

Addressing Excess Privileges

using Hitachi ID Access Certifier



1 Introduction

This document describes the business problem of privilege accumulation and the impact of this IT problem on organizations in the context of a growing set of regulatory requirements.

Having defined the business problem, this document then describes the process of access certification, used to respond to privilege accumulation in a manner consistent with regulations such as Sarbanes-Oxley, HIPAA, 21CFR11 and GLB.

2 The Challenge

2.1 The Regulatory Environment

Two common threads running through many regulations are privacy protection (e.g., HIPAA, GLB, PIPEDA, EU Privacy Directive) and corporate governance (e.g., Sarbanes-Oxley, 21-CFR-11). Privacy applies to customers, patients, investors, employees and so forth. Good governance applies to financial data, clinical processes, safety procedures, etc.

2.2 Compliance Requires AAA

Privacy protection and corporate governance both depend on effective internal controls. The challenge is to answer the questions:

Who can access sensitive data?	How are these users authenticated?	What can they see and modify?	Are users held accountable for their actions?
--------------------------------	------------------------------------	-------------------------------	---

These requirements can be restated as AAA: authentication, authorization and audit.

2.3 Problems with AAA

AAA infrastructure is nothing new and has been built into every multi-user application for decades. The problem is that a growing number of systems and applications, combined with high staff mobility, have made it much harder to manage user data in the existing AAA infrastructure.

With weak passwords, unreliable caller identification at the help desk, orphan accounts, inappropriate access rights and mismatched login IDs, AAA systems often enforce the wrong rules at the wrong time. The weakness is not in the AAA technology – it's in the business process for managing the user data on which AAA rests.

2.4 Addressing Problems with AAA Requires Identity Management

To address problems with AAA data, it is essential to implement sound processes to manage the data about users, so that only the right users get access to the right data, at the right time.

This is accomplished with:

- Better control over how users acquire new entitlements and when entitlements are revoked.
- Correlating user objects between systems and applications, so that audit logs can be related to people.
- Periodic audits of entitlements, to verify that they remain business-appropriate.
- Logging of both current and historical entitlements, to support forensic audits.
- Stronger passwords and more robust authentication in general.

3 Access Certification

The Hitachi ID access certification process addresses the problem of finding and removing excess security entitlements.

The certification process is based on a simple premise: **business stake-holders can identify inappropriate user rights assigned to users with whom they have close business relationships.**

Hitachi ID Access Certifier builds on this basic observation, delegating access review, cleanup and certification to managers, application owners and group owners throughout an organization. Three types of business stake-holders lead to three types of access certification:

- **Org-centric Certification**

Access Certifier can leverage organization chart data, to identify relationships between managers and their subordinates. Using this data, managers can be asked to review the access rights of their subordinates. Requests sent to managers, along with reminders, change authorizations, etc. all leverage the Access Certifier workflow engine.

The Access Certifier process for Org-centric certification works as follows:

- Access Certifier periodically (e.g., quarterly or biannually according to corporate policy) requires managers to review the access rights of their staff. Certification requests are sent by e-mail and the workflow engine sends automatic reminders and escalates requests above managers who failed to respond.
- Managers respond by signing into Access Certifier using their network or directory login ID and password, to start their certification process.
- The dashboard interface presents managers with a list of their staff, asking them to identify any staff (user profiles) that no longer work for the organization. These will be removed later.
- For each remaining, legitimate user, an access profile is displayed, with a list of login accounts on Access Certifier target systems. Target systems are described by name, a description of their business function and a link to an external HTML page providing further identifying information, such as screen-shots and longer descriptions.
- Managers identify no-longer-needed accounts and flag them for later removal.
- Managers view a list of security group memberships that their staff have on target systems. As with login accounts, security groups are identified by name, a description of their business function, a link to a pop-up HTML help page. Managers are asked to identify no-longer-appropriate group memberships.
- Managers complete the process above for every direct subordinate and provide an electronic signature after reading a statement to the effect that their access review is complete and they certify that the remaining users, accounts and group memberships are appropriate.
- After a manager completes his review and certification, any proposed changes (removed users, deactivated accounts, eliminated group memberships) are bundled into security change requests and submitted to the Access Certifier workflow engine. These requests will normally require further authorization, from system owners or higher managers and will ultimately lead to users, accounts and group memberships being deleted from target systems.

- Certifications are collected up through the organization's hierarchy. Manager A is unable to sign off on his own certification until all of his subordinate managers (B, C, ...) have likewise signed off on theirs. This creates downward pressure through an organization to complete the review process, since upper managers are motivated to complete by regulatory requirements (e.g., Sarbanes-Oxley, HIPAA, etc.). This motivation leads to global completion of the certification process.
- Since no manager can have a very large numbers of direct subordinates, this process scales to even the largest organizations. Time to complete an enterprise-wide audit depends on the depth of the organizational structure, rather than the organization's size.

• **Application-centric Certification**

Access Certifier can be configured to request reviews of user accounts and security group memberships within individual applications, by those applications' owners. Application owners are prompted and reminded to perform these reviews by the Access Certifier workflow engine.

The Access Certifier process for Application-centric certification works as follows:

- Access Certifier periodically (e.g., quarterly or biannually according to corporate policy) requires application owners to review a list of users that have login accounts to their applications and their security group memberships within those applications. Reviews are performed one application at a time.
- Application owners respond by signing into Access Certifier using their network or directory login ID and password, to start their certification process.
- Application owners first review a list of users with login accounts to their application and flag for later removal users who should no longer have access.
- For each remaining users, application owners review sensitive security group memberships and flag inappropriate group memberships for later removal.
- Group memberships are identified by ID, a descriptive name and optionally a link to an HTML page containing an arbitrarily verbose description of the group's business function.
- Application owners complete the review process and provide an electronic signature after reading a statement to the effect that their access review is complete and they certify that the remaining login accounts and group memberships are appropriate.
- After an application owner completes his review and certification, any proposed changes (deactivated accounts, eliminated group memberships) are bundled into security change requests and submitted to the Access Certifier workflow engine. These requests will normally require further authorization, for instance from each user's manager.
- It should be noted that application-centric certification is appropriate to applications with modest numbers of users, such that the application owner recognizes the users personally and has some idea of what access rights are appropriate for each user. Larger applications and systems that span the entire organization are more appropriately supported by:
 - * Org-centric certification.
 - * Group-centric certification (for user groups of modest size).
 - * App-centric certification, where the application can be segmented into sub-components, each with its own owner.

- **Group-centric Certification**

Access Certifier can be configured to request reviews of user membership in security groups by each group's owner. Group owners are prompted and reminded to perform these reviews by the Access Certifier workflow engine.

The Access Certifier process for Group-centric certification works as follows:

- Access Certifier periodically (e.g., quarterly or biannually according to corporate policy) requires group owners to review a list of users with membership in their groups. Reviews are performed one group at a time.
- Group owners respond by signing into Access Certifier using their network or directory login ID and password, to start their certification process.
- Group owners review group memberships and flag inappropriate ones for later removal.
- Group owners complete the review process and provide an electronic signature after reading a statement to the effect that their access review is complete and they certify that the remaining group memberships are appropriate.
- After a group owner completes his review and certification, any proposed changes (deactivated accounts, eliminated group memberships) are bundled into security change requests and submitted to the Access Certifier workflow engine. These requests will normally require further authorization, for instance from each user's manager.
- In environments with large numbers of groups, it is helpful to draw data about group ownership from existing sources. Access Certifier can pull group owner data from target systems, such as Active Directory. This makes it straightforward to configure group-centric certification across thousands of individual groups.
- It should be noted that group-centric certification is appropriate to groups with modest numbers of users, such that the group owner recognizes the users personally and has some idea of what access rights are appropriate for each one. Larger groups are better served by Org-centric certification.

3.1 Benefits of Access Certification

Access certification offers substantial benefits over previous approaches:

- Hitachi ID Access Certifier is simple to deploy, providing a practical solution to a perennial security problem: finding and eliminating no-longer-appropriate security entitlements.
- Organizations can deploy access certification in just a few weeks, without getting bogged down in complex projects to define policy that determines which privileges are appropriate.
- Complete, accurate and up-to-date information which entitlements are **appropriate** is drawn from the one repository where it already exists: managers' knowledge of their own workforce.
- Network security is enhanced by identifying and removing orphan and dormant accounts, as well as inappropriate entitlements.

- By cleaning up excess security entitlements, Access Certifier supports regulatory compliance programs related to Sarbanes-Oxley, HIPAA compliance, FDA 21 CFR Part 11, PIPEDA, Gramm-Leach-Bliley, PCI-DSS and more.

3.2 Previous Approaches

Previous attempts to address the problem of finding and removing excess access rights have focused on policy-enforcement in general, and policy-based provisioning in particular:

Policy-based provisioning is defined as follows:

- Define a set of roles, detailed enough to capture the full access requirements of every user, on every managed system.
- Classify users into roles, such that their access requirements are fully specified by role membership.
- Reconcile access privileges predicted by the policy model against the access privileges users actually have on managed systems.
- Correct actual privileges to match those predicted by roles, either automatically or after human review and approval.

On an enterprise scale, where there are (tens of) thousands of users, employees, contractors and other principals are constantly hired, moved and terminated. This makes user classification difficult.

Role definition, where user responsibilities are subtly different, and where infrastructure is ever changing, is similarly difficult, because the target (a role model) is complex and moving.

Access privilege reconciliation may also be hard to implement, as it can flag more exceptions than human authorizers can realistically review.

The policy-based provisioning approach is challenging in complex organizations, because defining a comprehensive and appropriate policy is time consuming, difficult and expensive. These challenges apply equally to initial deployment and ongoing system sustainment.

4 Motivating Managers to Participate

In a large organization, there will be many managers, application owners and data owners who must perform periodic audits of user access privileges. It follows that some mechanism is required to ensure that these audits are in fact carried out and performed diligently.

Audits by application and data owners are straightforward – this can be made a core part of the responsibility of these stakeholders, and since there are relatively few such stakeholders, ensuring that they complete periodic user privilege audits.

Audits of users by their direct supervisors can be more difficult, since there may be thousands of such supervisors and it is hard to make them all comply with any single directive.

One approach to motivating managers to review the access rights of their direct subordinates is to require a signature at the end of every such review, but to block such signatures until subordinate managers have completed their own reviews. This signature underlies a legal statement by each manager, certifying that the remaining list of that manager's direct subordinates and their privileges, are appropriate.

With this process, an executive such as the CEO or CFO, who wishes to implement strong controls to support a regulatory compliance program, will pressure his direct subordinates to complete their own reviews. They will be unable to sign off until their own subordinates have finished and so a downward pressure through the organization to complete the audit is created. Whereas pressure to perform the user privilege reviews flows downwards from the top of the organization, results of the audit, including cleaned up user rights, flow back up from the lowest-level managers right to the CEO or CFO.

5 Advantages of the Access Certification Approach

The Hitachi ID Access Certifier process has several advantages that organizations can leverage:

- **Simple to deploy** – This is a practical approach to addressing an important business problem: finding and eliminating obsolete user privileges. Organizations can deploy Access Certifier in just a few weeks, without getting bogged down in role definition or user classification projects, which tend to be lengthy and expensive.
- **Accurate and up-to-date** – The information about who should have what access to what systems is drawn from managers with contextual knowledge, not IT staff far removed from day to day application usage.
- **Auditable** – The process is 100% traceable, providing complete confidence to senior executives about the validity of the cleaned privileges and of the process itself.

Please contact Hitachi ID to learn more about the Hitachi ID Access Certification Process and Hitachi ID's complete line of Identity Management Solutions.

6 About Hitachi ID Systems, Inc.

Hitachi ID Systems, Inc., formerly M-Tech Information Technology, Inc., is a leading publisher of identity and access management software. Hitachi ID products help organizations strengthen network security, lower IT support costs and improve user productivity. Hitachi ID customers achieve these results by implementing automation and self-service processes to more effectively manage passwords and other authentication factors, to provision and deactivate user access and to manage user privileges. Hitachi ID products have been deployed at over 840 organizations world-wide.

Originally founded in 1992 as M-Tech Information Technology, Inc. and acquired by Hitachi, Ltd. in 2008, Hitachi ID Systems, Inc. is a leading provider of identity and access management solutions.

Hitachi ID first identity and access management product, Hitachi ID Password Manager, has been commercially available since 1995. Today, Hitachi ID is the leading password management vendor world-wide and a leading provider of identity management solutions.

Hitachi ID currently has 140 employees. Hitachi ID has enjoyed strong financial performance, with 64 consecutive quarters of growth and profitability.

Hitachi ID is headquartered in Calgary, Canada and has regional offices in: Canada: Vancouver, Barrie, Ottawa and Montreal; United States: Denver, Dallas and New York, Australia: Brisbane.

Hitachi ID's customers include AT&T Wireless - 110,000 users, Best Buy, Bristol-Myers Squibb, Citi Corp, Ford Motor Company, Kimberly-Clark Corporation, NCR Corporation, Pitney Bowes, Schering-Plough Pharmaceuticals, Sears Roebuck, Siemens, Symantec, United Technologies Corporation, Wendy's International and many more. For more information on Hitachi ID and its products, please visit <http://Hitachi-ID.com/> or call 1.403.233.0740.