

# Hitachi ID Password Manager

Telephony Integration



# Contents

- 1 Introduction** **1**
  
- 2 Functional integration** **2**
  - 2.1 Self-service password reset . . . . . 2
  - 2.2 Self-service token management . . . . . 2
  - 2.3 Biometric voice print registration . . . . . 2
  
- 3 Usability and Internal Marketing** **4**
  - 3.1 Usability . . . . . 4
  - 3.2 Marketing . . . . . 4
  
- 4 User Identification Options** **5**
  - 4.1 Assigning unique, numeric IDs . . . . . 5
  - 4.2 Numeric mapping of alphanumeric login IDs . . . . . 5
  
- 5 User authentication options** **6**
  - 5.1 Numeric questions and answers . . . . . 6
  - 5.2 Biometric voice print verification . . . . . 7
  
- 6 Example Processes** **8**
  - 6.1 Touch-tone authenticated password reset . . . . . 8
  - 6.2 Voice print authenticated password reset . . . . . 9
  - 6.3 Password Manager-driven biometric sample enrollment . . . . . 11
  
- 7 Implementation Options** **12**
  - 7.1 Buying a new IVR system vs. extending an existing system . . . . . 12
  - 7.2 Turn-key IVR options offered by Hitachi ID . . . . . 12
  - 7.3 Leveraging an existing authentication process . . . . . 13
  
- 8 Integration Mechanisms** **14**
  - 8.1 Web service . . . . . 14
  - 8.2 Win32 API . . . . . 14
  - 8.3 ActiveX API . . . . . 14
  - 8.4 Unix shared-object library . . . . . 14

8.5	Command-line access from Windows . . . . .	15
8.6	Command-line access from unix . . . . .	15
8.7	Example function call sequence . . . . .	15
<b>9</b>	<b>Summary</b>	<b>16</b>

## 1 Introduction

This document outlines how Hitachi ID Password Manager can be integrated with an Interactive Voice Response (IVR) system, to enable:

- Self-service password reset from a telephone.
- Self-service token management from a telephone.
- Active enrollment of biometric voice print sample registration.

The remainder of this document is organized as follows:

- **Functional integration** describes the business processes that a Password Manager / IVR integration can expose.
- **Usability and internal marketing** outlines the usability concerns that a Password Manager / IVR integration should address, and how the solution should be marketed to its intended users.
- **User identification options** describes options for uniquely identifying users when they sign into an IVR system.
- **Authentication options** describes options for verifying user identity prior to making sensitive functions available.
- **Example processes** illustrates the user view of some possible system configurations.
- **Implementation options** outlines the various options organizations have for sourcing the technology required to expose Password Manager functions to a telephony channel.
- **Integration mechanisms** outlines the detailed technical mechanisms exposed by Password Manager to enable IVR integration.

## 2 Functional integration

There are three basic sets of desirable functionality that may motivate an integration between Hitachi ID Password Manager and an IVR system:

1. Self-service password reset and password synchronization
2. Self-service token management
3. Biometric voice print registration

### 2.1 Self-service password reset

Allowing users who have experienced a password problem to access self-service from a telephone, and resolve their own problem, is advantageous for several reasons:

- It allows users who forgot their initial network login password to resolve their own problem without any special measure to make this available from the workstation login prompt.
- It allows users who forgot their remote access (RAS or VPN) password to access self-service problem resolution without first connecting to the network.
- It encourages the use of self-service password reset in organizations where users are accustomed to getting service primarily with a telephone.

Since user authentication, password generation and password resets are all processed by the Hitachi ID Password Manager server, the telephone password reset automatically benefits from Password Manager's auto-discovery process, user profiles, password policy engine, e-mail integration and call tracking system integration.

### 2.2 Self-service token management

Users who sign into the network, or a remote access service, using a hardware token (most likely an RSA SecurID token) may experience problems and require service.

Possible SecurID token problems include users forgetting their PINs, losing their tokens, or users whose token clocks have drifted significantly away from the time reference on the ACE server.

These users may require service before accessing the network, so a telephony solution is desirable.

### 2.3 Biometric voice print registration

Organizations deploying a biometric voice print verification technology in their IVR infrastructure must acquire voice samples from the entire user population. Each voice print must be securely mapped to the particular user's user IDs in order to allow secure password reset.

Hitachi ID Password Manager can facilitate an automated, reliable, secure and effective process to prompt users to register, authenticate users prior to registration, map users voice prints to their system IDs, and enable the IVR system to securely capture their voice prints.

## 3 Usability and Internal Marketing

As with any self-service technology, usability and marketing are key to success. Users must be made aware of the IVR system's new features, and should have an incentive to use it rather than accessing manual service.

### 3.1 Usability

The IVR system must be easy to use. This means:

- It must be easy to access password reset, token management or registration from a frequently-accessed and well-known IVR system's menu.
- The process by which users identify themselves must be clear and easy to follow.
- The process by which users authenticate (prove their identity) must be clear and easy to follow.
- In the case of a password reset, it is preferable to have the system generate a random password, rather than asking the user to (awkwardly) enter it using a telephone.
- In the case of a password reset, it is preferable to reset all of the user's passwords, and clear any intruder lockouts, rather than having the user navigate a slow, sequential system- and function-selection process.

### 3.2 Marketing

Users must be made aware of the telephony integration. This means:

- The availability of the system should be advertised on multiple media. Examples include mass e-mails, distributed mouse-pads, text on workstation screen savers, text on workstation acceptable-use messages, etc.
- Users should be given the option of self-service problem resolution before they get the option of speaking to a human support analyst.
- Users should have a reasonable expectation of receiving better service from the system than from human support analysts. For example, the IVR system may notify users of the expected wait for human assistance, and continue to offer self-service even to users who elect to wait for a support analyst.
- In cases where registration is required or appropriate, users should be motivated to register – e.g., by prize draws.

## 4 User Identification Options

Users are identified on the network using alphanumeric login IDs. Since most IVR systems do not offer a reliable speech-to-text mechanism, they can only accept numeric input. This presents a challenge for a telephone password reset system: users must enter an alpha-numeric login ID, but the system can only accept a numeric ID.

### 4.1 Assigning unique, numeric IDs

In organizations where each network login ID is already associated with some unique numeric ID, the simple solution is to ask users to sign into the IVR system by keying in their numeric ID on the telephone touch pad.

Examples of such numeric ID include employee numbers, or home telephone numbers.

Alternately, if a user registration process will be used (e.g., to collect personal Q-A data for user authentication), then users may be asked to key in or select a new numeric personal identifier. An example might be the user's driver's license number. In this case, users will sign into the IVR with their new numeric ID.

### 4.2 Numeric mapping of alphanumeric login IDs

In some cases, numeric IDs are not available. This may happen if there are no existing numeric IDs available for all users, or if what numeric IDs exist are not correlated to network login IDs, or if a registration process is undesirable.

In these cases, users may be asked to sign in by pressing the keys on their telephone marked with the letters and numbers of their network login ID. For example, the user smith01 would type 7648401.

Since the digit mapping of two different alpha-numeric login IDs may produce the same number (e.g., poguh01 also maps to 7648401), an IVR system that uses this technique must allow for number collisions, and ask the caller to select the correct ID when the entered number resolves to more than one alpha-numeric login ID.

## 5 User authentication options

Users who sign into an IVR system to access a secure function, such as a password reset, must not only identify themselves, but also prove their identity using a process which is appropriately hard to fool. In other words, the rate of false-positive user authentication must be acceptable.

For example, if users can access a self-service password reset, then the difficulty of fooling the IVR authentication process must be comparable to the difficulty of cracking a password.

### 5.1 Numeric questions and answers

A simple process to authenticate users is to ask them to answer one or more personal questions. Personal questions should have the following characteristics:

- Answers should be private – relatively hard for anyone other than the user to come by.
- Answers should be easy – users should be able to quickly and reliably answer the questions, without having to remember anything new, and with a low likelihood of making mistakes.

Examples of personal questions that a user may be able to answer with some expectation of privacy, without remembering anything new, include all or parts of the following numbers:

- Social Security Number.
- Employee number (if this is typically secret).
- Driver's license number.
- Insurance policy number (if printed on a card the user carries with him, or if used often).
- Date of birth (of self or a close family member).
- First or current home telephone number.

Since all of these may be acquired by a third party, it makes sense to use more than a single question, to randomize which questions are used for any given authentication session, and to lock out users who repeatedly fail to authenticate.

**Note:** Using too few numeric Q-A pairs, or using data that is too easily acquired by an intruder, will have the effect of reducing password strength on the network. Biometric voice print verification is a stronger technology, and is described below.

## 5.2 Biometric voice print verification

A simpler, more secure, but more costly process for caller authentication is to capture a voice print sample from each user during a registration process, and to subsequently authenticate callers by asking them to speak one or more phrases, so that their new response can be compared to their registered sample.

Biometric voice print verification is commercially available, can yield effectively zero false-positive recognitions, and low false-negative failures (on the order of 1% to 2% of valid authentication attempts ending with a failure to recognize the speaker).

Biometric voice print verification requires that a voice print sample be collected in a secure manner from each user prior to the first instance where the user must access the system. Password Manager can drive this process, as described in [Subsection 6.3 on Page 11](#).

## 6 Example Processes

The following are three example processes that illustrate how Hitachi ID Password Manager and an IVR system can co-exist:

### 6.1 Touch-tone authenticated password reset

Password reset using a telephone, with touch-tone caller authentication and a randomly-generated password (to minimize alpha-numeric input on a telephone) works as follows:

1. **User:** forgets password or triggers intruder lockout.
2. **User:** dials the support number, navigates to the “password problems” section.
3. **Hitachi ID Telephone Password Manager server:** prompts the user to key in a personal ID, such as an employee number or a numeric mapping of the user’s alphanumeric network login ID (e.g., smith01 maps to 7648401).
4. **User:** keys in the ID.
5. **Telephone Password Manager server:** connects to the Hitachi ID Password Manager server.
6. **Password Manager server:** looks up the user’s profile.
7. **Password Manager server:** selects random subset of the user’s questions.
8. **Telephone Password Manager server:** prompts the user to answer the selected questions.
9. **User:** keys in (numeric) answers to the selected questions.
10. **Telephone Password Manager server:** forwards answers to the Password Manager server.
11. **Password Manager server:** compares answers to registered data.  
 . . . Repeat if failed, continue if success, possible lockout.
12. The process by which the user chooses a new password proceeds as follows:
  - (a) **Telephone Password Manager server:** asks Password Manager to generate a random password for this user.
  - (b) **Password Manager server:** provides a random, policy-compliant password string.
  - (c) **Telephone Password Manager server:** enunciates the password and asks the user to accept / retry.
  - (d) **User:** presses a digit to accept the password choice.
  - (e) **Telephone Password Manager server:** asks Password Manager to reset passwords for this user, on selected systems, to the requested password string.
  - (f) **Password Manager server:** attempts password reset immediately and possibly queues it up for retries.

- (g) **Password Manager server:** may set the “password expired” flag on new passwords, so that the user will be forced to choose a new password at login time.
- (h) **Password Manager server:** writes a ticket to an incident management system.
- (i) **Password Manager server:** sends the user a confirmation e-mail.

## 6.2 Voice print authenticated password reset

Password reset using a telephone, voice print caller authentication and a randomly-generated password (to minimize alpha-numeric input on a telephone) works as follows:

1. **User:** forgets password or triggers intruder lockout.
2. **User:** dials the support number, navigates to the “password problems” section.
3. **Hitachi ID Telephone Password Manager server:** prompts the user to key in a personal ID, such as an employee number or a numeric mapping of the user’s alphanumeric network login ID (e.g., smith01 maps to 7648401).
4. **User:** keys in the ID.
5. **Telephone Password Manager server:** connects to the Hitachi ID Password Manager server.
6. **Password Manager server:** looks up the user’s profile.
7. **Password Manager server:** selects random subset of the user’s questions.
8. **Telephone Password Manager server:** prompts the user to answer some questions.
9. **User:** speaks answers into the telephone.
10. **Telephone Password Manager server:** compares answers to voice characteristics stored on file.  
... Repeat if failed, continue if success, possible lockout.
11. The process by which the user chooses a new password proceeds as follows:
  - (a) **Telephone Password Manager server:** asks Password Manager to generate a random password for this user.
  - (b) **Password Manager server:** provides a random, policy-compliant password string.
  - (c) **Telephone Password Manager server:** enunciates the password and asks the user to accept / retry.
  - (d) **User:** presses a digit to accept the password choice.
  - (e) **Telephone Password Manager server:** asks Password Manager to reset passwords for this user, on selected systems, to the requested password string.
  - (f) **Password Manager server:** attempts password reset immediately and possibly queues it up for retries.

- (g) **Password Manager server:** may set the “password expired” flag on new passwords, so that the user will be forced to choose a new password at login time.
- (h) **Password Manager server:** writes a ticket to an incident management system.
- (i) **Password Manager server:** sends the user a confirmation e-mail.

### 6.3 Password Manager-driven biometric sample enrollment

Registration of user voice print data using the Hitachi ID Password Manager web form and deployment infrastructure works as follows:

1. **Password Manager server:** extracts a user list from one or more target systems nightly.
2. **Password Manager server:** compares the list of users to those who have registered a voice print.
3. **Password Manager server:** e-mails unregistered users (up to a certain number of users per run) a request to register, with an embedded URL.
4. **User:** receives notification in e-mail, clicks on URL.
5. **Password Manager web interface:** prompts the user to type his network login ID.
6. **User:** types his network login ID.
7. **Password Manager web interface:** prompts the user to type his current NOS password.
8. **User:** types current password.
9. **Password Manager web interface:** validates the password against the indicated system.  
*... repeat if authentication failed, lockout if too often.*
10. **Password Manager web interface:** prompts the user to dial a number with his telephone, wait for a prompt and key in a (long, random, single-use, time-expired) PIN.
11. **User:** dials phone number, pauses, PIN.
12. **Hitachi ID Telephone Password Manager server:** asks Password Manager to validate that the PIN is valid and current.
13. **Password Manager server:** sends the Telephone Password Manager system the user's NOS login ID.
14. **Telephone Password Manager server:** prompt the user to select a personal, numeric identifier (e.g., SSN, D/L number).
15. **User:** keys in the number he will use to identify himself to the Telephone Password Manager system in the future.
16. **Telephone Password Manager server:** prompt the user for a speech sample.
17. **User:** answers the question on the telephone.  
*... repeat above two steps for multiple samples.*
18. **Telephone Password Manager server:** tells Password Manager that the user is now registered and should not be prompted to register again.
19. **Password Manager server:** updates internal user profile to indicate completed Telephone Password Manager status.

## 7 Implementation Options

Hitachi ID Password Manager can be integrated with a telephony user interface in a number of ways:

### 7.1 Buying a new IVR system vs. extending an existing system

Hitachi ID offers two options to customers who wish to enable telephone access to Hitachi ID Password Manager:

1. Purchase a turn-key IVR system, designed specifically for authenticating callers and providing self-service password resets, from Hitachi ID.

Turn-key system options are described in Section 7.2.

If an existing Automatic Call Direction (ACD) system is in place, then it must be configured to forward relevant calls to the Password Manager IVR system.

2. Extend the existing IVR system to provide front end password reset functionality, (and potentially, biometric voice print authentication), using Password Manager as a “back end” to provide user authentication and general password management services.

In this case, the call flow logic on the existing IVR system is modified to prompt the user for identification and authentication information. The IVR is programmed to verify user authentication by calling either:

- (a) Password Manager (if using keypad PIN authentication), or
- (b) an external voice print biometric system (if using voice prints) implemented by the customer (eg. Nuance, Speechworks).

Once the IVR has authenticated the user, it can make calls to the Password Manager server to request various password reset services.

Password Manager can be integrated with almost any existing IVR system, as described in Section 8 on Page 14.

The software required to integrate Password Manager with any existing IVR system is included at no additional charge. (Particular IVR systems may also require software extensions as available from the IVR vendor, eg. XML over HTTPS).

### 7.2 Turn-key IVR options offered by Hitachi ID

Hitachi ID offers a turn-key IVR option, Hitachi ID Telephone Password Manager, which uses touch-tone caller authentication, and leverages the Web-based Hitachi ID Password Manager registration process to build user profiles for numeric Q-A authentication.

This solution is tightly integrated with Password Manager, using the secure API described in Section 8 on Page 14.

Note that Password Manager has an open interface specification, which allows other IVR biometric voice print authentication systems, such as Vocent, to leverage Password Manager for general enterprise password management.

### **7.3 Leveraging an existing authentication process**

Organizations with an existing IVR system may choose to continue to use an existing caller authentication process, or to strengthen it prior to activating self-service password reset.

The existing identification and authentication process may have to be replaced because it is not secure enough, and would weaken password security if it enables self-service password reset.

## 8 Integration Mechanisms

Hitachi ID Password Manager exposes APIs suitable for use by an IVR system over a variety of communication channels. In each case, strong encryption makes it possible to securely locate the IVR system at a different site from the Password Manager server.

### 8.1 Web service

A web service allows IVR systems and other applications to remotely invoke methods on the Hitachi ID Password Manager server, to perform functions such as user and account lookup, Q-A authentication, random password generation, and to initiate password resets or to clear intruder lockouts.

Remote applications normally access the web service over HTTPS for security, and must provide a 128-bit secret key to prove that they are authorized to use the API at all.

Organizations wishing an extra level of security may periodically change the authentication key, and limit the range of IP addresses that are permitted to access the API to just legitimate IVR systems or other applications.

IVR systems that support integration using web services include those from Intervoice and Nortel/Periphonics.

### 8.2 Win32 API

The same integration functions available through the web service ([Subsection 8.1 on Page 14](#)) are available in a Windows 32-bit DLL. This DLL communicates with a TCP/IP socket listener service on the Hitachi ID Password Manager server, and the two end-points implement a secure communication protocol that includes mutual authentication, random session keys and 128-bit IDEA encryption.

Windows-based IVR systems, such as those from Apropos, can readily link against this DLL.

### 8.3 ActiveX API

An ActiveX (COM) wrapper is provided for the Win32 DLL described in [Subsection 8.2 on Page 14](#), to enable IVR systems that more readily integrate with ActiveX components to tie into Hitachi ID Password Manager. Other than different calling / linking semantics, this is the same Win32 API as described earlier.

### 8.4 Unix shared-object library

The same integration functions available through the web service ([Subsection 8.1 on Page 14](#)) are available in a Unix shared-object library. This library communicates with a TCP/IP socket listener service on the

Hitachi ID Password Manager server, and the two end-points implement a secure communication protocol that includes mutual authentication, random session keys and 128-bit IDEA encryption.

Unix-based IVR systems, such as those from Lucent / Avaya, can readily link against this shared object library. (A UnixWare binary is made available for this popular system).

## 8.5 Command-line access from Windows

A command-line wrapper that uses the Win32 DLL API is available, to enable integration from Windows-based IVR systems that cannot directly link to DLL libraries, but can invoke command-line programs.

## 8.6 Command-line access from unix

A command-line wrapper that uses the Unix shared object is available, to enable integration from Unix-based IVR systems that cannot directly link to shared object libraries, but can invoke command-line programs.

## 8.7 Example function call sequence

The touch-tone-authenticated password reset process described in [Subsection 6.1](#) on [Page 8](#) is implemented by calling the following library functions, using any of the API variants described above:

- **PPInitialize** – initialize the API and connect to the Hitachi ID Password Manager server with a suitable address and encryption key.
- **PPFindUser** – lookup a user with a numeric identifier. Note that **PPFindIVRUser** might also be used, if the user keys in a numeric mapping of his alphanumeric network login ID. Where **PPFindUser** returns 0 or 1 matched user records, **PPFindIVRUser** might return more and the IVR system must ask the user to select just one.
- **PPGetUserQuestions** – get a list of authentication questions that the user might be required to answer. The IVR system must be pre-programmed with speech recordings for every available question, or a text-to-speech engine.
- **PPValidateUserAnswers** – validate that the answers keyed in by the user are correct.
- **PPRandomPassword** – called at least once, and possibly several times, to generate a random password, and read it out to the user as a possible new password.
- **PPChangePassword** – reset all passwords for this user to the new value. Alternately, **PPGetUserAccounts** and **PPSingleReset** may be used to allow the user to reset individual passwords, rather than every one.

## 9 Summary

Self-service password reset, self-service RSA SecurID token management and automated registration of biometric voice print samples can all be implemented by integrating Hitachi ID Password Manager with an IVR system.

Password Manager licensees may choose to purchase a dedicated IVR system from Hitachi ID, specifically for these applications, or to extend an existing IVR system to include new call logic. Integration is available for every kind of existing IVR system, through multiple language and platform bindings of a powerful Password Manager API.

User identification can be implemented using speech-to-text technology, or user input of unique numeric identifiers or numeric-mapped network login IDs.

User authentication can be implemented using either text prompts for personal information, followed by touch-tone input of responses, or using biometric voice print verification technology.

System integration for a telephony-enabled password management system can range from one or two days of effort to activate a turn-key, touch-tone enabled IVR system up to two or three weeks to extend an existing biometric system.