

1 Authentication Management



Managing The User Lifecycle

With The Hitachi ID Management Suite

The evolution of password management beyond password synchronization and reset.

2 In the beginning...

- Password management products mostly started out doing just two simple things:
 - Password synchronization.
 - Self-service password reset.
- Integrations were relatively simple:
 - Windows NT / Novell NetWare / Sun LDAP.
 - Maybe a database or two.
- The user interface was simple:
 - Web browser.
 - Easy as 1 ... 2 ... 3:
 - * Sign in with a login ID.
 - * Type your password or answer a few questions.
 - * Choose a new password.
- *This is so simple, any summer student could write one.*

3 But then things got complicated

- Users forget their primary password
 - Catch 22: can't login, so can't open a browser, so can't SSPR, so can't login.
- Companies deployed lots of applications.
 - 100 SAP servers?
 - 10 mainframes?
 - 1000 Unix boxes?
 - 1000 databases?
- Enterprises started using this stuff, globally.
- Password management grew to meet these requirements:
 - GINA DLLs – SSPR for locked out users.
 - Lots of connectors – synch and reset app passwords.
 - Translation / localization was added.
- *This is not a summer student project any more!*

4 Complexity keeps growing

<i>Mobile workforce</i>	<ul style="list-style-type: none"> • Users need access to SSPR from anywhere, even before they establish a VPN connection.
<i>Global network</i>	<ul style="list-style-type: none"> • There may be hundreds of AD DCs. • Users can't wait for changes made at one site to affect their account at another.
<i>Smart cards and tokens</i>	<ul style="list-style-type: none"> • Users forget their PINs and need to reset those too.
<i>Smart phones</i>	<ul style="list-style-type: none"> • These have passwords too. • Should be both supported and leveraged.
<i>Full disk encryption</i>	<ul style="list-style-type: none"> • Every security-conscious organization is deploying it and feels the pain of key-recovery.
<i>Integrate with IDM</i>	<ul style="list-style-type: none"> • Provision a user – and don't wait before he can do SSPR. • Authenticate before launching a federated connection (SAML, WS*, Shibboleth).

5 It's not just passwords any more

Users need to manage more authentication factors today:

- **Passwords** – likely will never go away.
- **Smart cards** – unlocked with a PIN.
- **Token PINs** – unlocked with a PIN or password.
- **Hard disk encryption** – must type a password before the OS will boot.
- **PKI certificates** – unlocked by a password or PIN.
- **Voice or other biometrics** – need to be enrolled.
- **Security questions** – first enrolled and periodically refreshed.
- **Cell phone number/provider** – can act as another authentication factor.

6 Many valid use cases

Self-service and enrollment basically mean that a user signs in with one authentication factor before updating another:

Use case:	Login with:	To do this:
Password synch	<ul style="list-style-type: none"> • Current password. 	<ul style="list-style-type: none"> • Choose a new password.
Self-service	<ul style="list-style-type: none"> • Security questions. • Smart card or token. • Cell phone (random PIN via SMS). • Biometric. 	<ul style="list-style-type: none"> • Choose a new password. • Reset token PIN. • Reset smart card PIN. • HDD key recovery.
Enrollment	<ul style="list-style-type: none"> • Current password. • Smart card or token. 	<ul style="list-style-type: none"> • Fill in security questions. • Provide voice print. • Register cell phone.

7 Small, one-platform solutions

- Many vendors are creating "silo" solutions to streamline support for their own products.
- Examples:
 - RSA: including self-service PIN reset with token system.
 - McAfee: including self-service HDD key recovery with SafeBoot.
 - Smart card vendors: getting into PIN reset too.
 - Quest, Namescape, many IVR vendors and some help desk vendors and probably many others make AD-only SSPR systems.
- The whole point of identity management systems is to eliminate "security in a silo" solutions!
- Enterprises don't want users to enroll 3 or 4 different profiles of security questions, or to support multiple infrastructures.
- ***What's needed is a consolidated, enterprise-class system to manage all authentication factors.***

8 Enterprises should demand better

- A single system to manage all authentication factors.
- Integrations with all of their major systems and applications.
- Support for mobile users – SSPR, cached credentials, etc.
- Integration with user provisioning, for "instant-on" capability.
- Integration with federation/WebSSO, for "login here, access app there" capability.
- Support for smart card PIN reset (note: this can never be done via a telephone).
- Support for token PIN reset.
- Support for hard drive key recovery.
- Support for collecting old and distributing new PKI certificates.
- Many authentication options: passwords, security questions, tokens, smart cards, biometrics, cell phones.
- Many enrollment options: security questions, biometrics, phones.
- ***This is much more than just SSPR!***
- ***This is AUTHENTICATION MANAGEMENT.***

9 Authentication management technology

- SSPR:
 - Web UI (of course).
 - GINA DLL (for 40% of issues that are Windows lockouts).
 - GINA Service (same as GINA DLL but without the risk).
 - Windows 7 Credential Provider (new PCs need this).
 - Telephone / IVR (for mobile users and orgs that prefer the phone).
 - Secure Kiosk Account (to avoid client software deployment).
- Self-service, non-password:
 - Smart card PIN reset (must be done using ActiveX in browser).
 - Token card PIN reset (at least for RSA).
 - PKI certificate management (at least for Lotus Notes).
 - HDD key recovery (becoming urgent for many customers).
- Mobile users:
 - UI should work in a small browser (phone).
 - Manage Blackberry passwords.
 - SSPR for mobile users over temporary VPN.
 - Update cached passwords on Windows after a PW change.

10 User adoption

- Most of these processes depend on user cooperation:
 - Enrollment: typically to populate answers to security questions.
 - Self-service: rather than calling the help desk.
- Users will not volunteer to do either.
- To get user adoption, we need a combination of things:
 - Frequent reminders.
 - Accessible UI (e.g., available when needed).
 - Hard to miss UI (e.g., access from login prompt, portal, etc.).
 - User friendly UI (e.g., no training required).
 - A carrot (e.g., synchronized passwords; dinner for 2).
 - A stick (e.g., slow response if you call the help desk).
- It helps if some of these things are built right into the authentication management product.

11 Hitachi ID Password Manager

Password Manager is the only product on the market that meets all of the requirements of enterprise authentication management.

- Authenticate with and manage any factor:
 - Passwords
 - Token and smart card PINs
 - Security questions
 - Cell phone / SMS PIN
 - Voice biometrics
- Smart card PIN resets is via ActiveX.
- HDD key recovery is via telephone.
- Managed user enrollment is built-in.
- Access from anywhere:
 - Web browser (any)
 - Smart phone (any).
 - Locked out workstation (GINA service, SKA).
 - Mobile laptop (temporary VPN).
 - Voice phone (IVR).

12 Services Engagements

- Some of these features are complicated to setup.
- Just as "authentication management" is more powerful than "password management," these projects are going to be longer.
- Examples:
 - SSPR for mobile users – need to integrate with and customize temporary VPN connection.
 - Smart card PIN reset – need to integrate with one-off card management system and with whatever card readers and cards have been deployed.
 - HDD key recovery – needs IVR plus key recovery server integration.
- Expect 30+ day deployments, even if there are just 2-3 integrations.