HP Integrated Login

HP Integrated Login coordinates the use of security systems and improves the usability of computer systems running the HP-UX* operating system.

by Jane B. Marcus, Navaneet Kumar, and Lawrence J. Rose

The HP Integrated Login product provides major usability gains for customers deploying enhanced security technologies on computer systems based on the HP-UX operating system. In this article, we describe the customer needs and the HP Integrated Login solution.

As computer networks expand, and as pirates more frequently travel the information superhighway, customers require more stringent methods for securing data and accounts. The base HP-UX operating system provides standard UNIX® security mechanisms, but these do not meet all the needs of security-minded customers. There are many security technologies available commercially and in the public domain. HP customers sometimes wish to deploy one or more of these technologies on the HP-UX platform.

Security technologies use passwords to verify the user's identity and determine access rights to data and services. A user must enter a password and the password must be verified before access is granted. For example, basic HP-UX security requires that a password be entered for the user to gain access to the HP-UX machine. In addition to machine entitlement, passwords also may be used to verify the user's right to access protected services (e.g., mail systems) in the user's environment.

Security-minded customers see many benefits to deployment of enhanced security technologies—for example, protection against impostors and network eavesdroppers. However, placing additional security technologies on top of the HP-UX system can create a burden to the users of the system. When multiple security technologies are deployed (to monitor access to various protected services in the user environment), each technology requires password verification. Thus, a user may be forced to type in a password for the HP-UX system and then for each additional security technology. Furthermore, the use of multiple security technologies creates a complex task for users when passwords need to be changed in multiple places.

Customers need enhanced security, but they also want usable systems. Customers want to operate in a familiar environment, and do not want to learn many new commands for accomplishing basic tasks. When faced with a lengthy or complicated process, typical users may ultimately compromise the security of their systems by writing down passwords and procedures that might otherwise be forgotten. Customers will not accept a burdensome process for their users.

HP Integrated Login

The HP Integrated Login product has evolved to meet the customer needs discussed above. The original product for the HP-UX 9.x operating system was developed in response to DCE† customer requirements and was delivered primarily for use by HP's DCE customers. However, with the HP-UX 10.0 release, the HP Integrated Login product has been made extensible, so that it can serve the HP-UX community at large. The latest HP Integrated Login provides library interfaces that allow a generic set of security technologies to be integrated with HP-UX. The customer has maximum flexibility to choose and deploy appropriate technologies. Since DCE has an outstanding security technology, we expect that HP Integrated Login users will most often choose DCE for their security needs, but the HP Integrated Login product can support other technologies equally well.

The primary purpose of the HP Integrated Login product is to allow HP-UX users a convenient method for incorporating other security technologies into the standard HP-UX environment. Users should be able to use familiar HP-UX tools to accomplish familiar tasks. Thus, HP Integrated Login extensions have been added to several standard HP-UX 10.0 utilities.

The most important functionality delivered by HP Integrated Login is a single-step login: the user enters a password once at login time, and this password is used to grant access to the HP-UX machine as well as verify access among all the configured security technologies. The HP-UX 10.0 commands login and su have been enhanced to include single-step login capabilities. Also, the HP user desktop (HP VUE) has been integrated to support multiple security technologies. Login information is propagated throughout the entire VUE session and logins need not be repeated when new VUE windows are opened.

Password consistency is fundamental to most HP Integrated Login deployments. A user chooses one password, and this password is adopted across all security technologies. Thus, the user can supply the password once and the HP Integrated Login utilities transparently perform logins to each configured security technology on behalf of the user. The HP-UX 10.0 passwd command has been integrated to synchronize passwords for the user, so that a requested password change can be propagated to all configured security technologies. Likewise, user information commands chfn and

† DCE is the Distributed Computing Environment. See article, page 6.

chsh are provided to allow changes to finger and user shell information across security technologies. (Finger information includes the user's real name, location, and telephone number.)

It is typical of the UNIX operating system that several operations are password-controlled—for example, file transfer to or from a remote machine and screen lock or unlock. Integrated file transfer protocol (ftp) and HP VUE lock utilities have been provided. Consistent with other HP Integrated Login utilities, these operations verify user access for all configured security technologies based on one user-supplied password.

The HP Integrated Login product provides extensions to HP-UX commands to support multiple security technologies on top of the HP-UX system. The extension method involves a new shared library provided with HP-UX 10.0. Integrated HP-UX utilities make calls to this shared library (libauth.sl). The libauth library calls handle various security tasks such as password verification for login and password changes. Thus, HP-UX utilities relinquish to libauth the direct responsibility for supporting diverse security technologies. Furthermore, these HP-UX utilities have no awareness of multiple security technology configurations, and have no knowledge of the details of how these security technologies function.

HP Internal Customer Needs

Enhanced security technologies on top of HP-UX have existed for some time. Before the creation of HP Integrated Login, several security technologies had independently been integrated into the HP-UX system. Each security technology had its own login method, and each security product would spin off new versions of HP-UX login commands and HP VUE to incorporate the technology's login implementation. These efforts were difficult to coordinate, and there grew to be many different versions of HP-UX login commands to accommodate all of these security technologies. One HP Integrated Login goal was to replace the myriad of login implementations with one generic login methodology. This was expected to solve a number of different problems, including the HP support cost to maintain multiple code bases. The solution required the definition of a generic login procedure, flexible enough to accommodate all the existing login methods.

Extensibility

HP Integrated Login supports multiple security technologies. The HP Integrated Login configuration file declares which technologies are being integrated. Typically, the HP-UX machine administrator uses HP Integrated Login administrative tools to create and maintain this configuration file. Each technology declared in HP Integrated Login's configuration file must provide a technology shared library. This shared library will be dynamically loaded by the HP Integrated Login library (libauth), which coordinates all underlying security technologies. The libauth library determines the names of the technology shared libraries and the order in which to load them based on the contents of the HP Integrated Login configuration file. Fig. 1 shows the resulting architecture. The libauth library needs no special knowledge of any security technology library that it loads. Well-defined interfaces exist between the libauth coordination library and the security technology shared library.

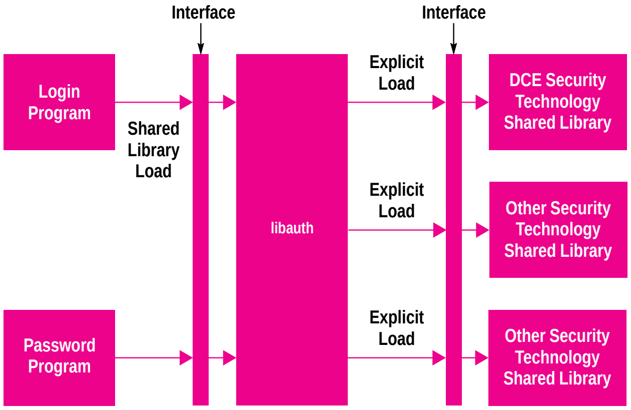
Interface
Interface
Login Program
Password Program
Shared Library Load
libauth
Explicit Load
Explicit Load
Explicit Load
DCE Security Technology Shared Library
Other Security Technology Shared Library
Other Security Technology Shared Library

Fig. 1. The extensible architecture of HP Integrated Login.

From HP-UX commands, the following can occur:

- The HP-UX command dynamically loads the HP Integrated Login shared library (libauth).
- The libauth library reads the HP Integrated Login configuration file and dynamically loads the configured security technology libraries.
- The HP-UX command makes library calls to libauth to handle login and password functions.
- The libauth library makes library calls to security technology libraries.

An exception in the HP Integrated Login library strategy is the method by which basic HP-UX security is provided. While the HP Integrated Login configuration may specify the use of basic HP-UX security, there is no HP-UX technology library to be dynamically loaded. Rather, the HP-UX commands handle basic HP-UX functions from within the command code.

The libauth library is shipped with the HP Integrated Login product, and is dynamically loaded by the integrated HP-UX commands and HP VUE. HP-UX utilities use libauth to integrate security technologies, but the basic HP-UX security code is always accessible since it is contained within the HP-UX utilities. Thus the HP-UX 10.0 utilities can still provide standard HP-UX functionality on systems that do not have libauth installed. While the integrated commands must be aware of their use of libauth, the commands are completely unaware of libauth's use of underlying security technology libraries.

Configuration of Multiple Technologies

The HP Integrated Login configuration file is used to define a login policy to be used on a particular machine. The policy specifies which technologies are in use. When multiple security technologies are in use, the relative priority of these technologies must be configured for HP Integrated Login operation. One technology is configured as the primary login technology. This primary login technology will be the initial technology to be consulted for user password verification. If the primary login succeeds, the user will be granted access to the HP-UX machine, and additional logins can then proceed (transparently) to verify the user with other security technologies.

In case the primary login does not succeed, a fallback technology can be configured. If the user can be verified with the fallback security technology, the user is granted access to the HP-UX machine, and again, other configured logins can then proceed.

The importance of the fallback strategy cannot be understated. Security technologies often have dependencies on network communications and cannot function if the network is not intact. For some customers, it is unacceptable for users to be denied access to their local machines because of network problems. The HP Integrated Login fallback strategy allows customers who require a high level of robustness to use HP products with confidence.

The relationship between the primary login technology and the fallback login technology must be well-understood. In some cases, the primary login technology may attempt to synchronize the fallback technology with current user information. For example, when DCE serves as the primary login technology, it is an HP Integrated Login option to automatically populate the HP-UX user information database (i.e., the /etc/passwd file) with information from the DCE security database. In most cases, the /etc/passwd file will never be accessed at login time, because DCE, as the primary login technology, will verify the user. However, when DCE is unavailable, HP-UX login security can be used as a fallback to log in all users known to DCE. Such an arrangement is advantageous for administrators who want to maintain user accounts in one primary location, but also want to facilitate fallback logins where necessary.

In other cases, administrators may purposely wish to maintain some users in one security technology database and other users in a different security technology database. The HP Integrated Login configuration of primary and fallback login technologies can facilitate this process. The HP Integrated Login libauth library will consult the primary login technology first to verify the user, but if this user is not known to the technology, HP Integrated Login can be configured to consult the fallback login technology.

In addition to configured primary and fallback login technologies, other login technologies can be configured. These logins will be done transparently for the user, in the order in which they have been configured with HP Integrated Login. The purpose of these additional logins may be to enable user access to some protected service in the user's environment. These additional logins will only be attempted if the primary or fallback login has succeeded, that is, if this user has been granted access to the HP-UX machine. Errors occurring with these additional logins are nonfatal, meaning that the user session can proceed even if one or more of these additional logins fails.

The organization of technologies in the configuration file is used by libauth to determine the order in which technologies should be loaded and accessed. We call libauth's ordering of technologies the *policy chain*, and it reflects the configuration of primary login, fallback, and additional login technologies. The policy chain is used by libauth to make decisions on how to sequence through the configured technologies.

The configuration file may also contain directives to libauth regarding handling of login errors. These directives logically become part of libauth's policy chain and determine libauth's actions in the event of login failures. For instance, the configuration file may specify that a login failure because of an incorrect password entry should result in a denial of machine access, regardless of whether this password may be verifiable by other configured technologies in the policy chain. The libauth library's actions in this case would be to stop the login sequence after the initial failure and refrain from cycling through the security technologies. The behavior of libauth is configurable, so it is also possible to specify a configuration that authorizes libauth to pass the login request to the next technology in the policy chain.

The configuration file also includes a mechanism to pass configuration information to the security technology libraries that will be loaded by libauth. Configurable parameters can be specified for each specific security technology. These parameters are meaningful only to the security technology library and are determined by the security technology library provider. For instance, a specific security technology may support the notion of a session lifetime. A configurable parameter called LIFETIME may exist in the HP Integrated Login configuration file to be passed to the security technology when being loaded by libauth. The libauth library will pass the configuration information to the security technology library, but will not use or process this information in any way (thus preserving the extensibility model).

libauth Login Processing

To accomplish a login that results in a user session, several behind-the-scenes events must occur. The procedure consists of three phases: the initialization phase, the login phase, and the session-setup phase.

During the initialization phase, the HP Integrated Login policy is read from the configuration file. The libauth library proceeds to load the security technology libraries and charges them to run through their respective initializations. Initialization failures from any of the security technology libraries cause libauth to mark the technology as inaccessible. When security technologies are inaccessible, libauth must adjust its understanding of the policy chain to reflect the effective policy. Upon successful initialization, libauth and the security technology libraries exchange entry point information. This makes it possible for two-way communication to occur between the security technology library and libauth. The libauth library can now call the security technology library interfaces to handle security tasks, and the security technology libraries can communicate messages and error status.

The login phase is a two-step process. Step one determines whether the user should be granted access to the local system. Prompts are issued for the user name and password, and subsequently the primary login technology library is called to verify access. Logically, this step may be considered a Boolean operation which simply returns a yes or no answer regarding the user's entitlement to access the local system. Depending upon the configured policy chain, libauth may continue on failure to the configured fallback technology, or may deny access.

The second step in this login phase (after having granted machine access) is to complete any additional logins that should be done. These additional logins may be needed to enable operations with some protected services once the user session begins. In current implementations, additional logins can only succeed if the password entered is valid for this user across all security technologies. However, libauth code is in place to support different passwords for additional security technologies, although this code is not yet in practical use. The method for supporting multiple passwords depends on the primary login technology's ability to securely store passwords to be used with other security technologies. A successful login with the primary login technology would result in the stored passwords being passed to libauth for use with the other technologies in the policy chain.

The session-setup phase is for establishing the user session. The information about how to set up the session is retrieved from the underlying primary login technology database. In particular, the user and group IDs must be set for the new session, and the user shell must be started. In addition, the exportation of environment variables occurs. If any configured technologies require special environment variables to be set, these environment strings are passed back to the HP-UX command so that they are exported at session-setup time.

Password and Information Processing

The libauth library interfaces oversee changes to user information, such as password, user shell, and finger information. The HP-UX passwd command, for example, loads libauth to coordinate password changes. The libauth (and technology library) initialization phase described for login processing is the first step here as well.

Before calling libauth to make a password change, the passwd command calls libauth to check the new password that has been proposed. Most security technologies apply password strength checking algorithms to newly created user passwords. These algorithms test whether the new password meets certain criteria. For example, one HP-UX requirement is that the new password must have at least two alphabetic characters and at least one numeric or special character. For password strength checking, a libauth interface determines if the selected password is acceptable to all configured security technologies. The password is rejected if any of the security technology libraries rejects it, and the operation fails.

If the proposed password is acceptable, the command calls libauth to contact the primary login technology. The primary login technology will then change the password in the primary login technology's user database. Failure to change information correctly with the primary login technology causes the entire operation to fail. If the change succeeds, libauth follows the policy chain to request password changes in all other security technology databases. If a failure occurs for this user with any of the additional (i.e., optional) technologies, an error indication is recorded and the next technology in the chain is tried. If a failure occurs during a password change operation, the password may no longer be consistent across all technologies. An error indication clearly states this and gives advice on how to remedy the situation manually.

Some details of the policy chain configured in the HP Integrated Login configuration file do not apply to password processing. The configuration file is used to determine the primary login technology. However, libauth password interfaces make no attempt to deal with a configured fallback technology in case of error.

The libauth library interfaces allow other user information to be changed. The user's shell can be also changed. In all cases, changes to user information start by attempting to make the change in the database of the primary login technology. Successful changes cause the operation to continue down the policy chain to completion.

Other libauth Interfaces

Aside from password and login functionality, other libauth interfaces are available to HP-UX commands.

For security technologies that include the concept of login expirations, libauth supports a refresh operation. For example, suppose that the user's machine has been left locked by the VUE screen lock program, and the user's login expires before the user returns to unlock the machine. The libauth refresh interface allows bypassing some of the details of the full login process, although reprompting of the password is required for this step to maintain security.

Another libauth interface resets the current login information. This interface is used by commands that can switch between users, such as ftp and su. The reset action cleans up any residual login information, effectively terminating a previous login across all security technologies.

Choosing a Primary Security Technology

An HP Integrated Login goal is to simplify user administration among multiple security technologies. When multiple security technologies are deployed, multiple user information databases may coexist. These *registries* are repositories of user-related information, and different technologies require the storage of different types of information about a user. HP Integrated Login configuration of a primary login technology determines which registry is most important for maintaining user information. The primary login technology's registry assumes the role of the main location for user information, and registries from other technologies are logically subservient. For example, if the password that the user has provided is determined to be incorrect when checked against the main registry, HP Integrated Login may be configured to deny access without further checking of the password against other technology registries. If the user requests a change of password and for some reason the main registry cannot entertain the change, no attempt is made to request the change in other registries.

When deploying multiple security technologies, the choice of the main registry is very significant. System administrators might ask what features such a registry should have. Especially in a networked environment, this registry must be highly available and reliable, since users may be denied access if it is not in operation. The main registry must be capable of storing critical user information, including but not limited to user name, user identifier, password, group identifier, home directory, and login shell. Since user information is likely to change as we move towards more complex systems, built-in extensibility of the registry is highly desirable.

We find DCE to be an excellent choice for the main security technology. The DCE security service registry satisfies all basic requirements for a main registry.

The DCE registry is highly available. The implementation allows for a collection of one master and several replicas, so user information can be obtained from multiple (but consistent) sources. Replicas are copies of the master information and are read-only sources of information. If a replica goes out of service, others are available to provide user information. If the master goes down, a suitable replica can be transformed into a master. If service degrades because of heavy demand, additional replicas can be added to expedite requests. Consequently, the service is scalable and reliable.

DCE uses Kerberos™ authentication protocols and is highly secure in a distributed environment. For example, DCE does not transmit passwords in the clear across the network. This feature is not particularly useful if other technologies do otherwise, but the main registry should not be the weak link.

The OSF DCE 1.1 registry is extensible. System administrators can extend the registry to hold arbitrary user information. For example, DCE 1.1 uses this extensibility feature to support password aging (mandating that passwords be changed regularly) and password strength checking.

DCE is serviceable. Logging and audit trails can be used to diagnose error conditions.

In summary, we find DCE to be the logical choice for the primary login technology and to serve as the main registry of user information. (See the article on page 41 for more information about DCE security services.)

Login Access Using HP Integrated Login and DCE

Although the HP Integrated Login design does not require it, our implementation works very well with DCE providing the main registry of user information. This solution is robust and allows administrators to focus their efforts on maintaining user information in one location: the DCE registry. Fig. 2 illustrates how HP Integrated Login uses the DCE registry.

Customers with robustness requirements often choose to configure HP-UX security as a fallback technology. As described earlier, the fallback technology is used when the primary login technology is unavailable. With DCE as the primary login technology, DCE is unavailable when the network is not operational. Since HP-UX security is local to the machine and is unaffected by network errors, an HP-UX fallback may be a good choice. However, if the fallback registry is to provide access that is consistent with the main registry, it must be kept consistent with the main registry. Support for keeping the registries synchronized is obviously needed.

For this purpose, DCE provides a tool, passwd_export, that exports the information in the DCE registry to the native HP-UX registries, /etc/passwd and /etc/groups. When HP Integrated Login is installed, a system administrator can configure the HP-UX command cron to run passwd_export periodically to keep the registries consistent.

DCE user accounts are valid across the DCE network environment. Once established in the DCE registry, a DCE user can log in from any machine in the user's DCE environment, with no other special administration required. The DCE registry is implemented as a centralized network service, with requests travelling back and forth over the network from the registry to the client machines. However, DCE allows registry user information to be overridden at the local machine level. In this case, information is taken from the local machine rather than from the DCE network registry. An override mechanism is important to machine administrators wishing to customize their individual machines. For example, in a traditional UNIX system, each machine has a superuser account root. Machine administrators do not want the root account to share a password with all root accounts on machines in the DCE networked environment. Rather, machine administrators want to maintain the password for the root account locally. In this case, administrators must override the information in the main registry in favor of information stored on the local machine.

To handle such cases, DCE provides support for an override file. This file has a format similar to the traditional UNIX /etc/passwd file. If a user is maintained in the override file, the user's access to the machine is verified based on the override file entry and is not verified by the DCE registry. By common use, root is maintained in the override file to ensure that for superuser privileges a local password is required. The DCE override file is only readable by the superuser account and as such is more secure than the HP-UX /etc/passwd file.

Since DCE is a scalable, reliable, and secure service, some installations with especially stringent security requirements may wish to disable fallback login verification. In general, customers can rely on DCE to provide consistent service as

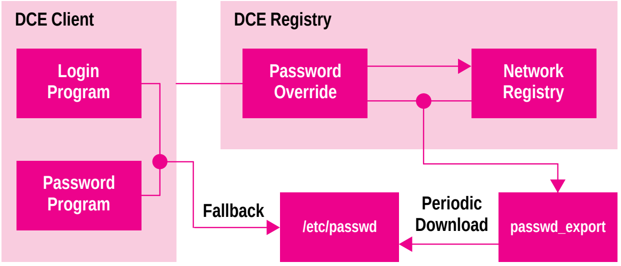

Fig. 2. Integrated login using the DCE registry.

long as the network is operational. Some customers disable fallback to basic HP-UX security because the HP-UX /etc/passwd file is inherently less secure than many customers require. For HP Integrated Login DCE configurations with no fallback technology, most logins will be disabled if there are network problems. However, users being administered in the DCE override file will still have login access in case of network failure, since the override file is stored on the local machine and is unaffected by network errors.

Login Information Maintenance: DCE and HP-UX

Suppose HP Integrated Login has been configured with DCE as the primary login technology and HP-UX security provides the fallback technology.

Example 1. A user wishes to change a password. We have two registries to consider: DCE and HP-UX. The following sequence of events occurs:

- Since DCE is the main registry, the old and the desired new passwords are obtained and passed to the DCE security technology library.
- The DCE registry verifies that the old password was correct and further determines if the new password is strong enough. If these checks pass, the user's password is changed in the DCE registry.
- No attempt is made to contact the fallback registry (/etc/passwd) at this time. However, libauth could propagate the password change to other configured technologies.
- After a certain interval configured by the system administrator, passwd_export runs and exports the changed password information to the HP-UX /etc/ passwd file. Thus, the fallback plan to HP-UX remains intact with this synchronization.

Example 2. A user whose account information is stored in the DCE override file requests a password change:

- The libauth library passes the request to the DCE security technology library. When user account information is kept in the DCE override file, passwords are changed in the override file only. The DCE registry is not changed at all.
- When passwd_export runs, it exports the changed password from the override file to /etc/passwd. This is how the local root user can change its password.

Example 3. A user requests a shell change:

- The chsh command calls libauth to pass the new shell information to the primary login technology library (DCE).
- If configured, passwd_export runs and exports the changed shell information to the HP-UX /etc/passwd file. Thus, HP-UX and DCE registries remain synchronized.

If passwd_export is not run periodically, some traditional UNIX commands and library calls with dependencies on the /etc/passwd file might use stale data. For example, the ls command gets user information from the /etc/passwd file. If the /etc/passwd entry for this user is not kept consistent with the information in the DCE registry, the ls command may be relying on old data for this user.

Login Information Maintenance: NIS and DCE

Suppose HP Integrated Login has been configured with HP-UX as the primary login technology. By way of clarification, it should be noted that NIS support falls under the generic HP-UX umbrella because HP-UX commands have been integrated with NIS for several years. At present, the code to support NIS is retained in the HP-UX commands. Thus, when HP-UX security has been configured, this effectively can include NIS if it has been deployed in the HP-UX environment. Currently there is no way to ensure full account consistency between NIS and DCE because there is no NIS utility comparable to DCE's passwd_export. Thus, users added to the NIS registry must also be added to the DCE registry by the system administrator.

Example 4. A user password change is requested and the HP-UX system (NIS) is the main registry, that is, password verification by NIS determines the user's right to machine access. Suppose also that DCE has been configured for additional login because users need access to some DCE services.

- The user wishing the password change must present the old password and the desired new password. The passwd command calls libauth.
- The libauth library tells the passwd command that the HP-UX system has been configured, so the passwd command inline code handles this password change operation.
- If the user's account is in the local /etc/passwd file, the password is changed there. If the user's account is maintained in the central NIS registry, the password is modified there.
- The passwd command calls libauth to propagate the password change to other configured registries. This request is passed to the DCE technology library and, if successful, results in a password change in the DCE registry. If for some reason the password cannot be changed in the DCE registry, the user is advised to try changing the DCE password again later. The passwd command now provides a command line option to change a password in a specified registry.

The Single Sign-on Problem

HP Integrated Login operates on HP-UX machines only. Much work remains to be done for customers who need a higher level of flexibility and integration. For example, a PC user on a Novell network would like to enter a password at network login time and have this password also validate access for other integrated systems. Unfortunately, there are extremely complex problems associated with login and password synchronization across operating systems and across hardware platforms. This larger problem is often called the single sign-on problem, and is being addressed by an industry working group of which HP is a coleader.[1]

Summary

The HP Integrated Login product addresses the needs of customers wishing to deploy multiple security technologies. HP Integrated Login improves usability by providing single-step login. Options to configure fallback login technologies ensure robustness in the event of network failure. HP Integrated Login is especially convenient for customers deploying DCE, because DCE and HP Integrated Login together provide the tools required for maintaining a high level of consistency between DCE and the HP-UX system for user account information.

HP Integrated Login has been made extensible, beginning with the HP-UX 10.0 release. HP-UX customers are not locked into any particular security technology by design, and customers can incorporate new technologies without changing the underlying commands framework. Customers use the same set of UNIX tools that they are already familiar with, because these utilities now use the HP Integrated Login shared library to support multiple security technologies. Costs to HP are reduced by the centralization of support for multiple security technologies on the HP-UX platform.

Acknowledgments

We wish to acknowledge the efforts of our teammates in creating the HP Integrated Login product. In particular, the contributions of project manager Frederic Gittler and Daniel Nguyen are outstanding. Also, a special mention must be made of John Brezak, who did early prototype work for the HP Integrated Login project.

Reference

1. *OSF Single Sign-On (SSO) Working Group Draft Paper/RFC*, February 1, 1995. Accessible on the Worldwide Web at URL http://www.dstc.qut.edu.au/MSU/research_news/osf/sso/draft.2.html.