

Attestation of Identity Information

*An Oracle White Paper
December 2008*

Attestation of Identity Information

INTRODUCTION	3
CHALLENGES AND THE NEED FOR AUTOMATED ATTESTATION.....	4
KEY FACTORS, BENEFITS AND TYPICAL USE CASES	5
INDUSTRY TRENDS.....	6
ORACLE’S ATTESTATION SOLUTION.....	7
ORACLE’S ATTESTATION ROADMAP SUMMARY	10
CONCLUSION.....	11
REFERENCES	11

Attestation of Identity Information

INTRODUCTION

The major emphasis now placed on stringent enforcement of internal controls and regulatory compliance within corporations of all sizes results from a number of recent government and industry initiatives – such as the Sarbanes-Oxley Act (SOX) of 2002 (sections S-O 302, 404 and others), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the European Anti-Fraud (EU-AF) Office, and Basel II, that require full disclosures of corporate accounting practices, prevention of corporate fraud, and individual privacy protection.

The Information Technology Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA), the leading associations of professionals in information systems audit, control, security and governance, offer an open standard – Control Objectives for Information and related Technology (COBIT) – that enables organizations to focus their IT activities in support of overall business objectives.

In March 2004, the US Public Company Accounting Oversight Board (PCAOB) adopted a standard entitled “An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.”

The standard identified the following pervasive information technology controls necessary to achieve overall control criteria:

- Program development
- Program changes
- Computer operations
- Access to program and data

The standard outlines specific requirements for auditors monitoring transaction flows – how they are initiated, authorized, recorded, processed and reported on. This involves the use of information technology (IT) systems and applications for automating internal processes.

CHALLENGES AND THE NEED FOR AUTOMATED ATTESTATION

The process of authorizing established internal controls, processes, policies, programs, and data, is commonly referred to as “Attestation”.

Each organization is expected to implement a tailored IT control approach that fits its size and complexity, cognizant of the constraint that internal controls can provide only reasonable assurance of achieving an organization’s IT control objectives.

The Sarbanes-Oxley Act, which has fundamentally changed the business and regulatory environment, is the result of firm resolve by the US Congress to improve corporate responsibility. The Act aims to enhance corporate governance through measures that will strengthen internal checks and balances, and ultimately strengthen corporate accountability. The directives of S-O 404 require that management provide an annual report on its assessment of internal controls over financial reporting.

S-O 404 requires a company’s independent auditor to attest to management’s assessment of its internal controls over financial reporting. Organizations must ensure that appropriate IT controls are in effect. Management must provide their independent auditors the full documentation, evidence of functioning controls, and results of testing procedures.

An attestation process includes the reviewers, the data to be attested to, and the schedule for attestation activities.

These drivers require all organizations with trade-able securities in US markets to authorize and validate user identity information for all internal and external users, including their entitlements, as well as the access policies and workflow processes defined by and in use within various divisions in the organization.

The process of authorizing established internal controls, processes, policies, programs, and data, is commonly referred to as “Attestation”. An attestation process includes the reviewers, the data to be attested to, and the schedule for attestation activities.

In most corporate entities that comply with S-O 404, attestation is typically handled by use of manual processes and spreadsheets, which can be very time consuming and costly. Such manual processes are prone to human errors and involve repetitive efforts at every audit. By automating these routine tasks, organizations can realize significant time and cost savings in executing the processes required to demonstrate full compliance with industry regulations.

KEY FACTORS, BENEFITS AND TYPICAL USE CASES

Internal controls are required over an organization's IT environment, computer operations, access to programs and data, program development, and program changes. Access controls over programs and data become increasingly important as companies operate globally.

“IT is considered one of the most challenging areas to address for S-O 404 compliance. In particular, ‘access to programs and data’ has resulted in many deficiencies, and remedying it has been a large task.” ~ KPMG

Source: KPMG LLP (printed with permission from KPMG)

Automated attestation capabilities allow organizations to quickly and periodically attest to who had access to what, when, how and why, across the organization's business and IT environment.

Thousands of internal and external users from around the world may try to access and use IT systems and applications, and effective access controls can provide a reasonable level of assurance against inappropriate access and unauthorized use. As a result, organizations need to enforce adequate access control policies, via multiple enablers, such as secure passwords, firewalls, data encryption and cryptographic keys – all of which can be effective methods of preventing unauthorized access. User accounts, roles, and related access privilege controls restrict the IT systems and applications to only authorized users, thus enabling appropriate segregation of duties. There needs to be frequent and timely reviews of user profiles that permit or restrict access to various systems and applications within the enterprise. Immediate deletion of user accounts and passwords for terminated employees must be enforced. An organization can protect its programs and data by preventing unauthorized use of and access to its IT systems and applications.

Automated attestation capabilities allow organizations to quickly and periodically attest to who had access to what, when, how and why, across the organization's business and IT environment. The frequency of attestation audits can range from once a year to once every quarter.

Automated attestation complements existing internal control mechanisms and provides a means to verify the data, practices and policies put in place for ensuring compliance. This becomes particularly critical due to frequently changing dynamics of the user population – in terms of the number of users accessing corporate systems, the changing statuses and roles of employees and contractors, and the specific resources accessed by different users at different times.

The use of automated attestation features enables organizations to create and follow standard practices and policies across various departments within an organization, while ensuring that the organization is meeting diverse regulatory compliance requirements. This can be achieved without costly, time-consuming, and error-prone manual processes.

INDUSTRY TRENDS

Many of the leading identity management vendors today provide technology that enables secure management of user identities across heterogeneous systems and applications. But very few vendors currently offer any attestation (also referred to within the industry as periodic access reviews or recertification) capabilities as part of their identity management offering.

Following up on extensive market research and specific customer demands, Oracle has taken the lead in offering automated attestation capabilities within its comprehensive identity management suite offering.

To ensure effective and sustainable compliance, organizations must perform periodic reviews and attest to the fitness for purpose of user entitlements and access policies. It is not just user identity information that needs to be or can be attested to. The associated user entitlements, roles, access policies, workflow processes, and user transactions need to be attested to and reported on. Organizations need to authorize and validate all processes, actions, and data associated with internal and external users of IT systems and applications.

Following up on extensive market research and specific customer demands, Oracle has taken the lead in offering automated attestation capabilities within its comprehensive identity management suite. As customer adoption of this capability grows over the next few years, fueled by the significant value that it provides, it is expected that other identity management vendors will follow this lead, offering automated attestation capabilities for identity and access data.

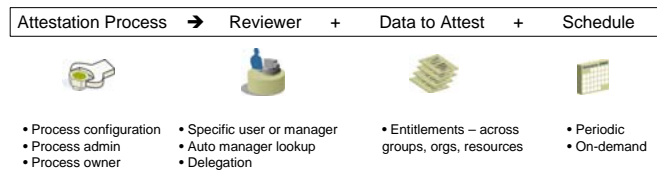
Other existing standalone attestation products in the industry today lack the scalability and performance required for enterprise deployments. They do not provide the links to trigger corrective actions and cannot easily be upgraded to handle attestation of data other than user entitlements, such as workflows and policies. Major effort is required to integrate such stand-alone attestation products with provisioning and compliance solutions.

ORACLE'S ATTESTATION SOLUTION

Oracle's automated attestation capabilities involve presenting user identity and fine-grained entitlement data to authorized reviewers for sign-off on the data's accuracy, and providing reviewers with the means to document and correct any inaccuracies.

As part of its comprehensive identity management suite, Oracle has enhanced its identity audit and compliance automation component that includes automated auditing, reporting and attestation features. An attestation process, as defined in Oracle Identity Manager (OIM), includes the reviewers, the data to be attested to, and the schedule for attestation tasks.

Process Automation – Attestation



Source: Oracle Identity Management team

Oracle's automated attestation capabilities involve presenting user identity and fine-grained entitlement data to authorized reviewers for sign-off on the accuracy of the data and providing reviewers with the means to document and correct any inaccuracies. Attestation processes can be run on demand or can be scheduled for periodic execution at regular intervals, whether it is once a year, once every six months, or once every quarter.

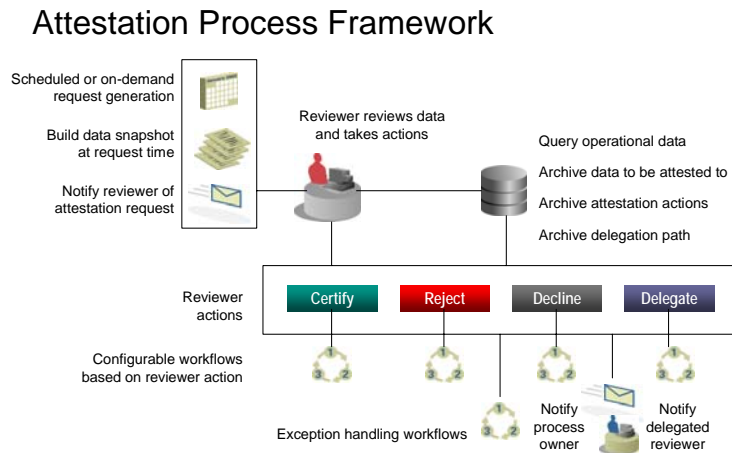
Specific actions that can be undertaken by a reviewer for specific attestation requests include the ability to certify, reject, delegate or decline each entry in the attestation request.

The data to be attested to can range from basic user profile data to access privileges or entitlements assigned to users and roles. Specific actions that can be undertaken by a reviewer for attestation include the ability to certify, reject, decline or delegate each entry in the attestation request. Reviewers can enter specific comments for each entry in the request to justify the action taken, and they can enter generic comments that apply to all entries in the request.

Each attestation request may contain a number of entries – for instance, to include each entitlement assigned to each user – and the reviewer has the ability to take one of four actions – certify, reject, decline, or delegate – for each of these entries. The reviewer can select responses for some of the entries in the request, save the selections, then review the request again at a later time to complete the actions for other entries, and finally submit the entire attestation request for processing. E-mail notifications are sent to the reviewer and the users affected, so they are aware of the actions taken on the data. Each of these attestation requests is archived for subsequent auditing and reporting.

Resources can be tagged as “financially significant” and the user entitlements for such resources are automatically selected to participate in attestation processes. Optionally, specific resources that are not tagged as financially significant also can be selected for attestation on demand.

All data and actions taken on attestation requests are also archived for subsequent auditing and reporting purposes.



Source: Oracle Identity Management team

The diagram above illustrates Oracle’s attestation process flow and framework.

First, a scheduled or on-demand attestation request is generated and a snapshot of the data required for the attestation task is compiled. The reviewer is then notified of the attestation request. The reviewer logs into the system and views the attestation request displayed in his/her attestation inbox. The attestation request is typically composed of a number of entries, one for each item of user profile data or user entitlement data to be attested to for each user. The reviewer can make one of four selections for each entry:

- Certify – reviewer attests to the data as accurate
- Reject – reviewer marks the data as inaccurate
- Decline – reviewer refuses to perform any attestation on this entry
- Delegate – reviewer delegates the attestation task for this entry to an alternate reviewer

The reviewer has the option of making the selections only for a subset of the entries in the request, saving the actions taken, and then returning at a later time to complete the attestation request. The reviewer can also enter individual comments for each entry or a generic comment for all entries in the request. Once the reviewer has completed taking an action for each entry, he/she can submit the entire attestation request for further processing. At this point, e-mail notifications are sent to the reviewers, the users, and the process owners associated with this attestation request.

Key features of Oracle's current attestation offering include:

- Step-by-step definition of attestation processes
- On-demand or periodic scheduling of attestation tasks and processes
- Attestation of users' fine-grained entitlements across multiple resources
- Ability to tag resources as "financially significant" for participation in the attestation process
- Ability to certify, reject, decline, or delegate each item in an attestation request
- Fine-grained attestation actions for each entitlement for each user for each resource
- Notifications to reviewers, users, and process owners regarding attestation actions
- Reports on attestation requests processed – summary by reviewer, by user, and by resource
- Archiving of attestation data – for periodic auditing and reporting
- Archiving of attestation actions taken – for periodic auditing and reporting

Included below are sample quotes from customers who have deployed OIM (previously known as Xellerate).

"In support of our 2004 S-O 404 audit, we saved at least 12 man-weeks on 'who has what' auditing across our over 50 SOX-critical applications via TAC (powered by Xellerate, now part of OIM), versus manual data capture" ~ Tom King, CISO, Lehman Brothers

Source: Lehman Brothers (printed with permission from Lehman Brothers)

"While working through the steps to comply with Sarbanes-Oxley, we discovered that we needed to pay more attention to how employees were given access to sensitive data and programs. Although we had created written access-control policies, they were enforced haphazardly, if at all. We installed Xellerate (now part of OIM) to automate the management of our 90,000 user identities. When someone asks for an audit trail of access privileges, the relevant documentation is contained in the Xellerate (OIM) system" ~ Michael Bryan, Director of IT Governance, Nextel Communications, as it appeared in InformationWeek, Mar 21, 2005.

Source: Nextel Communications (printed with permission from Nextel Communications)

ORACLE'S ATTESTATION ROADMAP SUMMARY

Apart from attestation of users' fine-grained entitlements currently offered by the Oracle identity audit and compliance component, the ability to attest to additional entities – including access policies, provisioning policies, workflow processes, approval chains, roles information, and financial transactions – is planned for future releases.

Additional features planned for future releases include fine-grained target population definition to allow for arbitrarily complex selection of sets of users to whom specific attestation processes apply, the ability to insert custom queries for target population definition, support for sequential and parallel multiple reviewers, complex delegation mechanisms, attestation request escalation mechanisms, the ability to customize attestation processes, drill-down from reports to specific data attested to, operational and historical reports on attestation requests, and attestation gap analysis.

As part of the Oracle Fusion Middleware project, the attestation features of OIM are to be leveraged by other Oracle products, including Oracle E-Business Suite, PeopleSoft Enterprise, JD Edwards Enterprise One, and Siebel CRM, to centralize and enhance application-specific compliance features.

Other features planned for future releases include a separation of duties framework, advanced integration with business role management systems, integration with audit and data vaults, and integration with business intelligence and business monitoring tools.

CONCLUSION

Attestation is one of the key elements of identity audit and compliance. Organizations can realize major benefits in terms of time and cost savings by automating the process of attesting to all data related to identity management and by deploying an automated attestation solution in their heterogeneous business application and corporate IT environment. This can be an effective tool to quickly and periodically complete audit reviews, and to effectively meet regulatory compliance requirements in a timely manner.

REFERENCES

- “IT Control Objectives for Sarbanes-Oxley – The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting,” IT Governance Institute, April 2004
- “COBIT,” IT Governance Institute, July 2000

ORACLE FUSION MIDDLEWARE

Attestation of Identity Information

Authors: Pradeep Bhoj, Ed King, Nishant Kaushik
Contributors: Hormazd Romer, John Aisien, Naga Nagarajan

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2005, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.