



The ID-Certify Solution

ID-Certify is a Hitachi ID solution designed to ensure that user access rights accurately reflect business needs. ID-Certify addresses the problems of orphan and dormant accounts and of privilege accumulation by periodically requiring managers, application owners and group owners to review user privileges, identify inappropriate rights and certify that remaining rights are still needed. Inappropriate rights pass through a change authorization workflow and are ultimately removed from IT systems.

The Regulatory Compliance Challenge

Policy of Least Privilege

Effective internal controls demand a policy of least privilege, which means that user entitlements are deactivated promptly when no longer required.

Complex IT Infrastructure

Ensuring appropriate access rights for thousands of users distributed globally across open, legacy, vertical and custom applications is challenging.

Dynamic Organization

User needs constantly change, making a purely policy-driven administration strategy impractical.

Annual Reporting

Sarbanes-Oxley requires companies to submit an annual statement that attests to the state of their internal controls.

Key Business Benefit

ID-Certify is the only system to provide CEOs and CFOs with the assurance that proper internal controls have been implemented and verified in accordance with SOX section 404 and other corporate governance and privacy legislation.

The access certification process is based on the premise that business stakeholders, if presented with a description of each user's current rights, can identify inappropriate rights and ask that those rights be removed.

ID-Certify automates review and cleanup of user rights:

- Managers review a list of their subordinates and each one's security rights.
- Application owners review a list of users with access to their application and their rights within that application.
- Group owners review a list of users that belong to their security group.

Appropriate security privileges are certified and inappropriate privileges are deleted.

A Stringent Regulatory Environment

Recent incidents of financial fraud and inappropriate disclosures of personal data, combined with the current climate of security awareness, have led to new regulations regarding corporate governance and privacy protection. Regulations such as Sarbanes-Oxley, HIPAA, PCI, FDA 21 CFR 11, EU Directive 2002/58/EC and PIPEDA all demand strong internal controls. Organizations subject to these regulations face serious penalties and potentially ruinous lawsuits in the event of non-compliance.

Given the demand for effective controls, it's important that current users only have the privileges they require to do their work. It's also critical that when users leave an organization, their access rights are terminated promptly and reliably.

In reality, when users change responsibilities, they usually acquire new access rights but rarely relinquish old ones. As a result, users accumulate privileges as their responsibilities change over time. In addition, many organizations do not have a central, up-to-date database that tracks every login ID of every user. This can lead to incomplete access termination and the retention of privileges long after a user leaves an organization.

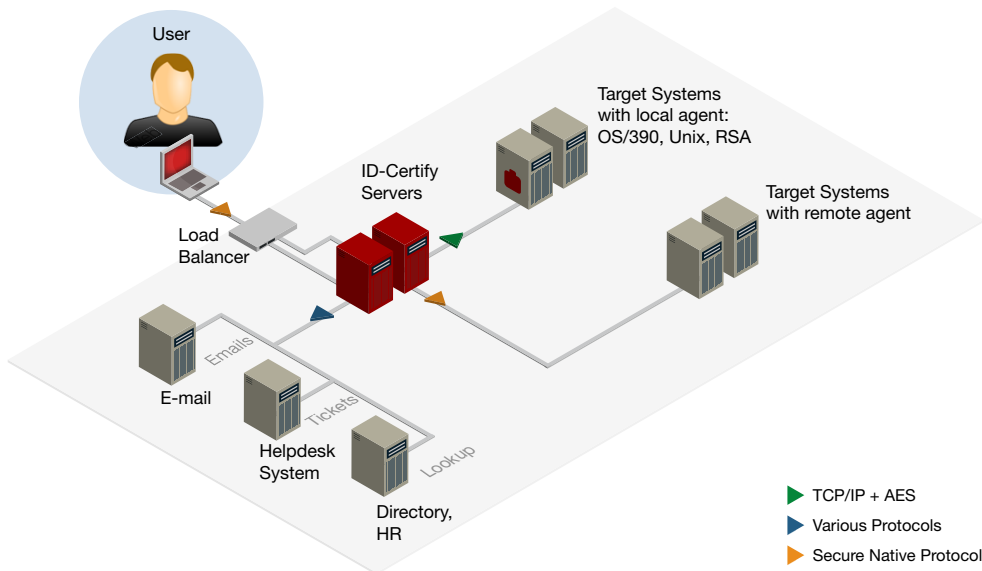
THE ACCESS CERTIFICATION PROCESS

Organization-centric approach

ID-Certify periodically invites each manager to review the access rights of their direct subordinates. Using a web interface, managers identify and remove terminated staff, transfer reallocated staff and delete inappropriate security privileges. Managers are asked to sign off on their certifications but cannot do so until their subordinate managers have completed their sign-offs, which creates downward pressure throughout the organization to review the process.

Application-and group-centric approaches

ID-Certify periodically invites application and security group owners to review the list of users and privileges within their application or group. This is an effective solution where application and group owners know their users.



TARGET SYSTEMS INTEGRATION

Directory:

Windows domains, Active Directory, eDirectory, Novell NDS, any LDAP

File/Print:

Windows NT, 2000, 2003; Novell NetWare, Samba

Databases:

Oracle, Sybase, SQL Server, DB2/UDB, Informix

Unix:

Linux, Sun, HP, IBM, Compaq, SGI, Unisys, SCO, DG; passwd, shadow, TCB, Kerberos, NIS, NIS+

Mainframes/minis:

MVS/OS390/zOS, VM/ESA, Unisys, Siemens, OS400, OpenVMS, Tandem

Applications:

Oracle, PeopleSoft, SAP; open plug-ins for SQL, ASPs, web services and more

Groupware:

MS Exchange, Lotus Notes/ID files, Lotus Domino/HTTP, Novell GroupWise

Networking:

RAS, routers, firewalls

Flexible Agents:

Target API, Telnet, TN3270, TN5250, HTTP(S), Web Services, command-line, SQL code, LDAP attributes

SUPPORT INTEGRATION

Automatically create, update and close tickets on:

- Axios Assyst
- SupportSoft SmartIssue
- Magic Service Desk
- Clarify eFrontOffice
- FrontRange HEAT
- HP Service Desk
- CA Unicenter
- Tivoli Service Desk
- Peregrine ServiceCenter
- Remedy AR System

Additional integrations through e-mail, ODBC, web services and web forms integration.

ID-Certify is part of the Hitachi ID Management Suite, which also includes: P-Synch for password management, ID-Synch for user provisioning, ID-Archive for privileged password management, ID-Access for group management. For more information about Hitachi ID and its products, please visit the corporate web site at Hitachi-ID.com, the product web sites at ID-Synch.com, P-Synch.com, ID-Certify.com, ID-Archive.com, ID-Access.org or call 1.403.233.0740.

Hitachi ID Systems, Inc.

© 2008 Hitachi ID Systems, Inc. All rights reserved. Hitachi ID, P-Synch, ID-Synch, ID-Access, ID-Discover, ID-Telephony, AdMax and ID-Certify are registered trademarks of Hitachi ID Systems, Inc. in the United States and Canada. All other marks, symbols and trademarks are the property of their respective owners.

Hitachi-ID.com