Open Group Guide

Framework for Secure Collaboration-Oriented Architectures (O-SCOA)

Open Group Guide

Framework for Secure Collaboration-Oriented Architectures (O-SCOA)

ISBN: 1-937218-03-4

Document Number: G127

Published by The Open Group, September 2012.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Open Group Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This Document

This Open Group Framework for Secure Collaboration-Oriented Architectures (O-SCOA) specifies the requirements for secure design of enterprise IT architectures that support de-perimeterized[1] operations.

The Secure COA Framework was originally developed by the Jericho Forum and published in a series of 23 Secure COA Requirements Papers over the period 2006 to 2009.

This Guide collates all these Secure COA Requirements Papers, along with the Jericho Forum Commandments (design principles) that they adhere to, into a single readily-accessible publication. It specifies all the essential components required for architecting secure systems for deployment in de-perimeterized environments; i.e., without depending on securing the corporate perimeter.

[1] For the definition of de-perimeterization, see Section 2.2.

Target Audience

This O-SCOA Framework provides system and security architects and designers with a single volume specifying the design requirements that need to be satisfied in order to deliver secure operation, globally, over any network, and so enabling them to create secure computing architectures which satisfy the Jericho Forum Commandments.

It also provides IT business managers with insights into the business benefits that adopting this O-SCOA Framework will provide – these being to give confidence that in meeting today's demands for improved business efficiency through IT collaboration (sharing/exchanging information with their business partners, suppliers, customers, and outworkers) their IT operations will remain secure against increasingly sophisticated threats and new vulnerabilities.

Trademarks

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following in the development of this Guide:

- Members of the Jericho Forum over the period 2006-2009 who variously wrote and edited the Secure COA Requirements Papers. Prominent among these members were the following leading contributors, whose affiliations at the time these papers were written are included below:

  — John Arnold, Capgemini

  — Guy Bunker, Symantec

  — Pete Burnap, University of Cardiff

  — Ian Dobson, The Open Group

  — Jeremy Hilton, University of Cardiff

  — Paul Simmonds, ICI

  — Adrian Seccombe, Eli Lilly

  — Stephen Whitlock, Boeing

  — Andrew Yeomans, Dresdner Kleinwort Bank

- Members of The Open Group Security Forum who reviewed and edited the 23 Secure COA Requirements Papers into a consistent single O-SCOA Framework Guide

Referenced Documents

The following documents are referenced in this standard:

- CobiT (Control Objectives for Information and Related Technology); refer to www.itgovernance.co.uk.
- EU Directive 95/46/EC: The protection of individuals with regard to the processing of personal data and on the free movement of such data; refer to http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.
- eXtensible Access Control Markup Language (XACML); refer to www.oasis-open.org/committees/xacml.
- Guide: Core Identifier Framework Matrix (G071), published by The Open Group, April 2007; refer to www.opengroup.org/bookstore/catalog/g071.htm.
- Guide: FAIR – ISO/IEC 27005 Cookbook (C103), published by The Open Group, November 2010; refer to www.opengroup.org/bookstore/catalog/c103.htm.
- Guide: Requirements for Risk Assessment Methodologies (G081), published by The Open Group, January 2009; refer to www.opengroup.org/bookstore/catalog/g081.htm.
- IETF RFC 5209: Network Endpoint Assessment (NEA): Overview and Requirements (June 2008); refer to tools.ietf.org/search/rfc5209.
- ISO 7498-2:1989: Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.
- ISO/IEC 10181-3:1996: Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework.
- ISO/IEC 15408: Information Technology – Security Techniques – Evaluation Criteria for IT Security (Common Criteria).
- ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management.
- ITIL (Information Technology Infrastructure Library); refer to www.itil.co.uk.
- Technical Standard: Risk Taxonomy (C081), published by The Open Group, January 2009; refer to www.opengroup.org/bookstore/catalog/c081.htm.
- The Open Group Guide: Jericho Forum® Self-Assessment Scheme (G124), published by The Open Group, March 2010; refer to: www.opengroup.org/bookstore/catalog/g124.htm.

- The State of Enterprise 2.0, Dion Hinchcliffe, October 22, 2007; refer to blogs.zdnet.com/Hinchcliffe/?p=143.
- TOGAF®, developed by The Open Group; refer to www.opengroup.org/togaf.
- Trusted Computing Network (TCN) Specification (IF-TNCCS-SOH); refer to www.trustedcomputinggroup.org/groups/network.
- Trusted Platform Module (TPM) Specifications; refer to www.trustedcomputinggroup.org/specs/TPM.
- UK Government Business Impact Table; refer to www.cesg.gov.uk/policy_technologies/policy/media/business_impact_tables.pdf.
- UK Government Risk Assessment Accreditation Document Set; refer to http://interim.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf.
- US Sarbanes-Oxley Act; refer to www.sox-online.com.
- White Paper: Identity Management (W041), published by The Open Group, March 2004; refer to www.opengroup.org/bookstore/catalog/w041.htm.
- White Paper: Information Security Strategy, Version 1.0: A Framework for Information-Centric Security Governance (W075), published by The Open Group, October 2007; refer to www.opengroup.org/bookstore/catalog/w075.htm.
- White Paper: Security Principles for Cloud & SOA (W119), published by The Open Group, December 2011; refer to: www.opengroup.org/bookstore/catalog/w119.htm.

1 Introduction

1.1 Objective

This Guide specifies the requirements for a Framework for Secure Collaboration-Oriented Architectures (O-SCOA) in a single, readily-accessible volume.

Until now, the O-SCOA Framework was published only as a set of 23 separate papers which were separately available as free downloads from the Jericho Forum publications web site,[2] over the period from June 2006 to January 2009. The requirements that a COA-compliant security framework must meet are encapsulated in the Jericho Forum Commandments, so these too are included in this Guide.

1.2 Background

In February 2009, the Jericho Forum, a Forum of The Open Group, launched its Secure COA Framework, specifying the requirements that must be met in order to architect effective security into Enterprise Architectures so as to enable secure business collaborations over any open network, with business partners, suppliers, customers, contractors, outworkers – in today's world where business operations demand sharing of high-value information efficiently over the Internet and in the cloud. These business operations involve information being transmitted outside an organization's corporate perimeter – boundaryless information flow – into de-perimeterized environments.

In "de-perimeterization" terms, a laptop or other PDA that is properly secure is a device that you can operate at the same level of security when you are located outside your business's corporate perimeter as when you are inside that perimeter.

The O-SCOA Framework describes:

- The COA concepts
- The framework components, each one in sufficient detail to describe the requirements for that component in order to satisfy specified criteria for secure de-perimeterized operations

1.3 Overview

In addition to capturing all 23 of the original Secure COA Requirements Papers specifying the COA in one volume, this standard includes dependent context:

[2] Refer to the Jericho Forum publications web page at www.opengroup.org/jericho/publications.htm.

- The business case for why business managers should respond to the challenges of de-perimeterization, by adopting strategies to migrate their IT systems towards a COA framework.
- The Jericho Forum Commandments (design principles) for building systems which will operate securely in de-perimeterized environments; i.e., where security does not depend on securing a corporate perimeter of any kind. Note that this non-dependency does not mean that the O-SCOA Framework proposes that firewalls and other security measures within the corporate perimeter should be dispensed with; on the contrary they provide valuable defense-in-depth.

The Jericho Forum Commandments are also applicable to securing cloud computing environments, so this O-SCOA Guide is fully applicable to cloud computing.

1.4 Structure of this Document

- The business case for de-perimeterization
- How securing cloud computing is a natural extension of the O-SCOA Framework
- What the Jericho Forum Commandments mean
- The concepts underlying SCOA
- The SCOA high-level framework – describing the primary function of each main component in the Framework, and how the components inter-relate
- For each component:
  - — Why that component is needed – what problem is it addressing, and why it matters
  - — What security requirements that component fulfils
  - — How those requirements fulfill the need
  - — Known limitations and constraints which require further consideration

2 The Business Case for De-Perimeterization

2.1 The Drive Towards Connectivity

Computing evolution can be viewed in terms of increasing connectivity over time, starting from no connectivity (stand-alone) to the extensive connectivity we have today.

The primary driver for this evolution stems from business demands that IT systems deliver improved business efficiency by enabling collaboration – sharing/exchanging information with business partners, suppliers, customers, contractors, outworkers, etc. – while still demanding that all operations remain secure against increasingly sophisticated threats and new vulnerabilities.

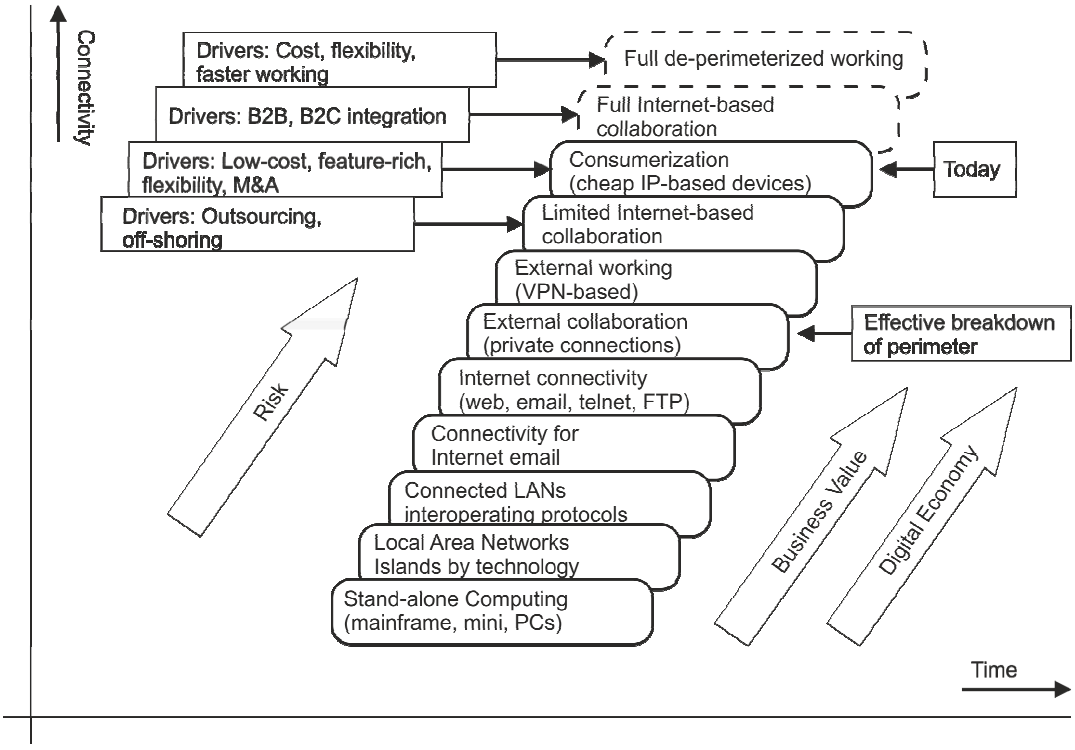


Figure 1: Increasing Connectivity over Time

2.2 De-Perimeterization

Increasing connectivity represents a continuing security challenge – how to secure the information being shared/exchanged when it leaves or enters an organization's corporately managed perimeter. Private connections, VPN-based tunnels, and wireless (mobile) connections bypass perimeter firewalls. Hence we needed a new approach to the challenge of our eroding

corporate perimeters. In this situation, information security needs not only to be appropriately applied while the information is in transit over open insecure global networks (including the Internet), but also when transiting to and from the corporate perimeter to its endpoints. The term "de-perimeterization" describes this major information security challenge.

Note: De-perimeterization is the challenge, not the solution. In 2004 when the Jericho Forum adopted this security challenge and proclaimed the need for a new approach to securing our IT operations, many security industry leaders rejected it as an issue that existing traditional "perimeterized" security solutions could manage, even though there was ample evidence to the contrary. By 2009, de-perimeterization had gained recognition and majority acceptance. It will continue as an inevitable trend that will eventually impact every business operation.

2.3 Cloud Computing

The same business drivers for increased connectivity and business collaboration were recognized as applicable to cloud computing. Cloud is a de-perimeterized environment. Cloud computing brought to business managers' attention the promise of huge reductions in business IT costs – inviting business managers to exploit the huge computing power, storage, and applications resources (all outside the corporate perimeter) that are available in the cloud, at almost immediate availability and amazingly low cost.

This, however, also brought to business managers the realization that with their confidential business information and perhaps also their custom software applications then moving outside their corporate perimeter into "who knows where" – maybe even outside their own national borders – they needed firm assurances from cloud providers that these high-value assets (information, custom software, etc.) were secure from risk of theft or other loss, were held in compliance with applicable regulatory regimes which were auditable, were guaranteed to be available, and could be retrieved from the cloud without leaving any information behind. At this time, for medium and high-value operations – even in "private clouds" – such reassurances remain still largely insufficient to satisfy business managers, their partners and customers, and their auditors.

How secure is a corporation in entering into business collaborations in the cloud? The Jericho Forum advanced understanding of several types of cloud when it published its Cloud Cube[3] model for understanding cloud architectures. Each type offers different characteristics which represent different risk profiles, each thereby affecting varying degrees of flexibility and collaboration features, and each needing different security solutions to match. It is important for a business to appreciate the distinguishing features of each type of cloud, in order to manage its corporate risk profile.

Cloud computing is part of the secure business collaboration picture – aimed at enabling end-to-end secure operation over any network, irrespective of whether you're located inside or outside of your increasingly dissolving corporate perimeters.

[3] Jericho Forum Cloud Cube model; refer to: www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf.

2.4 Information-Centric Protection

A business's corporate information, and its custom software applications, represent far greater value than the cost of their IT system infrastructure; i.e., their hardware, and commercial off-the-shelf operating systems and applications. So the business priority for security is to focus on protecting its information and custom software[4] – in both cases, moving the protection as close to the data as possible – to protect their most valuable assets.

2.5 More on De-Perimeterization

2.5.1 The Inevitable Trend

Network security perimeters are being eroded. De-perimeterization is impacting all IT-dependent businesses, as the demand for more connectivity and business collaborations outside the corporate enterprise increases.

Consumerization is driving towards an IP address on every electronic device. The explosion in availability and business functionality in low-cost, pervasive, fast, reliable, cheap PDAs with Internet connectivity is evident everywhere.

Business "relationships" of every type are rapidly increasing. Managing connectivity for these relationships needs to include handling wholly-owned and partially-owned subsidiaries, and collaborative relationships with other businesses that are also competitors in other business areas.

Key indicators of the impact of de-perimeterization include:

- The increasing mismatch between the (legal) business border and the network perimeter as businesses become more integrated resulting in their relationships becoming increasingly unclear
- Business demanding to interconnect systems directly where B2B relationships exist
- The need to have good network connectivity and access to all organizations with whom you have a business relationship
- Distributed and shared application software across business relationships
- Increasing numbers of applications using technology that bypasses firewall security at the perimeter (typically using web-based techniques that can legitimately traverse the perimeter)
- Increasing inability of traditional firewalls and other network perimeter controls to combat malware that uses web and email-based techniques

[4] See The Open Group White Paper: Information Security Strategy, Version 1.0: A Framework for Information-Centric Security Governance, October 2007 (W075); available at: www.opengroup.org/bookstore/catalog/w075.htm.

2.5.2 Business Benefits

Business managers require their IT systems to be not only secure in the sense of protecting their information assets, but also agile so they can be adapted quickly to new ways of working so as to exploit new business opportunities/directions and their associated operations and processes. They understand that "security" must operate as an enabler (not an inhibitor) for collaborative working, expansion, and speed-to-market.

Efficiencies in collaboration with business partners bring multiple benefits. A small selection of examples include:

- Enable direct B2B integration of ERP systems with your major partners, enabling better exchange of data and closer co-operative working
- Allow legal, commercial, and quality-of-service borders to align with the network and infrastructure implementation, while paying only for the bandwidth and infrastructure the business actually needs
- Allow your business partners, partners in joint-contract ventures, suppliers, etc. to access directly the information you want to share with them as simply as if they were physically connected at one of your offices or sites
- Allow direct electronic interaction with customers
- Move remote offices from being slow and expensive-to-manage networks to having direct, fast, and cheap local network connectivity, with better performance and significant cost savings

The O-SCOA Framework responds to the challenges of de-perimeterization. It identifies a set of enabling technologies that:

- Reduce complexity, and therefore costs, by unifying and simplifying solutions
- Enable business flexibility, cost-effective bandwidth, and infrastructure provision
- Provide increased security, thereby reducing risk
- Enable multi-vendor outsourcing – simply and effectively
- Provide a simpler and thus more auditable environment
- Provide true defense-in-depth, from the network through to the actual data

2.5.3 Why De-Perimeterization is a Disruptive Change

Up to the time when business demands for ever greater connectivity grew too great, evolution of security solutions tended to be additive. They were typically characterized as a succession of "sticking plaster" (band-aid) solutions. Also, interim solutions to connectivity demands, such as VPN technology, were often applied as quick solutions, with little regard for how they undermined the security infrastructure they were fitted into – in particular how they bypassed perimeter firewalls on which great reliance to secure the corporate perimeter to external networks had long been placed.

Only by accepting that de-perimeterization is an inevitable trend have we been able to realize a new architectural mindset that addresses in a holistic way the connectivity challenges we need to secure.

Most network-based security controls and "solutions" – such as Network Intrusion Detection (NID) systems and Network Access Control (NAC) – operate to support existing corporate network operations, in the misguided assumption that doing so provides "defense-in-depth", when in fact an ever-increasing percentage of an organization's business is operating outside of the traditional perimeter.

Many organizations have tried to segregate the corporate network into security "zones", each behind their own firewall. While this approach can provide an interim step in an organization's transition to de-perimeterization (this can be termed "shrinking the perimeter" and "micro-perimeterization"), it is not correct to think of this as synonymous with de-perimeterization. Widespread micro-perimeterization in fact adds network and management complexity, and creates more potential points of failure and bottlenecks for network traffic, all of which is not viable in the long term.

De-perimeterization requires security to be at the heart of the organization's distributed technology architecture. To be effective it must be consistently implemented in end-user devices and application services, and surrounding the organization's critical information assets themselves. This is not new. Rather, it reinforces what has been known for years – that unless security is built-in from the ground up it will rarely be effective or efficient in achieving the intended goals.

2.5.4 Architecting for De-Perimeterization

It is worth repeating that "de-perimeterization" is the security challenge. The O-SCOA Framework provides an effective approach to assuring security of Enterprise Architectures for the future.

Fundamentally, this new approach requires developing a migration strategy to implement an organized transition towards a COA. Since the security challenges that global connectivity brings are much wider than the traditional security requirements in corporately perimetered IT systems, the scope of a secure COA is similarly significantly extended.

3 The Jericho Forum Commandments – Design Principles

3.1 Overview

In 2006, the Jericho Forum published its Commandments (design principles) for effective security in de-perimeterized environments).

These Commandments comprise 11 security principles, under five subject areas:

- Fundamentals
- Surviving in a hostile world
- The need for trust
- Identity, management, and federation
- Access to data

which together provide a comprehensive statement defining:

- The security principles that must be observed when designing architectures and infrastructures for a de-perimeterized future; in this respect they provide security guidelines to IT architects and designers
- Criteria which can be used as a benchmark to measure/assess how effective any given security architecture is for secure operation over any open network; i.e., in de-perimeterized environments

Each commandment is supported with concise rationale that provides guidance on key underlying precepts.

Whilst building on "good security", these Commandments specifically address those areas of security that require specific attention in order to deliver security architectures that are effective in de-perimeterized environments. They do not aim to include basic traditional security principles, which are extensively described elsewhere.[5]

3.2 Self-Assessment Scheme

The Jericho Forum Self-Assessment Scheme[6] takes each Jericho Forum Commandment in turn, and asks "nasty" (i.e., difficult, searching, probing) questions to reveal how effectively a given

[5] See The Open Group White Paper: Security Principles for Cloud & SOA, December 2011 (W119); available at www.opengroup.org/bookstore/catalog/w119.htm.
[6] See The Open Group Guide: Jericho Forum® Self-Assessment Scheme, March 2010 (G124); available at: www.opengroup.org/bookstore/catalog/g124.htm.

information security product or solution meets the criteria implicit in that Commandment. It then gathers the answers into a Self-Assessment Scorecard.

The "self-assessment" aspect of this scheme is important – it is a self-policing scheme to ensure that it is low-cost and low-maintenance. It does, however, represent high value to those who care to use it, in particular:

- To product suppliers who wish to show how well their product(s) or solution(s) satisfy the Commandments
- To customers who wish to check how well a product or solution meets their security requirements
- To IT architects and designers who want to check how secure their designs are

3.3 The Commandments

First published in April 2006, the Jericho Forum Commandments have stood the test of time as a robust set of security design principles which are used by security architects and designers worldwide as design principles, and to evaluate how sufficiently a security architecture satisfies the requirements implicit in these design principles.

The 11 security design principles, in five sections, are listed below.

3.3.1 Fundamentals

1. **The scope and level of protection should be specific and appropriate to the asset at risk.**

   Business demands that security enables business agility and is cost-effective.

   Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.

   In general, it's easier to protect an asset the closer protection is provided.

2. **Security mechanisms must be pervasive, simple, scalable, and easy to manage.**

   Unnecessary complexity is a threat to good security.

   Coherent security principles are required which span all tiers of the architecture.

   Security mechanisms must scale; from small objects to large objects.

   To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms.

3. **Assume context at your peril.**

   Security solutions designed for one environment may not be transferable to work in another. Thus, it is important to understand the limitations of any security solution.

Problems, limitations, and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

3.3.2 Surviving in a Hostile World

4. Devices and applications must communicate using open, secure protocols.

Security through obscurity is a flawed assumption – secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.

The security requirements of confidentiality, integrity, and availability (reliability) should be assessed and built in to protocols as appropriate, not added on.

Encrypted encapsulation should only be used when appropriate and does not solve everything.

5. All devices must be capable of maintaining their security policy on an untrusted network.

A "security policy" defines the rules with regard to the protection of the asset.

Rules must be complete with respect to an arbitrary context.

Any implementation must be capable of surviving on the raw Internet; e.g., will not break on any input.

3.3.3 The Need for Trust

6. All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place.

Trust in this context is establishing understanding between contracting parties to conduct a transaction and the obligations this assigns on each party involved.

Trust models must encompass people/organizations and devices/infrastructure.

Trust level may vary by location, transaction type, user role, and transactional risk.

7. Mutual trust assurance levels must be determinable.

Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.

Authentication and authorization frameworks must support the trust model.

3.3.4 Identity, Management, and Federation

8. Authentication, authorization, and accountability must interoperate/exchange outside of your locus/area of control.

People/systems must be able to manage permissions of resources and rights of users they don't control.

There must be capability of trusting an organization, which can authenticate individuals or groups, thus eliminating the need to create separate identities.

In principle, only one instance of person/system/identity may exist, but privacy necessitates the support for multiple instances, or one instance with multiple facets.

Systems must be able to pass on security credentials/assertions.

Multiple loci (areas) of control must be supported.

3.3.5 Access to Data

9. Access to data should be controlled by security attributes of the data itself.

Attributes can be held within the data (DRM/metadata) or could be a separate system.

Access/security could be implemented by encryption.

Some data may have "public, non-confidential" attributes.

Access and access rights have a temporal component.

10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.

Permissions, keys, privileges, etc. must ultimately fall under independent control, or there will always be a weakest link at the top of the chain of trust.

Administrator access must also be subject to these controls.

11. By default, data must be appropriately secured when stored, in transit, and in use.

Removing the default must be a conscious act.

High security should not be enforced for everything; "appropriate" implies varying levels with potentially some data not secured at all.

4 SCOA Framework Concepts

4.1 Overview

SCOA-compliant architectures enable enterprises to operate in a secure and reliable manner in a de-perimeterizing environment, where it is the growing norm to interact with other businesses, partners, suppliers, customers, and outworkers, irrespective of the location of the data or the number of collaborating parties. They support business needs for faster and more flexible collaborative business arrangements.

The O-SCOA Framework defines the key components within which interoperable, secure solutions can be provided to meet these business needs. Thus, systems, networks, and whole "Enterprise Architectures" can be considered to be compliant with the O-SCOA Framework if all the components defined in the Framework are appropriately implemented.

Implementing an SCOA entails adoption of the applicable Jericho Forum Commandments. Particular attention is necessary to Commandments JFC#4 through JFC#8, which cover the areas of operating in a hostile environment, trust, and authentication.

4.2 Scope and Features

The O-SCOA Framework generalizes conventional architectures. It provides:

- Increased emphasis on the requirements listed in the Framework as "principles". These are traditionally only seen as external or boundary interface concerns in Enterprise Architectures.
- A user repository (keyed on people identifiers) generalized into a contract repository (keyed on relationship, or obligation identifiers). A contract repository records agreements, and the obligations and capabilities that ensue from them.
- An accounting log (keyed on system events), generalized into a reputation repository (keyed on business events). A reputation repository records user actions and compares them to applicable contracts, and, depending on whether or not the actions are in accordance with the contract, upgrades or downgrades a reputation.

The architecture formed by combining Service-Oriented Architectures (SOAs) with available security protocols (SAML or other XML) is insufficient to support SCOA. The following elements are also valuable:[7]

- The Standard Security Management System (ISO/IEC 27001).

[7] Note that we include mention of brokers and repositories. While these are not strictly within the intended scope of this document, they are mentioned because of their importance in the complete picture.

- Business processes that manage the collaborations founded on practices found in CobiT.
- Service management capabilities detailed in ITIL.
- The architecture capabilities defined in TOGAF.
- A powerful language for describing access policies and delegations (XACML Version 3.0 or similar).
- Access managers that will enforce an externally-required or end-to-end policy.
- Attribute brokers that will establish a requester's identity, credentials, and attributes to an appropriate degree of confidence, based on information from multiple authoritative sources (e.g., attribute authorities).
- Performance managers that will record what a user or system does at the level of business events, judge whether the user or system has acted in accordance with a contract or other agreed obligation, and report on their compliance profile. Today, this is a rather neglected field. It includes audit log managers and reputation systems.
- Contract brokers that will negotiate and agree new collaborative understandings between collaborating individuals in ways which do not violate their "owning" organization's and jurisdiction's existing policies and contracts. These new contracts must be expressed in an open standard language which can be interpreted by performance managers and access managers – eBXML is a strong candidate. The contract brokers must be able, in turn, to read the open standard output language of the performance managers and attribute brokers.

4.3 Implementation Considerations

Implementing a COA-compliant architecture results in building a high-level business framework that uses the capabilities of SOA, in addition to other relevant standards and practices, to enable secure collaboration. While an SOA meets many of the functional and non-functional requirements of a COA, other standards and practices such as TOGAF, CobiT, and ITIL also need to be engaged.

A fundamental shift in thinking is required to implement a COA-compliant architecture, moving from the thinking of a hedgehog – an animal that rolls into a tight prickly perimeterized ball at any sign of threat – to that of a strawberry plant, which puts all its key genetic material securely on its outside, as well as sending out suckers to extend the plant's domain. The O-SCOA Framework also provides a high-level pattern for how a previously developed information system can be re-architected to support effective and secure collaborations across corporate boundaries. Enterprises that want to operate in a network of business partners will do well to implement a COA-compliant architecture, and encourage their partners to do likewise.

Open standard interfaces need to be defined between the O-SCOA Framework's architectural elements. A key requirement is to define at the semantic level the meaning of trust/confidence and a trust management model,[8] to assure secure business collaboration between co-operating

[8] Refer to the forthcoming Open Group Guide to Trust Management – A Control Framework for e-Business Collaboration, which is currently under development in The Open Group Security Forum and is expected to be published by end-2012.

parties. These dependencies are addressed in the O-SCOA Framework, in terms of identifying the principal components in an "architect's view" diagram, and providing a requirements description for each component.

5 O-SCOA Framework – Primary Components

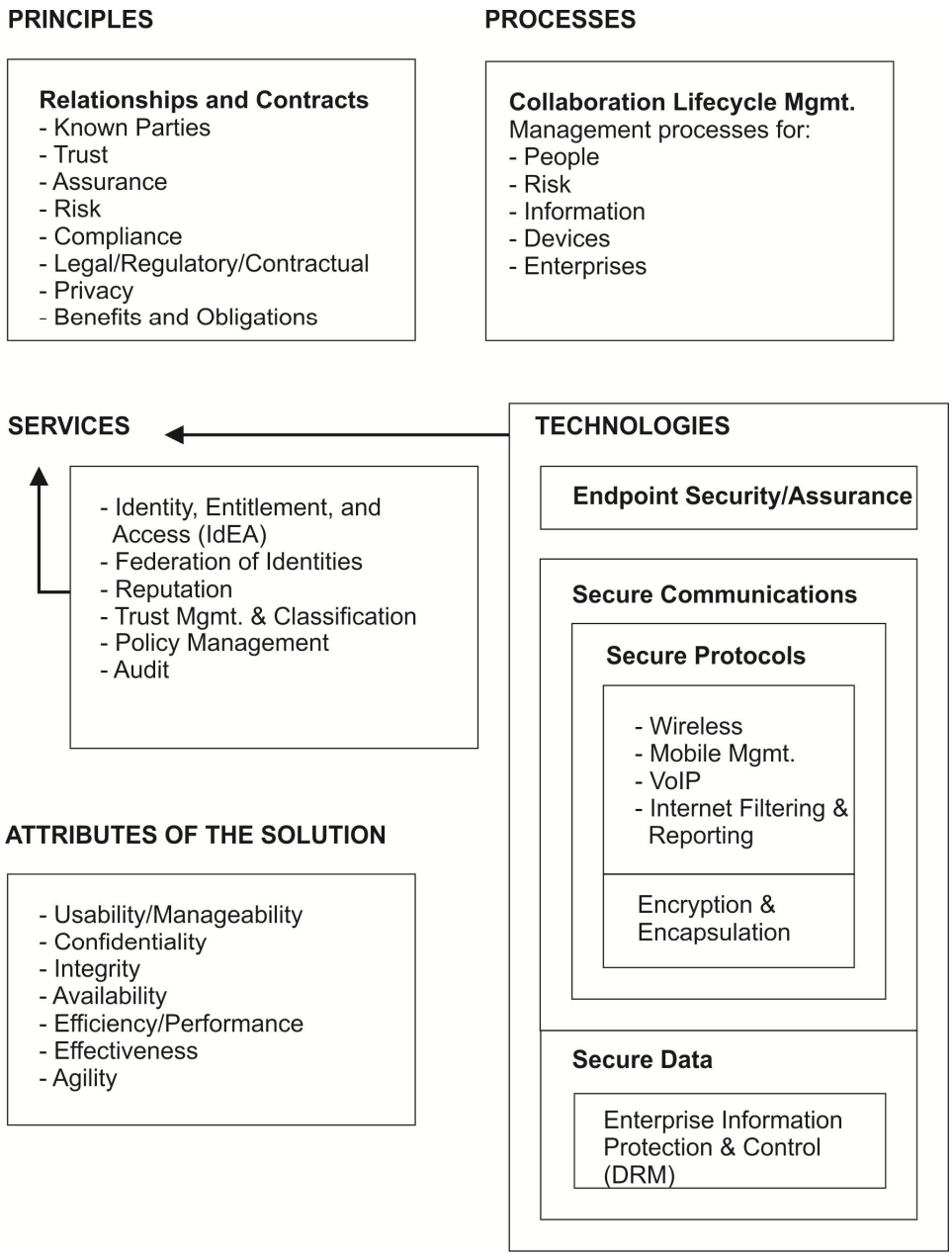


Figure 2: O-SCOA Framework

The O-SCOA Framework diagram identifies the principal security components, under five headings:

1. Principles
2. Processes
3. Services
4. Attributes of the Solution
5. Technologies

The Principles, and the Attributes of the Solution, require relatively short descriptions so are described in this chapter.

The other main component types – Processes, Services, and Technologies – each require significantly greater description so are outlined briefly in this chapter and then further described in more detail in the following Chapters 6 through 8.

5.1 Principles

The Principles group of components covers relationships and contracts.

These are characterized in two forms:

- Requirements (must haves)
- Constraints (shall nots)

5.1.1 Known Parties

Know who – or what – you are transacting with.

All components of a transaction chain must be known to the contracting parties at all of its endpoints. These components are selected by collaborating parties, during contract negotiations. Collaborating parties are responsible corporate or individual entities, whose identities are well defined and whose activities are controlled by legal, economic, ethical, and technical means. A collaborating party may be a consortium, in which case the consortium must indemnify its members (and provide other economic, ethical, and technical controls) so that other collaborating parties may safely collaborate with consortium members. In the case where individuals are engaged, they must initiate interaction through an accredited identity service provider.

5.1.2 Trust

Agree the level of trust/confidence at which you will be transacting.

The collaborating parties have the ability to agree/define appropriate (known) degrees of confidence in the components in a transaction chain, including the environment in which the components are operating.

5.1.3 Assurance

Verify that the agreed level of confidence applies.

Prior agreements between collaborating parties define their obligations to respect each other's intellectual property and to provide adequate technical security during a collaborative transaction.

5.1.4 Risk

The collaborating parties can make an assessment of any proposed transaction based on the communicated levels of trust with factors closely or significantly related to the transaction: identity, confidentiality, integrity, availability, location, environment (space in which it is being used), data sensitivity, transaction value, time, etc.

5.1.5 Compliance

Collaborating parties agree to periodic inspections and security audits. The results of these inspections and audits are published within the collaborative group. Non-compliant parties may be sanctioned or expelled.

5.1.6 Legal/Regulatory/Contractual

The collaborating parties must comply with applicable legal, regulatory, and contractual requirements and be able to resolve conflicts that may arise between these, through effective verification and enforcement mechanisms. Additionally, compliance to local, legal, and regulatory requirements alone is unlikely to be good enough to meet all business requirements.

5.1.7 Privacy

Privacy is a particularly important requirement that the collaborating parties must meet. Increasingly, privacy is being defined in legislative safeguards which are the consequence of widespread belief in privacy as a fundamental human right. At its root is an expectation by customers, suppliers, business partners, and employees that organizations will undertake to use information about an individual ethically so that it is not divulged or otherwise exploited if it is reasonably considered to be "private".

5.1.8 Benefits and Obligations

Contractual obligations, service-level agreements, customer expectations, corporate policy, and norms of good corporate citizenship are requirements that need to be aligned and implemented.

5.2 Processes

The outline descriptions for the Processes components in this chapter require significant additional explanation so are expanded in Chapter 6.

Enterprise processes are evolving as outlined in Enterprise 2.0[9] by Professor Andrew McAfee of Harvard Business School, which defined Search, Links, Authorship, Tags, Extensions, and Signals (SLATES) as key transformational elements that are changing the way organizations do business. Well-implemented COA-compliant architectures will maximize the value of collaborations, using various SLATES elements, while managing information risks to an acceptable level.

There are five key Collaboration Lifecycle Management processes:

- Person
- Risk
- Information
- Device
- Enterprise Relationships

collectively known as PRIDE. These need to be managed by organizations that wish to achieve these transformations in a reliable and trustworthy manner.

5.2.1 Person Lifecycle Management

These are processes that manage an individual's joining, operational authentication, and access management within, and departure from, a collaboration. The processes would also include the management of individuals that are not employees or, more generally, members of the managing entity. Such processes take into account the identity, personas, capabilities, reputation, and potential impact of each of the individuals.

5.2.2 Risk Lifecycle Management

These are processes, methods, and approaches that identify, classify, and manage the information risks involved in collaborations across organizations.

5.2.3 Information Lifecycle Management

These are processes that effectively and efficiently manage the creation, reading, update, and deletion of information assets in a collaboration. These processes would include audit, monitoring, and information protection activities.

5.2.4 Device Lifecycle Management

Processes for introducing devices, identifying and maintaining device trust levels, and removing devices involved in collaborations. Removal of devices involves eradication of all information assets from the device.

[9] The State of Enterprise 2.0; refer to: blogs.zdnet.com/Hinchcliffe/?p=143.

5.2.5 Enterprise Relationship Lifecycle Management

Processes that ensure that collaborations are managed according to the state of the relationships involved and the value and/or risks they introduce. Initiating, operating, and closing down collaborations emanating from an enterprise would include a means of mapping the critical relationships between all the collaborating parties. Such processes would also have the ability to identify collaborating parties that are endangering the enterprise, and rapidly close down offending relationships. The processes would also have the ability to identify the most valuable relationships in order to ensure their appropriate development and protection. Such processes are also valuable during mergers, acquisitions, or divestitures.

5.3 Services

The outline descriptions for the Services components in this chapter require significant additional explanation so are expanded in Chapter 7.

These services may be provided by one or more of the collaborating parties, or a third party. Whichever one is used will have significant implications on how the services are provided.

5.3.1 Identity Management, Federation, and Reputation

The credentials of principals (organizations, individuals, systems, devices), and associated attributes required for identification, authentication, and authorization decisions, should be expressed in a standardized form, so they can be validated and accepted by the systems of any member of the collaboration or service providers.

5.3.2 Trust Management and Classification

The trust management issues addressed here are covered in more detail in the forthcoming Open Group Guide to Trust Management – A Control Framework for e-Business Collaboration, which is currently under development in The Open Group Security Forum and is expected to be published by October 2012.

5.3.2.1 Business Impact Levels

A common language and set of definitions for Business Impact Levels is required. We define five levels:

- Catastrophic
- Material
- Major
- Minor
- Insignificant

Note: Financial levels would be different for different individuals and enterprises.

5.3.2.2 *Information Classification*

A common taxonomy is required for defining the sensitivity of information assets aligned with risk-based assessment of business impact of an incident or threat. There are identity, legality, and temporal components of information classification, all of these being context-sensitive. We base information sensitivity on the G8 Traffic Light Protocol – four levels:

White Public: public distribution, unlimited control.

Green Normal Business: business community-wide.

Amber Sensitive: established named groups only.

Red Highly Sensitive: Specific to named recipients only.

5.3.2.3 *Impact Sensitivity Categorization*

The requirement here is to develop a common language (taxonomy) and set of trust levels defining impact sensitivity of information, based on measures of Confidentiality, Integrity, Availability, and Authenticity (CIA&A).

Note: Service or System Criticality is potentially a separate area of classification.

We define six levels:

T5 Catastrophic

T4 Material

T3 Major

T2 Minor

T1 Insignificant

T0 None

5.3.2.4 *Control Stratification*

A set of standardized information trust categories by trust level is required, using the standard CIA&A frame and adding identity. We define a six-level trust taxonomy for authenticity:

C5 ASSURED (biometric)

C4 AFFIRMED (positive physical or logical authentication)

C3 PROVEN (authenticated by trusted third entity)

C2 CONFIRMED (confirmed by strong attributes)

C1 ASSERTED (self-asserted)

C0 UNKNOWN (no authenticity assertions made – anonymous)

5.3.2.5 *Trust Management Architecture Segmentation Model*

A coherent architectural model is required to map the trust management components (business impact levels, information sensitivity levels, information sensitivity levels, and CIA&A category levels) into an effective operationally aligned structure.

5.3.3 Policy Management

The collaborating parties, and service providers, have the ability jointly or separately to evaluate, manage, and implement the policies and rules for authorizing and de-authorizing principals and collaborating parties.

5.3.4 Information Taxonomy and Semantics

This has also been described as Meta-Information Asset Management. This component addresses the requirement for collaboratively-shared data to be appropriately secured in storage, transit, and use – based on the agreed risk and performance requirements for the information contained in this data as a result of its classification. Principals accessing the data are identified, authenticated, and authorized. These requirements must be maintained through the complete document lifecycle, from creation through to destruction, by an appropriate Information Lifecycle Management process (see Section 5.2).

5.3.5 Audit

Transfers, storage, and retrieval of collaboratively shared data, and associated business controls, are auditable events. There is an associated requirement for a common notion of "event" across all collaborating parties and systems. Collaborating parties may require each other to conduct spot-audits on individual data objects and the actions associated with them, either overtly or without alerting the individuals using these objects to the increased audit activity. The collaborative group may require summary audit reports on data transfers, storage, and retrieval to be published at some regular interval within the group. The audit information needs to be of adequate quality to meet the needs of each collaborating organization, including the rigor required for forensic evidence in law. A key driving principle in audits on COA-compliant architectures is transparency between partners.

5.4 Attributes

Attributes enable you to measure whether you are achieving your objectives.

5.4.1 Usability/Manageability

Security measures are non-intrusive, readily managed by the relevant governing enterprises, and easily understood by the individual end user.

5.4.2 Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (see ISO 7498-2).

5.4.3 Integrity

The property that data has not been altered or destroyed in an unauthorized manner (see ISO 7498-2).

In considering this component, we distinguish between assuring the integrity of the information asset and its authenticity:

- Integrity is assurance that information has changed from the original only when those change(s) were duly authorized, and has not changed otherwise.
- Authenticity is assurance that the original information has not been changed.

5.4.4 Availability

The property of being accessible and usable upon demand by an authorized entity (see ISO/IEC 10181-3).

Information shared between collaborating organizations should not be rendered unavailable either by mistake or by an adversary. This implies that any "at rest" encryption keys are escrowed, and that information is held in open standard formats.

5.4.5 Efficiency/Performance

Security measures should not greatly affect the latency, bandwidth, or total cost of data retrieval, storage, or transmission. This implies that collaborating partners must possess the means to rapidly access decryption keys for all data in their possession for which they continue to have access privileges, allowing rapid data retrievals and offline malware scans.

5.4.6 Effectiveness

COA-compliant architectures should provide an effective approach to organizing and controlling secure data transport and storage among a wide range of existing and future corporate information systems.

5.4.7 Agility

COA-compliant architectures must take into account the dimensions of timeliness and flexibility, so as to enable development of business-driven Enterprise Architectures that are appropriately flexible and adaptable to facilitate changes in business operations with optimal rapidity and ease, with minimal disruption.

5.5 Technologies

The outline descriptions for the Technologies components in this chapter require significant additional explanation so are expanded in Chapter 8.

This group of components delivers the key technologies that are required to deliver the Services described in Section 5.3.

5.5.1 Endpoint Security/Assurance

Endpoint security is about raising the level of inherent trust in computing devices to a point where all the devices involved in a transaction meet the criteria of trust for that transaction (JFC#1 and JFC#7).

The trust level needs to vary in accordance with a range of factors, including risk, transactional value, location, and time.

For two endpoints to transact with each other, there needs to be a level of mutual trust between them (JFC#7), commensurate with the transaction that is to take place (JFC#6).

5.5.2 Secure Communications

Most enterprises use computers that connect to the Internet, employing wireless communications internally, with the majority of their users connecting to services outside the enterprise perimeter, and partners and collaborators regularly connecting to the enterprise's internal network with their own computing devices. The brand/image of all business organizations relies on secure information flows.

In the de-perimeterized world, the use of inherently secure communications is essential (JFC#4) to provide protection from the insecure data transport environment. Inherently secure communications products, services, and protocols should act as fundamental building blocks for secure distributed systems, adaptable to the needs of applications while adhering to requirements for security, compliance, and performance. Most networks are fundamentally insecure; it does not matter what infrastructure you have, if the principals on the network are trusted without good cause, the network is inherently insecure. Networks can be designed to be inherently secure.

Many organizations continue to deal with the issue by simply extending their "untrustworthy" network by the misuse of IPSec, and building VPN tunnels. The key here is in the "P", for if the central network is not private the virtual network cannot be private either; to assume otherwise is to put information at risk.

5.5.3 Secure Protocols

5.5.3.1 Wireless

Organizations should regard wireless security on the air-interface as a stop-gap measure until inherently secure protocols are widely available. Also, the use of flexible interoperable 802.1x integration to corporate authentication mechanisms should be the out-of-the-box default for all Wi-Fi infrastructure. Additionally, organizations should adopt an "any-IP address, anytime, anywhere" (referred to as a "Martini model"[10]) approach to remote and wireless connectivity, with full roaming mobility solutions that allow seamless transition between connection providers.

[10] Multiple Access Real-Time IP Network Implementation; so named after a popular European advertisement for the drink "Martini" in which the memorable slogan "any place, anytime, anywhere" was adopted into popular language.

5.5.3.2 *Mobile Management*

From a security stance, all public networks, wired or wireless, should be regarded as hostile. However, the ability to make a transparent wireless connection remains elusive due to the lack of standards in this area, especially around Wi-Fi. The use of mobile devices and applications designed to the Jericho Forum blueprint[11] implies that mobile working should be a seamless user experience. A de-perimeterized environment, where the end-device is assumed to be in a hostile environment (whether on an internal or public IP address) and security is designed appropriately, is ideal for working in the wireless world.

5.5.3.3 *Voice over IP (VoIP)*

With many large organizations seeking the cheapest options for internal long distance telephone calls, using the Internet as a transport is a very attractive option. With Internet connections being used, interception, recording/replay, etc. can happen anywhere on the network. VoIP is often used under the flawed assumption that sharing the data infrastructure is acceptable because the internal network is secure. The lack of security built in to VoIP products and protocols means that companies are unable to deploy VoIP securely in a de-perimeterized environment, where return on investment is significantly more complex than just the replacement of an existing internal telephone exchange.

5.5.3.4 *Internet Filtering & Reporting*

Accessing web sites carries risk – to users who are misled into inadvertently straying to inappropriate sites, and arising from data that is returned being free from malicious content. As end computing devices move into a de-perimeterized world, then it is essential that all data feeds have adequate levels of integrity, irrespective of their physical location/connection. There are two separate problems to be solved. Firstly, an architecture that allows operation in a de-perimeterized environment, and secondly the provision of a distributed filtering service.

5.5.3.5 *Encryption and Encapsulation*

Making a secure, trusted connection over the Internet remains a key challenge. Encapsulating the message protocol in a VPN tunnel, which is often an IPSec tunnel, does not avoid vulnerabilities to worms, viruses, or hackers, in the same as any other computer on the network to which the IPSec tunnel terminates.

5.5.4 Secure Data

Secure data is a term that is often linked with concepts involving Digital Rights Management (DRM), which in turn is commonly associated with protecting digital arts/music/entertainment media. We are more concerned here with the generic requirement for the digital management of rights to access information/data, which may better be described as Enterprise Information Protection & Control (EIPC).

[11] The term "blueprint" was adopted by the Jericho Forum to capture how the Jericho Forum Commandments define the security principles for assuring effective security in de-perimeterized environments, and their use to validate how this O-SCOA Framework supports architecting secure systems for de-perimeterized environments. See also Chapter 3.

EIPC addresses:

- Copy, Store, Move, and Use (CSMU) of information/data
- Integrity of the information/data in question

In a de-perimeterized world it is generally easier to provide granular levels of data protection. The closer the protection mechanism is to the data, the more effective the protection can be. JFC#9 states that: “Access to data should be controlled by security attributes of the data itself”, while JFC#11 states that: “By default, data must be appropriately secured when stored, in transit, and in use”.

6 O-SCOA Framework – Processes

This chapter provides detailed descriptions for the "PRIDE" process components in the O-SCOA Framework:

- Person Lifecycle Management
- Risk Lifecycle Management
- Information Lifecycle Management
- Device Lifecycle Management
- Enterprise Relationship Lifecycle Management

6.1 Person Lifecycle Management

6.1.1 Problem Statement

Person lifecycle management covers the processes that manage an individual through the lifecycle from when they join, are operationally authenticated and assigned access and authorization permissions, are then maintained (through perhaps several changes in roles through their lifecycle), and depart. This is historically the traditional long-term view of person lifecycle management – through the point when they join to the point when they leave.

In today's business collaboration world, where collaborative activities – with business partners, suppliers, customers, and staff and contract individuals – are increasingly required, these operations must be handled speedily and comprehensively.

Further, in the new world of collaborative activities in cloud computing, where collaborative activities may take very short times (of the order of minutes rather than months or years) business demands that collaborations must be speedily set up, and equally speedily closed.

The processes required include the management of individuals, including non-members of the managing entity. Such processes need to take into account the identity, personas, capabilities, reputation, and potential impact of each of the individuals.

6.1.2 Why Should I Care?

Organizations need to be able to demonstrate to partnering enterprises that their person lifecycle management processes are capable of efficient responses to changes in an individual's operational authorities and responsibilities.

Slow or incomplete handling of changes that respond to a person's operational authorities and responsibilities leave an enterprise open to serious risk of unauthorized activities – not just by the person alone but also through identity theft – rendering the enterprise and its partnering

enterprise(s) vulnerable to contractual failure as a minimum, and potentially to serious damage arising from unauthorized operations ranging from revelation of confidential information through to actioning of transactions which could threaten the enterprise's – and its partnering enterprises' – ability to continue in business.

6.1.3 Recommendations/Solutions

Primary source references include ITIL and ISO/IEC 27002 (Section 8).

Source of Master Data

Within an organization there needs to be master source of user information, associated with an authorized owner, to act as an authoritative source for managing sharing of information and applications, including for partnering between systems wishing to federate.

Authentication of Individuals

The proliferation of accounts, log-in names, and passwords (or stronger schemes) that a person has to deal with is expanding, at the expense of good security. A stop-gap solution is the generation of a private authentication solution – clubs whereby a group of interested parties can share and federate a single set of credentials. Such an example is the Trans-global Secure Collaboration Program (TSCP) used by the military and aerospace companies. Characteristics of any solution, however, include:

- Authentication of individuals, public schemes, clubs, strong authentication, personas
- Integration with any applicable national identity scheme
- Need to manage employment terms, conditions, and continuing entitlements, including pensions, share schemes, etc.
- Vetting
- Unused digital identities – do not re-use
- Lockout – with regard to re-authorizations
- Efficient on-boarding/off-boarding of individual or group identities
- Efficient updating of attributes
- Scalability, including compatibility with external business partners
- How to federate with partners – sets of people (not all) in the partner organization
- Role and use of identity brokers
- Nature of relationships – this will indicate what type(s) of identity credentials are required, and selecting key stakeholders who have "skin in the game" (self-interest) to motivate assembling and maintaining accurate credentials

6.1.4 Background and Rationale

Included in Section 6.1.3 above.

6.1.5 Challenges to the Industry

Challenges include the need for strong personal ID: the concept of being able to manage a personal ID that can be re-used wherever you go is very attractive. A single strong ID can be set once, and then re-used anywhere using an open standard set of APIs, preferably with the ability to set a series of "persona" facets of you, with limited information that you choose to expose – e.g., you may choose/need to give different personas to your place of work *versus* the tennis club.

Such current schemes lack the ability to integrate the level of strong authentication that many organizations require.

6.1.6 The Way Forward

Develop solutions to managing translation of a personal human identity into any desired number of digital identities (personas) which represent the electronic identity of that human individual in each of their desired personas in ways which:

- Provide the required strength of authentication
- Expose only the necessary amount of personal information so as to protect the personal privacy of the individual – this is particularly relevant where privacy regulations apply

6.2 Risk Lifecycle Management

6.2.1 Problem Statement

The O-SCOA Framework enables enterprises that build COA-compliant architectures to operate in a secure and reliable manner in an environment of increasing information threat, and where it is the growing norm to interact without boundaries, irrespective of the location of the data or the number of collaborating parties.

COAs involve a significant move of security emphasis from infrastructure to applications. This affects information risk management in that it makes information risks:

- More numerous, because the entities at risk are now application rather than infrastructure elements
- More severe, because there is less defense-in-depth and therefore a compromise is more likely to have an immediate business impact

6.2.2 Why Should I Care?

Security professionals who propose COA must be able to communicate with management about the risks involved.

Organizations need to manage and demonstrate compliance in a more complex risk environment.

6.2.3 Recommendations/Solutions

- Organizations need to manage risk in a way that is systematic and closely relates to the organization's business environment and security architecture.
- Organizations need to express and manage information risks in the same way as any other risk. In particular, they should use methods that are, or can be made to be, quantitative.
- Extensive tool support will be required by all but the smallest organizations to allow information risks to be managed properly.

6.2.4 Background and Rationale

Understanding an organization's security requirements requires an understanding of three inter-related areas:

- The business context for security – the rules and policies in force, the assets handled and their values, and the stakeholders and users. Expected costs, service levels, and benefits are also best understood at this level.
- The security architecture – the structures, links, and security controls in place within the organization. These determine the accesses (from users to assets) and hence the risks.
- The risks – undesired events with their impacts and probabilities of gain as well as loss.

Figure 3 shows how these areas influence each other.

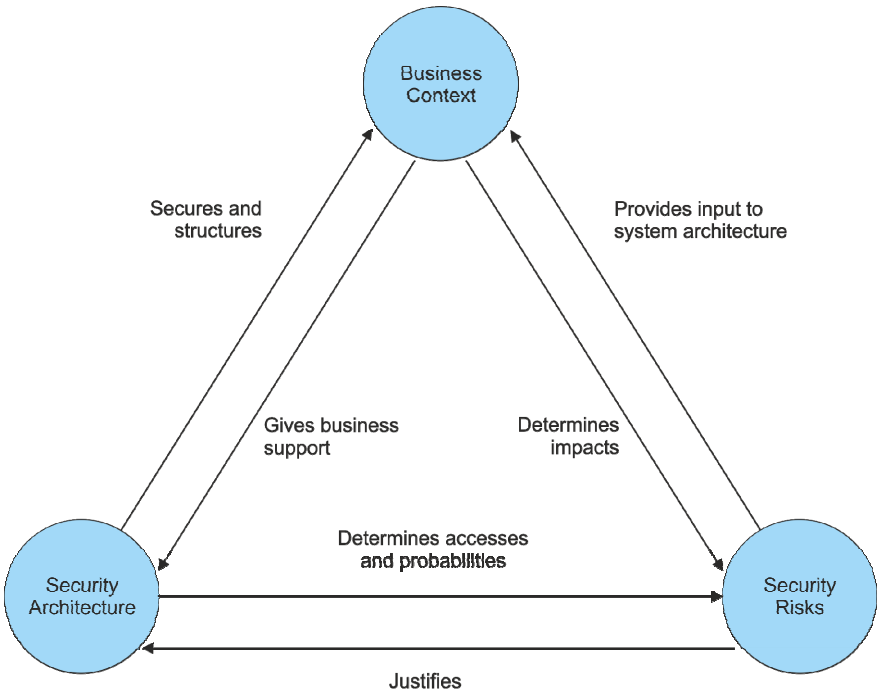


Figure 3: Business and Security/Risk Inter-Relationships

A perimeterized security architecture leads to a complex set of structures, but the security risks are minimized in number. A de-perimeterized security architecture, on the other hand, leads to a flatter, simpler set of structures; assets are potentially exposed to more users, so the risks are more numerous and have more immediate business impact.

Having more risks means that the risks must be more carefully structured to ensure they are manageable.

6.2.5 Challenges to the Industry

Standards are required in this area to permit:

- Development and application of effective tools
- Evaluation and acceptance of risk, both within and between organizations

Standards are required for describing the following:

- Security architectures:
  - — We already have ISO/IEC 27001/2, but these standards do not facilitate automated risk management.
- Risk, in two key aspects:
  - — To establish a standard vocabulary (risk taxonomy) for describing the essential common terms in use in the industry. Even critical terms like threat, vulnerability, and risk itself, are used very differently across the industry, making it difficult to compare different risk assessment approaches for evaluating exposure to risk of loss.
  - — To adopt effective risk assessment methodologies which deliver objective, meaningful, consistent results.

6.2.6 The Way Forward

The Open Group has published a Risk Taxonomy Technical Standard, based on the Factor Analysis of Information Risk (FAIR) method, and also a FAIR – ISO/IEC 27005 Cookbook which explains how the Risk Taxonomy Technical Standard can be used alongside ISO/IEC 27005 (and by example also alongside other well-established industry risk assessment methodologies; e.g., CobiT, OCTET) to improve application of FAIR's more rigorous and quantitative approach to raise the quality of the risk assessment results.

Interesting other approaches in this area include the UK Government's Risk Assessment Accreditation Document Set.

6.3 Information Lifecycle Management

Many information and application assets within an organization have an associated value relative to the business impact of an incident or threat that affects the confidentiality, availability, authenticity, or availability of that nformation or application. The threat model for information and applications stored locally, within network perimeters, is different from that of those shared

in collaborative, de-perimeterized environments. The former allows an organization to control access to assets within a secured perimeter for a specified set of users, while the latter allows assets ”into the wild” where there is no perimeter in which to enforce access control and no finite set of users to control access for.

It is therefore essential that information and application assets are correctly and accurately classified to identify the organizations and individuals that should have access to them as well as the data handling requirements, such as secure storage and safe disposal, that are relevant to the information content of those assets.

It is also crucial that the confidentiality, integrity, authenticity, and availability of the assets are categorized and made clear in order to inform consumers of those assets how to secure the information/application in storage, in use, and in transit, outside of the secure perimeter.

6.3.1 Problem Statement

Shared information/applications have an associated value to their owner organization. Where they are shared in collaborative, de-perimeterized environments, the information content should be correctly labeled with information protection requirements according to an information classification scheme and impact sensitivity categorization – see the sections defining these items.

Information can often have a temporal aspect. For example, financial results can go from top secret to public domain overnight. Information classification and impact sensitivity categorization should be periodically reviewed and updated to reflect the current sensitivity of the information. Access controls should be modified in light of any changes to information classification. Automated updates significantly improve the efficiency of this operation.

The information classification, impact sensitivity categorization, access control requirement definition/modification processes, together with policy for the creation, storage, transfer, update, and deletion of information, all require an entire Information Lifecycle Management process which should involve a continual cycle of analysis.

6.3.2 Why Should I Care?

The ways in which computer users work are continually changing. Web 2.0 is bringing a cultural change and business drivers are forcing organizations to collaborate. At the same time, changes to data protection regulations (e.g., the UK Data Protection Act) are putting personal responsibility for data losses and exposures with the data controller within a business organization. It is more important than ever to maintain strict control over information, while at the same time allowing information to move into an environment over which organizations currently have minimal control. Organizations must begin to classify and categorize information that is to be shared in de-perimeterized environments in this way to maintain control over it and comply with legislative control, maintain control over the intellectual property of the information, and maintain control of their sensitive business information.

6.3.3 Recommendations/Solutions

Figure 4 details the information lifecycle management process model requirements for use in a COA, defining the actions that can be taken on information at any one time, the options available

while taking those actions, and the path an individual should follow to ensure that the information remains secure throughout its lifetime from creation to deletion.

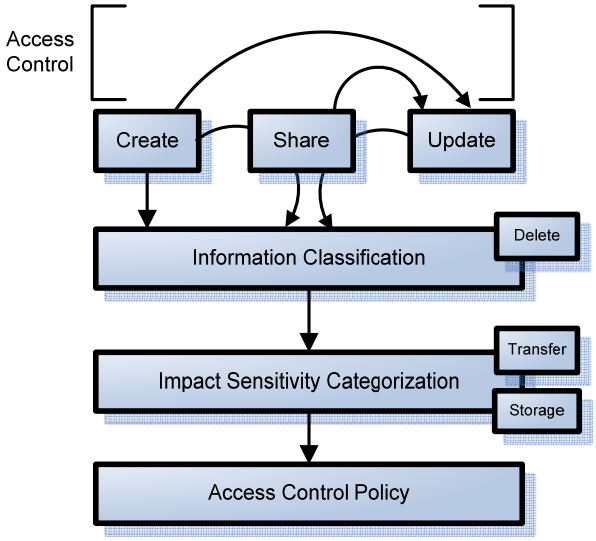


Figure 4: Information Lifecycle Management Process Model Requirements for COA

Information Creation

A lot of information is created as part of the everyday business process within organizations. Upon creation, the creator must consider the content of the information they are creating and make a decision as to whether or not it requires access control. If not, then its lifecycle can continue without applying the information lifecycle management process. If it is, the information classification, impact sensitivity categorization, and access control policy definition stages of the process must be performed.

Information Storage

Information must be stored appropriately to reflect the information protection requirements defined by the information classification and impact sensitivity categorization stages. Encryption is not mandated but is recommended for added protection from unauthorized exposure. If the information is highly classified or has high impact sensitivity, then confidentiality assurance must be considered. The physical location of the storage devices is also a significant consideration when legal compliance to data location or other similar business constraints apply.

Information Sharing

Information shared in collaborative, de-perimeterized environments is subject to a different threat model to information stored locally. In light of this, the information classification, impact sensitivity categorization, and access control policy definition stages of the process must be performed before sharing the information, even if this has already been performed on creation of the information.

Data Transfer

The information transfer protocol between collaborating parties should take account of the information protection requirements as defined by the information classification and impact sensitivity categorization stages. Encryption is not mandated, but if the information is highly classified or has high impact sensitivity, then confidentiality assurance must be considered. Endpoint compliance and the encryption of information in transit are example considerations.

Information Update

If the information is updated, the updater must consider the content of the information they are adding/updating and make a decision, using the information classification scheme and impact sensitivity categorization processes, as to whether or not the changes present additional and/or modified information protection requirements. Changes in access control policy and data transfer security are examples of such protection requirements that may change due to modified information content.

Information Deletion

Deletion of the information should reflect its classification and impact sensitivity labels. If the information is labeled as having to be securely destroyed, then just placing it in the system "Trash" is not acceptable.

Information Classification[12]

Information that is shared in de-perimeterized environments must be accurately labeled with information protection requirements according to the sensitivity of the content within the information resource in terms of a risk-based assessment of the business impact of an incident or threat.

The information creator or individual intending to share the information in a collaborative, de-perimeterized environment must consider the threat to the business if the information were accessed and/or modified by individuals with an identity outside of a particular domain. This could be the internal organization, external business community, or named specific individuals, details of which must be specified in the information classification scheme for the organization. Section 7.6 defines a positional scheme based on the G8 Traffic Light Protocol.

Information handling requirements, legality, and temporal aspects must also be considered at the information classification phase. Secure destroying of information, clear ownership rights, changes in classification after a particular date and time, and corporate governance constraints are examples of the detail that should be evident from the labeling process.

If the information requires classification according to the information classification scheme, the information must be correctly labeled.

[12] See also Section 7.6.

Impact Sensitivity Categorization

Information must be labeled with an impact sensitivity level based on the measures of CIA&A required to adequately protect the information *in situ*, use, and transit. Section 7.7 proposes a six-level impact sensitivity scale that represents the impact magnitude should the protection measures not be effectively deployed.

The creator or individual that is intending to share the information in a collaborative, de-perimeterized environment must conduct an impact sensitivity analysis to determine the controls required to maintain information assurance in a de-perimeterized environment in relation to the CIA&A requirements of the information.

Access Control

Authentication and authorization should be applied to principals requesting access to information. Section 7.8 details a set of levels for which trust in an identity can be assured.

Appropriate access control technology should then be used to enforce the authorization response. The de-perimeterization issue makes many of the current technologies that rely on perimeter security to enforce controls inappropriate for use in COA. Section 5.5.4 details the digital management of rights to access information and includes a position on how to control access to information in collaborative, de-perimeterized environments.

Access controls should be reflective of and responsive to the information security requirements defined in the information classification and impact sensitivity categorization stages.

6.3.4 Background and Rationale

Not all information carries the same value and associated information protection requirements. Consequently, there must a way of classifying information so that the different and most important information protection requirements can be identified for any given piece of information by anybody accessing or sharing it. The classification scheme should be concise and clear so that it can be applied quickly and accurately by any person or process creating or sharing information that is of value to an organization.

Access to some information may be limited to specific identities. These identities could be public, domain-specific, organization-wide, departmental, or even specific individual details. Other information may be limited based on environmental conditions such as worldwide location while requesting access or endpoint compliance of the machine requesting access.

Data handling is often an important issue. Simply deleting information does not destroy it, so controls such as electronic shredding could be mandated on the most sensitive information. Likewise, secure and tamper-evident data transfer and storage protocols may also be enforced for particularly sensitive information.

Information classification schemes and impact sensitivity categories should reflect the requirement for these controls in their choice of labels and allow an organization, data controllers in particular, to identify and make clear the information protection requirements of their information through the assignment of such labels to information, so that internal and external users know how it must be handled and controlled throughout its lifecycle.

6.3.5 Challenges to the Industry

Shared Taxonomy

Establishing an agreed standard taxonomy for the entire information lifecycle management process and all of its components, including information classification and impact sensitivity categorization, is essential to enable the taxonomy used by one organization to be correctly understood, interpreted, and implemented by all other collaborating organizations, so as to correctly protect the shared information according to its organization-specific (owner's) requirements.

Enforcement

The information lifecycle management process must be enforced for all information shared in de-perimeterized environments to ensure information security is correctly managed outside of the owning organization's corporate perimeter. The key driving principle in COA audit is transparency between partners. Creating an audit trail of who created, accessed, updated, and deleted information, and maintaining an accurate and complete trail of changes to information classification and impact sensitivity categorization labels, is essential to meeting the rigor required for forensic evidence in law.

6.3.6 The Way Forward

Organizations need to run pilot operations trialing information classification and impact sensitivity categorization schemes as part of their internal operations, and then moving the successful information lifecycle management process model into a collaborative domain. De-perimeterization is happening; data protection laws are becoming more powerful and will soon carry civil penalties; and business drivers are forcing organizations to collaborate. It is essential that the information lifecycle management process begins to become part of everyday business activity.

6.4 Device Lifecycle Management

In a collaborative, de-perimeterized environment, if a device needs be trusted then the management of devices becomes critical when collaborating with another device, system, or service.[13]

The entire lifecycle of a device needs to be managed, from the point of device creation or on-boarding[14] process to register external devices as permissible to connect to other devices, systems, or services through managing the device and ensuring the software/OS environment on the device is in an updated state, to eventually repudiating the device and potentially deleting any sensitive data or configuration information from it.

[13] Refer to JFC#6 and JFC#7 on the need for trust.
[14] "On-boarding" is defined as the process of enrolling a device or person such that they have the capability to be recognized by the systems with which they need to interact.

Whether the device is a client or server, the same issues exist, and while the lifecycle will be similar it will probably be managed under a more formalized process for servers.

6.4.1 Problem Statement

Device lifecycle management is often poorly practiced, with corporate businesses who run a locked-down end-user computing configuration with heavily customized software management systems getting close to the required level of management – but often only inside the corporate boundary, and at the cost of end-user productivity – while full management when roaming the Internet is only available in a closed ecosystem with correctly configured/locked-down "closed" devices.

The current status is increasingly at odds with the proliferation of types of devices (especially PDAs), business demands for flexibility, and the conflict with operating a locked-down model *versus* consumerization of devices.

6.4.2 Why Should I Care?

Business is demanding more connectivity outside the enterprise. Commoditization of technology is driving towards any-to-any connectivity on every electronic device, with those devices having ever lower cost with more "intelligent" functionality built-in. Business "relationships" of every type, from subsidiaries to relationships with other business that are also competitors in other areas, all require connectivity. Pervasive, fast, reliable, cheap Internet connectivity is becoming available everywhere.

Responding to all these business demands requires effective lifecycle management for networked devices of every kind.

6.4.3 Recommendations/Solutions

Key Issues for a COA

As already mentioned, appreciating the Jericho Forum Commandments (design principles) on the need for trust is critical here:

- JFC#6: All people, processes, and technology must have declared and transparent levels of trust for any transaction to take place.

  Trust in this context is establishing understanding between contracting parties to conduct a transaction and the obligations this assigns on each party involved.

  Trust models must encompass people/organizations and devices/infrastructure.

  Trust level may vary by location, transaction type, user role, and transactional risk.

- JFC#7: Mutual trust assurance levels must be determinable.

  Devices and users must be capable of appropriate levels of (mutual) authentication for accessing systems and data.

  Authentication and authorization frameworks must support the trust model.

Need for Consistent Intranet/Internet Management

The management of devices must function identically irrespective of whether a device is connected to the intranet or Internet, with the operation of such management secure. All protocols involved in the management of the device must be inherently secure.[15]

Provisioning, Fixes, Suitable Software, and Patches

The provisioning of new software, the de-provisioning and/or removal of old or unsuitable software, together with patch management, and configuration of software must cover all software (OS, BIOS, and application software) on the device. The provisioning mechanism must be secure and all protocols involved in the provisioning of the software must be inherently secure.

On-Boarding – Registration

Where a level of trust is required for a device to collaborate with other devices, systems, or services, then there must be an on-boarding or registration process. This registration process may be manual (as in the case of building a new corporate PC, or a server) but ideally should be *ad hoc* and not make assumptions about where the device is trying to register from.

The capability for *ad hoc* on-boarding is especially important in the case of alien (unknown/non-on-boarded) devices that are required to collaborate, where the on-boarding process involves network-based access. Here, mutual trust assurance levels must be determinable for the two systems (registration service and new device) involved in the transaction.

Identity of Device

The device needs to be capable of positively and uniquely identifying itself to other systems in a form that cannot be subverted (thus, using a MAC address is not a suitable level of authentication).

This may involve using an existing suitable key on the device, loading a key, or using software, as part of the registration process, or could be achieved by federating the device's identity from the organization with which you are collaborating.

Suitability of Device to Interact

Information about the end-device state and capability, combined with the (automated) risk assessment, should all affect an assessment of how suitable a device is to interact.

Factors that may dictate how a device can interact include:

- Amount of memory
- Presence of a particular installed application
- How the connection is being made

[15] See Section 8.2.

- The network speed and/or cost of connection

Depending on the interaction, it may be possible to vary the method of interaction to better suit the circumstances in which the two collaborating devices find themselves, potentially with a negotiating process to find a mutually agreeable method of interaction.

Off-Boarding Devices

Devices that are on-boarded must have a complementary process to off-board them. Preferably this should be part of a continual process to ensure and re-validate the need for device-level access, especially where devices are not under your direct control.

Recovery of Data and Key Repudiation

Where devices have been off-boarded or where the access changes, then any local data on that device may need to be recovered or destroyed. Keys may need to be repudiated, and potentially any software that was loaded onto that device as part of the on-boarding and/or management process should be removed and de-licensed.

The Need to Federate Devices and/or Applications and/or Services

Just as devices under your control are managed in an authorization database or directory, so devices of trusted parties should be able to connect via federated access to their authorization database, in the same way that user access can be federated.

Endpoint Security Configuration Management

Where the transaction taking place requires a level of trust in the integrity of the operating system and software, then there must be a secure method of establishing the acceptability of the configuration state of that device, and a decision made about whether to allow that transaction/collaboration[16] or use an alternative method of collaborating.

Device Remediation

The ability to lock-out a device from the transaction/collaboration process until it is remediated is essential. Ideally, a device that requires remediation will be locked out of all transactions (via (say) a change of rules to its personal firewall) until it has been remediated. Such lock-out and remediation must function irrespective of whether the device is intranet or Internet connected and (dependent on the transaction) could potentially happen during the transaction.

6.4.4 Background and Rationale

This is covered in Section 6.4.3.

[16] Refer to Section 8.1.

6.4.5 Challenges to the Industry

Gateway Connections

Endpoint security checking performed at a network or perimeter entry point is generally flawed in a de-perimeterized environment.

In a de-perimeterized environment the communication will be (secure) protocol-based rather than the action of a device or user authenticating to a network device. Thus, the network connection process (and thus the ability to intercept and check the device) will have already taken place, in the worst case on a public Wi-Fi or other network that is outside of your control.

Vendor-Neutrality

When an endpoint device is already part of a management ecosystem (for example, a laptop from a consulting company visiting your site one day a week), then local systems should be able to leverage this to allow access, and should even allow federated device access in the event that an established business relationship exists. End-devices, users, and companies will not tolerate an increasing set of unique endpoint solutions being loaded and probably interfering as part of a local on-boarding process.

Vendors should collaborate to develop such secure standards.

Connecting via a Tunneled Connection

The current method of using a generic (open to all protocols and services) IPSec (or SSL) tunnel to allow alien devices into your closed network is severely flawed, and highly undesirable. Such solutions have the potential to open up both endpoint and network to problems that may exist at either end, and do not meet the need for inherently secure communications[17] to reduce the attack surface and thus help provide both least privilege and defense-in-depth.

6.4.6 The Way Forward

Current device management solutions need to be enhanced to operate in a collaborative/de-perimeterized environment. Such solutions not only need to be able to support a multitude of devices, but also need the additional capability to securely communicate their status to other partners in any collaboration.

Vendors should also be working with the producers of consumer devices to identify methods by which these devices can be on-boarded to allow their operation in a collaborative environment.

Relevant applications will need to be enhanced to support the validation of devices when making a connection request to their systems.

[17] Refer to Section 8.2.

6.5 Enterprise Relationship Lifecycle Management

6.5.1 Problem Statement

We readily recognize a number of the important lifecycle management processes as involving information management. These include information/document lifecycle management, device lifecycle management, and people lifecycle management. Risk also has a lifecycle that needs managing, particularly in the area of vulnerability lifecycle management.

However, in this world of rapidly changing collaborations, not many have recognized the need for managing the lifecycle of the enterprises with which we collaborate. The length of time a collaboration will be required to run is rapidly falling, as are the expectations of the time (agility) needed to set up new collaborations (and close them down).

There is a growing need to be able to effectively manage the lifecycle of the enterprises with which we do business. At present, there is not one clear model for enterprise relationship lifecycle management that integrates all the various functions involved in managing the relationships in such a lifecycle.

6.5.2 Why Should I Care?

Today, collaborations are set up by multiple functions across most enterprises. The implications of this largely disintegrated approach are that it is slow, resource heavy, costly, and does not readily spot or address systemic or enterprise risks – this at a time when our businesses are expecting agility, speed, and low cost in setting up new collaborations. How long does it take your organization to "on-board" or "off-board" an enterprise, ensuring that the appropriate contracts are in place, or data is repatriated, and dealing with all the other regulatory implications of such activities? There are some organizations today that have partner on-boarding and off-boarding processes that take more time than the average lifetimes of their partnerships. It is also key that we know those organizations that have access to our sensitive data.

6.5.3 Recommendations/Solutions

Organizations are encouraged to name an owner of the enterprise or partner lifecycle management process, and, working across all the related functions, look to reduce the timeline in the processes involved in enterprise relationship lifecycle management. They need to take the times of the key lifecycle management processes from being measured in months, to being measured in minutes. This is not a technical measure; it is an organizational one, which must have as one of its key goals the protection of information assets.

6.5.4 Background and Rationale

Managing the energy and resources involved in setting up new collaborations or partnerships will be a key new capability for future organizations. Importantly, managing the information implications of such a process will be key part of the PRIDE processes (see Figure 2).

6.5.5 Challenges to the Industry

As described in Section 6.5.4 above.

6.5.6 The Way Forward

Given that a growing proportion of the information assets of our organizations are being made accessible to and being handled by our business partners, enterprise relationship lifecycle management is a key control mechanism we should develop as part of our protection measures for those information assets.

How many other enterprises handle your most sensitive information assets today? If you don't know, is it not time to find out and work out how best to assure their security?

7 O-SCOA Framework – Services

This chapter provides detailed descriptions for the Services components in the O-SCOA Framework:

- Identity Management: Federated Identity
- Trust Management
  - — Overview
  - — Business Impact Level
  - — Information Classification
  - — Impact Sensitivity Categorization
  - — Control Stratification
- Policy Management
- Information Taxonomy and Semantics
- Audit

7.1 Identity, Entitlement, and Access (IdEA) Management

7.1.1 Background

Identity, Entitlement, and Access (IdEA) is core to secure operations in all spheres of life, and in computing operations, "digital identity" is particularly challenging. When the Jericho Forum developed its SCOA requirements, it deliberately positioned "identity" as an item to be addressed separately, precisely because it is a complex subject which has to be addressed separately. The only concession in the SCOA requirements was to evaluate federated identity. Accordingly, federation of identities is included in this Guide – see Section 7.2.

Many identity management solutions are available in today's marketplace. None to date, however, have demonstrated that they provide a sufficient solution to the requirements for globally acceptable levels of trusted identities in cyberspace – by which we mean identities which provide acceptably high levels of authentication sufficient to use for computer operations involving sharing of medium-to-high value information or similarly medium-to-high value transactions. This remains a major barrier to business confidence in taking medium and high-value confidential operations and transactions into de-perimeterized environments, including cloud computing.

Consequently, identity management requirements in the digital world continue to be a major focus of work programs in many information security groups around the world, including

increased government initiatives to develop e-Citizen capabilities and to safeguard national critical infrastructures.

7.1.2 The Jericho Forum Identity Commandments

In July 2010 the Jericho Forum started its own project on IdEA management. It adopted the same approach as it has done in the past – to first analyze and define the fundamental principles for the issue in question – in this case "identity in the physical world and its translation into the cyberspace world". The result was the Jericho Forum Identity Commandments, which were published in May 2011.

They specify 14 design principles which are essential requirements that any globally interoperable trusted identity solution in cyberspace must satisfy. These Identity Commandments are aimed at IT architects and designers of both Identity Management and Access Management systems.

7.1.3 Identity Key Concepts

When the Identity Commandments were published, the Jericho Forum recognized that trusted identities in our digital world are important to everyone who wants to work online – e-business managers, e-commerce operations, and individual e-consumers. In order to safeguard their ability to control and manage their own identity and privacy, every online user should support creating an identity ecosystem that satisfies these Identity Commandments. We needed to develop supporting collateral to explain in non-technical terms why.

Accordingly, the identity key concepts were developed from the Identity Commandments. These are now published in two forms:

- A set of five "identity key concepts" video tutorials:[18]
  - — Video #1: Identity First Principles
  - — Video #2: Operating with Personas
  - — Video #3: Trust and Privacy
  - — Video #4: The Bigger Picture, Entities and Entitlements
  - — Video #5: Building a Global Ecosystem
- An associated Guide to Identity Key Concepts[19]

7.2 Federation of Identities

7.2.1 Problem Statement

The majority of user authentication schemes today still use user ID and password. The burden to users of managing large numbers of user IDs and passwords has led to proposals for federated

[18] The Open Group Identity Key Concepts video tutorials are available at: https://collaboration.opengroup.org/jericho.
[19] The Open Group Guide to Identity Key Concepts is available at: https://collaboration.opengroup.org/jericho.

identity systems, where a single set of credentials can be used to authenticate with several organizations which have agreed to work together as a federation.

An additional problem is the ease with which a person's user ID/password credentials can be captured when the underlying rationale for using them is that they are intended to be kept private, but this problem is not considered further in this document.

7.2.2 Why Should I Care?

To fully develop the potential of boundaryless electronic business, users need simpler and stronger ways to authenticate to organizations and between organizations (JFC#8). These must also meet the business requirements for different and changing degrees of trust between organizations, and allow for equal partnerships.

Privacy concerns must be visibly met, with the data under control of the data owner, normally the end user, and disclosure should be limited to the least amount necessary.

However, several federated identity approaches require one organization – the identity provider – to be in a privileged position in control of the issuance and/or validation of credentials. This approach limits the application of federated identity, as naturally most businesses do not wish to pass control of a major asset – the identity of their customers, staff, contractors, and other business partners – to another organization. It may also imply an asymmetric relationship, where users show their credentials to the identity provider, without necessarily being able to easily mutually verify its credentials. It is frequently difficult to mix different credential verification services within an organization; the implementation assumes that the same technology will be used throughout.

Additionally, several federated identity approaches combine user credentials (proof of identity) with user attributes (such as personal data). This leads to potential privacy issues, which may also cause legal problems, especially if the credentials and attributes are passed across national borders. Complex proposals have been made to allow the user to control which attributes may be passed between organizations.

Further, most approaches have been limited to authenticating human users. As is now commonly accepted, devices, applications, and resources (including even locations, such as meeting and other accommodation rooms) also need to be able to authenticate themselves.

7.2.3 Recommendations/Solutions

Many federated identity technologies do not directly match the key business needs and trust relationships required in a de-perimeterized environment.

To support business-to-business service provision, a person granted one or more credentials in one authentication/authorization domain should be able to use these credentials with another organization. This implies that the second organization must be able to check credentials with the first organization, and also that each organization must be able to supply authorization information, which is then combined to define the final authorization permissions (JFC#8).

There should be no requirement for a privileged identity provider. Instead, peer-to-peer authentication should be supported. Business models using a separate identity provider may also be supported.

Systems should support the use of several different credentials and authentication technologies referring to the same individual. Different credentials may be used in different contexts (JFC#3) – for example, to distinguish different roles taken by the same individual – and may also affect the trust level to be used (JFC#6). There should be no requirement for homogenous credential technology; any system should be flexible and extensible.

Clearly distinguishing between credentials and attributes will clarify use of data, help meet privacy legislation, and also ease the introduction of new authentication techniques to replace passwords. In general, shared secret credentials should not be transferred to other organizations, due to the increased risk of compromise. Instead, identity assertions or seamless pass-through authentication should be used. This applies whether the identity information is being transferred between organizations, or between component layers of an application (JFC#8).

In most cases, data attributes should be held by the end user, rather than centrally stored by a third party. For browser-based applications, a standardized data form schema would make it simple to pass the same data to different organizations completely under user control. Individuals should be able to choose which sets of attributes are used for a given transaction (work/home address, credit card selection) (JFC#8).

7.2.4 Background and Rationale

The federated identity approach has been proposed for business-to-business service provision for employees, where one organization manages the user credentials and authorization to systems run by the other organization.

7.2.5 Challenges to the Industry

In no particular order of priority:

- Create common schemas for the majority of transaction data attributes requested, including name, address, and payment details, to remove the need for centralized attribute storage.
- Mutual authentication should be used by default.
- Peer-to-peer authentication should be permitted, without the need for a privileged identity provider.
- The currently assumed role of an individual should be made explicit to systems.
- Subject attributes should not be used as credentials.
- Credentials and authorization information should be able to be transferred between organizations using open protocols and standards, and be simple to manage the equivalence relationships.
- It should be possible to support a multiplicity of credentials and technologies for an individual.

7.2.6 The Way Forward

Development of heterogeneous federated peer-to-peer identity systems will allow simpler and stronger authentication schemes that will meet the corporate requirements of de-perimeterized environments.

7.3 Reputation

7.3.1 Problem Statement

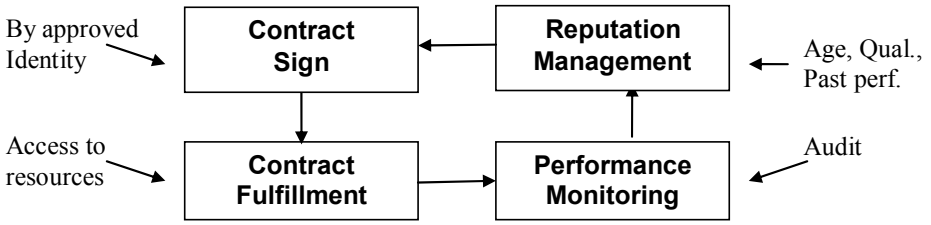
Deciding whether to approve a contract for business collaboration with another organization (or several other parties) involves risk management by each party that sensitive data shared between the collaborating organizations will be handled with appropriate measures that will assure its protection in accordance with the contractual agreement.

7.3.2 Why Should I Care?

Reputation of would-be business collaborators is a critical indicator as to the reliance to be placed on forming collaboration agreements, informing the business decision-making process both in assessing the level of risk involved, and in deciding what terms, conditions, and constraints to include in any agreement.

7.3.3 Recommendations/Solutions

An effective reputation management resource would significantly improve the reputation information available for making best-informed and therefore lowest-risk decisions on proposed new collaboration contracts.



Contracts are key to assuring reliable business collaborations. The contract lifecycle provides the means to manage the process. Reputation management is a key component in this contract lifecycle:

- Taking in reputation information about a given organization from past experiences and performance against earlier contract fulfillments, from all sources
- Providing structured information into the decision-making process for signing up to a new collaboration contract with that organization

7.3.4 Background and Rationale

A significant consideration in making risk management decisions to collaborate with other organizations is the reputation of those organizations. Reputation is a form of trust that a party (organization, process, or person) has earned for demonstrating how reliable they are in fulfilling business agreements. It is measured in terms of past experience: the more there have been good experiences, the better is the reputation. Conversely, and more importantly, just one bad experience can severely damage what was a good reputation. People naturally wish to do business with others they trust, and reputation is a significant consideration in deciding whether the risk is acceptable and if so under what contractual terms.

A particularly valuable feature of reputation is that it is a social concept involving aggregation of real-world information based on experiences – not only your own direct experience, but also of the experiences that others have shared within the same operating community – be it a golf club, a car dealer, a restaurant, or a multi-national corporation.

The problem is how to manage reputation experience in ways which provide valid information that enables informed risk-based decisions to be made.

Reputation management is practiced by many individuals and organizations who variously collect information on:

- Age
- Qualifications
- Credit history
- Past performance in dealings
- Criminal record
- Employment
- Health
- Plus a wide range of references/testimonials, including rumor and unsubstantiated gossip

to assess how the current standing, credibility, and past performance demonstrated by a potential collaboration party combine to represent an acceptable risk for going ahead with further collaboration agreements with them.

Herein lie two major problems:

- How to ensure that the ever-increasing volume of "experience" information is true/accurate? When was it last validated/updated? In short, how reliable is it as a basis for making a sound risk decision?
- How to compile this reputation information into a managed form that renders it as a reliable resource for informing business managers in making sound risk decisions based on reputation?

7.4 Trust Management: Overview

Note: Refer to the forthcoming Open Group Guide to Trust Management – A Control Framework for e-Business Collaboration, which is currently under development in The Open Group Security Forum and is expected to be published by end-2012.

7.4.1 Problem Statement

It is well known that e-commerce transactions require a level of trust between participants in that trust, in this context, gives each partner confidence that the other will fulfill his part of a bargain in the future.

Trust, in this business context, relies primarily upon contracts (to specify the behavior that is required) and an enforcement mechanism (to punish and deter non-performance). For this to work in an e-commerce environment, a process is required to register and verify each party's identity. However, the problem with registration processes is that they are hard to automate and, therefore, expensive. This creates a "friction" that resists the growth of e-commerce.

The cost of registration can largely be reduced by sharing it between organizations. This is facilitated by mechanisms such as federation, which is designed to share identities and authorizations between organizations, thus extending their use. Today's federation mechanisms are oriented towards federating customer identity between members of a supply chain and, by agreement, between related supply chains. They aim to facilitate interactions between a customer and an organization.

However, there is a need for federation between organizations, to make the federation process easier to automate, and to create new mechanisms, such as reputation, for sharing trust information.

Additionally, a common legal infrastructure, in the form of standardized contract templates, is required to facilitate de-perimeterized e-commerce.

7.4.2 Why Should I Care?

Trust is crucial to all human interactions and therefore the ability to express trust electronically is essential to successful electronic collaboration (JFC#6).

Registration and trust management, however, are expensive and often complex due to differing policy requirements.

De-perimeterization requires the ability to share reputation information between organizations (JFC#8) and thus reduce costs.

7.4.3 Recommendations/Solutions

Effective trust management is important in securing electronic transactions involving multiple organizations. The recommendations/solutions here explain an effective approach to "trust", and focus on its use for electronic business. They include a generic trust architecture framework within which trust decisions can be made, and within which accountability can be supported. They then propose the creation of a "trust broker" to handle an organization's trust relationships.

7.4.4 Background and Rationale

Within the context of this standard, trust can be either:

- A verb – a decision to rely upon someone's future performance of a contract, or
- A noun – confidence that someone will meet a contract, based on their perceived capability, intentions, and an accountability mechanism.

Whichever definition is adopted, trust is a vital pre-condition for successful collaboration.[20]

Central to this definition of trust is the idea of a contract. A contract involves two parties (which can be people or organizations), a set of rules about what each should do, and an accountability mechanism for handling failure by a party. A contract does not have to be a legal contract, written down and signed; it can simply be an informal code of behavior within a community.

An accountability mechanism can include measures such as criminal prosecution, civil action, disciplinary action, or merely ostracism from a community. Clearly, an accountability mechanism cannot function unless the identity of the failing party is known.

7.4.4.1 Co-operation

Trust is an essential precondition for co-operation among people and organizations. It allows two parts of a transaction to be separated in time; for instance, a customer pays a supplier, expecting delivery of a product in a week's time, because of trust in the supplier's stated terms. A party chooses to co-operate with another in a trusting way because he believes some combination of the following:

- The trusted party is well disposed towards him.
- It is in the trusted party's best interests to comply.
- The trusted party has the necessary competence, skills, and resources to comply.
- An accountability mechanism exists that can force the trusted party to comply.

Trust is a social phenomenon; a wide variety of social structures have evolved over many years to encourage and enforce co-operation, ranging from marriage to contract law. Many of these were based in the past on face-to-face contact. Today, business and social interactions are increasingly being performed electronically. This creates new processes, such as authentication and authorization, for managing trust. Authentication links an electronic agent to a real-world identity that forms the basis for an accountability mechanism; and authorization represents a degree of trust or competency that has been assigned to the identity. An authorization represents a contract, an agreed set of rules about how the holder and granter of the authorization will behave.

[20] Trust is a risk management issue so must be considered within an overall risk management framework. This is outside the scope of this O-SCOA Framework standard.

7.4.4.2 Organizations

People naturally create organizations, and an organization has many of the legal rights of an individual person. For instance, it is a legal person that can enter into contracts, but an organization cannot *do* anything real. It must delegate its capabilities, either to owned equipment (plant), to people (employees), or to other organizations (sub-contractors) to fulfil contracts. Even contract signing must be delegated to employees and directors.

When organizations co-operate as potential provider and consumer of a service, the service provider has to ask the questions: "Am I prepared to work with this business?", and "Is this user empowered to commit his business to work with me?" The service consumer will enable its users by provisioning them with authorizations on the service. It asks the questions: "Am I prepared to sign this service contract?", and "Am I willing to allow this user to commit me to it?" before doing so.

In order to work together, organizations need to accept, and therefore understand, each others' contracts. Increasingly this will need to be done in an automated way. Businesses also need to be able to account for the contracts/authorizations they have agreed to (both as producers and consumers) in order to understand the obligations they are currently under.

7.4.4.3 Reputation

How does one party decide to trust another? It must decide whether the party is trustworthy or not, based on the proposed contract and a perception of the other party's past performance. Good performance in similar areas makes it probable that the other party will be trusted. A record of performance constitutes "reputation" – good or bad.

This begs the question of how two strangers can ever come to trust each other. Two mechanisms are possible here:

- Parties may share reputation information with others they trust, allowing one party to take advantage of another's experience.
- A party may choose to trust a stranger in a small way initially, based on global accountability mechanisms such as the law, then escalate trust based on good performance.

7.4.4.4 Trust Architecture

The figure below illustrates a potential trust architecture to implement these concepts.

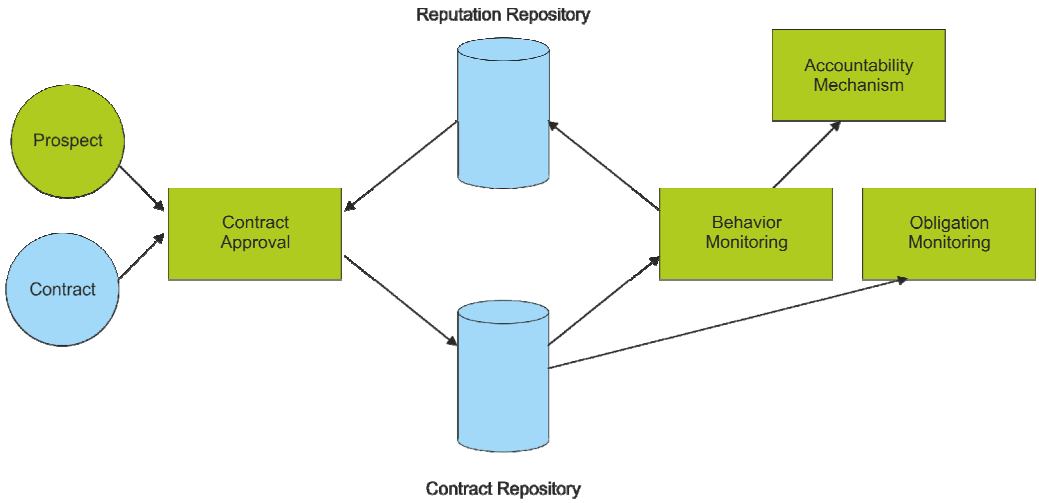


Figure 5: Trust Architecture for Contract Management

Within the figure:

- The *Contract* is an agreement an organization is considering entering into. This could be a business contract, or the allocation of a group membership in a directory.
- The *Prospect* is the other party in the contract. This could be a user applying for membership of a group.
- *Contract Approval* is the decision-making process for whether or not to enter into the contract. It will use information in the reputation repository in making this decision.
- If the contract is signed, it will be entered into the *Contract Repository* so the organization can monitor its assets and liabilities. The contract repository can be considered to be part of the organization's accounts. In many organizations, the contract repository is implemented as group memberships in an LDAP user directory.
- As the contract is executed by both parties, a *Behavior Monitoring* process ensures that the trusted party is complying with the contract; and *Obligation Monitoring* ensures that the organization itself is complying. In the electronic world, this is implemented by access management, provisioning, and user audit.
- The *Accountability Mechanism* is invoked if the other party is not complying with the contract.
- The *Reputation Repository* records information that is known about other parties, their attributes, and their past behavior. This is the basis of contract approval decisions. It may be implemented by user attributes in an LDAP repository.

Note: The examples given above relate to group memberships. Similar analogies could be applied; e.g., license management or a shopping cart on a web site.

7.4.4.5 *De-Perimeterization*

The architecture above involves a single person or organization acting alone. The model should be generalized to support de-perimeterization.

One form of de-perimeterization comes from sharing reputation information between organizations. This can be done in several ways:

- Direct mechanisms such as federation
- Introduction protocols whereby one party can recommend someone to a third
- Market-oriented reputation services (of which modern day services such as Experian can be considered a fore-runner)
- Peer-to-peer mechanisms such as the eBay reputation system

Another form comes from improved mechanisms for delegating contracts. Existing access management and provisioning systems will evolve to being "trust brokers". The figure below illustrates a trust broker concept.

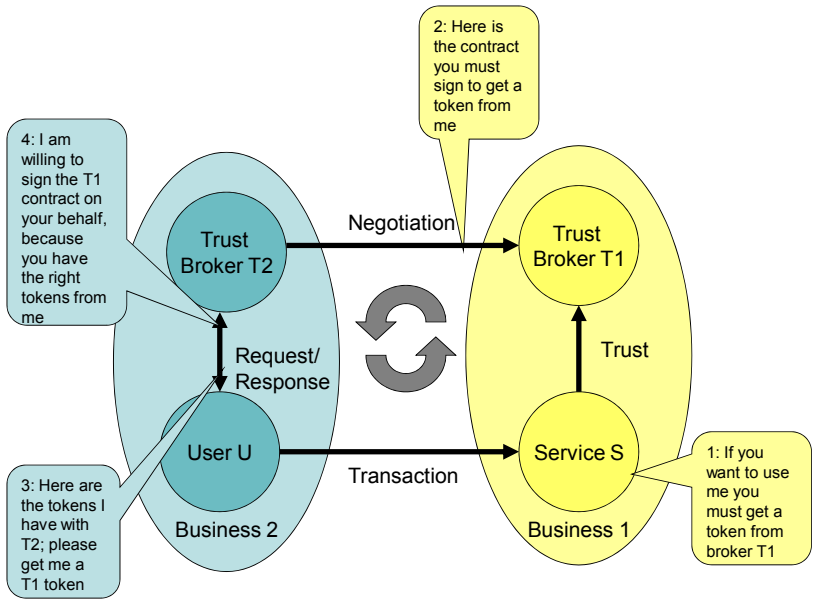


Figure 6: Access Management and Provisioning as Trust Brokers

The two businesses use trust brokers to control delegation of contracts between them. Initially this process would be mostly manual, but it will become more and more automated as authorizations become more standardized.

7.4.5 The Way Forward

A variety of trust models are possible, with varying levels of technical implementation. A catalog of such models would form a useful reference source. Of particular interest here is the e-rights smart contract model and the inherently secure e-programming language proposed by

Miller, Szabo et al.[21] We should also investigate the issues involved in standardizing authorizations between organizations.

Vendors should develop trust broker (software and services) to link identities and authorizations between organizations.

Organizations should investigate the benefit to be gained from linking the agreement of a contract with provisioning it automatically. They should also consider the adoption of standard legal infrastructure to support de-perimeterization.

7.5 Trust Management: Business Impact Level

7.5.1 Problem Statement

Back in the time when businesses were predominantly "local" and to a large extent insulated from each others' operations, it really didn't matter very much how we defined the business impact of information risks, for we knew what we meant in each business and we didn't have much need to share that meaning with others. Collaboration and the business need for it back then was not a significant imperative for most businesses in a global or even national context, and certainly was not a requirement at the frequency and set-up speed that collaborations are demanded today.

Today, parties in a collaboration need more clarity over the controls that apply in their relationship. With the increased importance of collaboration, it is becoming more important to be able to share the implications of a risk in terms of the potential business impact. We need to do so in a manner that is universally understood. This document recognizes that there is no such commonly agreed scale available to communicate with sufficient granularity the impact of information risk on businesses.

7.5.2 Why Should I Care?

Without a commonly agreed communications tool, enterprises will not be in a position to effectively share with their partners the implications of a particular information risk. With such a tool, it becomes possible to communicate in a manner that allows the collaborative management of information risks. Also, it is not straightforward to automate the processes for managing risk if the impact is not commonly understood.

7.5.3 Recommendations/Solutions

We need to promote development of a standard business impact scale that would be associated with information of different sensitivity, appropriate information controls, and trust levels.

This proposal defines six business impact levels, with the first unlikely to be used in a business context. It is assumed that there is no need to define "No Impact".

- Disastrous: Significant loss of life, collapse of multiple enterprises or a country's economy, significant global environmental incident.

[21] Refer to http://erights.org/elang/index.html.

- Catastrophic: Loss of multiple lives, significant financial loss, collapse of an enterprise, significant countrywide environmental incident.
- Material: Accidental loss of life, financial loss of reportable sums of money, significant brand impact, significant local environmental incident.
- Major: Significant injury, significant financial loss, brand impact, local environmental incident.
- Minor: Injury, financial loss, local brand impact, minor environmental incident.
- Insignificant: Negligible injury, slight financial loss, negligible environmental impact.

These levels are directly equivalent to the UK Government Business Impact Table. Other relevant references are available from the OECD, and from national standards organizations in many countries.

7.5.4 Background and Rationale

Being able to quantify the impact in a qualitative frame enables understanding of impact and allows for dialog and negotiation.

The four impact domains considered in this document are:

- Impact on human life
- Financial impact
- Brand impact
- Environmental impact

Naturally, impact levels will vary greatly between different enterprises, based on their nature, size, etc.

Examples of risk tools developed in the past to communicate the potential size of specific risks in nature include:

- Admiral Beaufort developed his Beaufort wind scale in 1805, allowing sailors to identify and communicate in a commonly understood manner the threat from wind force.
- Charles Richter and Beno Gutenberg developed a scale in 1935 (the Richter scale) to report earthquake magnitudes (the levels for which were: Micro, Minor, Often, Light, Moderate, Strong, Major, Great, Devastating, Epic).

One important difference to understand with a business impact scale is that it is not measuring the size of the risk event; a given information risk would not necessarily have the same business impact on each party in a collaboration. However, the ability to be able to share in commonly understood terms the business impact that a given risk might have on both parties, allows for appropriate negotiation between those parties over the risk controls or mitigations that should be employed.

Similarly, it is also important to note that the financial implications of an event will not always be the same for each party. The impact of losing $10,000 in a very small start-up will feel very different to the impact felt by a large corporate organization losing the same amount. The important thing to consider is that the terms in a business impact scale convey the true implications of a risk event for each party.

7.5.5 The Way Forward

Recognition of the need for a business impact scale of the nature described in this document is a key first step. Those who do so can then work together to create and encourage global adoption of an open standard that will allow common understanding on business impact levels.

At this stage, we envisage that key attributes of a successful business impact scale standard to include:

- Sufficient granularity (some scales used today have just three levels)
- Clear, understandable definitions of business impact

A business impact standard is not of course a substitute for performing effective risk assessment/analysis evaluations[22] to enable business managers to understand what impacts their existing exposure to risk could have on their business operations, so they can take informed decisions on how best to manage (accept, mitigate) their exposure.

7.6 Trust Management: Information Classification

The aim of this requirement is to demonstrate how information classification can be used to enhance security within a secure COA. While there has been a great deal of work done on information classification, this has tended to be bespoke to any and every organization that has used it. Furthermore, classification has traditionally only been used on a very small percentage of information assets. In the new de-perimeterized world this is no longer a realistic option.

7.6.1 Problem Statement

Within organizations, information is growing at a huge rate, and with the costs of digital storage falling to very low levels, it looks to continue to grow in the foreseeable future. In a de-perimeterized environment this problem is greater – data is going to be created and utilized by more than just employees – with partners, suppliers, consultants, and customers all having a hand in your data.

Ultimately, the classification of information corresponds to the level of protection afforded it and so consistency is required, not only within an organization but also across organizations living in the de-perimeterized business environment.

Current information classification systems are designed for specialists to use and subsequently only a very small percentage of information is labeled. The problem is worsened when you look at some of the other factors which need to be taken into account when looking at protecting information.

[22] See Section 6.2.

7.6.2 Why Should I Care?

Value of Data Varies Over Time

Classifying a document is not a static problem; it varies over time. For example, an initial document may not contain any sensitive information until its third draft when acquisition targets are named. While this process can occur relatively quickly over a matter of days, the process can take a great deal longer; for example, state secrets may become de-classified after 50 years.

Therefore, any classification mechanism needs to take time into account.

Risk to Data Varies by Location/Geography

Information being accessed via a cyber-cafe probably needs to be treated and protected differently to that which is being accessed on a desktop inside head office. It may be that some information which has been classified as "highly sensitive" is not allowed to be accessed from a cyber-cafe, or even from a smart phone. For example, good practice in local health authorities is not to allow health records on smart phones in case they are lost (even though they tend to have encryption and other adequate security measures implemented on them).

While the classification of the data remains constant no matter where it is, the risks are different and a policy engine working with classification to protect information needs to take geography and/or location into account.

Consistent Information Classification is Hard

If something has been classified, especially when it is done by an individual, then consistency becomes an issue. What one person thinks of as being "highly sensitive" another might think is just "sensitive", and a third might think is "public". For example, a CEO probably deals in "highly sensitive" information all the time, whereas a sales manager doesn't. For the sales manager, they may classify an ongoing deal as "highly sensitive" when the correct labeling would be "sensitive".

The problem becomes harder still when working with a secure COA. When there are multiple parties specifying classification there needs to be agreement on how the classification is carried out and how the information is subsequently handled. A government's "sensitive" information probably requires more rigor applied to it than a widget manufacturer!

7.6.3 Recommendations/Solutions

Key Issues for a COA

Thus, the key question for anyone designing an information classification system in the COA is: "What levels of classification do you require and how do you protect the information at each level?". Any checking must extend beyond the pure operation systems checks to (potentially) include being able to assert the security status of applications that will be used in the transaction as well as (potentially) checking that unwanted applications are not running. Such checking may

be one-time, or may need to be continuous dependent on the type of collaboration and the process involved in the transaction.

Classification Levels

While there are a number of different information classification systems around, a simpler "less is more" approach should be taken to reduce confusion. To this end, the proposal put forward by the G8, commonly called the "Traffic Light Protocol", has four levels:

White Public: public distribution, unlimited control.

Green Normal Business: business community-wide.

Amber Sensitive: established named groups only.

Red Highly Sensitive: Specific to named recipients only.

Tagging classification using colors has to be augmented with another visual clue such as an icon. We need icons for the following classifications:

- Highly Sensitive
- Sensitive
- Normal Business
- Public

Personally Identifiable Information

While the classification level is outlined above, it is worth drawing out one other category of information: Personally Identifiable Information (PII). Protection of PII has become a global issue after a number of data leaks from companies and governments alike. Legislation to protect PII continues to evolve, particularly in North America and Europe.

The EU Directive 95/46/EC defines PII as:

Article 2a: "Personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

Examples of this include, but are not limited to:

- Full name
- National identification number
- Telephone number
- Street address
- Email address

- IP address (in some cases)
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity

This information is often classed as “sensitive”, although the consequences of it being lost or leaked means that it should probably be treated as “highly sensitive”.

Information Classification Taxonomy

While the classification levels outlined above are useful, organizations are also interested in classifying information to provide additional information; for example, is this information related to Mergers and Acquisitions (M&A) or is it just a social event. For this reason, organizations may want to look at a classification taxonomy, especially when sharing information in an O-SCOA Framework. In that way, design documents can be separated from legal ones, and so forth.

There are a number of different methods for creating taxonomies as well as a number of standard ones; for example, the Dewey Decimal Classification system for library books. It is worth noting that creating taxonomies can be difficult and that in many cases the law of diminishing returns is rapidly reached, but the people defining the taxonomy may never reach the end. Defining and agreeing a number of high-level categories is worthwhile and these can then be used by individuals as well as automated classification tools.

Automated Classification

With the ever-increasing quantity of electronic information and records, the need for automatic classification is also growing. Automation can be used to address the changing requirements based on time and geography as well as content.

The rules for classification of information need to be defined. There are some patterns in information, such as credit card numbers, which are universal and easy to define. For others, keyword, phrases, or regular expressions are used and it is relatively simple to use the same definition across multiple classification engines. However, there are also statistical analysis tools which result in a classification being given. These tend to be proprietary and the definitions almost impossible to share among the classification engines in order to ensure consistency.

If automatic classification is used, then it is worth considering archiving the definitions and ensuring that the version used is also stored with the classification. In that way it will be possible to tell how a particular document was classified and therefore the actions that happened because of it.

Multiple Classifications

When classifying information into a taxonomy there are probabilities attached, usually based on statistical analysis. In this case, there can then be multiple classifications with attached probabilities. While it is usually only the most probable classification that is acted upon, it may be useful to take into account the second or third probability, especially if they are relatively close. For example, if a piece of information is classified as "Social.. 0.78", "M&A... 0.77" then the second classification would result in completely different handling of the information than the first.

7.6.4 Background and Rationale

This is included in Section 7.6.3.

7.6.5 Challenges to the Industry

Current classification methods and mechanisms are proprietary. While it is relatively simple to define criteria for some information, such as credit card information, most company confidential information is unique to the company that creates it. A common method of defining classification rules is required to enable the sharing of information classification. Similarly, there needs to be a standard method to tag information with the classification, including sensitivity, taxonomy, and probability.

For open COAs to share information effectively, information classification information needs to be shared. In order for that to occur, the key vendors in the space need to agree an open specification/standard they will all use by which such classifications and definitions can be shared.

7.6.6 The Way Forward

The ability to consistently classify information at all points in its lifecycle and across the entire IT infrastructure is critical. If the information cannot be classified correctly, then it will not be able to be managed appropriately. Static classification of information by the information owner is not workable in today's global environment and so consistent automation is also required.

7.7 Trust Management: Impact Sensitivity Categorization

Information must be classified using an appropriate classification scheme – see Section 7.6. The classification of information will define associated information protection requirements in terms of restricting the circulation of information based on identity, legality, and temporal components. CIA&A must also be considered for information created within organizations. Thus, information must be categorized to reflect the level of business impact that would occur if any of these requirements were not correctly enforced.

Business impact is generally financial and will vary in magnitude depending on the size and economic health of the organizations. Financially healthy companies will suffer less than financially healthy companies with the same value of impact.

7.7.1 Problem Statement

The access and usage of information controlled using Enterprise Information Protection & Control[23] (EIPC) tools in de-perimeterized environments should reflect not only the restricted circulation of information as required by an information classification scheme, but also the storage, handling, transport, and environmental restrictions associated with the information in terms of impact sensitivity should its CIA&A be compromised.

For example, information classified as "Amber" using the G8 Traffic Light Protocol information classification scheme has associated information protection requirements that represent the need to limit the circulation of that information to a specific domain such as internal organization or a collaborative working group. The business impact of access (confidentiality) or modification (integrity) of that information outside of this domain; the lack of availability of the information when required within the domain; and changes to the information without the consent of the data originator (authenticity) within the domain, will reflect the economic impact associated with any of these occurrences.

7.7.2 Why Should I Care?

Without appropriate classification, information circulation cannot be restricted appropriately. From a confidentiality point of view, encryption and access controls can suffice without information classification for maintaining information protection in de-perimeterized environments, as long as appropriate de-perimeterized access controls are used. However, for integrity, availability, and authenticity a different model is required. Impact sensitivity categorization can define appropriate information usage and handling controls in relation to these requirements.

7.7.3 Recommendations/Solutions

The requirement here is to develop a common language (taxonomy) and set of trust levels defining impact sensitivity of information, based on measures of its CIA&A. (Note that Service or System Criticality is potentially a separate area of classification.)

The number of trust levels needed for impact sensitivity depends on the nature of the business information involved, but six levels should be sufficient for most requirements:

T5 Catastrophic

T4 Material

T3 Major

T2 Minor

T1 Insignificant

T0 None

[23] See Section 5.2.5.

The magnitude in terms of financial impact will vary depending on the economic size of the organization. Based on The Open Group Guide: Requirements for Risk Assessment Methodologies, Figure 7 suggests the numeric value of magnitude for a large Fortune 100 company. What has significant impact for them may be catastrophic for an SME, so the $ values must be adjusted to suit each organization.

Magnitude	Range Low End	Range High End
Disaster	1,000's of Deaths	
Catastrophic	Death/Company Ceases to Trade	
Material	$250,000,000	→
Severe (SV)	$10,000,000	$100,000,000
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

Figure 7: Impact Sensitivity – Exposure to Magnitude of Loss

7.7.4 Background and Rationale

The business impact level associated with information, together with the information classification label, drive the requirement for controls to be applied to manage the way in which users access and handle data. Controls to consider include the following five items.

Information Creation

It is important to consider the impact sensitivity of new or recreated information. Sometimes information can be secured by not actually creating it at all if there is no real requirement for it. For example, creating information that contains multiple types of personal identifiable information from different data sources for the sake of ease-of-access to all information could have high impact sensitivity if not properly secured and is not actually of importance to business process; therefore, it should not be created in the first place.

Information Storage

The risk associated with storing information must be considered both internally and in de-perimeterized environments. From a confidentiality aspect, the information may require secure storage; i.e., storage on encrypted file systems. From an integrity point of view, the modification of information may require audit or tamper-evident data storage to be used so that any changes to the information can be detected and traced. The availability requirement may suggest multiple back-ups and mirrors of the information to be supported in case any of the file servers become unavailable. It may also be essential to continually monitor the state of the back-ups and mirrors to ensure guaranteed access to information in the event of system failure. There is no point having back-ups if they are also offline.

Information Sharing

CIA&A requirements must be considered before sharing any classified information. Simply encrypting and providing access controls may suffice for confidentiality, but in some business processes this requirement is not adequate to support secure business process. Where availability, integrity, and authenticity are important aspects of information sensitivity, appropriate consideration should be given to the circulation of the information and to who may gain access and modification control of it.

Information Transfer

Information transfer over inherently insecure protocols must be secured using appropriate mechanisms. CIA&A should be protected from information interception and/or modification in transfer. Availability may be an essential requirement in critical information systems. Thus, the information transfer mechanisms must guarantee availability and end-to-end transfer at all times.

Information Deletion

Information with high business impact in terms of CIA&A must be securely destroyed when its useful lifetime ends. Simply deleting it (moving to "trash") does not destroy the content. Secure "digital data shredding" must be performed.

7.7.5 Challenges to the Industry

The ability to consistently classify information at all points in its lifecycle and across the entire IT infrastructure is critical. If the information cannot be classified correctly, then it also cannot be managed appropriately. Static classification of information by the information owner is not workable in today's global environment; therefore, consistent automation is also required.

7.7.6 The Way Forward

Defining an agreed, standardized taxonomy for information classification is essential to the success of trust management in de-perimeterized environments.

7.8 Trust Management: Control Stratification

Information must be classified using an appropriate classification scheme – see Section 7.6. The classification of information will define associated information protection requirements in terms of restricting the circulation of information based on identity, legality, and temporal components. CIA&A must also be considered for information created within organizations. Thus, information must be categorized to reflect the level of business impact that would occur if any of these requirements were not correctly enforced, as defined in Section 7.7.

Information classification and impact sensitivity categorization drive control requirements to ensure the protection of information in de-perimeterized environments. As well as controlling the creation, handling, transfer, and deletion of information as defined using impact sensitivity categorization, it is also essential to establish a level of trust in the identity of entities that access and handle information, and even the controls that provide this protection. Control stratification

enables trust in an identity to different levels based on the level of authentication given by an entity.

7.8.1 Problem Statement

In a de-perimeterized environment, information classification should define the domain in which information is allowed to be circulated; for example, internal organization or inter-organizational collaboration groups. Impact sensitivity categorization of information should mandate controls to be enforced that protect the information protection requirements in terms of CIA&A, during the information lifecycle within the specified domains. For example, if information classified as Amber is sent outside of the specified shared domain, the controls should prevent the information from moving. Likewise, if the endpoint location of shared information is within the domain but the location is not backed up or mirrored, the information should be prevented from moving if there is a high impact requirement for availability.

A third consideration in our trust management model is control stratification. This extends the considerations of information classification and impact sensitivity categorization to include the identity assurance of an entity accessing or handling the information as part of the operational process. For example, information with specific classification and impact sensitivity categorization labels must only be accessed by entities given clearance to access such information classified with that label and to perform actions that maintain the required levels of CIA&A assurance. The higher the impact sensitivity, the more important it is that the entity requesting access can prove to be who they say they are (authentication), and the higher the requirement for the authentication result to be trusted. For low-level information, a simple user name and password may suffice. For high-level information, two-factor authentication with the addition of a secure token may be necessary. For the highest-level impact sensitivity, biometrics may be required.

7.8.2 Why Should I Care?

The entities responsible for accessing and handling information are responsible for its protection and survival throughout its lifetime. If it has been decided that information is sensitive enough to classify, then it must be ensured that the classification is recognized when allowing access to entities who intend to handle, store, transfer, and delete information within an organization and externally, in collaborative, de-perimeterized environments.

The identity of entities responsible for information must be trusted to a level based on the level of business impact they can threaten while in this position of responsibility. Categorizing trust in identity can allow you to distinguish between trusted and untrusted entities for any given piece of information by mapping the assured trust level provided by the entity to the level of business impact defined by information classification and impact sensitivity categorization.

7.8.3 Recommendations/Solutions

The requirement here is to develop a common language (taxonomy) and set of trust levels in the identity of entities accessing and handling information. A set of standardized identity trust levels should be defined, using the standard CIA&A frame and adding identity. We define six levels of trust taxonomy for authenticity as follows:

C5 ASSURED (biometric)

C4 AFFIRMED (positive physical or logical authentication)

C3 PROVEN (authenticated by trusted third party)

C2 CONFIRMED (confirmed by strong attributes)

C1 ASSERTED (self-asserted)

C0 UNKNOWN (no authenticity assertions made – anonymous)

7.8.4 Background and Rationale

It is essential when considering the CIA&A requirements of information that the identity of an entity attempting to access and handle the information can be assured to specified, standardized levels to ensure its identity can be trusted to fulfil the defined CIA&A requirements of that particular piece of information. Identity does not only refer to people, it can include devices, systems, network, and environments.

For example, the fire alarm system within a building handles critical information when the signal is set to sound the alarm in the event of fire. Thus, the information transferred to the fire alarm has a catastrophic impact sensitivity value in terms of availability. The entities accessing and handling information in this case are the cable that carries the signal to the fire alarm, and the endpoint that sends the signal. Identity assurance through control stratification must mandate the assurances required from the entities. The information is classified as critical; therefore, the identity of entities accessing and handling the information must be at least "affirmed" to be able to handle this level of information. The identity of the cable must be trusted to carry the signal. To guarantee this, it must be physically affirmed to be tamper-evident, availability monitored, and fireproof. The endpoint that sends the signal must be affirmed as being backed up, mirrored, and tamper-evident so that it can be trusted to maintain connection to the fire alarm at all times, especially in the event of emergency when buildings may be damaged or on fire.

If identity assurances cannot be given to this extent, the information must not be accessed or handled using these entities as it means placing the information in an insecure environment in terms of CIA&A. Not all entities need to identify themselves to this extent; only those accessing and handling information classified at the highest levels.

7.8.5 Challenges to the Industry and Way Forward

Consideration of the identity of entities accessing and handling information to this level is essential to maintaining trust in the environment in which information lives out its lifecycle. Even more so in environments that are de-perimeterized and in which organizations do not always maintain control over the actions and configuration of entities that access and handle their information.

It is important to consider the implications of the assurances offered (or not offered) by entities outside of an organization's immediate control.

7.9 Policy Management

7.9.1 Problem Statement

We believe that protection should be applied close to data (JFC#1, JFC#9), and that firewalls should be "quality-of-service separators" providing defense-in-depth wherever they perform effective protection functions.

This approach leads to access policies evolving from coarse, infrastructure-oriented statements to fine-grained business-oriented ones. But herein lies a problem – there are many more data items than there are firewalls. If each data item has to be individually protected, how are we going to manage the enormous number of information access policies we will need?

7.9.2 Why Should I Care?

Efficient information access policy management is critical to securing an agile, rapidly changing enterprise.

The problem of how to specify, apply, and enforce information access policies on mobile data is critical if privacy and intellectual property rights issues are to be properly addressed. In particular, e-business relies on free flow of information, but information owners need confidence that their information will be properly handled by the holders.

7.9.3 Recommendations/Solutions

We believe that:

- Information access policies must be expressible in powerful languages that can accurately capture the intention of the creator.
- Secure systems need to separate out the administration points, decision points, and enforcement points for information access policies.
- Businesses need to adopt new techniques for understanding their security imperatives so they can be accurately encoded.
- A set of interoperable global identifiers needs to be developed.
- Where organizations exchange data, they should also expect to exchange information access policies covering how that data should be handled.

7.9.4 Background and Rationale

What is an Information Access Policy?

A security policy is a rule that an organization must follow in order to meet its security objectives. An information access policy is a particular type of security policy specifically related to the security of information and its underlying data. There are many types of information access policy; some examples are given below:

- *Personnel information shall be readable by the subject, the HR department, and the subject's manager.* This is a business-oriented human-readable policy. It is generic, in that it can be applied to many different assets.
- An Access Control List (ACL) file is a machine-readable policy. It is infrastructure-oriented and applies to just a single object.
- *Users must not install applications on their laptops without permission from the security department.* This looks like the previous business-oriented policy, but note that it does not actually say what applications are permitted and which are not, nor does it even give criteria for permitting an application. Rather, it describes a procedure for obtaining permission ("ask the security department").
- *A software or DRM license is a form of policy*. This is a machine-readable business-oriented policy and may specify controls over copying and expiry.

It should be clear that policy statements are critically important in controlling organizations and computer systems.

We can see a dichotomy above between human-readable and machine-readable policies. IT systems, of course, run off machine-readable policies, but these are hard for humans to understand. Human-readable policies, on the other hand, cannot be understood by computers.

Another distinction above is between specific information access policies that cover a single asset, and generic policies that cover whole classes of asset. Many machine-readable policies today are specific. That means that a separate policy must be written for every asset, even if it takes a similar or identical form to a previous policy. It becomes very difficult to check that all policies in a class are correct, and it is very difficult to keep policies in step with changing requirements. Many organizations will have millions, or even billions, of data items, and it is not practical to devise a separate policy for each one.

Finally, the machine-readable policies above are expressed using very basic language; for instance, a file ACL is expressed using user identities, group memberships, and the "or" operation. It is not capable, therefore, of encoding many of the business-oriented policies given above. This lack of expressive power makes it hard to accurately reflect business requirements, and hard to keep policies up-to-date as infrastructures change and as data becomes more mobile. Such requirements tend to be implemented by dedicated program code, and thereby become hard to understand, test, and maintain. A fine-grained policy needs to be much more accurate than a coarse-grained one.

What is Hard about Information Access Policies?

Most organizations have no idea what their information access policies are – even (especially) those which claim to have a documented security policy.

More than that, the question of how to relate an information access policy to the business imperatives that justify it is only just starting to be asked. This makes it hard to know how to create a business-oriented information access policy.

Most real-world policies need to cope with numerous exception conditions. For instance, a doctor should not see medical records without the subject's consent, but if the subject is wounded and unconscious he cannot give consent so there will need to be a legitimate way to bypass the information access policy – audited two man rule, for instance.

Many information-based services use data from many different providers, who have to give this data to a customer or supplier in order for the service to function. Once the data is handed over, the owner loses control over it.

The data owner has to be able to:

- Set an information access policy about how his data should be handled
- Have some confidence that his data will be handled according to the information access policy
- Have confidence that the information access policy is bound to the data for the life of the data, including copies of data

The situation can quickly become very complex, with most real-world services using data from many different providers, each with its own information access policy requirements, processed through several stages, each of which may change the requirement.

7.9.5 Challenges to the Industry

Information access policy requires organizational change as well as technical innovation.

Organizations need to understand what their information access policies really are. It is important to realize that there will be many governance patterns for policies; for example:

- Automated Control: The owner of a data item specifies an information access policy about how it may be used. All holders of the item must consult the policy before they may give access to it.
- Workflow-based Control: In this case, it is not possible to specify a simple information access policy that a machine can follow, so the data owner (or his delegate) must be involved personally in the authorization process.
- Accountability: In this case, the data owner trusts a data holder to control access to his data, but retains the right to know who has accessed his data and why, and to hold accessors accountable for their access.
- Time-limited Permissions: The data owner gives permission for a very short period of time after which the data holder must seek permission again.

7.9.6 The Way Forward

To allow such complex models to operate, systems must be able to separate information access policy administration (which will be done by the data owner), policy decision (which will be done by the owner or his delegate), and policy enforcement (which must be done by all data holders). This is the basis of standards such as XACML.

Information access policies need to become more sophisticated than ACLs. Essentially they are specialized programs. Experiments have been conducted into expressing policies as proof obligations, for example. XACML is a valuable step in this direction, but only a step.

The industry needs an efficient and interoperable means to manage identities between different attribute authorities. The Open Group Core Identifier Framework Matrix goes some way to evaluate the issues involved. Identity and entitlement management is, however, a major challenge in the de-perimeterization space.

7.10 Audit

7.10.1 Problem Statement

IT audit is about the formal verification and validation of the quality and effectiveness of IT controls to support the overall business control objectives. From a security control perspective the residual IT security risks are relatively well understood in a network perimeter protected environment. This perimeter-based protection model has led to an IT audit practice that has matured into given sets of frameworks, methodologies, approaches, and models with certain sets of assumptions. CobiT (Control Objectives for Information and Related Technology) represents such maturity in IT control frameworks and is commonly referenced among IT auditors.

Our assessment is that there is no strategic impact on the underlying IT audit control framework(s) that have been serving as the foundation for IT audit, arising from the impact of the Jericho Forum Commandments.

However, a valid question to ask is whether the tactical/operational aspects of IT audit can scale to meet the challenges in a de-perimeterized operational environment. This document addresses this question.

IT security controls are important aspects of regulatory compliance, so the impact on the area of regulatory compliance is also addressed briefly in this document.

7.10.2 Why Should I Care?

Without an appropriate IT audit scope, important IT controls within an organization may not be fully tested – thus leading to higher levels of risk including regulatory compliance risks, if these controls are ineffective.

IT audit is a measurement of IT risk management, which translates into business risk management.

Improper management of IT risks carries severe business impacts if regulatory non-compliance is revealed. The US Sarbanes-Oxley Act represents an example.

The fundamentals of IT audit require the ability to demonstrate the same risk-based control quality in a de-perimeterized environment as in a bounded environment. The quality of Test of Design (TOD) and Test of Effectiveness (TOE) in a de-perimeterized environment is required to be no less than as in a perimeterized environment.

Without the proper understanding and appreciation of the major changes taking place as de-perimeterization steadily increases, an organization may fail to meet their auditor's expectations, unless the audited organization promotes good communication of the impact that de-perimeterization has on how effective audit of their organization needs to be conducted.

Against a landscape of increasing threats, vulnerabilities, and regulatory compliance demands, the need will similarly increase for evidence that adequate and appropriate governance of information security has been implemented and continues to operate effectively across the scope of the organization and its IT infrastructure.

7.10.3 Recommendations/Solutions

Audit

While there is no clear strategic impact to the fundamentals of IT audit described in the prevalent IT control frameworks such as CobiT, there are significant impacts to the tactical IT controls in terms of scalability and operational complexity for the IT audit community which impact the cost/effort involved in audit. The impacts are sufficient to require strategic planning and architecture upgrades for highly regulated companies. Product vendors should also be part of the advanced planning to provide cost-effective solutions.

Some of these tactical impacts can be linked to future control practices described by a number of other O-SCOA Framework requirements – such as Internet filtering & reporting, endpoint security, and Enterprise Information Protection & Control (EIPC). As organizations become increasingly de-perimeterized, several changes need to be considered from an IT audit tactical perspective:

- Control points that were centralized and external to applications and systems will change (endpoints have shifted). The shift in control points will create new scenarios of controls that are more application-centric and data protection-centric.
- Reliance and assumptions of controls over traditional internal components, such as a WAN or LAN, may no longer be relevant or appropriate (audit scope changes).
- A sampled assessment of de-centralized components may not give a clear picture of the overall IT control environment (partners spread spyware, business boundary *versus* IT boundary).
- The focus and importance of core IT systems may need to change; for example, increased reliance on data center, client, and application controls.
- Additional foundation services (identity, audit, monitoring) may need to be included in the scope of future audits.

As such, IT auditors need to understand the potential changes in their client's IT environment in order to appreciate how the goal of maintaining effective internal controls has shifted. This is crucial to the success of an effective and relevant audit.

Compliance

There is a need to build a body of best practice from both the audited and the auditor communities. Key components include the following:

- A Code of Practice and assurance process for information security governance across the scope of the shared organization/infrastructure. (The ISO 27000 series standards and certification process meet this need.)
- Approved security implementation guidelines for supporting infrastructure; e.g., desktop, server, firewall, etc. Many individual organizations have developed their own or allowed limited sharing of them within selected security circles. The industry will benefit significantly from establishing a generic set of industry-recognized profiles.
- Assurance guidelines for technology components, critical to the security of the supported information systems. (The Common Criteria meet this need.)
- Real-time monitoring processes that can detect and report potential security vulnerabilities or breaches of security.

7.10.4 Background and Rationale

Audit

IT audit services at major auditing organizations are based on and structured around industry-recognized control frameworks such as CobiT. The impact of de-perimeterization on the IT infrastructure and protection measures that are effective in de-perimeterized environments are significantly different to those in perimeterized ones – particularly with regard to perimeter firewalls and data-centric security. The auditors need to understand this, and the organizations being audited need to appreciate their responsibilities to partner with their auditors to explain how their systems meet the fundamental requirements underlying the audit objectives.

Our extensive study on prevalent control frameworks and taxonomy concluded that the CobiT high-level control objectives:

- Processes – as defined within four domains following the PDCA model (Plan-Do-Check-Act): Planning & Organization, Acquisition & Implementation, Delivery & Support, and Monitoring
- Principles or qualities of the control objectives – as defined by seven categories: Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, and Reliability of Information

are not strategically impacted by the Jericho Forum Commandments.

However, the tactical impact analysis must be derived from the prevalent IT audit practice including feedback from the IT audit community.

Compliance

In organizations where the traditional "hard" network perimeter no longer exists, a new governance model is required that ensures that each node/endpoint is fit-for-purpose.

The Common Criteria (ISO/IEC 15408) for specifying security requirements for products and systems – allow us to specify the security features of a system and how it has been developed and tested, including independent third-party checking of claims. They are organized as a set of building blocks from which a range of complete standards can be built. The building blocks specify components of security solutions or development/test approaches in a technology-independent way. Some components can be customized to particular requirements, and it is also possible to develop new components. There is a common misconception that the Common Criteria are bureaucratic and costly to follow. This is certainly true of some existing standards and evaluation methods, but the Common Criteria also allow for low-cost, non-bureaucratic standards to be built if that is desired.

Within the sphere of the O-SCOA Framework, the Common Criteria can be exploited to identify common component types and then develop a standard security functionality standard for each component. Components would include the following:

- The access device – the equipment a person uses to access a computer system.
- The server device – the equipment an automated service executes upon.
- The authentication service – to authenticate users, organizations, devices, or services.
- The authorization service – to authorize users, organizations, devices, or services.
- The audit service – to maintain and query a record of events.

7.10.5 Challenges to the Industry and Way Forward

Typical organizations moving towards a de-perimeterized environment need to take on board the following challenges:

- Expanding the corporate boundary of the network
- Thinking of the internal network as a semi-public or public network
- Pushing more applications and systems into data centers that are Internet-accessible
- Developing applications that are Internet-enabled and take advantage of security controls such as transport layer security, authentication, and authorization controls
- Relying more on endpoints in the network to protect themselves using patching, firewalling, and anti-virus technologies
- Identifying users and devices that connect to business systems and applications
- Patching and managing devices that connect to corporate systems from remote and often untrusted Internet sources

- Providing users who may be employees, customers, business partners, or third-party suppliers with access to business applications
- Providing a bridge between legacy systems and Internet-accessible services
- Supporting a variety of remote access methods through wireless, dial-up, VPN, 3G, etc.

The following sections discuss some of the key challenges that face IT auditors and those being audited when looking at a de-perimeterized organization.

Audit Planning

Before starting the audit, the auditor needs to understand the strategy that the organization is following and where the organization is along its roadmap. Planning the audit of a de-perimeterized environment is just as important as conducting the audit itself. Because of its de-centralized nature, auditors choosing inappropriate systems and controls may miss core foundation systems or waste time with inappropriate systems.

Audit Scope

When scoping a client's IT environment, care needs to be taken to ensure that appropriate systems, environments, and applications are covered to meet business and audit objectives.

Additional services may be developed to provide foundation services within a de-perimeterized environment. These services may need to be added into the scope of an audit.

Traditional centralized services may not be appropriate, if de-centralized controls have been adopted. In addition, the following core foundation capabilities will need to be covered in the scope of an audit:

- Authentication and authorization services
- Time-stamping
- Monitoring and auditing
- Encryption in transit and storage including data fields
- Endpoint security policy – firewalls, anti-virus, anti-spyware, etc.
- Application security controls, such as transaction and workflow-related
- Security at entry points, such as VPNs, remote users, wireless users
- Third-party communications
- Trust relationships with external parties – business partners, suppliers, customers
- Data center controls/SAS 70
- Management of outsourced providers

Review of Audit Assumptions

A de-perimeterized environment may lead to audit assumptions being revisited. For instance:

- *Old audit assumption*: "We can rely on centralized controls and just audit these."

  Revised audit assumption: "Several centralized foundation services may exist to support the de-perimeterized environment and they need to be included in the scope of the audit. Additionally, de-centralized controls, such as those at endpoints (clients and/or applications) may need to be looked at on an individual basis."

  Shift in thinking: IT controls will have to be moved towards endpoints such as data centers, applications, and clients.

- *Old audit assumption*: "The internal network is secure and out of scope from application audits."

  Revised audit assumption: "The internal network is or could be semi-public or public and as such all applications need to assume that the internal network cannot be fully trusted."

  Shift in thinking: The organization's internal network may no longer be truly internal – several business partners, third-party suppliers, and other users may have access to the network.

- *Old audit assumption*: "Taking a sample of systems and applications is representative of the IT environment."

  Revised audit assumption: "The scope and scale of audits may need to expand to factor in centralized and decentralized points of control."

  Shift in thinking: Each system and application will have a combination of centralized and de-centralized IT controls. Controls will be built closer to the applications and users themselves.

Performing the Audit

When conducting the audit, the auditor will need to identify where controls can be relied upon from a centralized and de-centralized perspective.

Checklists for effective IT audits are to be developed that will take into account balancing the business context served by the IT environment and associated IT controls for proper value and assurance.

8 O-SCOA Framework – Technologies

This chapter provides detailed descriptions for the Technologies components in the O-SCOA Framework:

- Endpoint Security/Assurance
- Secure Communications
- Secure Protocols:
  - — Wireless
  - — Mobile Management
  - — VoIP
  - — Internet Filtering & Reporting
- Encryption & Encapsulation
- Secure Data

8.1 Endpoint Security/Assurance

Endpoint security status can be used to enable access within a secure COA. We recognize the work achieved by the Trusted Computing Group[24] in this area, and expect that implementation of solutions suggested in this section will rely on much of the their work.

8.1.1 Problem Statement

In a de-perimeterized environment, secure collaboration between two devices is achieved by their security association rather than trying to keep the network pure. Thus there is a need to be able to validate that the endpoint is secure, and assert that status as part of any transaction.

With most current endpoint checking solutions there is an over-reliance on network-level authentication; that is, at the point at which you are able to assert a level of control over a device connecting to the network. This approach is flawed in a de-perimeterized environment, where the endpoint device connects to a "foreign" network (say a public IP, or Wi-Fi hotspot) and then connects directly to devices inside your organization using inherently secure protocols.

Thus the key question for anyone designing an endpoint security solution in a COA is: "What triggers the checking and when do you need to do it?". Any checking must extend beyond the pure operation systems checks to (potentially) include being able to assert the security status of applications that will be used in the transaction, as well as (potentially) checking that unwanted

[24] Refer to: www.trustedcomputinggroup.org.

application are not running. Such checking may be one-time, or may need to be continuous, dependent on the type of collaboration and the process involved in the transaction.

8.1.2 Why Should I Care?

Connection Issues

There are two questions to be asked when a system or user tries to initiate a collaborative session (distinct from "tries to connect", which implies that the check is only performed at connection initiation):

- Are they allowed to collaborate? Does the device and/or the user have the necessary credentials to make a connection (probably a bi-directional check (JFC#7))?
- Are they in a fit state to connect? This is a risk decision based on attributes of the system being used for the collaboration, its ability to assert its status, and the security requirements defined for the collaboration to take place.

When designing systems for use in COAs the goal should be to design out as many dependencies on the collaborating systems as possible.

The points at which trust needs to be validated will vary on the risk and the type of transaction. Some transactions will necessitate that trust can only be established at the start of the transaction, but a more preferable solution will be to perform continuous checking (a security heartbeat), and better still will be for the application itself to revalidate (or request revalidation of) the trust levels, potentially as the types of transaction being requested of the application changes (for example, requesting a bank balance *versus* transferring money).

Security status could be established via a bi-directional trust or the use of a third-party "in-the-cloud" trust brokers' service.

The addition of Trusted Platform Module (TPM)-aware software, or software download, has the potential to provide levels of trust/assurance. However, the problem with any trust system is the potential for that software or communication to be interfered with or impersonated.

Need for Secure Communication

All components of the trusted computing module(s) within a device, the anti-malware, the personal firewall, hardware, operating system, etc. need to be able to securely communicate their status.

The communication of status in a de-perimeterized environment must be vendor-neutral as no presumption can be made that a particular vendor solution will be present on either endpoint.

If a third-party or trust broker is being used to assert the status of a device, then the endpoint(s) will need to securely report their status, logs, etc. to its parent/home trust broker.

When designing a system to assert trust, then it is important to remember that the collaboration may be multi-way, or even use broadcast protocols.

Need for Remediation

Where an endpoint does not meet the required level of trust, then one option will be to allow (or force) that device to remediate itself, with the endpoint locked-out from the transaction/collaboration process until it is remediated.

Ideally, a device that requires remediating will be locked-out of all transactions (via, say, a change of rules to its personal firewall) until it has been remediated. Such lock-out and remediation must function irrespective of whether the device is intranet or Internet-connected.

Rather than bar the transaction if a device does not meet the required standard, it may be possible to modify the transaction method, or access allowed, based on the evaluated risk. A negotiation process may need to take place to establish the optimal method of a mutually trusted collaboration possible between devices. The negotiation may be direct or via a trust-broker.

Calculation of Risk

The calculation of risk and thus the decision to collaborate generally needs to be an automatic process that happens in the background without the user being aware that (if it is successful) it has taken place. Should the transaction be refused, then the workflow in establishing that connection may involve the user in an "are you sure" choice (assuming this is a user-to-system transaction and not a system-to-system transaction).

Such risk decision will be based on a variety of factors pertinent to the desired transaction, including;

- The physical/geographic location of the device(s)/users(s)
- The patch status of the device
- The operating system, status, and patch level (programs running, registry settings, etc.)
- Whether the device can safely hold data (is the container encrypted, can such a container be killed, or are its keys repudiated, etc.)
- Can it securely communicate (does the device speak the appropriate secure protocols)
- The availability of the appropriate application(s), and/or ability to downgrade the application used – see above
- The date and/or time of the transaction
- The identity of the user
- The nature of the transaction

Although some of these factors in the risk calculation can be derived, most will need to be communicated by the device in a standard, secure, and open format.

Risk calculations must be dynamic and relevant to the transaction in progress rather than a single transaction on entry to the system (or worse still, the network). Dependent on the risk, some systems and/or people may only be allowed a basic level of low-risk transaction (for example,

view-only access). A combination of the above factors combined with a risk calculation should define whether access is barred, allowed but limited, or full.

8.1.3 Challenges to the Industry

Current endpoint security solutions are proprietary, and generally designed to operate in homogenous, perimeterized environments. There is a need to embrace open standards such as:

- Trusted Computing Network (TCN) Specification (IF-TNCCS-SOH) is available for download and implementation.
- Network Endpoint Assessment (IETC RFC 5209)

Key to developing secure COA is the ability of the components that determine and/or demonstrate the security status of an endpoint device to communicate that status in a secure way, irrespective of where that endpoint device is physically located or connected.

To achieve this, the key vendors in the space need to agree an open specification/standard they will all use by which such status can be securely communicated, and then prove their interoperability.

8.1.4 The Way Forward

The ability to communicate security status will allow this information to be used by endpoint and intermediate devices in automated risk calculations.

The ability to query the status of a device, directly or via third-party brokers or other certification devices or services, has the potential to allow applications, and other devices in the path (such as identity-aware firewalls) to be able to request this information to make access decisions (both network and application), and also to set granular levels of access to both functionality within applications as well as to information.

8.2 Secure Communications

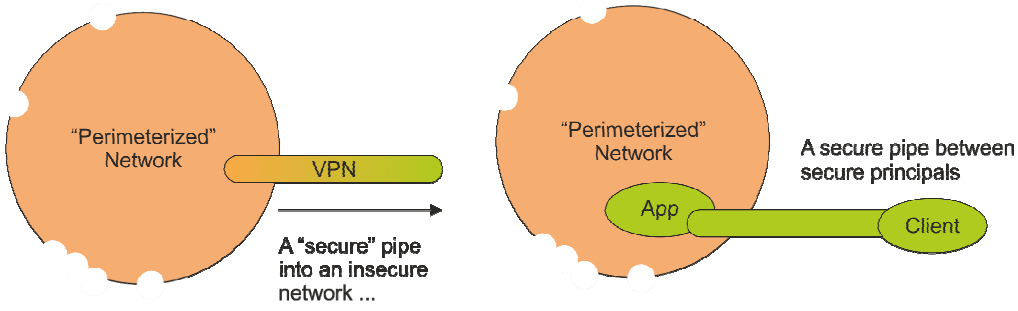


Figure 8: Secure Communication – Perimeterized Network

8.2.1 Problem Statement

In earlier times, if an enterprise presumed it had control over its network, and if it had few external connections or communication, it was feasible that the connections between operational

computers probably were not an unacceptable risk. This required that any visitors to the enterprise with electronic devices had no ability to access the network, all users were properly managed, and that they abided by enterprise rules with regard to information management and security.

This is now a rare situation. Most enterprises use computers that are connected to the Internet, employing wireless communications internally, with the majority of their users connecting to services outside the enterprise perimeter, and partners and collaborators regularly connecting to the enterprise's internal network with their own computing devices. Additionally, there is the emergence of targeting Trojans and worms that rely on our use of this old "internal trust" architecture to propagate.

In the de-perimeterized world, the use of inherently secure communications[25] is essential (JFC#4) to provide protection from the insecure data transport environment. Inherently secure communications products, services, and protocols should act as fundamental building blocks for secure distributed systems, adaptable to the needs of applications while adhering to requirements for security, compliance, and performance.

Inherently secure communications, products, services, and protocols do not introduce unacceptable business risk.

8.2.2 Why Should I Care?

Most networks are fundamentally insecure. It won't matter what infrastructure you have; if the principals on the network are trusted without good cause, the network is inherently insecure.

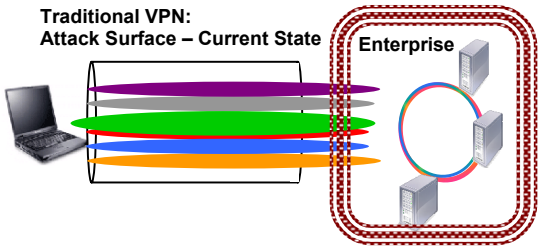
Networks can be designed to be inherently secure. Traditionally they have not been so. Relying on the good behavior of all principals on a network is a behavior that characterized the "perimeterized" world; i.e., "We have big thick walls around us and we trust everyone and everything on the inside!". This was even then a false claim. Luckily, few individuals at that time understood how to leverage this fundamental network architecture vulnerability; it was the realm of well-funded foreign state intelligence services, whose primary target was military secrets. Today, legitimate business demands for globalization and collaboration and "just-in-time everything" is accelerating the de-perimeterization of our networks.

In addition, a growing number of economically-motivated organized criminals are now taking advantage of this growing vulnerability in our network architectures. Unfortunately, our network security architectures have not been adapting to this new environment; nor have protocols, products, or services been developed to resolve this growing threat. Many organizations continue to deal with the issue by simply extending their "untrustworthy" network by the misuse of IPSec, and building VPN tunnels. The key here is in the "P", for if the central network is not "private" then the virtual network cannot be private either; to assume otherwise is to put information at risk. Simply put, the brand/image of all business organizations is reliant on secure reliable information flows.

The use of general-purpose VPNs or tunnel technology carries with it additional risks. Typically VPNs carry all of the communications between a client and set of servers and are terminated at

[25] An inherently secure communications protocol is authenticated, protected against unauthorized reading/writing (probably encrypted), and has guaranteed integrity (is non-repudiatable).

the enterprise perimeter. So, the security association is between a client computer and perimeter device, not a specific service. There are several points of vulnerability here. First, there is the potential for one protocol, once compromised, to target a different protocol or service. For example, a Trojan sent via email could actually be targeting a database server with an SQL injection attack. A second issue is that since these VPNs usually terminate at the perimeter, the information they are carrying has the least protection at the enterprise's weakest point. Thirdly, the security association is between the client and VPN service, not client and server. The following three diagrams illustrate these vulnerabilities and how they are successively minimized.

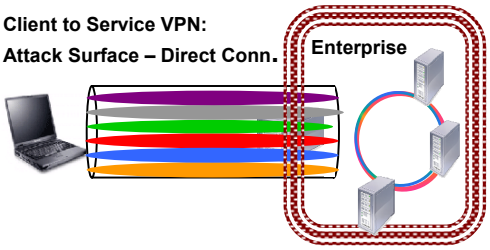


One general-purpose tunnel for all traffic:

- Weak protocols mixed with strong protocols allow malicious code to spread
- Single crypto codebase

Tunnel terminates at perimeter:

- Information exposed at weakest point
- No security association between client and server
- Traffic mixed on intranet
- Easy to inspect traffic

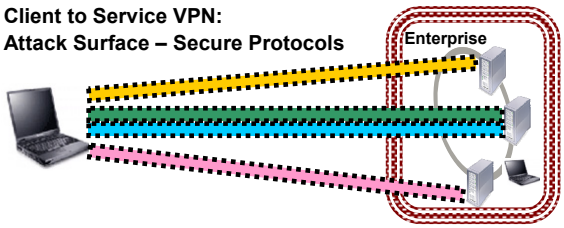


One general-purpose tunnel for all traffic:

- Weak protocols mixed with strong protocols allows malicious code to spread between protocols
- Single crypto codebase

Tunnel terminates at service:

- Direct security association between client and server
- Traffic not available to intranet
- Perimeter not needed
- Difficult to inspect traffic if still using perimeter controls



Tunnel terminates at service:

- Direct security association between client and server
- Traffic not available to intranet
- Perimeter not needed
- Difficult to inspect traffic if still using perimeter controls

Applications use built-in tunnel capability:

- Each protocol isolated
- Only services/ports in use exposed
- Greater risk of poor tunnel implementations

8.2.3 Recommendations/Solutions

Rather than use a general-purpose tunnel, applications should incorporate their own secure tunnel technology. This technology, referred to here as inherently secure protocols/communications, improves security in several ways:

- It supports the capability for the client to create a secure association directly with the server or service.
- The scope, or attack surface, is limited to the specific service or protocol involved in the communication. This limits the exposure both by reducing the number of protocols involved to just those associated with the requested service, and also by limiting the number of machines involved – from potentially the entire intranet, to only the servers related to the invoked service. So, as in the example above, if a client is accessing email using a direct connection and sending a Trojan targeted at an SQL protocol, it will only reach the mail server, which will ignore it.

Some specific examples of applications that include inherently secure protocols as part of their communication capability are mentioned below.

As a minimum, all sensitive information should be communicated in an inherently secure manner which does not rely on the underlying security of the communications infrastructure of the collaborating organizations. Organizations should architect inherently secure methods of communications developed using products, services, and protocols that are designed from the ground up always to meet the users' expectations of privacy, safety, and legitimacy, delivered through effectively managing the CIA&A of all the relevant principals. Imagine a world where all communications of sensitive information assets occur in a secure manner which cannot be cost-effectively compromised, and all non-public information is transmitted using appropriately secure communications products, services, and protocols that integrate closely with each application and user.

The communications products, services, and protocol(s) used should have the appropriate level of data security and authentication. The use of a protective security wrapper (or shell) around an application protocol may be applicable; however, the use of an encrypted tunnel negates most inspection and protection and should be avoided in the long term.

It is essential that the properties of any protocol that underpin the trust relationships involved are transparent. Otherwise, mismatches or implicit contextual assumptions will result in the associations between identities, keys, permissions, and obligations between communicating parties. Basically, inherently secure communications, products, services, and protocols will not introduce unacceptable business risk. Inherent security will become an "expectation" similar to "Dial Tone". "Do you remember when they used to transmit our information without securing it!" will be similar to "Do you remember when they used to deliver our mail by pony express!".

8.2.4 Background and Rationale

Some organizations are utilizing new protocols to enable secure application-to-application communication over the Internet. These are business-to-business protocols; more specifically ERP-system-to-ERP system protocols that include the required end-entity authentication and

security to provide the desired trust level for the transactions. It takes into account the Jericho Forum Commandments on context (JFC#3), trust levels (JFC#7), and risk (JFC#1).

There are a wide variety of application (system-level) protocols in use, but a much smaller number of secure protocols to choose from. In practice, integration may be poor or impossible, designers may make "one size fits all" assumptions (JFC#3) about the security of a protocol for a particular purpose, or the requirements actually achieved may be short of the ideal when nominally secure protocols are built into actual implementations. The resultant protocol TCP/IP "stack" will therefore be unfit for use in the de-perimeterized world.

The Need for Open Standards – To Provide Interoperability

The reason that the Internet still uses a set of insecure protocols is because these protocols are *de facto* lowest common denominator standards, which are open and free for use. If all systems are to interoperate – regardless of operating system or manufacturer, and be adopted in a timely manner – then it is essential that protocols must be open and remain royalty-free.

The Need for Default Security: Secure "Out-of-the-Box"

For inherently secure protocols to be adopted, it is essential that systems start being delivered with only inherently secure protocols, or with the inherently secure protocol as the default option.

Working Towards the Future

Currently, organizations have limited choices depending on their requirements and constraints for flexibility/manageability, trust, vendor interoperability, the need to deploy client software (agents, browser plug-ins, etc.), and performance.

Vendors are starting to offer hybrid protocol solutions that support multiple security policies, system/application integration, and degrees of trust between organizations and communicating parties (their own personnel, customers, suppliers, etc.). Unfortunately, the inevitable result is proprietary solutions that are unlikely to interoperate, and whose security may be difficult to verify. It is, therefore, important to start to classify the various solutions that an organization uses or is contemplating using.

Ultimately, if a device is capable of working using only inherently secure protocols then it should be possible to utilize a TCP/IP stack that is immune from attack (other than a DOS attack) as any protocol that is not inherently secure would be simply ignored.

Additionally, if an organization's border will only permit inherently secure protocols (potentially filtered at all routers) then the need for other traditional border protection may become irrelevant.

8.2.5 Challenges to the Industry

Inherently secure protocols must be open, royalty-free, and interoperable (JFC#3).

Current proprietary inherently secure protocols should be made fully open, royalty-free, and documented, or discontinued.

Inherently secure protocol reference implementations should be released under a suitable open source or General Public License (GPL) arrangement.

Companies should review their products, protocols, and services and consider replacing inappropriate products, protocols, and services; i.e., those that are not inherently secure.

Organizations should disclose to the public the secure communications capability of transaction processes dealing with sensitive information assets; i.e., a user will be able to identify whether inherently secure communications are in use. An ISC[26] certification scheme would be valuable here.

End users should be educated on the value of inherently secure protocols and how to recognize when they are in use.

8.2.6 The Way Forward

Requests to industry security standards groups:

- Develop inherently secure communications; guidelines, patterns, use-cases, and standards
- Develop examples of protocol misuse
- Refine the protocol usage matrix below

Requests to industry architecture standards groups:

- Refine architecture development methodologies like TOGAF to specifically incorporate security elements such as inherently secure communications.

[26] Internet Systems Consortium (ISC); refer to: www.ics.org.

Protocol Usage Matrix

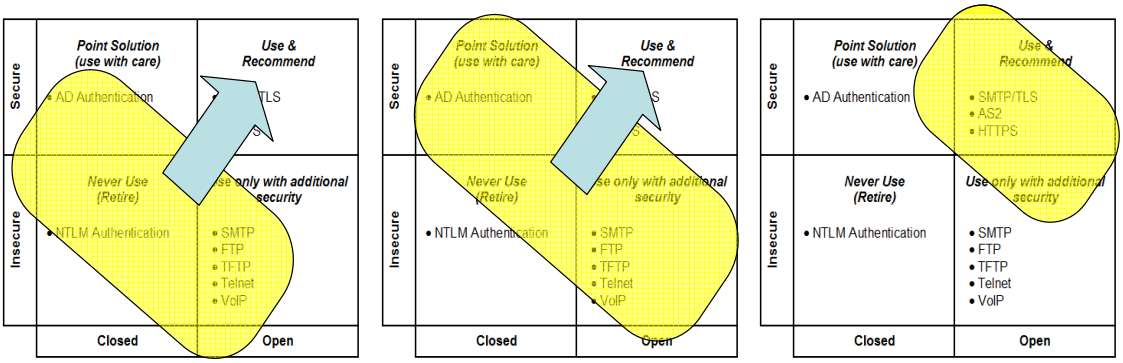
The matrix below is a simple method for organizations to assess the protocols in use within their systems.

	Closed	Open
Secure	Point Solution (use with care) AD Authentication COM	Use & Recommend SMTP/TLS AS2 HTTPS SSH Kerberos
Insecure	Never Use (Retire) NTLM Authentication	Use only with additional security SMTP FTP TFTP Telnet VoIP IMAP POP SMB SNMP NFS

Figure 9: Protocol Usage Matrix

Evolution not Revolution

Today we predominantly operate in the lower-left quadrant of the protocol usage matrix, above. There is an immediate benefit that can be gained by analyzing existing protocols in use and moving to secure versions. Most modern systems should easily be able to eliminate the reliance on closed and insecure protocols.



Today Near Future Tomorrow

Figure 10: Protocol Usage Future Directions

As we progress, new systems should only be introduced that either have all protocols that operate in the Open/Secure quadrant, or operate in the Open/Insecure on the basis that anonymous unauthenticated access is the desired mode of operation.

8.3 Secure Protocols: Wireless

8.3.1 Problem Statement

For mobile working, connectivity via wireless – whether inside the corporate environment or via publicly available hot-spots, Wi-Fi, Wi-Max, or Cellular Data (GRPS, Edge, 3G) – offers the ability to roam while remaining connected to your resources. The issue for most corporates is how they provide secure connectivity for their mobile workers, and end up with a trade-off of usability, cost, complexity, and functionality.

For most mobile usage outside of the corporate WAN the use of IPSec VPN and 2-factor authentication is the most common standard, but whilst fine for static connectivity, say in a hotel room, it is restrictive for quick use "on-the-go". The use of wireless inside the corporation is a known security risk and is generally implemented in a number of ways:

- Totally untrusted – The users still need to use VPN and 2-factor authentication; this does not encourage "occasional" use, neither is it user-friendly.
- Authenticated usage – Using WPA2 and Radius or similar AAA solution users can enter a password, or 2-factor authentication that permits access but secures the air interface.
- Background authentication – If the connection of the PC uses a directory service which performs 802.1x authentication of the hardware and validates the user's cached credentials, this would provide the most user-friendly solution.

The flaw in all these solutions is that there are actually separate problems:

- Protection of the air-interface against unauthorized usage
- In the public space, the protection and generation of revenue
- In the corporate space, the protection against intrusion inside the corporate boundary
- Authorization of the user to make a connection into the corporate WAN
- Privacy and confidentiality of data transferred over the connection

8.3.2 Why Should I Care?

The deployment of wireless within an enterprise exposes the corporate network outside the physical constraints of the building. Thus, any mis-configuration or weakness effectively de-perimeterizes the whole organization.

Current "secure" solutions are expensive and costly to manage and only work within a limited enterprise deployment. Conversely, systems that are secure (through employing inherently secure protocols) can utilize any wireless solution (corporate or public) without need for complex location awareness. With such a secure de-perimeterized solution, it is possible to

implement a much simpler infrastructure; thus achieving significant cost savings. In this new environment, risk to the corporation of unauthorized use is substantiality reduced, and while the business may choose to provide an open solution, they may still wish to implement some degree of connection authorization, thus guaranteeing their wireless users quality of service.

8.3.3 Recommendations/Solutions

Looking at these problems both as separate problems and in a de-perimeterized manner reduces the complexity and provides an increase in security.

8.3.4 Background and Rationale

Need for Inherently Secure Protocols

Provided that the protocols used by the end-devices are all inherently secure protocols[27] (JFC#4), all end-devices are capable of being deployed on the raw Internet (JFC#5), and it then becomes irrelevant whether the end-device is connected on a public network, public wireless of whatever type, or a privately managed network – whether wireless, or wired.

Operating in this environment, the question then arises: "Why would a company need a private wireless network?" To which the answer is: "They may not any more".

The provision of a private network in a de-perimeterized world is now not driven by the need to provide security. Instead, private networks (wired or wireless) are areas of network connectivity where a company can provide control over the traffic, ensuring that adequate bandwidth is available where they require it, and that performance meets the needs of the applications they are using over that network. This is a quality-of-service issue and has little, if nothing, to do with security.

Need for Connection Control on Wireless and Wired Networks

When implementing a wireless infrastructure for corporate use in a de-perimeterized environment, why can you not simply run an open network? This may be a viable option for a company that has non-corporate devices on its network every day.

The other option is to implement background connection control based on 802.1x or similar connection control mechanism. Authentication may be based on user or device or both (JFC#6). This will allow companies to implement quality-of-service measures (rate limiting/bandwidth control) based on the device trying to connect. It could also require non-company devices (devices not inside the realm of your 802.1x credentials) to authenticate manually – for example, via a redirected web page – similar to a hotel or public hot-spot.

8.3.5 Challenges to the Industry

- Companies should regard wireless security on-the-air interface as a stop-gap measure until inherently secure protocols are widely available.

[27] An inherently secure protocol is authenticated, protected against unauthorized reading/writing (probably encrypted), and has guaranteed integrity (is non-repudiatable).

- The use of flexible interoperable 802.1x integration to corporate authentication mechanisms should be the out-of the box default for all Wi-Fi infrastructure.
- Companies should adopt an "any-IP address, anytime, anywhere" (what Europeans refer to as a "Martini model") approach to remote and wireless connectivity.
- Provision of full roaming mobility solutions that allow seamless transition between connection providers.

8.3.6 The Way Forward

Accelerating the use of inherently secure protocols will allow enterprises to provide a simpler, yet more secure and holistic approach to remote and mobile access.

8.4 Secure Protocols: Mobile Management

This section augments Section 8.3, highlighting the practical problems in the operation of wireless networks that need to be solved as responses to the effects of de-perimeterization deliver the security architectures to enable secure roaming.

8.4.1 Problem Statement

For a truly mobile device, operating to de-perimeterized principles, a wireless connection is required to achieve optimal connectivity while roaming. From a security stance, all foreign networks, wired or wireless, should be regarded as hostile. However, the ability to make a transparent wireless connection remains elusive due to the lack of standards in this area (especially around Wi-Fi) that inhibits secure operation in de-perimeterized environments.

8.4.2 Why Should I Care?

The use of mobile devices and applications designed to the Jericho Forum blueprint[28] implies that mobile working should be a seamless user experience.

By applying the Jericho Forum Commandments and applying other generic security measures appropriately, working in the wireless world in which the end-device is assumed to be in a hostile environment (whether on an internal or public IP address) may be assumed to be safe.

However, if working in a foreign (or public) networked environment, whether wired or wireless, the user has no control over their network, from quality of service, connection authentication, or cost of the connection, thus negating the advantages that a de-perimeterized solution provides.

[28] The term "blueprint" was adopted by the Jericho Forum to capture how the Jericho Forum Commandments define the security principles for assuring effective security in de-perimeterized environments, and their use to validate how this O-SCOA Framework supports architecting secure systems for de-perimeterized environments. See also Chapter 3.

8.4.3 Challenges to the Industry

In a Corporate Environment

In both a wired and wireless corporate environment the primary problem to be solved is whether the device is permitted to connect to the network and consume both network and corporate resources – primarily bandwidth, both intranet and Internet.

In an environment where corporate devices are connecting to a corporately managed network, access authorization solutions can be performed using 802.1x or other such access mechanism. Integrating this with RADIUS and corporate directory services will ensure that the connection is transparent to permitted users or devices.

Identity federation has the potential to allow devices from business partners and other trusted users also to authenticate. Identifying those users as "trusted" means they could potentially be subject to different bandwidth and quality of service rules.

For devices unable to authenticate (probably guests/visitors) the connection will depend on corporate policy with the device possibly being allowed to connect subject to an interactive user login. While transparent Internet access via a wired connection is feasible, many companies will be reluctant to extend the same openness via a wireless network for fear of uncontrolled abuse by the non-visitor.

In an External Corporate Environment

In an external corporate environment the issue is as above, but reversed. It will depend on what facilities they have in place to manage guest or visitor connectivity. In a de-perimeterized world they can safely allow connections using their network.

In a Public Environment

Once outside the managed corporate environment, the problems begin with variable standards to manage connection. In the Wi-Fi domain, there is the promise of a fast and simple connection with performance equivalent to a wired connection. However, with no standard for authentication and charging, most users connecting to public Wi-Fi attempt but rarely complete the connection. With no public "cell-handover", use while mobile in this environment is almost always doomed to failure and thus restricted to "static" use in hotels (generally as a wired alternative).

In the cellular world, the connections are generally slower but access is more transparent to the user. However, high data charges and even higher roaming charges make this restrictive for many users, although use while on the move usually works well and is reliable.

Issues when Outside the Corporate Environment

- Authentication to a foreign network is rarely transparent.
- The cost of the connection varies with the medium used and the location.

- There is a diverse set of charging and payment/collection mechanisms.
- A least-cost/highest-bandwidth connection cannot be automated (scripted) with an increasing number of options available (Wired, Wi-Fi, WiMax, GPRS, 3G).
- No standard method exists for understanding cost and bandwidth for making connection options based on corporate policy (and the ability to express that policy electronically).

There are companies who specialize in aggregating various forms of remote connectivity and, when working in a part of the world where agreements to such arrangements are in place, reasonably seamless connectivity can be achieved. However, this is neither true roaming nor a true de-perimeterized environment. Where applications are reliant on session integrity (e.g., voice) then the application needs to design out, if possible, the effect of a variable quality connection that mobile usage delivers.

Assumptions

When connecting via wireless, the security of the data should not be reliant on the network, because the transport mechanism will provide no integrity for the data, and the confidentially and integrity aspects of security can only be provided by using inherently secure protocols (JFC#4) and secured data (JFC#11).

Inspection and understanding of the protocol in use (while not of the data itself) will allow the traffic type to be determined and thus allow quality of service features to be applied where feasible. The origin and destination of data packets can be inferred while operating in any network environment.

8.4.4 The Way Forward

Key to making transparent mobile de-perimeterized working a reality is the ability to express the Wi-Fi hotspot "contract" (rate and other costs) electronically. The client must also transparently try to authenticate the network itself (JFC#7), understanding http/https redirected login pages and 802.1x, such that an automatic decision can be made to allow (or deny) a connection based on corporate or personal policies.

8.5 Secure Protocols: VoIP

8.5.1 Problem Statement

With many large organizations seeking the cheapest options for internal long distance telephone calls, using the Internet as a bearer is a very attractive option. Voice over IP (VoIP) is being increasingly deployed in the corporate environment to take advantage of an organization's existing Internet connections.

However, the problems inherent with normal phone conversations still exist in VoIP, with additional problems added. Conversations can be monitored, hijacked, overheard, and so on. With wire-connected telephone conversations, interceptions are more difficult unless undertaken by lawful interception, but with Internet connections being used, interception, recording/replay, etc. can happen anywhere on the network. VoIP has been sold using the flawed assumption that

sharing the data infrastructure is acceptable because the internal network is secure. The lack of security built in to VoIP products and protocols means that companies are unable to deploy VoIP securely in a de-perimeterized environment where the return on investment is significantly more complex than just the replacement of an existing internal telephone exchange.

8.5.2 Why Should I Care?

Potential cost saving on long distance telephone/conference calls is a strong corporate driver, and VoIP may be (incorrectly) considered no less secure than standard phone calls. Verbal communications are as important to manage corporately as written communications are, as in many jurisdictions legally binding oral commitments may be made or breaches of ethics/law may be committed. Within a closed corporate environment, anyone with access to the network would be able to tap into conversations and record them for later analysis, etc. With the increasingly dissolving corporate perimeter, this vulnerability becomes greater. Disclosure of important information through the use of VoIP may be interpreted as constituting a legal offence of due diligence, because organizations should rightfully know that it is inherently insecure.

Vendors are attempting to overcome these issues by developing proprietary protocols to secure inter-organizational communication – generally by tailoring the main communications protocol used in VoIP (Session Initiation Protocol (SIP)). These vendors, in order to protect their investment in firewall products, often wish to perpetuate the perimeter mindset – but even within a corporate perimeter (if maintained) VoIP is not secure. Other vendors market proprietary products that enable VoIP between individual users, but these are not suitable for corporate use because one would have to know all likely recipient phone numbers or be able to find them on the vendor's Internet-based directory, and this is not acceptable for most enterprises.

8.5.3 Recommendations/Solutions

The protocols used to enable VoIP do not meet the requirement to utilize inherently secure protocols[29] (JFC#4), and neither are the system and end-devices (phones) capable of being deployed on the raw Internet (JFC#5).

Currently, corporate VoIP deployments generally make the flawed assumption that the corporate intranet is secure (JFC#11) and thus placing corporate voice traffic over a single shared network is an acceptable risk.

In a corporate environment, there is a need for a single VoIP system and associated enterprise directory to support a wide variety of end-devices – from hardware (dedicated) phones, to soft-phones and VoIP phones embedded into mobile/cell devices.

Clearly this mix of VoIP devices dictates the need for interoperability and an open, inherently secure protocol that will enable an enterprise to deploy a device-agnostic VoIP infrastructure giving a feature-rich, yet flexible environment that extends beyond the enterprise's perimeters. Such a system should work securely across both the enterprise and consumer/SME environments (JFC#3). This ability has been demonstrated with the GSM/GPRS/3G mobile standards which is based on an open, non-proprietary system.

[29] An inherently secure protocol is authenticated, protected against unauthorized reading/writing (probably encrypted), and has guaranteed integrity (is non-repudiable).

8.5.4 Background and Rationale

Current Industry Position

VoIP uses a mix of proprietary protocols (tailored SIP and others) and generally defaults at the basic level (reduced operational capability) to the SIP protocol. The VoIP product vendors simply accept this situation. With each vendor tailoring their product's use of SIP differently, there is the potential for vendor lock-in across an organization, and for interoperability problems in establishing calls where different and potentially incompatible products and services are in use at each end.

Need for Open Standards

The reason that the Internet still uses a set of insecure protocols is because these protocols are *de facto* lowest common denominator standards, which are open and free for use. If all systems are to interoperate – regardless of operating system or manufacturer – and be adopted in a timely manner, then it is essential that protocols must be open and remain royalty-free (JFC#4).

Secure "Out-of-the-Box"

All components in a VoIP implementation:

- Should be secure "out-of-the-box" according to an industry agreed profile
- Should maximize interoperability
- Should be capable of withstanding attack (JFC#5)

Additionally, if a VoIP environment is to be successful, then the end-devices must be capable of being securely maintained and updated "down the wire" – so an update methodology should be built into devices and be part of any secure VoIP standard (JFC#8).

End-User/Mutual Authentication

Potentially, a VoIP deployment inside the corporate environment can in some cases mirror a Plain Old Telephone Service (POTS) deployment and use no authentication based on the compensation of a physical (building) security boundary.

However, in a true de-perimeterized environment, VoIP phones can be deployed in workers' homes, hotels, temporary location, mobile cellular devices, and other insecure environments. Thus the device and protocol should support a standard and strong method of strong mutual authentication (JFC#7 & JFC#8).

Self-Defending Phone

Because VoIP is reliant on processor/software within a proprietary phone or provided as a soft client, it cannot be assumed that the device is fully protected against malicious software, or is fully patched. Also, a VoIP phone must be capable of surviving safely when directly connected

to the raw Internet (JFC#5). Thus, a VoIP phone should only use an inherently secure protocol (JFC#6). The device should ignore (black-hole) all other protocols.

VoIP Protocols

Any secure VoIP protocol must be open and interoperable. The protocol must be capable of ensuring:

- Secure communications – specifically multi-hop (end-to-end encryption)
- Organizational/business functional requirements, such as forwarding, conferencing, etc.
- Control and configuration of the end-device
- End-device update/maintenance/remediation
- End-device and controller authentication
- Strong and mutual user authentication (user-device, user-user, where required)

8.5.5 Challenges to the Industry

- If inherently secure VoIP protocols are to become adopted as standards then they must be open and interoperable (JFC#4).
- Companies should pledge support for moving from proprietary VoIP protocols to a fully open, royalty-free, formal standard.
- A secure VoIP protocol reference implementation should be released under a suitable open source or GPL arrangement.
- All vendors should review their products and associated protocols and move swiftly to replacing current insecure or proprietary usage by inherently secure VoIP protocols.
- End users should demand that VoIP protocols should be inherently secure.
- End users should demand that VoIP protocols used should be fully open.

8.5.6 The Way Forward

When a VoIP device is capable of working using only inherently secure VoIP protocols, then it should be possible to utilize a TCP/IP stack that is immune from attack (other than a DOS attack), as any protocol that is not inherently secure would be simply ignored. This will allow VoIP to be deployed in a single phone system independent of the network.

8.6 Secure Protocols: Internet Filtering and Reporting

8.6.1 Problem Statement

In an environment where access to a secure computing device is governed and controlled by inherently secure protocols, the problem still remains of how access to untrusted environments such as the web is controlled.

When accessing the web, three problems exist:

- Ensuring that where you browse is in line with the applicable (corporate, country, personal, or home) policy on web browsing in the enterprise from which you are browsing
- Ensuring that what a web server delivers back is free from malicious content
- Ensuring that all end-devices, no matter where, or how they are connected, are appropriately protected

Existing solutions involve installing filtering solutions in a DMZ which generally cover only those users inside the intranet. The same level of filtering is rarely available for SME or home users. Where a corporate policy exists for remote users, it involves either leaving mobile users unprotected or insisting that all web access requires that the user first initiates an authenticated VPN tunnel back to the corporate environment.

8.6.2 Why Should I Care?

Browsing the web is a risky pastime:

- Unsuspecting users who are deliberately lured to web sites by unsolicited emails
- Inattentive users who follow-up on URLs that are deliberately mis-spelt in the hope of luring the unsuspecting browsee
- Careless users who stray to sites that are clearly inappropriate or visit an appropriate site that has been hacked and malicious code inserted

There is a need to ensure that users are provided with a web browsing experience that both protects them from inadvertently straying to inappropriate[30] sites and ensures that wherever they browse the data returned is free from malicious content.

As end-computing devices are moved into a de-perimeterized world, it is essential that all data feeds have adequate levels of integrity irrespective of their physical location/connection.

[30] An inappropriate site could be defined by corporate policy, local legal restrictions, or age restrictions.

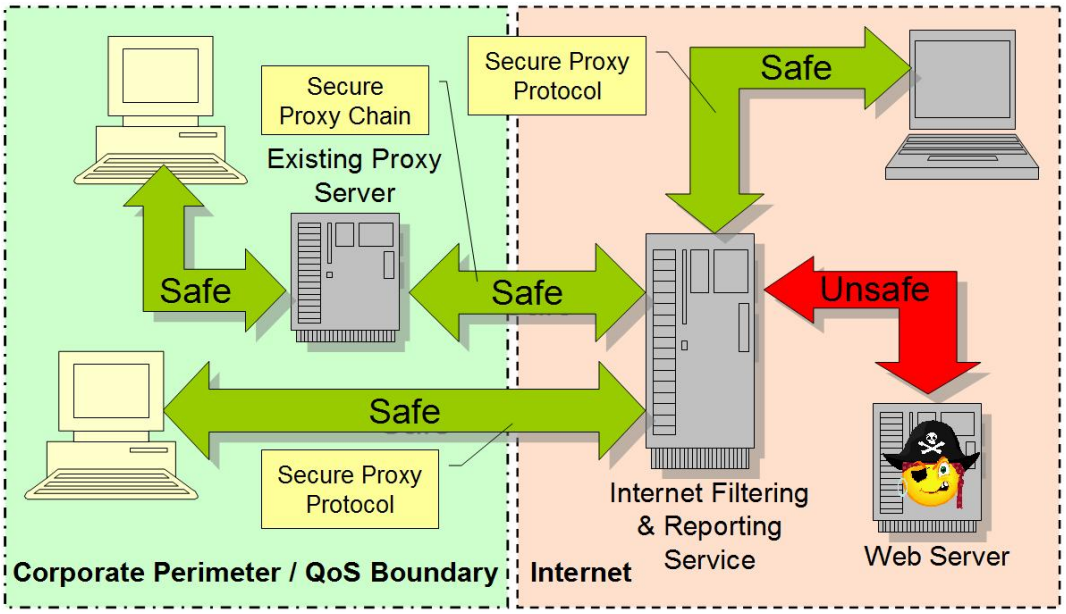


Figure 11: Safe versus Unsafe Connections

8.6.3 Recommendations/Solutions

There are two separate problems to be solved:

- An architecture that allows secure operation in a de-perimeterized environment
- The provision of a distributed filtering service

8.6.4 Background and Rationale

Architecture – A Service or Internal Solution?

In a truly de-perimeterized environment, whether this is provided as a service or as an internal solution should be irrelevant. In the interim, as the computing world migrates to a de-perimeterized world, this does have relevance and will probably be decided by the company stance on how such services are provided.

For the company that will provide this internally, this is simply a service that resides in the DMZ (or multiple DMZs) capable of accepting connections from either roaming devices on the intranet or internal devices on the Internet.

For the company that prefers to buy this as a service, existing corporate proxies can proxy-chain to the service allowing connection to intranet clients, while corporate devices on the Internet are capable of connecting to the service directly.

Achievement of 100% Web Filtering

To ensure that 100% protection exists at all times, all web traffic, regardless of where the device is physically connected (JFC#5), must be filtered.

There is an issue when a remote user needs to make an initial local connection for authenticating/paying for access when typically using a local hot-spot or hotel. This issue is compounded by the plethora of web redirection methods for authentication/payment.

There is a need for a standard, agreed method/protocol for web charging to be agreed by the industry, thus allowing a standard secure interface to separately handle those access requests.

Connection from the End-Device to the IFR Service

The proxy connection should be both mandatory and secure, allowing the passing of the credentials of both the device and the user (JFC#6 & JFC#7), together with other essential user attributes to be passed, thus enabling:

- Permission to use the service and possibly charging based on the end-device and/or authenticated user

  This implies that a third party, external service provider would be able to allow access to their services, based on being able to establish a user as part of a company with whom they have a current contract to provide filtering services.

- Access rules to web sites applied based on end-device and/or authenticated user and user attributes

- Full logging by device, user, and other group attributes

Filtering Features

Most of the filtering features are available in existing products available today. However, operating in a de-perimeterized environment will necessitate operating in a distributed environment, where multiple, replicated IFR environments allow users to connect to the local service or DMZ while common filtering rules are applied and reporting is consolidated into a central report interface, irrespective of the actual hardware or route used to access the Internet. Key features include:

- Full use of the credentials passed to services, allowing the implementation of rules, filtering, reporting, and granular access by user-name, machine-name, user's business, and business groups.

- Passed user information and business hierarchy information must support a variety of browsers or be browser-independent.

- The ability to define access, by web site category and time of day (local time required), total access time, and/or limit/throttle data throughput.

- The ability to force the redirection to an Acceptable Usage Policy or Standard (AUP/AUS) page on first use by a user and/or at defined periods thereafter. The AUP page should cope with multi-lingual options.
- Should a site being accessed not be categorized, then the options should be to fail open, to categorize using an AI engine, or fail closed.
- All denial screens should be customizable and contain the reason for denial together with the option for users to request approved override and/or re-categorization. These requests should be directed to the appropriate person in the IFR system (management) hierarchy or optionally should integrate with an external workflow program.

Filtering Capability

Key features include:

- Standard URL filtering by database lookup of known categorized sites with corporate-wide blocking of standard blocked categories (hate, criminal methods, racism, etc.)
- A wildcard capability for black-list and white-list; for example, http://*.my-company.com
- Sufficiently granular categorization of sites (40 plus) + subcategories if required
- Intelligent handling and differentiation of port 80 tunneling traffic, such as IM, Limewire, Skype/VoIP, video and audio stream, with the ability to handle ports other than 80 & 443 (for video stream, etc.)
- Inspection of https for malicious content, and/or a definable policy for how https is handled when scanning for potential malicious/inappropriate return traffic
- The ability to identify proxy-sites that deliberately mask the actual URLs as well as those that accidentally mask/bypass the URLs, such as those that may be cached
- Blocking by computer name and/or individual user (typically for shared accounts or kiosk-type systems) or restriction to a list of URLs – in addition the ability to restrict web access to a paired computer and user account – for example, only the user account "kiosk1" on computer "pc-kiosk1.mydomain.com"
- Blocking filtering by attachment/file-type and the ability to identify and filter on content (such as streaming media) rather than URL
- The ability to allow access to a single site but block (for example) streaming video, or at a more generic level allow the category "sports sites" but disallow streaming media from those sites
- Banner/advert replacement or blocking, to minimize page distortion or corruption; the option of replacing adverts with key messages
- The ability to white-list sites or groups of sites based on individual users or groups of users (preferably using integration with existing groups – say from active directory)

Screening for Malicious Content

- In a de-perimeterized environment, an untrusted web site needs to have its trust level raised to ensure the user is presented with browsing that is 100% free of malicious content.
- The systems should bar known sites with malicious code on that site.
- Scanning of files and other non-HTML code for viruses and malicious code.
- Use of heuristic detection to ensure a 100% malicious code browsing experience.
- The guarantee of zero malicious content (ActiveX, Files, Downloads, ZIP, Java, etc. Spyware, including poisoned links).
- The option to block files (such as ZIP files) that are password protected such that their files contents cannot be inspected to ensure they are clean.

Service Provision

In an externally provided service, this service should:

- Be tiered to the Internet at a suitable level.
- Have access-points or POPs that are globally available, thus ensuring that the mobile de-perimeterized workers take only a short hop to the nearest POP and from there directly to the Internet; multiple global POPs also provide global load-balancing and resilience.
- As a global service, there needs to be 24x7 support.
- With a global external service, the only component should be the secure interface between the local browser and the service, thus minimizing upgrades or changes which are the responsibility of the service provider.
- Once filtered; all protocols between systems must be inherently secure (JFC#4).

Systems Management

- The ability to allow management at a business, sub-business, group, or user level, and the ability to allow groups within groups for ease of long-term management
- Simple management interface, allowing either centralized or distributed business day-to-day management at appropriate levels within the business
- The ability to define granular, hierarchical access with different access privileges, and abilities for administrators of the system access to configuration, rule-sets, management, logs, reports, etc. (JFC#10)
- Fast replication of rule-set changes, across all global systems

Logging and Reporting

The features required by such a service include:

- The ability to automate/schedule and run predefined reports and custom reports that can be distributed by email.
- Hierarchical access, with restrictions on those people able to run reports that identify named users. Audit trails and alerting (via email) should reports on identifiable users be requested to ensure the privacy of individuals is safeguarded (JFC#10).
- The facility to anonymize the usage so that the service providers, and or managers, can see usage (and abuse), but are not able to identify the individuals.
- The ability to report the extent of Internet use, not just by individuals, but also aggregate to departments and locations, with suitable safeguards on individual privacy.
- Real-time reporting on filtered conditions to monitor for specific occurrences.
- Retention and archiving of log data, of a quality and integrity enabling it to be usable as evidence in a potential court case.
- Configurable data retention policies, to meet business, industry, regulatory, and/or country-specific requirements.
- Browser type and version detection and reporting.
- Encryption of all log data – if on a shared database.
- The ability to back up all logs, configuration, data, etc. (but in encrypted form, thus allowing both storage off-site and also proof that that data has not been tampered with).
- Tripping and alerting (via email or even SMS) on:

  — Categories and keywords

  — Excess use/threshold trip

  — Excess blocking/threshold trip
- Potential (bot) access to suspect sites (typically an infected computer “calling home”).
- XML for standardized reporting (with other security tools).
- Aggregation of data from global proxies into a single interface or a single report.
- Ability to give an accurate figure of unique users over a defined period (potentially to assist with charging)

8.6.5 Challenges to the Industry

- We need a “standard” for web page redirection that allows a minimal subset of protocol exchange to allow access to be granted by either password, token, certificate, pre-authentication, or payment card.

- The industry needs to agree a standard mechanism for secure proxy connectivity with credentials being passed.

8.6.6 The Way Forward

Accelerating the use of inherently secure protocols for proxy connections, with the ability to use those protocols either within the corporation or outside, will allow enterprises to provide a simpler yet more secure and holistic approach to web access.

8.7 Encryption and Encapsulation

8.7.1 Problem Statement

How you make a secure, trusted connection over the Internet is one of the key debates as the industry strives for de-perimeterized solutions that it can implement in its existing systems.

To the charge that the protocols they are using are inherently insecure, the unenlightened reply from the industry is "no problem – we can encapsulate it in a VPN tunnel", to which usually they mean an IPSec tunnel.

8.7.2 Why Should I Care?

The use of VPN tunnels, while appropriate in a few cases to solve particular security problems (see later), has no value in a de-perimeterized future.

A laptop on the end of an IPSec tunnel may have been authenticated onto the network with two-factor authentication, even endpoint checked, but is still as vulnerable to the worm, virus, or hacker in the same ways as any other computer on the network to which the IPSec tunnel terminates.

8.7.3 Recommendations/Solutions

Enterprises should plan for remote working solutions that do not rely on VPN tunnels, but instead utilize inherently secure solutions, allowing working directly in the Internet.

The industry should reject the use of VPNs to encapsulate insecure protocols, and work to support, use, and develop inherently secure alternatives.

8.7.4 Background and Rationale

Tunnels are Point-to-Point

A tunnel is just that. It connects a start to a destination and forces all traffic to go down it. In the corporate environment, that IPSec tunnel is often used to connect remote computers into the corporate environment, by extending the corporate perimeter to the device in question.

Even though the resources you are trying to access may be a few miles away, your data may travel half way round the world to where the tunnel terminates, only to return to the system you are trying to access.

Tunnels are Generally Singular

Most VPN tunnels are set up as singular entities. There is no concept of the opportunistic creation of on-the-fly tunnels, or the creation of multiple tunnels each with the most efficient route for each transaction.

In a de-perimeterized world, a device should be routed to its resources by the most efficient method. Moreover, individual applications on a device should each be able to be individually routed to their destination.

Tunnels Need Creating

The creation of an encapsulated, encrypted tunnel requires negotiation and set up, not only for authentication but also negotiation of the standards to be used. Generally, trying to get a reliable tunnel created between two different vendors is impossible, and certainly not reliable for *ad hoc* or on-the-fly tunnel creation.

Inspection, or Lack of it

Whereas an inherently secure protocol using either IPv4 or IPv6 will allow limited inspection, even if the data cannot be read, data encapsulated in a tunnel cannot be inspected in any way. All that can be understood is the start and termination points of the tunnel.

There are circumstances where this may be desirable, where the anonymity of the packets is desirable because of deduction that could be made from the headers. However, if security at this level is required, IPSec will almost certainly not be the technology of choice.

Where to Use

- VPN tunnels: These are a valid stop-gap solution for connecting remote workers back into the still-perimeterized corporate environment.
- Site-to-site connections or island-to-island connections: In the transition to a de-perimeterized architecture, where an area of secure connectivity is connected to another area of secure connectivity, this will be a useful solution.
- System-to-system: Here a system that requires to be semi-permanently connected to another system could validly use a VPN tunnel.

Where Not to Use

Tunneling technology should not be used to encapsulate a single protocol; for example, to extend VoIP from a corporate environment to a home worker. Neither should it be used to encapsulate insecure protocols where secure protocols are available; for example, FTP and sFTP.

SSL VPNs

While this is a different technology, as their proponents try to mirror the features and advantages of IPSec VPNs, so the same issues arise.

8.7.5 Challenges to the Industry

As recommended earlier:

- Enterprises should plan for remote working solutions that do not rely on VPN tunnels, but instead utilize inherently secure solutions, allowing working directly in the Internet.
- The industry should reject the use of VPNs to encapsulate insecure protocols, and work to support, use, and develop inherently secure alternatives.

8.7.6 The Way Forward

Encapsulation using IPSec, while a valid current stop-gap solution, has little place in a de-perimeterized future for Internet security, and should not continue be used as an excuse to not fix the current insecure protocols at their root cause.

8.8 Secure Data

Our preferred term to cover "secure data" in enterprise computing is Enterprise Information Protection & Control (EIPC) – to avoid confusion with the term Digital Rights Management (DRM) which is commonly linked with the entertainment industry rather than enterprise business.

EIPC addresses:

- The digital management of rights to access information/data
- Control over that information/data – Copy, Store, Move, and Use (CSMU) of works
- Integrity of the information/data in question

Information protection needs to cover all data – from word processing documents to data within databases and executable code. It covers both enterprise and personal data, and is not just confined to protecting entertainment media, which is usually generically referred to as Digital Rights Management (DRM).

Information control is concerned with the business processes that, for confidentiality, segregation of duties, legal and commercial purposes, perform operations that track rights, rights holders, licenses, sales, agents' royalties, and/or associated terms and conditions, using digital technology to apply and enforce the control.

EIPC does not mandate encryption. Within a secure system, data may be unencrypted and other technologies such as hash functions or watermarking may be adequate if tamper protection or proof of ownership rather than confidentiality is required.

8.8.1 Problem Statement

In a de-perimeterized world it is generally safer to provide granular levels of data protection, with finer granularity being applied the closer the protection mechanism is to the data.

JFC#9 states that: “Access to data should be controlled by security attributes of the data itself”, while JFC#11 states: “By default, data must be appropriately secured when stored, in transit, and in use”.

On systems under your control, the storage of unsecured (typically unencrypted) data that is reliant on system or even network security controls is a flawed situation. The lost laptop computer with unsecured client information, or the database administrator who has access to personal information in their database, are both examples of situations where the data is inappropriately protected.

On data held outside of your immediate control, there is a need to manage, change, or revoke access for data, as well as the need to manage versioning and reduce concurrency.

EIPC, correctly applied, offers the ability to provide protection and management at the data layer irrespective of the location of the data.

Current EIPC solutions are mostly proprietary, limiting their applications by enterprise domain, operating system family, or to specific applications, and as such they provide little or no support for secure enterprise-to-enterprise collaboration. In addition, many current solutions greatly expand the attack surface by including extensive identity management systems in the access decision process.

There is no current standard for creating, marking, or otherwise managing the metadata required to describe the security attributes of information. It is not possible to fully understand the necessary information protection requirements nor communicate them to enforcement mechanisms without a mechanism to hold this information and an understandable, common set of semantics to communicate it.

8.8.2 Why Should I Care?

The security of the data must reside with that data (JFC#9) if it is to be adequately protected.

Data leakage via personal lapses, process imprecision, network file-shares, FTP (file transfer), email, USB disk, CD burner, old-CDs, or even floppy disks and output devices (such as printers) is a major issue. Locking down the hardware generally inhibits business, is hard to manage, and is not a viable solution for most organizations.

Today’s business depends on an agile and responsive ecosystem, and organizational data regularly needs to exist outside of the organization, with partners, vendors, and suppliers or potentially anywhere a business relationship exits. Once outside the organization, it is almost impossible to control, manage access to, or even withdraw access from that data.

Events change the intended rights and classification of data. The need for people to have access to data changes over time. For example:

- Financial results that go from “top secret” to “in the public domain” overnight, or are pre- and post-“embargoed until” time
- Price lists that expire at the end of the month
- The person who works for your organization one day and a competitor the next

Access also needs to change at times of disasters or public emergencies.

EIPC is a valuable tool for maintaining control of an enterprise's intellectual property while allowing it to be distributed and used across the enterprise's value chain. It's unlikely that all members of the value chain (customers, suppliers, partners, etc.) will have the same IT capabilities or environments, or that an enterprise can dictate those environments. Without interoperable standards for EIPC, this critical technology will fail to support the extended enterprise in managing its information.

Data that is being properly managed will both:

- Control access to that data
- Be able to define/limit what the person/system is able to do with that data

8.8.3 Recommendations/Solutions

EIPC has to:

- Be simple to apply and manage in a complex corporate environment (JFC#2) while not impeding intended access to that data and the rights to what you can do with the data
- Prevent data leakage, whether accidental, through incompetence, or a malicious act

It must not rely on a pervasive, ubiquitous real-time network connection (unless this attribute is defined for a particular document) thus enabling off-line working in aeroplanes, remote places in the world, or any other environment where real-time connectivity is not available.

EIPC of data is not just about data in discrete files. A data record in a database should also be subject to EIPC, as could individual emails, and EIPC should potentially extend to executable files. In a database, for example, a personnel file in an HR database should be accessible only by the person it refers to, their line management, and the HR manager for that department, thereby ensuring that the principle of segregation of duties is adhered to as well as protecting the privacy of the individual in question. As another example, while the database administrator may see, manage, back-up, and even port the data from one database manufacturer to another, they should not be able to read or manipulate the actual data itself.

In order to be really useful, an EIPC solution must work across an enterprise's entire value chain or between different enterprises that include approved partners, suppliers, customers, and others. This means that the customer marketplace needs EIPC solutions from different vendors to communicate using common protocols, semantics, and other related standards.

8.8.4 Background and Rationale

Key Escrow and Key Management

The encryption of documents with a password inevitably leads to documents that cannot be read because of lost passwords. The use of EIPC must enable the management of keys, key escrow, and/or access centrally such that access and functionality can be added/changed/revoked simply and easily.

Key management must operate (if allowed by the document EIPC attributes) in offline mode.

User Identity and the Management of Users Outside your Domain

As EIPC achieves wide acceptance then it will become increasingly difficult to manage the number of users and devices. Inside the organization (inside your locus of control), any EIPC must interoperate with the organization's existing authentication system (AD, Kerberos, LDAP, etc.) but also needs to operate effectively with third parties (outside of your locus of control) without compounding the problem – supporting full lifecycle management of those users as part of your EIPC system. Thus, any system must support working in a federated model (or similar) scheme (JFC#8).

The ease and ability to manage protected documents, potentially coming from multiple organizations, necessitates that client software must be standards-based and capable of interoperating with documents from multiple vendors.

Security Functionality

Dependent on the method of accessing/viewing the data, the security of the endpoint – and thus the ability to trust the operating environment, the user, and where it is actually connected – must be a factor in allowing access to the data.

In a trusted computing world, the client program must be capable of being trusted by the data it is processing to ensure that the data is operating in a valid (not spoofed) environment, such that the client is guaranteed to be able to enforce the attributes required – such as no-copy, no-print, no-screen capture, etc.

Temporal Data Classification

Data should be classified, typically by the data originator. However, data also has a temporal aspect (JFC#9). For example, plans for a new product, or stock market results, all change in classification over time. So when classifying data it must be possible to specify these temporal conditions.

Auditing of Digital Rights Information

EIPC must enable sufficient audit. This is especially important when data is being accessed by systems that are outside of the rights manager's control, such as third-party systems, or systems that are offline when interoperating with that data.

The linkage of any EIPC policy manager to the (corporate) directory should ensure adequate segregation of duties on sensitive data (JFC#10).

Control of Data

If EIPC is to deliver a viable corporate system, then data "in-the-wild" must be controllable, with the ability to effectively destroy that data (void all access), add and/or change and/or extend access, and change the EIPC attributes of the data.

Such controls must support and integrate into the data information management lifecycle, including support for archiving and the retrieval of EIPC data from that archive.

8.8.5 Challenges to the Industry

There is a lack of accepted standards in this area. Existing standards are inadequate. If EIPC is to succeed, then the items outline below must become accepted as industry standard.

The Client Interface/Software must be an Open Standard

EIPC must be pervasively available across a wide range of data formats and all platforms. Thus, open standards will allow developers to write for, and support, the widest range of platforms. Open standards ensure that the security principles can be thoroughly reviewed.

Just as it is undesirable/unlikely that any corporation can mandate that another company install and manage their preferred EIPC solution, so the prospect of having a client device that has to be installed and support many different EIPC clients, each with the prospect of interfering with each other or the system, will severely limit widespread adoption.

This means that there will need to be a standard API for creating and enforcing access rights on a given piece of information. There also needs to be a standard container for the information. In addition, there needs to be a standard protocol for communicating these access rights between the information owners or access right creators and people or applications that are requesting access.

Otherwise, a single EIPC client to an open standard will allow wide acceptance (JFC#2).

Standard Set of Agreed EIPC Classifications

Irrespective of whether EIPC is applied at document generation or later in the process, a document must contain (or have access to) all the relevant information/metadata required to process that document. This may be immediate, at some stage in processing or storage, or may be upon leaving the corporation.

To ensure that data can have EIPC applied, the programs that generate the original data files must be capable of embedding an agreed standard set of EIPC metadata without the need to know the EIPC product.[31] This will ensure that EIPC can be applied at a later stage – for example, if a document is transferred outside of a secure area/system, or automatically processed when a document is sent to an external email address.

Programs must also be capable of being forced (probably only in a corporate environment) to input EIPC metadata (for example, by a flag in a configuration file), ensuring that the entering of EIPC metadata can be mandated.

Interoperability presents challenges. Documents under EIPC control must have enough classification information in-the-clear to ensure that non-EIPC systems (such as other programs, storage systems, etc.) understand how to correctly handle that document. Such classification

[31] Dublin Core Metadata Initiative (DCMI) – refer to: www.dublincore.org/documents/dcmi-terms; ICE (Information and Content Exchange) and IMS (Instructional Management Specification) – refer to: www.getty.edu/research/institute/standards/intrometadata.

information must be protected to ensure that tampering with that in-the-clear information will be detectable.

8.8.6 The Way Forward

The continued development of interoperable online metadata standards that support a broad range of purposes and business models enables improved EIPC.

Existing EIPC vendors need to collaborate to define a single standard so as to avoid the industry fragmenting into proprietary point solutions, leading to fragmented industry and point solutions from which it will be very difficult to recover to open environments.

More open standards need to be defined for EIPC metadata – the control data used in the management and delivery of EIPC data. In particular, there needs to be:

- An open interface/API that can be used to manipulate/query the rights associated with the EIPC protected data
- A standard, extensible set of classifications as described above
- An open, inherently secure protocol for communicating between consumers of EIPC protected data and the server or enterprise that controls the data's EIPC attributes

Failure to do this will relegate EIPC in the transition to a de-perimeterized architecture to a niche market suitable only for internal corporate use. This will destroy its value for leveraging the enterprise-to-enterprise relationships inherent in our de-perimeterized environments.

Glossary

AUP/AUS	Acceptable Usage Policy or Standard
CIA&A	Confidentiality, Integrity, Availability, and Authenticity
COA	Collaboration-Oriented Architecture
CobiT	Control Objectives for Information and Related Technology
CSMU	Copy, Store, Move, and Use
DRM	Digital Rights Management
EIPC	Enterprise Information Protection & Control
FAIR	Factor Analysis of Information Risk
GPL	General Public License
IdEA	Identity, Entitlement, and Access
ISC	Internet Systems Consortium
ITIL	Information Technology Infrastructure Library
M&A	Mergers and Acquisitions
NAC	Network Access Control
NID	Network Intrusion Detection
NIST	National Institute of Science and Technology (USA)
PDCA	Plan-Do-Check-Act
PII	Personally Identifiable Information
POTS	Plain Old Telephone Service
PRIDE	Person, Risk, Information, Device, and Enterprise Relationships
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SLATES	Search, Links, Authorship, Tags, Extensions, and Signals
SOA	Service-Oriented Architecture

TCN	Trusted Computing Network
TOD	Test of Design
TOE	Test of Effectiveness
TOGAF	TOGAF, an Open Group Standard, is a detailed method and set of supporting resources for developing an Enterprise Architecture.
TPM	Trusted Platform Module
TSCP	Trans-global Secure Collaboration Program
VPN	Virtual Private Network
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Index