

Identity Governance Framework

Frequently Asked Questions (FAQ)

Nov 29, 2006

Table of Contents

What is the Identity Governance Framework?	1
Why is a new approach needed?	1
How will IGF benefit customers?	2
How will IGF benefit developers?	2
How will IGF benefit ISVs?	3
How will IGF benefit service providers?	3
Could you provide real-world examples of how Identity Governance Framework might be used?	3
What about Liberty Alliance/SAML? Haven't these problems already been solved by those frameworks?	3
What about Higgins, Bandit, CardSpace or WS-Trust? Don't they address this problem?	4
What about WS-Policy? Doesn't it address all of these different policy issues? ..	4
What's the value to Oracle of proposing a new identity framework?	4
What is the Identity Governance Framework comprised of?	4
How will the Identity Governance Framework be made available and when?	5
Will Oracle submit this framework to a standards body?	5
Does Oracle's have plans to adopt the Identity Governance Framework?	5
Are there other vendors who have endorsed this approach?	5
Who can join and participate in defining the Identity Governance Framework?	
How do I do so?	6
Where can I review the specifications and learn more?	6

What is the Identity Governance Framework?

The Identity Governance Framework (IGF) is an open initiative to address governance of identity related information across enterprise IT systems. As part of this initiative Oracle is releasing key initial draft specifications and making them available to the community. These specifications provide a common framework for defining usage policies, attribute requirements, and developer APIs pertaining to the use of identity related information. These enable businesses to ensure full documentation, control, and auditing regarding the use, storage, and propagation of identity-related data across systems and applications.

Sensitive identity-related data such as addresses, social security numbers, bank account numbers and employment details are increasingly the target of legal, regulatory and enterprise policy. These include, but are not limited to: the European Data Protection Initiative, Sarbanes-Oxley, and Gramm-Leach-Bliley as examples.

IGF assists corporations with increased transparency and demonstrable compliance with respect to policies for identity-related data. It would allow corporations to answer questions such as: Under what conditions may user social security numbers be accessed by applications? Which applications had access to customer account numbers on January 27, 2007?

Why is a new approach needed?

The governance and protection of sensitive personal information of employees, customers, and partners as it flows through IT systems is increasingly mandated by privacy and compliance regulations. However, to date there has been no easy way to enforce these controls across the typical heterogeneous IT environments. As a result, identity-related data (personal identifiable information, entitlements, attributes, etc) is sometimes scattered across numerous applications across an organization, making such prone to inconsistencies and even placing such information at risk. Alternatively, such information may be so strictly controlled that applications could benefit from it, are prevented from doing so. Organizations need a standards based solution that helps define policies, enforce controls, and track activities pertaining to usage of identity-related data.

Identity Governance Framework (IGF) will help enterprises easily determine and enforce how identity related information (including Personally Identifiable Information (PII), entitlements, attributes, etc.) is used, stored, and propagated between their systems. IGF will enable organizations to define enterprise level policies to securely and confidently share sensitive personal information between applications that need such, without having to compromise on business agility or efficiency.

How will IGF benefit customers?

Organizations are burdened with protecting sensitive personal information about their customers, employees, and partners. Data regarding social security numbers, credit card numbers, medical history and more are increasingly under scrutiny by regulations seeking to prevent abuse or theft of such information. To date privacy conscious organizations have reacted to these requirements by enforcing overly strict controls and processes that hinder business operations and impact productivity, flexibility, and efficiency. At the opposite end of the spectrum, some organizations do not take the care needed to safeguard this information, potentially putting identity-related data at risk without sufficient oversight and control.

The Identity Governance Framework will enable a standards-based mechanism for enterprises to establish “contracts” between their applications such that identity related information (including Personally Identifiable Information, entitlements, attributes, etc.) can be shared securely with confidence that this data will not be abused, compromised, or misplaced. Using this framework, organizations will have complete visibility into how identity information is stored, used, and propagated throughout their business. They’ll be able to automate controls to streamline business processes without fear of compromising the confidentiality of sensitive identity related information.

Developers will also benefit as the Identity Governance Framework will yield an industry agreed-upon way of how identity-related data is treated when developing applications. This will provide developers a standards-based way to easily write applications that use this data so that governing policies can be used to control it. This will result in faster application development times as well as guarantees of future compatibility for applications that are written to the eventual standards.

IGF benefits identity information providers such as Human Resources by allowing them to place tight controls on how restricted information can be used and by providing assurance that defined policies are being followed.

How will IGF benefit developers?

The Identity Governance Framework will yield an industry agreed-upon method for how identity-related data is treated when writing applications. This will provide developers a standards-based way to easily write applications that use this data so that governing policies can be used to control it. This will result in faster application development times as well as guarantees of future compatibility for applications that are written to the eventual standards.

Specifically, use of the CARML API will enable developers to defer deciding on how identity related information will be stored and accessed by their application. Developers will not need to worry about whether they should use a SQL database, LDAP Directory, or other system. In the past, developers were forced

to write highly specific code, driving technology and vendor lock-in. By using CARML declaration, applications will be support flexible deployment into a wide range of environments without the need for ongoing specialized developer enhancements. The IGF Attribute Service will do all the hard work of data retrieval, transformation, and policy-enforcement when it comes to identity-based information.

How will IGF benefit ISVs?

Independent Software Vendors developing packages business applications will be able to easily meet their customers' requirements for secure and auditable usage of identity related data. By writing to the IGF specifications and framework they will be able to leverage existing technologies and methodologies, while at the same time making their products interoperable out-of-the-box with other third party products.

How will IGF benefit service providers?

External or outsourced service providers (e.g. corporate procurement, business travel, HR, and payroll) who require and use identity-related data will now be able to provide documentation and audited use of identity-information making it possible for corporate clients to act as identity providers to ASPs. Together with federation technologies such as WS-Trust, and SAML, service providers will now also be able to trust attribute information from identity-providers directly without having to copy and replicate information thereby opening them to increased risk exposure.

Could you provide real-world examples of how Identity Governance Framework might be used?

Use cases are outlined in the "Identity Governance Framework Overview" whitepaper under the section titled, "Sample Business Cases."

What about Liberty Alliance/SAML? Haven't these problems already been solved by those frameworks?

To date, there has been extensive work by various standards groups on identity such as Liberty ID-WSF, OASIS Security Services (SAML), and more recently browser based or user-centric identity. IGF's goal is to complement those efforts. IGF focuses on the data exchanges and interactions that occur behind Web sites. An example might be a travel booking service communicating with the airline to book travel on the user's behalf. The objective of IGF is to take the next step and provide a governance framework for the use, storage, and exchange of identity-related data in a **services-oriented-identity** or "SOI" approach.

What about Higgins, Bandit, CardSpace or WS-Trust? Don't they address this problem?

Efforts such as Higgins, Bandit, and CardSpace are focused on user-centric identity privacy. They are primarily designed to empower end-users to control how information about themselves is shared with various service providers. They do not address the issues of policy and obligation of identity-related data between enterprise systems not directly exposed to the end-user. Identity Governance Framework is designed to complement and co-exist with these efforts.

Higgins/Bandit also have a data access component called IdAs. It is conceivable that IdAs could be adapted to be used as the data connector and modeling components for IGF's policy and service provider layers in an open source implementation. In this case, IdAs is a choice that could be made by an implementer of the IGF framework.

What about WS-Policy? Doesn't it address all of these different policy issues?

WS-Policy is a draft specification currently under development within the W3C. It provides "containers" that can carry different types of "service meta-data" and enables policy matching and selection from alternatives. The underlying service meta-data is drawn from specific domains such as security, reliability or other service properties such as identity, and fall beyond the scope of the WS-Policy specification.

The first working drafts of the specification have recently been published in November 2006. The next revisions of the CARML and AAPML drafts will appropriately reference these drafts.

What's the value to Oracle of proposing a new identity framework?

Oracle, as a vendor of business as well as infrastructure applications, recognizes the increasing importance of establishing policies to govern the use of identity-related data. We have heard this requirement from our customers and recognize the value of a standards-based solution to address this problem. A community driven specification will benefit not just Oracle, but our customers, other vendors adopting the standard, as well as developers writing to the standard.

What is the Identity Governance Framework comprised of?

The major components of the Identity Governance Framework include:

- Client Attribute Requirement Markup Language (CARML – pronounced car-mull) – a declarative contract document defined by application developers that informs deployment managers and service providers of the attribute usage requirements of an application.
- Attribute Authority Policy Markup Language (AAPML – pronounced app-mull) – A set of policy rules regarding the use of identity-related information from an identity source. AAPML allows identity sources to specify constraints on use of data provided by the source.
- CARML API – an API that makes it easy for developers to write applications that consume and use identity-related data in a way that conforms to policy set around the use of such information.
- Identity Attribute Service – a policy-enforced service for accessing identity-related data from multiple identity sources.

Oracle intends to take the proposed standards to external open standards bodies. It is expected that the final standard and components of the IGF will change as they grow to reflect the requirements and input of multiple vendors and customers.

How will the Identity Governance Framework be made available and when?

Oracle is actively working with other contributing members to gather broad industry input and to develop and publish final specifications. It is expected that finalized versions of the specifications will be made available in the coming year through an established standards body. Product based implementations are expected to follow thereafter.

Will Oracle submit this framework to a standards body?

Oracle and the contributing members are looking at appropriate standards bodies to host this work in an industry neutral standards-based way. It is the full intent of this group to submit the specifications through an established standards governing body.

Does Oracle's have plans to adopt the Identity Governance Framework?

Customers requesting such capabilities in Oracle's applications, middleware, and infrastructure products spawned the development of IGF. As standardization is achieved, Oracle intends to productize and integrate these features within its identity management offering, business applications, and middleware solutions.

Are there other vendors who have endorsed this approach?

Yes, several vendors have joined Oracle to advance this initiative further including CA, Ping Identity, Securent, and Sun Microsystems. For a complete list

of currently participating members, please consult the [Identity Governance Framework web site](#). Any interested vendor, customer, or service provider who would like to contribute to this effort is invited to join as well.

Who can join and participate in defining the Identity Governance Framework? How do I do so?

As an open initiative, the Identity Governance Framework is open to all vendors, customers, and service providers interested in advancing this initiative to full standardization. If you'd like to consider participating and becoming a contributing member, please e-mail igfinfo_ww@oracle.com.

Where can I review the specifications and learn more?

The current draft specifications are published on the IGF project web site located at: <http://www.oracle.com/goto/igf/>

Identity Governance Framework
November 2006

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 © 2006, 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 Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.