An Architectural View of Security for Cloud

Examining Policy-Based Security through Scenarios

A White Paper by:

The Security for the Cloud and SOA Project of
The Open Group Cloud Computing Work Group led by:

Omkhar Arasaratnam
Cloud Security Lead Architect, IBM
Cloud Work Group Steering Committee and Project Co-Chair

Stuart Boardman
Senior Business Consultant, Getronics Consulting
Cloud Work Group Steering Committee and Project Co-Chair

May, 2011
Table of Contents

Introduction 5
Terms 10
The Business Scenario 11
Identity, Entitlement, and Access Management 13
Conclusion 20
Further Reading 21
Acknowledgements 21
About the Authors 22
About The Open Group 22
Executive Summary

This White Paper is one in a series regarding Security in Cloud Computing. This series provides methods for enterprise architects to develop risk-based approaches to securing Cloud Computing. The method advocated is strongly based on key work products from the Security for the Cloud and SOA project in The Open Group, a joint venture between the Cloud and SOA Work Groups, in conjunction with the Security Forum.

This White Paper introduces a scenario-based approach to understanding the relationship between consumer and provider security policy, the possible discrepancies which may arise, and the options available for addressing those discrepancies. It focuses on Identity Entitlement and Access Management (IAM) as an example of policy-driven security concerns and uses this to illustrate an approach that can be applied to other aspects of Security in the Cloud. These will be addressed in subsequent White Papers in the series.

Through the scenario, we determine that Security in Cloud Computing (or indeed SOA) is not essentially different than approaching other federated policy scenarios but is in fact an additional driver for an open, collaborative stance. We also determine that taking a policy-based approach and leveraging open standards greatly increases the chances of achieving a successful outcome. By taking this approach, we ensure Boundaryless Information Flow in a secure, reliable, and timely manner.

---

1 IEAM would arguably be a better acronym. The Jericho Forum has recently adopted the term IdEA and will publish a discussion paper on this topic, the “Identity Commandments” in early May 2011. We use the IAM acronym in this document because it is widely used and understood. It is also arguable that these three topics should not appear under a joint heading, because that can create the impression that they are somehow coupled. This is discussed further in the context of the architectural building blocks used by this document.
An Architectural View of Security for Cloud

Introduction

Background

Cloud Computing continues to be a popular goal for IT departments and consumers alike. The prospect of a virtually unlimited capacity with little or minimal fees, limited obligations, increased flexibility, and agility is a dream come true. Many organizations are still apprehensive about leveraging Cloud Computing. In fact, according to most surveys, 60-80% of enterprises cite security concerns as the number one inhibitor to cloud adoption.2

This perception spurred the creation of a project under The Open Group Cloud Work Group charted to examine Security in the Cloud. The project was officially approved by the steering committee in early 2010. In mid-2010, the project also picked up responsibility for SOA Security, and has been producing work products focusing on the joint mission ever since under the title of “Security for the Cloud and SOA” as a joint venture between the SOA and Cloud Work Groups and the Security Forum.

The project has found that public Cloud Computing options are merely an additional choice when it comes to an organization’s IT sourcing decisions. Cloud Computing providers are not inherently insecure. Depending on the security posture of a particular organization, you might even find that some Cloud providers may have superior security postures to that of your own organization.

Approach

This White Paper is one in a series of several papers examining various security concerns regarding Cloud Computing. The purpose of this series is to help enterprise architects who are involved with Cloud Computing to understand how to approach security in Cloud Computing from a number of different perspectives and scenarios. This series will also provide suggestions regarding how to assess and mitigate security concerns in a risk-based manner. Each paper examines a different but complementary area of security based on the Security Architecture Building Blocks defined by the project.

Security Architectural Building Blocks

The Security Architectural Building Blocks will be the elements in a framework for Cloud Security. They are used both during analysis and when developing mitigating controls in risk-based approaches to security in Cloud Computing. The Architecture Building Blocks originated from the IBM Cloud Computing Reference Architecture and were donated to and accepted by the project in early 2009.

---

2 For example, Driving Profitable Growth Through Cloud Computing – IBM Study (conducted by Oliver Wyman), November 2008.
An Architectural View of Security for Cloud

This diagram illustrates each of the building blocks and how they relate to one another. Security Policy Management and Identity, Entitlement, and Access Management are highlighted because these are the areas of focus for this White Paper.

Command and Control Management

Command and control management represents the overall business and risk objectives of an organization. These objectives form the basis for all operations in the organization, including its risk tolerance and security posture.

Security Policy Management

This building block represents the realization of the business objectives decreed in Command and Control Management in the form of security policies. These security policies are the primary objectives of the security program which are realized through people, process, and technology in the blocks to the right hand side of Figure 1. Security Policy Management is therefore a central concern to all aspects of security.

Identity, Entitlement, and Access Management

Identity, Entitlement, and Access Management is concerned with ensuring that that appropriate entities have access to the appropriate resources, at the appropriate level, and at the appropriate time. This includes
management of the full lifecycle of an identity as well as the corresponding access control granted to a properly authorized identity as well as compliance reporting. That is the focus of this White Paper.\(^3\)

**Data and Information Protection Management**

This building block is concerned with the protection of data and information. This includes the controls which enable encryption, data integrity, data retention, and other aspects of security concerned with the confidentiality and integrity of information assets.

**Software, System, and Service Assurance**

Software, System, and Service Assurance focuses on how software, systems, and services are designed, developed, tested, operated, and maintained throughout the software lifecycle.

**IT Service Management**

This building block is actually a composite of other service management disciplines and a tie back to information security. For example, event, incident, and problem management as it relates to information security. This is an important intersection of information security with traditional IT disciplines.

**Threat and Vulnerability Management**

By proactively inspecting the infrastructure which runs the Cloud, this building block is able to proactively address new security threats which may have occurred in the infrastructure. This includes vulnerability scanning, virtual patching, and other aspects of security testing and response.

**Physical Asset Management**

Physical Asset Management addresses keeping track of the physical assets which make up the system.

**Risk and Compliance Management**

Risk and Compliance Management provides the means to analyze compliance to the specified control and procedures, and quantify and/or qualify the resulting risk. This assists the organization in evaluating the overall security posture and if it is in alignment with the risk objectives set out by Command and Control Management.

**Security Pattern**

The overall objectives for security are driven from Command and Control Management, which influences Security Policy. Security Policy dictates the objectives of Identity Access and Entitlement, Data and Information Protection, Software, System, and Service Assurance, IT Service, Threat and Vulnerability, and Physical Asset Management. Evidence and artifacts from these building blocks are used as input to Risk and Compliance Management, which provides compliance reports and risk exposure to Command and Control Management. This results in a closed loop system which allows Command and Control Management to adjust the policies which influence the other building blocks based on the relative risk exposure quantified or qualified through Risk and Compliance Management.

\(^3\) Nonetheless, it is important to understand that Identity, Entitlement, and Access are decoupled from each other. Identity is about more than just entitlements and access. Access control is not entirely dependent on identity and entitlements.
Scope

In this White Paper, we focus on a business scenario to illustrate the security concerns regarding Identity, Entitlement, and Access Policy Management in Cloud Computing. To focus on this subject, we have intentionally chosen an SaaS delivered via public Cloud. We do this because it enables us to address the most general class of issue. Some of these issues would have little relevance in a private and/or IaaS situation but the approach we describe would still be relevant. As an aside we note that SaaS is frequently offered as a public Cloud delivery model.

Principles

The Security for the Cloud and SOA project has defined a set of Security Architecture Principles. The following subset of those principles is particularly relevant to this White Paper:

• **Openness**: Openness is of primary importance in an enterprise environment. This includes support for all major platforms, runtimes, languages, support for major industry standards, published interfaces and algorithms, no security by obscurity, documented trust and threat models, and support for Common Criteria, and similar formal security validation programs.

• **Design for regulations**: Regulations drive many requirements in IT security projects, and regulations change over time. To handle this, it requires flexible support for the constraints set by government regulations and industry standards and traceability between regulations, standards, and business policies and the security policies used to implement them.

• **Design for privacy**: In the current age of data sharing, privacy becomes increasingly more important. Solutions should highlight the use of private information and corresponding data protection mechanisms, and enable the principles of notice, choice, and access.

• **Design for extensibility**: Good solutions are component-based and separate the management of mechanisms from the mechanisms themselves, to support a variety of mechanisms under the same framework. Already deployed systems must allow for the addition and extension of new mechanisms within the existing management framework.

• **Policy-based access to services**: Service consumption will be controlled by policy. Policies will be held externally from applications.

• **Multi-tenancy**: A Cloud Computing model must support isolation among multiple tenants of the Cloud.

The Cloud Security Alliance\(^4\) has also defined a set of Identity Management Principles for the Cloud, which will be published in the next version of the Guide. We draw the reader’s attention to a subset of those principles, which are generally relevant to our scenario:

• Cloud service providers should by default not seek to be identity providers unless there is a compelling public interest being served and IDP is a core business.

• Consumers should reward Cloud service providers who offer their services as relying parties to well-known and trusted identity providers and minimize their own collection of identity information.

• Strong authentication should be ubiquitous, flexible, and natively supported by the identity provider.

• Identity providers have a responsibility to issue IDs that can be used holistically by the individual, and not just for the relationship with that provider. This includes government enterprises acting as identity

---

\(^4\) Information regarding the Cloud Security Alliance can be found at the end of this White Paper.
An Architectural View of Security for Cloud

providers solely for their own employees and partners need to embrace a strategic direction to exit this business.

• Major Cloud identity providers need to publicly commit to “network-neutrality” principles to provide no competitive advantage to their own SaaS commercial applications over third-party SaaS commercial applications.
**Terms**

Throughout this White Paper there are a number of terms which we use in order to describe the scenario. For clarity, we’ve taken the liberty of defining the terms below.

**Buyer**

The buyer is the organization who contracts with the seller for the delivery of services.

**Seller**

The seller is the entity responsible for providing the Cloud services to the buyer. A seller might be a provider as well, but does not have to be. A seller may sell services to the buyer which are delivered by another provider. Ultimately, the seller has contractual accountability for delivering the services contracted by the buyer.

**Provider**

The provider is responsible for the delivery of some Cloud services. These services might be partial or full scope of the services purchased by the buyer from the seller. The provider may also consume services from other providers. For example, a SaaS provider may consume the services of a PaaS provider on which the SaaS application is delivered.

**Consumer**

The consumer is the entity which is the recipient of the services provided by the provider. In some cases, this might be an end user; in other cases a provider may also be a consumer if it relies on services delivered by another provider. For example, a provider who hosts their SaaS on a different provider’s IaaS.

**Responsibility versus Accountability**

The difference of accountability *versus* responsibility occurs in a number of different areas of business and IT; Cloud Computing is no different. When an organization makes a decision to embark on Cloud Computing, the organization itself is still accountable for the fulfillment of the Cloud-based service.

For example, an organization’s IT department may choose to leverage a public IaaS to address peak demand. In this scenario, the Cloud provider would be responsible for the delivery of the IaaS. However, the IT department would still be accountable for the overall delivery of IT services to the enterprise.
The Business Scenario

We use a scenario involving one buyer/consumer enterprise and three seller/provider enterprises. In addition, one of the sellers is both a provider and a consumer of Cloud services. By doing this we can more easily address a number of complexities whilst keeping the scenario manageable.

The actual business scenario (see Figure 2) involves a travel booking service. Enterprise A provides its users with a number of services via its enterprise portal and travel booking is one of them. It is important to the enterprise that it be completely transparent to users whether the service is provided internally or externally. Provider A offers such a service, which we'll call Travel Cloud. A travel booking organization cannot itself manage airline schedule and availability information nor can it issue tickets. It therefore makes use of the services of another Cloud provider, which we'll call Flight Cloud. For equivalent reasons Travel Cloud uses an accommodation service from Provider A: Night In The Clouds. The whole thing looks like this:

![Diagram of the Business Scenario](image)

Figure 2: Business Scenario: Overview

We can treat this as a set of three pair-wise buyer/seller relationships but have to take account of the fact that the role of Travel Cloud as a provider-consumer can create an indirect relationship between Enterprise A and the two other sellers, which can have significant implications from a security perspective. In particular, it is clear that data belonging to Enterprise A is exposed and potentially stored in interactions with three other parties and that Enterprise A has no direct control over two sets of interactions.

There are many security considerations involved here but this White Paper concentrates on just one major building block: Identity, Entitlement, and Access Management. These are not more important than any other aspect but are sufficient to illustrate the method meaningfully.

All parties will normally have their own policies for these aspects of security. How they approach Policy Management can vary and results in one of three situations (per pair-wise relationship):

1. Seller controls Policy Management and any buyer has to adapt to that situation.
2. Buyer controls Policy Management and sellers undertake to support that.
3. Both parties control Policy Management locally and a framework for policy exchange is implemented. Each of these situations will have its own implications for both responsibility and accountability for security concerns. In each situation we look at the mechanisms available for reconciliation of security policy between parties (and where necessary by one party alone) in such a way as to ensure that the actions carried out by the responsible party support the accountability needs of the other(s).

Note that we have included other buyer enterprises in Figure 2 to emphasize that multi-tenancy is an important factor. These other enterprises play no active role in our scenario.
Identity, Entitlement, and Access Management

In this section we focus on Policy Management building blocks, as these include identity and access policy.

Identity, Entitlement, and Access Management building blocks are of course also important.\(^5\)

For the most part, these ABBs can be assumed to be collocated with the responsibility for the Policy Management building blocks and the White Paper does not explore them in depth. The exception to this rule is Identity Provisioning, for reasons which will become apparent.

**Situation 1: Seller’s Rules**

If we reflect this situation in terms of IAM (Identity and Access Management), the core concern is that the master repository (i.e., the repository, which ultimately determines access rights) belongs to the seller. In other words all identities, roles, groups, and access policies must be present here and defined in the terms dictated by the seller. And of course the enforcement of policy takes place in the seller’s domain.

Implemented in the simplest form it also means that all user provisioning takes place in the seller’s domain and that there can be no complete Single Sign-On (SSO) for the services exposed in the buyer’s domain.\(^6\) It is also clear that this does not conform to our Openness principle nor with the CSA’s first principle (Cloud service providers should not seek to be identity providers). Moreover, it is questionable to what extent we can support either the Design for Regulations or Design for Privacy principles.

\(^5\) Note that there is no implied coupling between any of these building blocks. In particular, the vertical groupings should be understood to emphasize areas of similar concern and their loose relationship with the other areas. At the level of detail handled in this White Paper, access control is subsumed under Policy Management. Solution building blocks are treated separately and are not within the scope of this White Paper.

\(^6\) In these scenarios we are only concerned with responsibilities for building blocks in the context of Enterprise A being a consumer of the Travel Cloud service. The fact that Enterprise A probably authenticates its users on first access to the portal and potentially issues an SSO session ticket is not part of the scenario. Any action Enterprise A takes as a result of a (potential) user request for the Travel Cloud resource, is indeed part of the scenario. In the simple form of situation 1, no such action exists.
Clearly the responsibility for all the building blocks in this form lies entirely with the seller. Accountability is, as in all the situations and options we’ll consider, entirely on the Enterprise A side. Note that Enterprise A has no responsibilities here, because it does not manage any aspect of IAM for this specific service.

There are of course two other pair-wise relationships to be considered: Travel Cloud to Flight Cloud and Travel Cloud to A Night in the Clouds. If seller’s rules also apply here, each pair-wise relationship has a master repository but the complete scenario has three – and you can’t have three masters of the same information.

One relatively common way of addressing this is to make use of standards such as SAML (Security Assertion Markup Language) and SPML (Service Provisioning Markup Language) to enable a degree of transparency in both access control and user provisioning. That could lead to the deployment of building blocks illustrated in Figure 6.

In this case, Enterprise A does assume some responsibility, because users of the Travel Cloud service are provisioned in both in that domain and in the seller’s domain. Policy Management remains the responsibility of the seller because, for example, the authentication process that leads to the issuing of an SAML token has no direct bearing on the access to the Travel Cloud service.

---

7 If we were considering privacy, this would not always be the case. Some legislations would regard both buyer and seller as accountable, because the accountability is not to the organization but to a national or regional regulator.

8 The actual issuing of an SAML token is indeed a responsibility of Enterprise A but represents a finer-grained capability rather than a scenario-specific policy implementation.
Nevertheless we’re still left with a lot of complexity. It is not unusual that the format of repository information differs between seller and buyer, even if we can keep the semantics consistent. In general we have to assume that it will be necessary to map user information between parties both at provisioning (plus de-provisioning) and access time. That usually requires some custom functionality. If all parties are exchanging such information and if none of them has designed their identity and access policies with the entire scenario in mind we can easily reach the kind of situation shown in Figure 7 which fairly obviously leaves lots of room for disconnects. Nevertheless, the value of the scenario-driven approach is in exposing that complexity. That knowledge helps in risk analysis and the development of mitigating controls.

How could we simplify things? We can start by considering carefully for which entities access rights need to be configured in Flight Cloud and A Night in the Clouds. The consumer of these services is in fact Travel Cloud. There is no good business reason to provision Enterprise A’s users in either of those providers’ repositories. They are perhaps the owners of the end product (e.g., a flight ticket) but not the consumers of
the service.\textsuperscript{9} If we can take this approach, we can then simplify the scenario to three separate pair-wise relationships from the access control perspective. (Note: Privacy and other compliance concerns are not so easily dealt with but are not the topic of this White Paper.) Clearly this will depend on the capabilities of the three providers. The suggested approach is based on several of the core principles of the project, most significantly Openness (through SAML), and Policy-based Access. It also goes some way to supporting the CSA principles relating to the discrete and generalized role of identity providers.

**Situation 2: Buyer’s Rules**

This situation could be seen as the ideal world and is for that reason hard to realize. Essentially it requires the seller to trust the buyer to define and implement policies in such a way as to ensure that only a properly authenticated and authorized user can access the buyer’s service. The result is that any user coming from the buyer’s domain will automatically be granted access. This is in fact not difficult to implement reliably using SAML.

In reality of course not all users will have the same rights. How that is addressed will depend on the granularity of the seller’s application interface (UI or API). If finer-grained options are provided, then perhaps all authorization can be controlled on the buyer side and the seller simply needs to be able to manage their side of the SAML transaction.

If, however, the granularity is very coarse it will be necessary to provide additional claims (e.g., role) in the SAML ticket, which the seller can use to determine finer-grained access rights.

In either case the seller has no interest in the identity of the user other than possibly for auditing purposes.

So why might this be hard to realize? Well the initial problem is that many SaaS services are built around management of their own repository and may be unwilling or even unable to adapt to a more open model. However much we might want it to be different, it’s perfectly understandable that a provider would take this approach. It offers a lowest common denominator and is closer to the current situation with much proprietary business software running on-premise. In other words, it probably makes it easier to sell! On the other hand the Cloud paradigm may represent the best impetus to move from an outdated provider centricism to a more open approach. The problem is exacerbated if not all sellers in the scenario subscribe to the model. Also Travel Cloud needs to issue its own SAML tokens. Nevertheless, if industry forces are sufficient to promote adoption of the principles of Openness, Extensibility, and Policy-based Access as well as CSA principles relating to the discrete and generalized role of identity providers, then that change will happen.

\textsuperscript{9} So in fact the consumer is a software component belonging to and acting as a proxy for Travel Cloud. This is one illustration of the important fact that identity is not merely related to people but also to devices, code, organizations, data, and more. It may well be that a particular policy defines more than one identity to be relevant to the use of a particular service.
Situation 3: Cooperative

We now consider a model where all parties exchange identity and policy information as needed and as appropriate. This allows each of them to manage and enforce policy to the extent necessary for their own goals and obligations without impinging on the capabilities of other parties.

To achieve this the parties will need to support standards and protocols, which support such behavior. Apart from the already mentioned SAML (or WS-Federation), standards such as XACML and OAuth are available and increasingly widely used. Another relevant standard is InfoCard, best known in the Microsoft CardSpace implementation.

One approach to this is illustrated in Figure 9 below. Enterprise A has responsibility for Policy Definition and for all Policy Management in its own domain and for Provisioning of its own users. The three providers are each responsible for enforcement of these policies. Standards such as XACML and OAuth are used to transmit the policy information. It’s clear that this approach conforms to the principle of Openness and is directly Policy-driven. Moreover, it supports the principles of design for Privacy and Extensibility by minimizing coupling between parties.
One can easily foresee a number of variations on this where more than one party defines policy or controls a user repository. In these situations policy exchange is to a greater or lesser extent bilateral and user attributes are potentially exchanged but each party remains master of its own information. Both providers and consumers may well be reluctant to support multiple standards, whilst the alternative may be a lot of customization, mostly on the consumer side. If we take into account the multiple tenants of the three providers in our scenario, one could envisage considerable complexity in information exchange. One response to this is the comparatively recent appearance of a specialized form of Cloud provider, the Identity Service Provider (IdSP). This is a form of Cloud service aggregator, restricted to providing identity and policy services and is not (in general) the same thing as an identity provider.
Many variations on the deployment of building blocks in this situation may be considered. In principle the IdSP could also manage policy enforcement using policies defined by the buyer. The IdSP may also take on the role of identity provider (some do) or of a provisioning hub. The existence (and use) of an independent identity provider is advocated in the CSA principles. There is, however, no suggestion in the principles that this should be the same party as the IdSP. Consumers in particular need to look carefully at which building blocks are claimed by or available from an IdSP and ensure that this architecture will satisfy their security policy or that satisfactory mitigations can be put in place. In turn the security policies of all parties should take full cognizance of the principles we have highlighted.

As a final reminder before leaving the IAM topic, none of the options we have discussed change the fact that the accountability for compliance with Enterprise A’s policies remains with Enterprise A itself. A buyer may be able to hold a seller contractually accountable and some national privacy legislation mandates shared responsibility in that area but the buyer cannot divest him/herself of accountability. That makes it all the more important to properly understand responsibility and the full implication of which (relevant) building blocks are deployed where.
Conclusion

Security in Cloud Computing will continue to be a significant concern for enterprises as they move to embrace public Cloud Computing offerings. Security concerns cannot be typecast based on the Cloud service model (BPaaS, SaaS, PaaS, IaaS). They need to be examined with an eye to buyer versus seller security policy, accountability, responsibility, flexibility, and ultimately risk-based mitigating controls. These are the concerns of a thorough architectural approach. The Architectural Building Blocks and other work products produced by the Security for the Cloud and SOA project provide an excellent model of reviewing information security, and ensuring that both buyer and seller policies can be aligned.

Enterprise architects who look to leverage Cloud Computing can examine this, as well as other papers in the “An Architectural View of Security for the Cloud” series to understand how to methodically take a risk-based approach to applying security to Cloud Computing.
Further Reading


Open Enterprise Security Architecture (O-ESA), Guide (G112), published by The Open Group, April 2011; refer to: www.opengroup.org/bookstore/catalog/g112.htm.


SAML and SPML; refer to: www.oasis-open.org/specs.

XACML; refer to: www.oasis-open.org/committees/xacml/.

OAuth; refer to: http://oauth.net/.

Higgins Open Source Identity Framework; refer to: http://eclipse.org/higgins/.

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following individuals in the development of this White Paper:

- Stephen Bennett, Oracle
- Anthony Carrato, IBM
- Pascal de Koning, Getronics
- Rakesh Dharmala, CA
- Michiel Perdeck, Logica
- Paul Simmonds, Jericho Forum
- TJ Verdi, Boeing
- Stewart Wolfe, IBM
- Ian Dobson, The Open Group
- Chris Harding, The Open Group
- Andrew Josey, The Open Group
An Architectural View of Security for Cloud

About the Authors

Omkhar Arasaratnam

Omkhar Arasaratnam is an accomplished Certified Senior Security Architect with IBM. He is a member of the IBM Security Architecture Board, the IBM Cloud Computing Security Architecture Board, and co-leads The Open Group Cloud Working Group’s Security for the Cloud and SOA project. He is also actively involved in the International Standards Organization (ISO) JTC1/SC38 Study Group on Cloud Computing.

Omkhar is also an accomplished author and technical editor of several IBM, John Wiley & Sons, and O’Reilly publications. He also has five pending patents in the field of information technology.

Omkhar has worldwide responsibility for security architecture in some of IBM’s Cloud Computing services.

Stuart Boardman

Stuart Boardman is a Senior Business Consultant with Getronics Consulting where he co-leads the Enterprise Architecture practice as well as the Cloud Computing solutions group. He is co-lead with Omkhar Arasaratnam of The Open Group Cloud Work Group’s Security for the Cloud and SOA project and a founding member of both the Cloud Work Group and the SOA Work Group. Stuart is the author of publications by the Information Security Platform (PvIB) in The Netherlands and of his previous employer, CGI. He is a frequent speaker at conferences on the topics of Cloud, SOA, and Identity.

About The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry’s premier certification service, including UNIX® system certification. Further information on The Open Group can be found at www.opengroup.org.