing your most sensitive information assets?
The answer

Yes I do …
But usernames/passwords are

- One factor authentication only
- Unsafe
  - Key loggers
  - Dictionary attack
  - Social engineering attack
  - ...
- Expensive
On average

- Helpdesk calls per user per month: 1.75 (1)
- Duration of Help Desk calls: 12 mins
- Hourly cost of Help Desk staff: 38 €
- Hourly cost of company staff: 57 €
- % passwords Help Desk calls: 40% (2)

(1): Industry average, source META Group
(2): 40–70% reported by Authentication World (SSO Business Case)
Password costs

• On average, for a 1 000 employee company
• 700 calls / month related to passwords
• 13 300 € / month

Not true!

OK, let’s take 1/3:

4 430 € / month = 53 160 € /year
On the Desktop™
Value proposition
What is « On the Desktop »?
Solutions already exist

Network security
- Firewall/VPN
- Network Gateway Protection
- IPSec VPN
- Gateway MAIL Security
- Anti-Spam
- Anti-Virus
- Encryption
- Reporting
- In/Out Bound Content Inspection
- Policy Enforcement
- Gateway WEB Security
- Web Surfing Control
- Web Mail (See GW Mail)
- IM/POP Control
- Anti-Virus/Malicious Code

Authentification
- Access Control
- Identity Authentication
- Authorization
- 2+ Factors
- Web/Network/SSO
- Physical & Logical
- Inside/Outside
- Network Access Control (NAC)
- Endpoint Control
- Identity Mgt (Tokens)
- Control Management
- Reporting

Data protection
- Data Encryption
- Whole Disk (Laptop), File/Folder, Network Storage, Communications
- Confidiallity
- Encyption
- Data At-Rest
- Data In-Transit
- Disposal
On the Desktop addresses

DESKTOP PASSWORD:
r4ew01s5s8g
In a simple way

After you’ve opened your door …

… open your Windows® session
On the Desktop is

Convenient
Simple
Secure
On the Desktop Solution overview
The components
The Components

- **Prox**
- **Mifare**
- **iCLASS**
  - 2K to 32K
- **Crescendo**
  - C200
  - C700
Other technologies supported

Broad range of credentials portfolio

• Multi-technologies credentials:
  – Mifare
  – DESFire
  – Prox + DESFire
  – iClass + DESFire
  – Other combinations with EM and Hitag

• Credential add-ons
  – Prox & iClass sticker tags
Crescendo hosts your credentials

Multi-application access control (13.56 MHz)

Proximity access control (125 Khz)

JCOP
PKI contact chip
Crescendo all in one

- Low frequency and high frequency RFID
- Contact chip for PKI applications
- Applet loaded on the card
- Middleware bundled with the card
- All middleware updates and upgrades
MICROSOFT – Plug and Play
- Supports the Microsoft mini-driver program
- Requires no middleware installation
- Supports all MSCAPI functions
- Limited flexibility and administration tools native to Microsoft
- Full support in ILM

MULTIPLE PLATFORM SUPPORT
- Fully supports PKCS#11 and MSCAPI
- Full featured contact chip administration tools
- Crescendo middleware required
- Full support in ILM
Readers

A dedicated range

5325 CL 5321 CLi 6321 CLi

contact and/or contactless multi-technology readers
A3M / HID and Dell Partnership

Dell partnership delivered one of the first ever embedded contactless technology in a laptop in 2008

On the Desktop Reader Technology Included
Dell Latitude E6500 - Productgegevens

Dell™ Latitude™ E6500

De nieuwe Dell Latitude E6500 is ontworpen om de productiviteit verhogen en de totale aardappelstap kosten te verlagen. Deze laptop biedt grote<br>
verbeteringen op het gebied van de prestaties, duurzaamheid en beveiliging.
- Volledige functionaliteit, geprijsd conterpunt<br>  - Een verbeterde beveiligingsfunctie<br>  - Behoudzaamheid en comfort door de Latitude

Productkarakteristiek | Docking | Technische specificaties | Services en support

**Beveiliging**

Fysieke beveiliging,
kabelafsperringe en standaard, mediamodule en handelsschijffremedelingen.

Gebruiker- en systeembeveiliging

- Snelste afdoen en contactmet simmertecnieken
- Vingerafdruksleger of FIPS-ingeschreven (optioneel)
- TFM 1.2
  - Optionele gecodeerde hard-schijffeburering van de volledige schijf
- Centraal Vault – veilig beheer van aanmeldingsgegevens binnen een vertrouwd domein

Networkbeveiliging:

- 802.11 Wi-Fi Protected Access (WPA), 802.11i (WPA2), Virtual Private Network (VPN) 802.1x met EAP-medlen en compatibiliteit met CCM 4.0
Windows authentication based on HID cards.
Management and provisioning of Prox, iCLASS and/or Crescendo
Consumes virtual credentials
One virtual credential for every physical credential

Self–service for the user:
- PIN Unblock and Reset
- Emergency Access
- Enrollment / Provisioning
Two versions

Server

Workstation

navigo
Workstation

- Stand-alone client software application
- Enrollment and management of Prox, Mifare or iCLASS Cards
- Allows Emergency Access
Server

- Enrolment and management of Prox, Mifare, Crescendo
- Web Portal interface
- Centralized administration
- Emergency access
An advanced system management is required:

- Centralized administration
- Roaming: authentication on several workstations with one card

With Crescendo cards:

- A simple PKI logon solution
- PIN and PUK (PIN Unblock Key) in self-service
The mechanisms – Prox & Mifare

Prox – 125KHz

Card number

• Card n°
• PIN

Windows
User name & Password

PIN
The mechanisms - iClass

iClass – 13.56 MHz

Card n°
[card n° + PIN]

- PIN
- Card n°
- [card n° + PIN]

Windows
User name & Password

PIN
• Contactless authentication with Prox or iClass

  or

• Contact based PKI authentication, Windows standard

• For PKI, naviGO provides:
  – A certificates management interface, in a standard Microsoft architecture
  – Emergency access
On the Desktop advantages

• No impact on the physical access control system
• Uses cards that are already in the field
• Limited impact on the IT system
Support and maintenance

- **Standard support**, web portal in english, included:
  - Ticket creation and follow-up
  - On-line documentation
  - Frequently asked questions

- **Maintenance included**
  - Hardware warranty (2 years contactless readers, 1 year Crescendo cards, lifetime Prox and iClass cards)
  - 90 day software warranty
  - Software updates and upgrades included
naviGO is...

- Simple
  deployment, administration, and use
- Universal
  most RFID cards used for strong authentication
- Flexible
  self-service and administrator driven workflows.
- Convenient
  solution leveraging on cards in the field
On the Desktop pricing model

Prox reader

List price (MSRP) 78.08 euros

Virtual Credential 13.04 €

Workstation and server
Free of charge
Credentials and Credential Credits

- Credential = device (contactless card, PKI card)

- On The Desktop consumes “Credential Credits”
  - One Credential Credit per device (contactless card, PKI contact chip)
  - naviGO Workstation Standalone includes two Credential Credits
  - When used in Client / Server mode, credits must be obtained from naviGO Server

- Credential credits loading
  - Loading into Server is accomplished by the in house SysAdmin
On the Desktop

Support and maintenance
Support

FLAGRANT SYSTEM ERROR
The system is down. I dunno what you did, moron, but you sure screwed everything up.

In the unlikely event.....
Standard support layout

- End-User
- Administrator Niveau1
- Online support: http://support.hiddglobal.com
- Support level 2
- Level 3
Services opportunity

- Consulting / studies
- Presales support
- Installation
- Support & maintenance
Methods of Support

- Incoming
  - [http://support.hidglobal.com](http://support.hidglobal.com)

- Outgoing
  - Support Ticket
  - e-mail
  - Knowledge Base articles
  - Phone
  - Remote Diagnostics
On the Desktop

Architecture
Is the foundation for a password replacement solution that provides faster, easier, and more secure Windows log-on.

- Supports contactless log-on to both Windows XP and Vista
- Supports Prox and iCLASS cards.
- If a card is misplaced or lost or a PIN is forgotten, supports Emergency Access log-on.

![Diagram showing card and workstation interaction]

Validates card / PIN
Passes stored userID, password and domain to Windows LSA for upstream authentication
Reference Implementations
Reference Implementations
# naviGO Implementation Options

<table>
<thead>
<tr>
<th>Standalone</th>
<th>Client/Server</th>
<th>PKI</th>
<th>Mixed Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Contactless logon</td>
<td>• Contactless logon</td>
<td>• Contact (PKI) logon</td>
<td>• Mixture of Contactless and Contact (PKI)</td>
</tr>
<tr>
<td>• Single credential per PC</td>
<td>• Managed using naviGO Server</td>
<td>• Managed using naviGO Server</td>
<td>• Managed using naviGO Server</td>
</tr>
<tr>
<td>• No management server - standalone deployment</td>
<td>• Central policy management</td>
<td>• Central policy management</td>
<td>• Central policy management</td>
</tr>
<tr>
<td></td>
<td>• Supports roaming &amp; multiple credentials per PC</td>
<td>• Uses native Windows smart card capabilities</td>
<td>• Offers greatest flexibility</td>
</tr>
</tbody>
</table>

## Client Side

- naviGO Workstation
  - Workstation (Standalone)
- naviGO Workstation
  - Workstation (Client / Server)
- BaseCSP and naviGO Drivers for PKI
  - naviGO Workstation Software Not Required

## Server Side

- naviGO Server Software Not Required
- Server
- Server
- Server
What is a GINA?

‘GINA’ = ‘Graphical Identification and Authentication’

The GINA is a replaceable DLL component that is loaded by the Winlogon executable. The GINA implements the authentication policy of the interactive logon model and is expected to perform all identification and authentication user interactions. [Source: MSDN Library]

Microsoft provides a GINA with XP, but you can implement your own, if you wish to extend Windows’ authentication model
Why change the GINA?

- Windows only supports two authentication methods out of the box
  - User ID and Password
  - PKI Smart Card (using MSCAPI / BaseCSP) APIs

- To allow other methods, we need to replace the standard ‘msgina.dll’ with a custom one
GINA replacements are challenging..

- GINAs are complicated to program

- Other vendors may already have replaced the GINA on a given workstation
  - In theory, GINAs can be “chained”
  - In practice, this can cause deployment issues
What is a Credential Provider?

- When Microsoft designed Vista, it replaced the GINA architecture with a new authentication model.

A credential provider is a module that plugs into ‘LogonUI’.
Credential providers – key facts

- Credential providers are modular – easy to plug into the Windows system
- They are additive – multiple vendors can implement their own credential providers side-by-side other ones
- Microsoft ships two credential providers as standard
  - Username / Password
  - PKI Smart Card
On the Desktop

- To support Contactless and Emergency Access methods, let’s modify the desktop logon environment

- XP / 2K3 Server – GINA replacement
- Vista / 2k8 Server – Custom Credential providers
naviGO standalone
- No connection to naviGO Server
- A User enrolls on their local PC
- All administration is performed locally (no central policies)
- Supports two user credentials per PC
- Credentials cannot roam between PCs
- Suitable for “look and feel” demos, early proof of concept trials, and small self-managed deployments
naviGO Client / Server
- Manages and provisions Prox, iCLASS or Crescendo cards

- Benefits to the end-user
  - Cards can roam between desktops
  - Allows self-service unblock or reset of PINS

- Benefits to the IT Security manager
  - Supports self-service or attended issuance of two-factor authentication credentials (HID cards of any type)
  - Can handle contactless, contact or any mixture of card types
  - Allows central definition of management of users and policies
  - Increases system security with minimal impact to daily operations
  - Quick and easy to install and use
Server-Side Architecture

Optional component for use with Crescendo contact smart cards
Administrator’s Portal

System Dashboard
- Active sessions: 1
- Total users: 3
- Enrolled users: 2
- Unenrolled users: 1
- Lockouts: 0

Welcome to naviGO.
Use the workflow shortcuts for quick access to common tasks.

Workflow Shortcuts
- Manage users
- Manage user states
- Manage authentication methods
- Manage authentication sets
- Manage system roles
- Create Reports

Miscellaneous
- First time use workflows
- Global Settings

Tuesday
1/20/2009 2:23 PM
naviGO Server by HID Global
- Connected to naviGO Server
- Contactless and Crescendo users can enroll on server’s user portal, policies are centrally defined and managed
- Credentials can synch (roam) between PCs, and multiple credentials per PC are allowed
- Expected to be the norm for On the Desktop deployments
On the Desktop™
Try the solution !
Thank you for your attention!

For more information, please contact:
- Steven Commander @HID T 09 63 02 35 57
- Frédéric Sallandre @A3M T 01 64 25 73 12