



SIMDAT

Data Grids for Process and Product Development using Numerical Simulation and Knowledge Discovery
Project no.: 511438

Grid-based Systems for solving complex problems – IST Call 2
Integrated project



Deliverable - Draft

D4.2.1 – Summary of Industrial Policies related to Virtual Organisations for each Application Sector

Start date of project: 1 September 2004

Duration: 48 months

Due date of deliverable: 01/09/2006

Actual submission date: 23/10/2006

Lead contractor for this deliverable: BAE Systems

Revision: 1.0

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination level		
PU	Public	X
PP	Restricted to other programme participant (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Revision history

Date	Version	Author	Modification
10/03/06	0.1	M Turner	Initial Version
04/04/06	0.2	M Turner	Updated after reviewer's comments
10/04/06	1.0	M Turner	Final Version

Copyright

Copyright © BAE Systems and other members of the SIMDAT consortium, www.simdat.org, 2005.

Table of contents

1	Introduction.....	4
1.1	Definitions, Acronyms and Abbreviations.....	4
2	Requirements capture procedure.....	5
3	Industry IT Policy and VO's	6
4	Policy summary.....	7
4.1	ISO Standards	7
4.2	Other Standards / Frameworks.....	8
4.3	Additional requirements.....	10
5	Conclusions.....	12

1 Introduction

This document details the findings from the requirements gathering exercise carried out as part of the Administration of Virtual organisations work package. The objective of the requirements gathering exercise was to identify the organisational and operational constraints that a virtual organisation needs to operate within. The mechanism used for capturing the relevant industrial policies was to conduct a series of interviews with representatives from selected organisations within every application area.

This document will give a summary of the industrial policies that relate to VO operation and discuss what factors go towards defining these policies in industry.

1.1 Definitions, Acronyms and Abbreviations

VO	Virtual Organisation
ISMS	Information Security Management System
ISO	International Standards Organization
IEC	International Electrotechnical Commission
QoS	Quality of Service
UKMO	UK Met-office
HMG	Her Majesty's Government

2 Requirements capture procedure

The requirements and operational policies were gathered from a representative company from each application area. BAE Systems representing the Aerospace industry, Renault from Automotive, GSK for the pharmaceutical companies and The UK Met office for the meteorological sector. Meetings were held between the VO technology champions, application area participants and company information security personnel. The industrial policies discussed in these meetings are summarised in this document.

The scope of the policy capture was to identify how the industrial policies relating to collaboration and information security are defined and to try and capture a common set of requirements from the industrial policies of each sector. The requirements of interest were in those areas where the deployment of a VO would have implications and where the policies place requirements on the operation of the VO.

<i>Date</i>	<i>Sector</i>	<i>Attendees</i>	<i>Comments</i>
January	Aerospace	BAE Systems (including IT Security Manager)	Initial policies and security requirements captured and there is ongoing dialog with the IT Security Manager.
January	Pharmaceutical	GSK (including IT security representative), IT Innovation	Still require a meeting for more detailed discussions
February	Meteorological	UKMO (including IT Security Manager), ECMWF, BAE Systems	Topics covered included Information security – policy & legislative and current information security implementations and risk management issues. Documents provided to BAE Systems under NDA for analysis
March	Automotive	Renault (including Information Security manager), ESI, IT Innovation, Intel, BAE Systems	Topics covered included existing systems that operate across the firewall, authentication requirements, internal uptake of PKI and data life cycle management Clearer understanding of “data encryption requirement”

3 Industry IT Policy and VO's

The industrial IT policies that have the greatest impact on the uptake of Grid technologies and the deployment of a VO in an industrial scenario are the policies that relate to information security management. Information security management covers a wide range of topics that all have to be considered to protect company information, assets and to ensure secure day to day operations.

Each company develops its own set of information security management policies known as an Information Security Management System (ISMS). The common base for the ISMS is an ISO standard (ISO 17799) that outlines the topics that need to be addressed. This standard formed the base of the ISMS's of all the companies interviewed. Having an ISO 17799 compliant ISMS is seen as very important to the companies interviewed. For example Renault has had a ISO 17799 compliant security policy for over a year now. The ISO 17799 standard sets out the topics to consider for the ISMS but does not give a set of controls that can be checked against to form the basis of an accreditation, this falls to a second ISO standard – ISO 27001. This standard sets out a series of controls that have to be addressed in an ISMS and is detailed later in this document. The UKMO is formally required by the UK government to have a ISO 27001 compliant security policy.

Each organisation then builds upon the ISO standards with the particular requirements of their business. These individual requirements will come from individual business needs and best practice. For example, Renault's new product data is very commercially sensitive and so they have a requirement that all data is transferred and stored encrypted.

External organisations may also place requirements on the ISMS. For example BAE Systems works closely with the UK MOD and to do this has to comply with a set of requirements/policies dictated by HMG which, for example, allow it to run a network to a certain classification level. Failure to comply to these external requirements would result in loss of business.

For a VO to operate within a single organisation it would have to be shown that it complied with these top level policies. When it comes to a VO operating across multiple organisations a common set of policy statements would have to be agreed upon. With ISO 17799 forming the basis for most organisations policies there should be a common base to work from. Individual members' requirements can then be considered. For example part of Renault's policy is that data transfer is done using the https protocol with strong authentication, so any data transfers done in a VO that Renault is part of would need to use https. A problem arises with terms like strong authentication – in Renault's case this mean a 2 factor authentication using their Smartcard system but another party in the VO might have a different definition of strong authentication and another way of authenticating users. There has to be agreement on these policies between the participants when the VO forms.

Another point to come out of the discussion was that the main goal of information security is to manage risks. For VO and Grid technologies to be adopted the risks of introducing the new system would need to be fully investigated and understood by the organisations. It would have to been shown that any risk was far outweighed by the benefit and steps have been taken to minimise and mitigate any risk. This is true for any new technology deployed in an industrial IT system.

4 Policy summary

4.1 ISO Standards

One of the main points to come out of the discussions was that accreditation to standards is important for any information system. The two main standards in this area are ISO / IEC 17799:2000¹ and ISO / IEC 27001:2005¹. The two standards are briefly described below.

ISO / IEC 17799:2000 is the Code of Practice for Information Security Management.

A management standard that offers guidelines and best practice for information security. It does not give details on implementation or how-to's but addresses the topics that must be considered for effective information security management. This is used as a baseline for security standards and then augmented with any industry-specific requirements (i.e. national security requirements).

It addresses the following topics:

- Establishing organisational security policy
- Organizational security infrastructure
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

ISO / IEC 27001:2005 Information technology - Security techniques. Information security management systems – Requirements

Provides a specification for implementing an ISMS and can be used as a basis for certification and auditing. This standard gives details of a set of controls that must be included (or their exclusion justified) for an ISMS to be considered compliant. The controls are grouped into the topics addressed in ISO 17799:2000 but go into further depth concerning what must be in place for the ISMS to be standard-compliant. The section on operating system access control is given below as an example.

¹ <http://www.iso.org>

A11.5 Operating system access control		
Objective: To prevent unauthorized access to operating systems.		
	Objective	Control
A11.5.1	Secure log-on procedure	Access to operating systems shall be controlled by a secure log-on procedure
A11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

4.2 Other Standards / Frameworks

The following are descriptions of other frameworks and standards that are used by some partners when defining an ISMS. They are principally from the Aerospace and Meteorological sector requirements but each industry will deal with similar documents and the national legislation issues affect every sector.

HMG Memoranda

The Communications-Electronics Security Group (CESG) is the UK's National Technical Authority and produces a number of standards and memoranda that provide guidance and technical advice. In particular the *HMG Infosec Standard No 2* is of importance as it gives guidance on security policy structure, how security responsibilities map to business structures and how these responsibilities are can be shared when systems interconnect.

Information Assurance Governance Framework (UK Cabinet Office)

Outlines a framework for achieving stakeholder confidence in information assurance. The framework provides statements of best practice and identifies the principles of governance for a number of topics. Information assurance is defined as “the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users”. The following topics are covered:

- Leadership and ownership
- The procurement process
- Service agreements
- Standards and services
- Risk assessment and risk management
- Change management

- Accounting, audit and monitoring
- Incident management
- Business continuity
- Awareness, education and training
- Compliance

The Common Criteria

The Common Criteria (CC) are a set of internationally agreed criteria for establishing security requirements. These requirements are of known validity and can be used to build up standardised sets of requirements to fit different purposes, known as a Protection Profile (PP). The requirements and measures to be used for a specific product or system are then put into a Security Target (ST) that can claim conformance to one or more PP.

The CC defines seven Evaluation Assurance Levels (EALs) for evaluating PP's and ST's. These provide a way of assessing the level of assurance of a system.

The 'common criteria' is often used when specifying the level of assurance needed for a firewall. For example BAE Systems specifies that any firewall protecting a BAE Systems network must have been evaluated up to EAL4 under the Common Criteria Scheme, and be operated in line with CESG documentation.

National Legislation

When a VO operates across national boundaries there will be a set of national legislations, with which participants from individual countries will have to comply, that will affect the operation of the VO as a whole. For example, the UKMO have to ensure that they comply with the UK Data protection act and as a public authority they also have to comply with the UK Freedom of information act and non UK members of the VO will have to ensure that the operation of the VO as a whole does not affect this compliance.

4.3 Additional requirements

In the discussions the following additional points were raised; they were factors considered to be relevant to the operation of a VO in industry. Assuming that we have systems that are compliant with the ISO IT security standards (giving us a common level of information security) these are the other factors that each application area has to consider.

Adequate separation

The meteorological sector identified the following levels of trust:

- Internet (public) – zero trust (positive mistrust!)
- Customers – external entities with verifiable identity (1-way information flow ...outwards)
- Partners – external entities with verifiable identity from whom we accept inbound data / information or consume their services (2-way information flow)
- Internal

Any system would have to ensure adequate separation between the different levels of trust and this adequate separation is critical when engaging in collaborations.

Ensuring QoS of operational data

Within the Auto and Meteo application areas, separate private networks exist for passing data between organizations. Data on these networks is operational data and the networks exist to provide a high QoS and security for its delivery. Any implemented system should ensure that information from a lower level of trust does not impact the QoS on these private networks.

Application acceptance

For any grid software to be deployed widely on any enterprise network it would normally have to undergo some form of auditing/certification. In the automotive industry any software that has a potential impact on security has to undergo functional (or in some cases code level) testing. With some industries this testing will be in-house but a large number of companies outsource their IT and have their own software acceptance procedures. For example BAE Systems IT is outsourced and so any software to be deployed across the business has to go to the outsourced company for evaluation and acceptance testing.

Identify management and Authorization

Organizations all have pre-existing identity schemes and the mapping of these schemes onto the grid infrastructure would ease the adoption of grid technologies. Some organizations have pre-existing PKI infrastructures or are in the process of developing them but the policies of how these infrastructures interact in a VO have not been defined.

Data protection / Confidentiality / Integrity

As well as the controls for data protection from the outlined standards, some of the organizations had specific policies for handling of data. In the automotive sector, the data must be encrypted for transfer and storage and they would expect all members of the VO to do the same with any of their data while at the remote site.

5 Conclusions

The common base for IT policies in the application areas interviewed were the two ISO standards (ISO / IEC 17799:2000 and ISO / IEC 27001:2005). ISO 17799:2000 offers guidance for information security but no concrete requirements but ISO 27001:2005 gives a list of objectives and controls to meet those objectives. These controls give us a good place to start when analyzing current requirements against existing SIMDAT technologies. This is the next step within the VO work package and an analysis of these controls, and the additional requirements highlighted in this document, will be carried out. The aim of the analysis will be to try and produce a mapping between these requirements and the VO technologies. Gaps where the technologies do not fulfil the requirements and any new requirements arising from the new technology will be identified. The technology requirements will then be passed on to the Integrated Infrastructure work package to ensure that the SIMDAT middleware and technology will be able to fulfil the policy requirements.

This analysis, carried out with the identified standards in mind, will help the ease with which Grid based VO's can be adopted in industry.

End of Document