EURESCOM

Technical Information

OSS Interconnection Gateway Validation

OSS Gateway Validation Report

Volume 6: Annex 4 - Gateway Security

Authors:

Dave Milham, Kapur Birdy, Simon Griffiths (British Telecommunications plc)

Andrea Laganà, Giuseppe Cassone, (TELECOM ITALIA S.p.a.)

Paul Duggan (*eircom* plc)

Erik de Vink (editor), Jan-Arend Jansen, Toby Nanne (Koninklijke KPN N.V.)

Timo Wirkkala, Petri Juka (Sonera Corporation)

Jan Svensson (Telia AB)

Jaap Burgerhout HP

Barbara Berger Telcordia Technologies Inc.

Chuck Seibold, Jerome Andreani, Steve Watson (GE Global eXchange Services)

Abstract

This document is part of deliverable 2 of EURESCOM project P908.

This volume looks at the appraisement of gateways regarding security threats that are predicted to be relevant to European operators working in a regulated environment. There has been special attention given to defining boundaries between domains of governance by using gateways as trusted entities. The main benefits of using gateways are reduced costs and the focussing of interconnect at a limited number of points where exhaustive and costly security analysis can be justified and carried out efficiently. This can be done whilst supporting resilience (no single point of failure), accessibility and alternative routes based on business rules.

This volume contains a logical sequence of security processes that need to be carried out by a gateway operator of any size.

EDIN 0105-0908

Project P908

For full publication

July 2001

Executive Summary

Telecommunications operators use Operational Support Systems (OSS) to assist in carrying out the day-to-day functioning of their business. Interconnection of OSS between operators means that business systems and network assets are put at risk of abuse from a variety of sources. This volume looks at the appraisement of gateways regarding security threats that are predicted to be relevant to European operators working in a regulated environment. There has been special attention given to defining boundaries between domains of governance by using gateways as trusted entities. The main benefits of using gateways are reduced costs and the focussing of interconnect at a limited number of points where exhaustive and costly security analysis can be justified and carried out efficiently. This can be done whilst supporting resilience (no single point of failure), accessibility and alternative routes based on business rules.

This volume contains a logical sequence of security processes that need to be carried out by a gateway operator of any size.

- Threats and risk analysis – using a simplified but effective process for risk analysis.
- A general security policy framework that can be used in the configuration and deployment of secure gateways.
- A set of security requirements for use in the procurement of gateways that should have appropriate security functions integrated into them.
- A basic security evaluation method to check that the security policies are being fulfilled in the implementation of the gateway technology procured.
- The mutual agreements that need to be established and how trust can be established between gateway operators and in some cases third parties to support non-repudiation and liability.
- A test set up environment for security features.

The main security features offered by Gateways include:

- All interconnecting parties may view gateways as a secure trusted entity for Business-to-Business (B2B) transactions.
- Gateways can be used to establish relationships with Trusted Third Parties for example Certification Authorities and Registration Authorities.
- The Risk analysis for B2B applications is much easier than for a Distributed Systems approach such as those typical in Enterprise Application Integration (EAI).
- Gateways mediate between external security policies established on per trading partner basis, and the policies for internal business processes.
- Gateways support incremental evolution of business activities and changing security policies.
- Gateways provide a critical point of control for authentication, authorisation and audit of B2B transactions.
- Gateways provide a point of 'single sign-on' into an organisation.

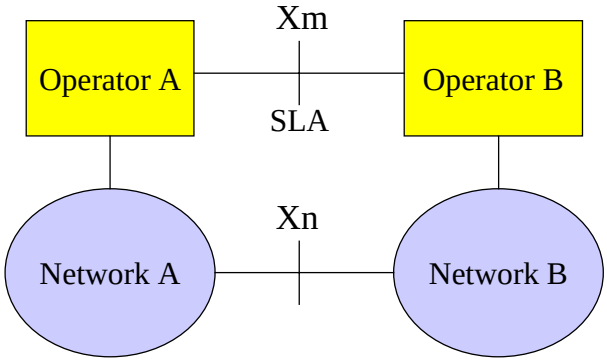
Table of Contents

Abbreviations

CIGP	Certification Authority
CERT	Computer Emergency Response Team
CRL	Certificate Revocation List
EB	Electronic Bonding
EESSI	European Electronic Signature Standardisation Initiative
IIOP	Internet Inter Orb Protocol
IPSec	Internet Protocol Security
OAM&P	Operation Administration Management & Performance
OCSP	On-line Certificate Status Protocol
OLO	Other Licensed Operator
OSS	Operation Support System
RA	Registration Authority
SP	Service Provider
SLA	Service Level Agreement
TGO	The Gateway Operator
TMF	TeleManagement Forum
TTP	Trusted Third Party
XML	eXtended Markup Language

1 Introduction

OSS interconnection between operators provides access through the management Xm interface as defined by the TMF. The operators may be of any size and may not have their own networks, in which case they are commonly called service providers.



The gateway concept has been developed to describe the interface technology for external access to OSS legacy systems by trading partners and customers, and to provide flexibility and responsiveness to new business developments. Without gateways, there would need to be full computability between each operator's systems, and all interconnection must be fully trusted. This document is only concerned with gateway solutions.

OSS interconnection gateways are being developed in an environment of: accelerating communications product and service development, increasing numbers of regulator licensed service providers, growing e-commerce usage with concomitant technological developments, and shrinking profit margins. The old ways of doing business between operators with clearly defined roles, markets, location and competitive boundaries are gone. What are also disappearing are long-standing business relationships where trust has been assured by personal contact and long established organisational structures.

The proper functioning of business in this new environment must utilise technologies to maintain the assurance of trust relationships in cost effective ways. This means that new ways must be found to identify what assets (financial, infrastructure, people) in companies need to be protected, who owns the risks to these assets, what threats exist in the real world and what countermeasures can be used to protect them. Inter-operator gateways will exist in an environment where companies that have a clear idea of how to maintain their own security, closely interwork with other companies that are of unknown trustworthiness or security status. Hence, gateways must be able to interwork with many different parties with differing technical, business and security requirements on the basis of appropriate mutual agreements for interoperation between security domains.

Gateways can be developed along tactical routes, providing customised interconnection functionality as and when required or they could be designed as strategic solutions, providing flexibility, high capacity and lower overall management costs. It is highly likely that many gateways will exist in larger operators, each with their own security attributes, and that these gateways will need to be unified in terms of overall security policies.

1.1 How to use this volume

To implement an OSS interconnection gateway that can act as a trusted entity and has security built-in requires that a full security design process is initiated at an early stage and continues throughout the life of the service. This volume outlines to processes that need to be followed by any company wishing to develop or use gateways and how the security issues surrounding OSS interconnection can be resolved.

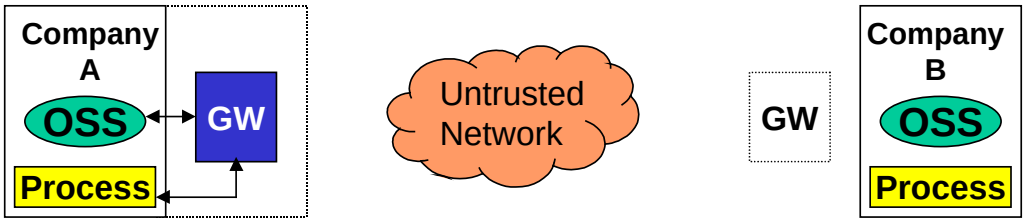
Each section in the main body of this volume explains the principles behind each of the activities that should be engaged in by people who are responsible for the security of the specific gateway being implemented. There is also an appendix related to each section that can be pulled out and

used as reference documentation at each stage of the security design process. This process starts with a risk analysis and continues through to forming agreements with other operators on security related issues. Each of the sections act only as a guide and can be modified to suit the purposes of the people responsible for the security of the gateway implementation. It is important to highlight that the ultimate responsibility for the security of a gateway is the owning company's and that this volume should only be used as a guide to best practice.

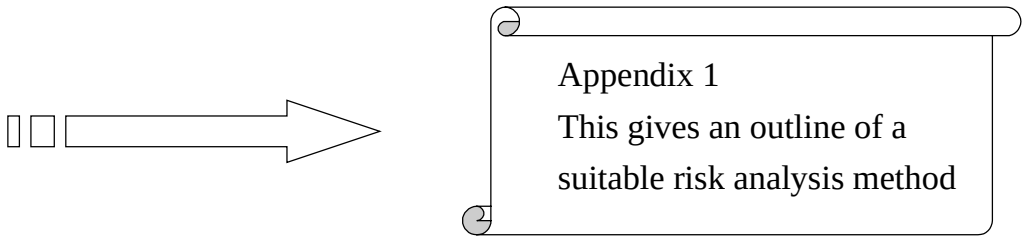
In what follows, company B (see figure below) has made a business decision to use gateway technology for its business-to-business transactions. Each of the stages given are only roughly in a time sequence. However the order is more to do with conceptual development and the sequence in which tasks need to be completed rather than indicating that one process starts when its predecessor finishes.

1.1.1 Section 2 - Risk Analysis:

The company B has decided to procure a gateway and must assess the risks to its own business and that of its customers. Company A represents one of many other possible companies with which Company B may wish to interoperate.



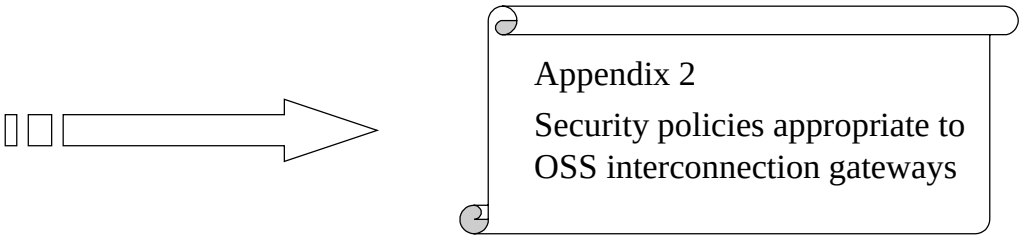
Section 2 on Threats and Risk Analysis presents the general threats that endanger the information and business processes related to the gateway. It also discusses a particular risk analysis method, viz. SPRINT – the Simplified Process for Risk IdeNTification as developed by the European Security Forum– that can be recommended for establishing the risk factor of the identified vulnerabilities for an interconnection gateway that is used in a certain context. The outcome of the risk analysis will be a list of identified threats that are critical to a safe operation of the interconnection gateway.



1.1.2 Section 3 - Security Policies

General corporate and gateway specific security policies need to be developed to provide the design guidance and management processes required to provide appropriate protection for Company B's assets as determined by risk analysis. At this point the requirements for gateway functionality and final implementation will be incomplete. The policies are enumerated here because although they are seen as internal policies for the protection of company assets there will be an impact on mutual agreements e.g. a wide variation of security policies from a norm as stated here could lead to a mismatch in mutual security requirements which would affect trust relationships.

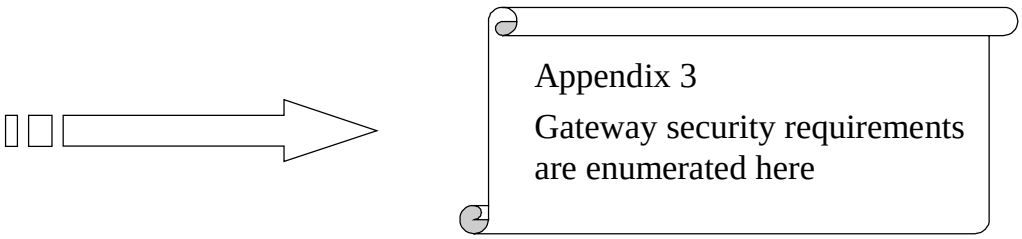
Section 3 on security policies will provide a framework of recommended generic security policies that should safeguard the business information and processes, etc. related to the interconnection gateway if they are implemented by operators. The greatest detail is devoted to the security policies that are of specific importance for the interoperability functionality of the gateway (e.g., customer-interfacing, non-repudiation, backoffice-integration, logging). The presentation of the security policies should support implementation, dependent on the gateway operator's needs and priorities, into various interconnection gateway security environments.



1.1.3 Section 4 – Security Requirements

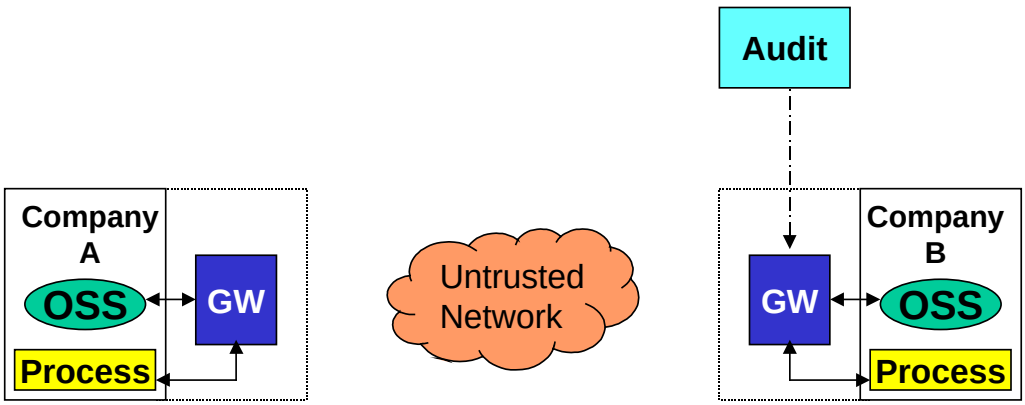
This section is targeted at gateway procurement requirements. It provides the guidance necessary for obtaining suitable gateway technology that can fulfil the security needs of the gateway operator (company B).

Section 4 on Security Requirements outlines the security requirements, which may be used by prospective gateway operators in the procurement of gateway products from vendors. OSS Interconnection Gateway products can be claimed to be P908-compliant if all the requirements are met. The security requirements are organised in such a way that their significance with respect to the gateway operators security policy can be made explicit.

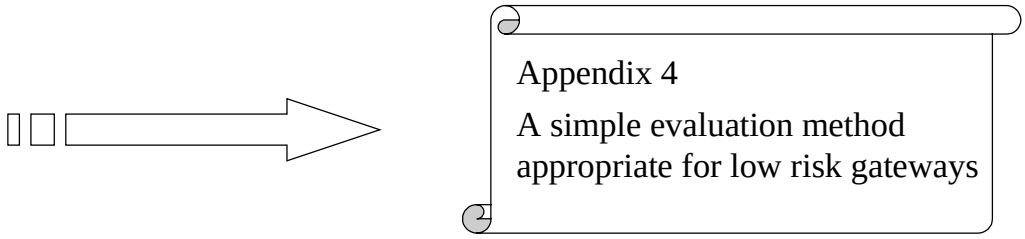


1.1.4 Section 5 – Evaluation

The implementation of the gateway needs to be checked and tested for compliance with security policies. The assessor could be internal or a third party auditor. This evaluation needs to take place before the gateway comes into operation. An external test gateway could be used at this point.

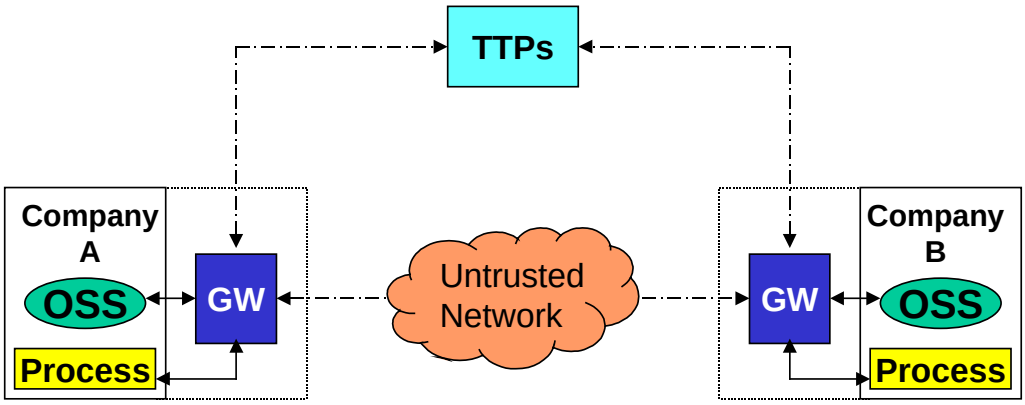


Section 5 on Evaluation and Certification presents an easy-to-use security evaluation method for interconnection gateway product implementations that could be used in assuring that the generic security policies, additional security policies generated by risk analysis and concrete security requirements are fulfilled if appropriate. The main goal is to foster security awareness and to give special attention to situations where a security goal is realised by a combination of gateway product provided security facilities on the one hand, and additional measures taken by the gateway operator on the other. Furthermore certification and accreditation with respect to international standard evaluation schemes, especially with respect to the Common Criteria, are recommended for use if justified by the business value of the gateway.

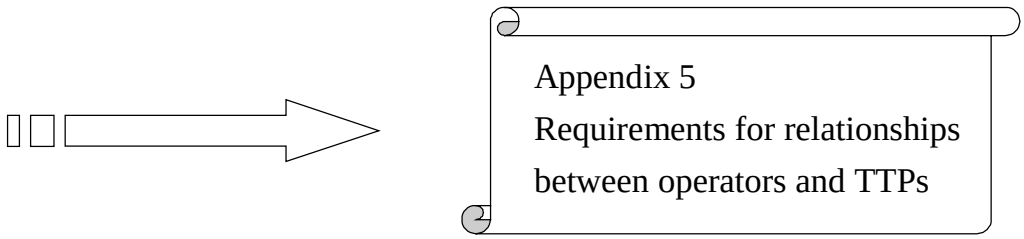


1.1.5 Section 6 – Mutual Agreements

The security of both interoperating parties must be based on mutual agreements that are satisfactory from either side. In many cases a trusted third party must be used to cover circumstances where mediation could be needed for security related events.

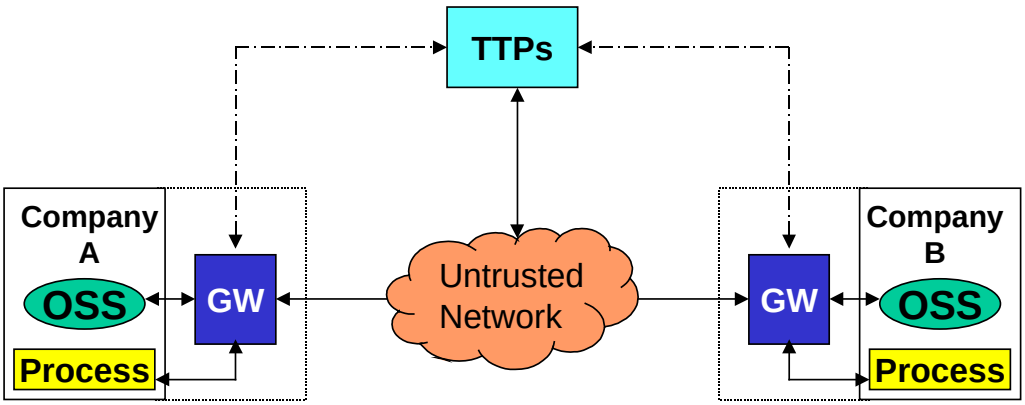


Section 6 on Mutual Agreements discusses, at an abstract level, security issues such as non-repudiation and liability that are relevant for an interconnection gateway. This provides general security-technical information, and complementary organisational and legal procedures regarding mutual agreement mechanisms that are anticipated to be crucial for the well functioning of the interconnection gateway. Also the role of trusted third parties and the generation of service level agreements are considered.



1.1.6 The fully operational gateway

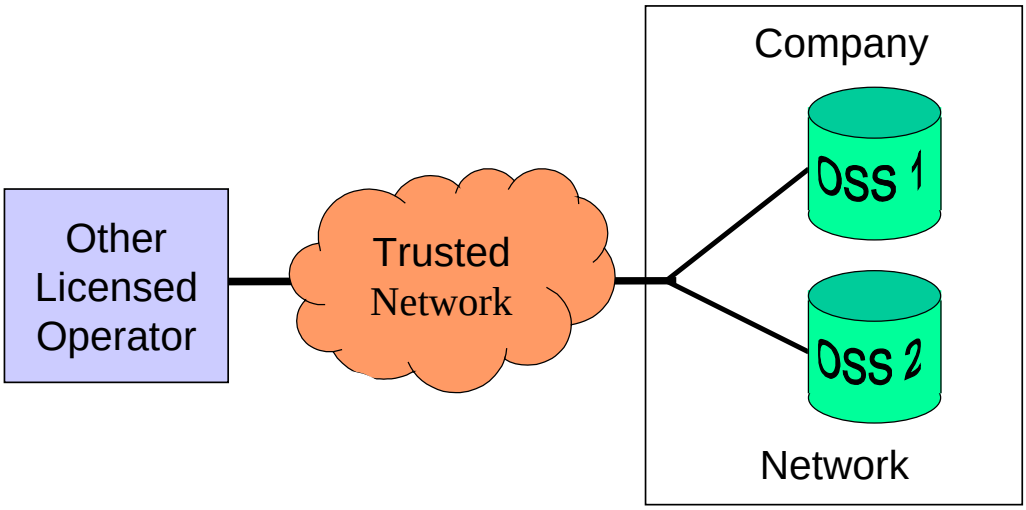
The gateway becomes operational. There are going to be many gateways and many TTPs. Each relationship has security implications for each of the companies involved. The security environment will be more stable if each party has followed these recommended guidelines.



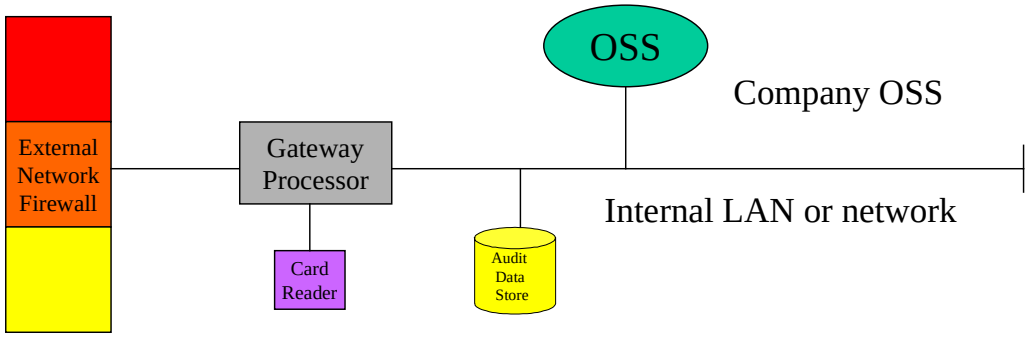
Finally, Appendix 6 on Security Test Strategy presents the set-up for the testing of several security building blocks that underpin the various security functions of gateways. The tests are based on use-cases that are selected from the concrete security requirements as given in Section 4. This comprises use-cases for adding a service provider, accountability for SLA-transgression, and high-value transactions. In part, the tests have been run on the gateway products of participating vendors, proving the proposed requirements to be practical.

1.2 Secure Gateway Architecture

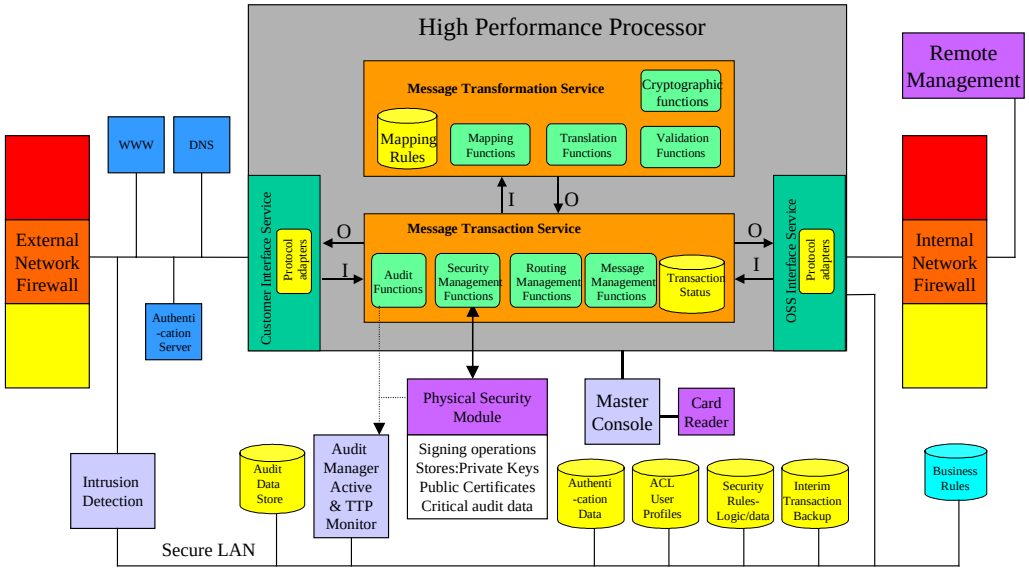
The basic gateway concept is to interface OSS legacy systems with trading partners and customers and to provide flexibility and responsiveness to new business developments. Without gateways there would need to be full compatibility between the OSS and the other operators systems, and all interconnection must be trusted.



The gateway must provide security features that this idealised model does not have. The simplest gateway model is given below.



In this case, the gateway processor is protected from external attack by a suitable firewall and has a card reader and some independent storage for log files. Most other security functions are carried out in the gateway processor or in the company's OSS. The company's internal network must be trusted both by the interconnecting parties and the company itself. As will be outlined later, the complete set of threats to gateway operators and interoperating parties using this type of design would not be adequately countered if high value assets were at risk. Hence a fuller design would be as given below.



This gateway design incorporates all round protection and could be treated as a trusted entity. The design details can vary, but the principles of protecting the gateway from both outside and inside of the company, and having a physically secure implementation are fundamental to the secure high capacity gateway concept.

1.3 Gateway Roles

Coupled to the gateway architecture and of equal importance is the way roles are defined for people with responsibility for gateway security.

1.3.1 Gateway Owner

The gateway owner in most cases will delegate executive responsibilities to a gateway manager. The ultimate responsibility for gateway security however rests with the owner.

1.3.2 Gateway Manager

The gateway manager has executive responsibility for gateway products and services, and provides and signs security policies. Security events and audit reports will be transmitted to the gateway manager. The gateway manager should not have privileged electronic access to the gateway other than as a basic user.

1.3.3 Security Manager

The security manager has day-to-day responsibility for the security of the gateway. The security manager will map authentication levels to roles (privileges) and will monitor audit logs. Any security events will be acted on, and any fixes or upgrades to the gateway will be controlled by the security manager. Logs can be altered, or switched on or off by the security manager, but only with authorisation from the trusted administrator and under the scrutiny of the internal auditor.

1.3.4 Trusted Administrator

The link between human resources within the gateway operator company and authorisation for access to the gateway takes place through the trusted administrator. The trusted administrator provides all users including the security manager and internal auditor with access rights. The trusted administrator cannot however open any username. They can only be opened based on a unique identity of employees. Also the trusted administrator can only have the role of trusted administrator and basic user rights. The security manager and internal auditor roles are also predefined and mutually exclusive by the individual's unique identity within the company. The trusted administrator also authorises the activation and disablement of logging.

1.3.5 Internal Auditor

The internal auditor's role covers the management and monitoring of log files and the capturing of access control lists. The logging of data is checked for conformance with security policies as specified by the gateway manager. Actions of the security manager and trusted administrator are logged. No deletions or alterations to logged data can be made by the internal auditor.

1.3.6 Users

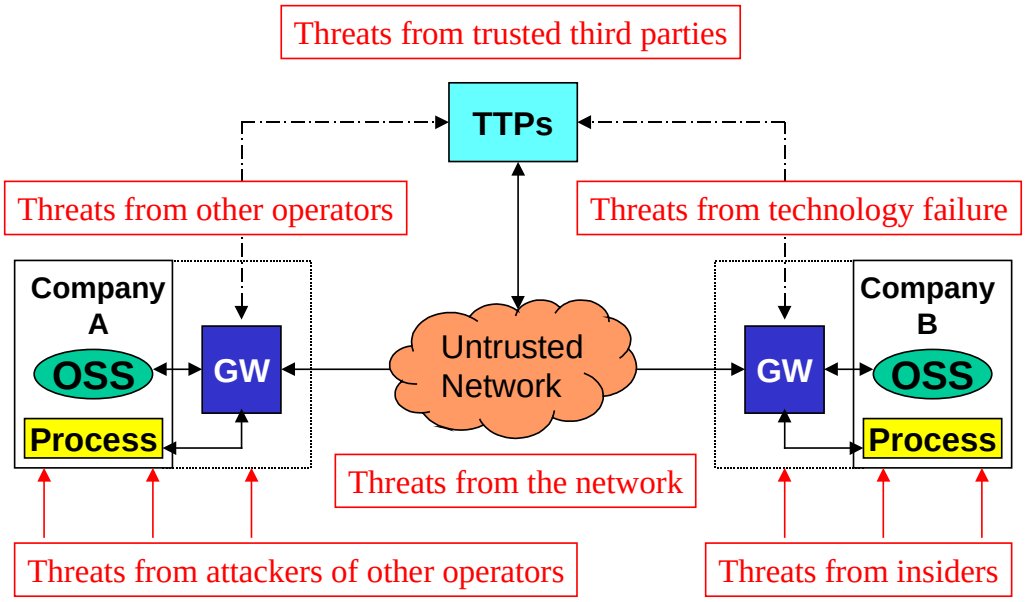
There are potentially many users roles but basic users shall not have access to log files, they cannot authorise users and cannot read or alter authentication data unless specifically authorised or directed to by the security manager.

1.3.7 Trusted Administrators in other operators

The role of trusted administrator is used to provide unique identities of company employees to other gateway operators. This allows users to use other gateways in the capacity of a company employee whilst maintaining anonymity with the external gateway operator.

2 Threats and Risk Analysis

The security risks that are of concern regarding interconnection gateways will depend on the particular deployment of gateway platforms and the environments in which they operate. Interconnection gateways that: process many transactions, serve many customers, handle high-value information and are well-known to the public, would be a more attractive target for attackers than gateways that are: low capacity, have a small number of clients, deal with low-value content and are relatively unknown. Impact and impairment of vulnerabilities of an interconnection gateway differ accordingly. However, vulnerabilities that are common to all interconnection gateways can be identified.



At the highest level, the gateway should be designed not just to be secure in itself, but to act as a point where security can be depended on when used for business to business transactions. The gateway should serve to protect company assets and avoid damage to the owning company's brand image if a security breach was to be publicised.

2.1 Assets at risk

It important to identify what needs to be protected i.e. the gateway operator's company assets. For generic gateway operators the following are expected to be identified:

The Gateway Operator's internal networks: Access to an operator's internal networks can result in a wide range of possible damage.

Integrity of Transactions or business logic: The results of altering data used by, stored or passing through the gateway could result in fraud, deception or other expense of either the Gateway owner or other operators.

Financial assets: Value transactions can be attacked with the aim of committing fraud or to reduce profits of the Gateway owner or other operators.

Service assets: Corruption of services offered through gateways can lead to loss of revenue or potential sales.

Management and maintenance time: The amount of time spent repairing damage and recovering from attacks needs to be minimised.

Competitive position: Timing is often critical in winning business and satisfying customer demand. Inhibiting the ability to deliver services can adversely affect a company's competitive position.

Service Availability: To another operator, denial of service attacks can be indistinguishable from unavailability caused by faults, failures in OSS or mismanagement. Gateway availability will be a prime asset.

The Gateway Operator's brand image: Any adverse publicity from security breaches can cause consequential losses to the company.

2.2 High Level Threats

A table of threats is given below. It lists generic threats to gateway operators and they overlap in some instances. Some of these threats can be countered by very basic security measures.

No.	Threat	Comments
T1	Unauthorised access to the Gateway Operator's internal networks and databases	Any direct access to the Gateway Operator's internal networks or databases through the gateway could lead to a variety of consequences.
T2	Access to confidential information stored in the gateway.	Access to data (including the Gateway Operator and SP customer information) relating to their telecommunications activities, passwords, etc.
T3	Eavesdropping of confidential data passed between operators	Any private data (including weakly encrypted data) that is passed between operators may be captured and analysed.
T4	Masquerade	A gateway emulator could be set up to present itself as an entity owned by a company but without that company's knowledge. This may be done by someone to commit fraud, to obtain confidential information, mislead the user etc.
T5	Improper use of the Gateway Operator's data obtained by an SP	The use of data (e.g. making private customer data public) obtained by an SP (or an attacker of the SP) from the Gateway Operator could be used to attack the Gateway Operator's interests.
T6	Inter-operation with insecure operators	Any SPs that do not co-operate with security policies could cause confidentiality or other concerns. Likewise operators that cease trading or are in dispute with the Gateway Operator may use information to the detriment of the Gateway Operator.
T7	Alteration of stored data	Any stored data could be corrupted or subtly altered to create maximum harm (e.g. altering order data or pricing information).
T8	Changing data in transit	Data transferred across a network could be altered or corrupted.
T9	Use of faulty or corrupt software	The gateway software could have security affecting faults or malicious functions (including viruses and trojans) that may be used to attack the Gateway Operator's interests. Such software may come in the form of upgrades or additional applications.
T10	Corruption of service management systems data	Gaining access to the gateway system would enable attackers to change routing tables, corrupt or delete data etc. Attackers here could include insiders with privileged access.

T11	Failure to supply or receive high integrity data	The Gateway Operator may fail to obtain usable data within reasonable time limits leading to the Gateway Operator/SP SLA transgressions. Likewise the Gateway Operator may fail to deliver such data to SPs.
T12	Denial of service attacks	Malicious overloading of network components or services to make a service unavailable to bone fide users. This may also be used to perpetrate other attacks.
T13	Intentional overwhelming gateway by SP	Large numbers of complex service requests, reconfiguration requests, etc.
T14	Opening defences when unavailability events occur	During e.g. major fault events security guard could be lowered to provide quicker fault management or service availability. Also system entry through test access points may also be possible. Attackers could corrupt data, read confidential information, insert bogus software etc.
T15	Non-recovery from failure or disaster	Suitable procedures need to be put in-place for cost effective business continuity plans. Since OSS interoperation has many interdependencies (service provision), a gateway becoming unavailable could adversely affect many SP's
T16	Deliberate unavailability of service or data	The inability to access data or service requested by the Gateway Operator could lead to the Gateway Operator/customer SLA transgressions more damaging to the Gateway Operator than to the SP.
T17	Fraud attacks	There are opportunities with gateways to carry out various forms of fraud. Included are: reconfiguration (via unsecured SP) to provide unpaid for service, Slamming, unsubstantiated compensation claims etc.
T18	Repudiation of actions	Disputing service delivered, service requests made, agreed prices etc. could be very damaging to either party (the Gateway Operator may both deliver and receive service).
T19	Failure of security software functions or hardware	e.g. Weaknesses in encryption algorithms may be discovered or the use of Smart Cards with weak physical security may lead to breaches.
T20	Failure of trust	If any operator is compromised then there would be a failure of trust leading to a breakdown of some security functions. A trusted third party being compromised would likewise cause disruption.
T21	Poor key management	Secret keys falling into the wrong hands (especially a CA) or becoming unavailable (possibly even on system performance grounds) could result in major security breaches or unavailability problems.

2.3 Antagonists

Since it is people who are responsible for security problems it is useful to classify types of antagonists:

External hackers: These are a continuing presence, especially for systems connected to the Internet. There is a very broad spectrum of hackers with a wide range of motives. Common ones are fraud, vandalism and curiosity. There are also threats from organized crime, and in the case of

larger telcos with national importance. We mention Information Warfare as an extremely severe threat. In such cases there is likely to be more than one perpetrator.

Insiders: These could act maliciously or accidentally to cause breaches of security. Often successful attacks are initiated by insiders, working in collaboration with others or just by being gullible.

Other licensed service providers or operators: These could in some cases be either inherently corrupt or pushing the bounds of acceptable behaviour. For instance, any loopholes in the law could be exploited to the full by unscrupulous operators causing damage to reasonable ones. Here some early arbitration may be called for.

Attackers of other operators systems: When there are failures in the security of other operators, by insiders or hackers, permissive policies in interconnected operators could be disastrous. Even when strict security controls are in place, any damage caused in such circumstances should be made the responsibility of the other operator (evidence may need to be collected for any subsequent litigation).

2.4 Risk Analysis

Risk analysis is the process of identifying security risks and vulnerabilities associated with a system, together with the formulation of adequate control measures that reduce these security risks to an appropriate level. It aims at making the security situation explicit; understanding the impact of the security breaches and provides a basis for the selection of pragmatic safeguards. The risk analysis will gain in extent and thoroughness when a formalised methodology is used to govern its utilisation. The commitment in time and effort though, should be proportional to the deployment of the system under consideration.

In the remainder of this section general aspects of risk analysis, in particular the 'threat → incident → impact → risk' chain will be discussed. Also the SPRINT risk analysis methodology as proposed by the European Security Forum (ESF) will be presented and illustrated in the present setting of interconnection gateways. SPRINT, abbreviating Simplified Process for Risk IdeNTification, is a business-oriented, structured and easy to use methodology. SPRINT starts from a concrete impact and then the relevant security threats are selected, bypassing the consideration of numerous other threats that do not apply.

2.5 General aspects

Knowing all threats and possible incidents doesn't suffice as a security strategy. The key issue is to minimise and possibly prevent damage. Measures should be focused on the aspects where the impact or risk is high. Analysis of manifestations of potential risk provide insight as to which actions are most appropriate to provide an acceptable and affordable security level.

A **security threat** is how a company or its assets can be adversely affected by malicious or accidental actions of people. An **incident** is a manifestation of a threat that causes loss or damage. An **impact** is the amount of damage that can be caused by a threat being realised. A **security risk** is the product of the probability of a security incident occurring and the magnitude of direct or consequential losses to a company being incurred.

An extensive risk analysis consists of an information analysis, threat analysis, impact analysis and risk assessment:

- The information analysis pertains to information and information flows in the process or system. It clarifies how information is represented, transferred and stored at process and system level.
- The treat analysis considers the threats in the live environment of the process or system. A rough indication regarding the threats that apply to the interconnection gateways can be identified using the generally applicable table below. All fields of the table are marked "Yes", hinting at the security of the gateway as vital.

	Confidentiality	Integrity	Availability
Malicious intent	Yes	Yes	Yes
Human failure	Yes	Yes	Yes
Technical failure	Yes	Yes	Yes
External causes	Yes	Yes	Yes

- The impact of a threat is related to the damage that is caused by security incidents. In order to get an estimate of this one can apply the so-called method of Annual Loss Expectancy or the so-called normative approach ("What is the borderline for losses to be just acceptable?").

Risk analysis methods and tools include AnalyZ, Besane, COBRA, Cramm, SARA and SPRINT. SPRINT has been chosen to be a good example of these tools since it is easy understand and apply by non-specialists, and is described below.

2.6 Risk Analysis using SPRINT

SPRINT is an acronym for the Simplified Process for Risk IdeNTification which is a risk analysis methodology focuses on a business process. In this context business process is defined as a process within an organisation where output is obtained dependent upon input and coherently interconnected process elements, (labour, resources, information, etc.) aimed at achieving a goal determined in advance. Such a business process is shielded from threats by security countermeasures. Application of SPRINT should result in a complete set of activities directed towards the establishment of security countermeasures that prevent unacceptable levels of damage being caused by security incidents. Here damage is measured along three dimensions: confidentiality, availability and integrity.

One of the characteristics already mentioned of the SPRINT method its having as its starting point the investigation of impairment. Another characteristic is the people involved in the business process decide themselves what is acceptable and what is not. The business managers should be able to estimate the amount of damage to assets that a treat being realised could cause and key individuals with knowledge of process handling and the activities of antagonists to the system can estimate the probability of the incidents happening. This way, management and processing experts are called upon during the risk analysis, not only because of the particular knowledge they possess, but also in order to create a larger support for the analysis itself and for the security measures that will be established.

Roughly three phases are distinguished in the SPRINT risk analysis. A first phase assessing the level of business risks associated with the business process, a second phase identifying the measurements that are necessary to keep the risks within acceptable bounds, and a third phase delivering a broadly supported plan of action for the realisation of the required countermeasures. The ownership of the risk analysis will rest with the business manager who is responsible for the business process involved and with a SPRINT co-ordinator. The SPRINT co-ordinator doesn't necessarily need to be a risk analysis expert. Individuals having the standing needed to work closely with the business management and with a good working knowledge of information security are well suited to play the co-ordinator's role. Although prior experience of risk analysis or training in the deployment of the SPRINT methodology is advantageous, co-ordinators will find themselves sufficiently equipped with common sense and the skills mentioned above. Generally speaking a SPRINT review can be completed in a couple of working days over a period of a few weeks with limited effort in preparation or in any other activities of the business manager and co-ordinator.

The first phase of the SPRINT risk analysis starts of with the gathering of knowledge of the business process by the co-ordinator in an open communication with the business manager and process experts. This can by achieved by interviewing the process specialists and operators of the systems involved, and by studying the documentation of the business processes and related systems. Then the business impact concerning the three dimensions, viz. confidentiality, integrity and availability, is established. Standard forms, one for each of the three dimensions, for documenting the first phase are available. All foreseen impairments are rated on their impact to the

business. These are the so-called business impact ratings. High ratings are accompanied by additional explanation.

The concern of the second phase is to identify the main threats and vulnerabilities in terms of confidentiality, integrity and availability, and to catalogue the controls to keep risks within tolerable bounds. This is done in a meeting of the co-ordinator, business manager and process specialists. Again, standard forms, one for each of the three dimensions, for documenting this phase are available. Ratings are assigned according to the likelihood the threats listed on the forms being realised. The ratings are the so-called vulnerability ratings. High ratings are further detailed. Appropriate controls need to be formulated as well. The wording of the controls usually follows from the description of the particular threat and the specific reason for the high rating.

The third phase focuses on the formulation of an action plan for implementing controls that sufficiently reduce the business risks. The assessment of the business impact on the one hand, and the threats, vulnerabilities and controls on the other. The proposed security controls as brought up in the second phase are prioritised in view of the established business impact and vulnerability ratings, their cost-effectiveness and ease of implementation. The resulting action plan also includes timelines, responsibilities and follow-up.

In Appendix 1 a possible fill-out is given for the forms as used in the SPRINT-method indicating the general security issues in the context of an OSS Interconnection Gateway.

3 Security Policies

3.1 Purpose

The security policies in Appendix 2 provide the full set of generic policies for OSS interconnection gateway security. The policies have been proposed to counter the threats to the gateway operator's assets. For each instance of gateway implementation, it is likely that some additional policies should also be developed to satisfy specific circumstances of the Gateway Operator. This may also lead to the modification of policies stated. The generic policies have been developed in the context of seeking workable interoperation security policies.

It is assumed that there is a general or corporate security policy available on which the generic gateway security policies can be based. In practical cases this could be BS7799 or equivalent, or it could be a framework security policy that is even more refined. However BS7799 is a widely adopted standard code of practice and can be regarded as a comprehensive catalogue of good security things to do. It has been coined that "BS7799 is to security what ISO 9000 is to quality". See, e.g., www.gammassl.co.uk for further information.

3.2 Policy Statements

Compliance with the policy statements, stated in Appendix 2, should ensure that OSS interconnection gateway systems are able to meet their business objectives with the minimum risk to the Gateway Operator. They are to be used in conjunction with the gateway system security requirements used in the procurement process. These Policies are either unique to Gateways, or are policies from the generic set of policies from IT security and electronic commerce. These Policies may be met through the use of appropriate technology, architecture or management processes, either individually or in combination. Critical to these are the processes needed to govern the roles played by individuals who control the security of the gateway. The Gateway vendor shall satisfy a large proportion of policies, but only the full Gateway Operators implementation will provide the rest. The total security of the Gateway is the responsibility of the Gateway Operator.

3.3 Policy Structure

The structure of the policy set given in Appendix 2 is given here. This structure indicates which policies are for the business level through to the technical implementation of gateways.

3.3.1 General Policies

This covers the general principles, policies and ethos that governs the gateway security environment. Overall gateway requirements, legal framework and regulatory requirements which must be reflected in policies are given and are the guiding principles on which gateway security will be based.

3.3.2 Information Security and the Protection of Assets

This covers how and why protection of information and other assets of gateway operators is needed. The understanding of information and its value is fundamental to reducing security risks.

3.3.3 Authorisation & Administration

The responsibility for protection against abuse of information and other assets rests with gateway operators themselves (i.e. directors or appointed employees). Access privileges to information and other assets must be properly authorised and managed.

3.3.4 Access Control & Authentication

Access to gateway services must be controlled. Entities making any connection to or via gateways must be properly identified as such and given appropriate privileges.

3.3.5 Accountability

Users must be held responsible for their actions throughout the life of gateway implementations. Intruders need to be identified and malicious acts must be detected and if possible rectified.

3.3.6 Implementation and Availability

The needs of solutions implemented in the real world must be addressed for gateways to start and continue to function properly. This set of policies encompasses the areas of design, VV&T and operational management that deliver security services.

4 Security Requirements

Security requirements are used in the process of procuring gateway technology. The gateway vendors need to respond to these requirements by stating how they are satisfied by their products. The reports, on how the requirements are satisfied and what additional measures are needed, should then serve as a basis to make a decision on which gateway to deploy. This information is also passed forward to the implementation team. At that stage, security polices will be implemented and residual risks identified.

The security requirements document (see Appendix 3) focuses on the following classes:

- *General Security* The security policy as formulated for the gateway should be in accordance with the general security policy of the gateway operator and addresses issues such as full documentation of deployed cryptographic techniques, minimality of operations and new vulnerability handling. The gateway should support secure operations and configuring of the security relationship for each other operator individually.
- *Architecture* In the design of the gateway platform there shall be functional and preferably physical separation of components for access by Other Licensed Operators, backoffice of the Gateway Operator and maintenance access and of security modules. In particular, customer data shall not be stored at the gateway. Interfaces are under the control of the Gateway Operator.
- *Authentication and Access Control* The gateway shall support multiple and strongly authenticated access. A Trusted Third Party will be responsible for key distribution and recovery. Access will be logged and can be disabled after repeated authentication failures.
- *Authorisation* In general, a message shall be forwarded by the gateway for further processing only if the message can be authorised. The gateway shall verify that the other operator concerned has the corresponding privileges. On an individual basis an Other Licensed Operator can be given permission to administer its own user accounts. A Trusted Administrator will be authorised to disable accounts.
- *Validation* The gateway shall authenticate each message as to its point of origin. Correctness and consistency of incoming messages will be checked. The content of outgoing message to any other operator will be checked on this other operator being the destination of the message. Multiple messages concerning a single request will be forwarded once by the gateway.
- *Confidentiality* All information communicated between the gateway and any other operator will be encrypted. The cryptographic techniques deployed in the gateway will not violate national regulations.
- *Integrity* The gateway shall support digital signatures as a means to guarantee the integrity of transactions. Incomplete transactions are revocable.
- *Availability* The gateway must be resistant to known denial of service attacks.
- *Data Separation* The separation of data of different other operators must be guaranteed. The Gateway Operator must be able to trace the actions of a Trusted Administrator of an Other Licensed Operator. Monitoring and auditing by a Trusted Third Party must be available on the gateway.
- *Auditing* The logging facilities of the gateway provide complete and time-stamped information at transaction level. In particular, it should be possible to use audit information in a court of law. Configuration of logging can be fully controlled by the Gateway Operator.
- *Fraud Management* The gateway supports processing of orders on the basis of an Other Licensed Operator's profile and provides mutual non-repudiation mechanisms. In case of a system emergency the gateway shall not permit "pass through" access.

The security requirements listed in Appendix 3 of this volume are reproduced from the EURESCOM P908 Deliverable 2, Annex 2 document, that contains a full set of requirements –not

only requirements related to security issues– for use in gateway procurement. They have been reproduced in this volume to give the person responsible for security, the complete set of guidance documents to be used in the full end to end security design process.

5 Evaluation and Certification

5.1 Evaluation form for detailed policy statements

The security policy implementation document given in Appendix 4 of this volume has been composed for ease of use. In many practical cases the individual policies mentioned there are expected to be relevant. However, in general, the gateway operator can have good reasons not to adopt a certain security policy statement. In fact, there may be valid arguments in specific circumstances, not covered by the generic setting assumed here, to mark some policies as Not Applicable (NA). By adopting other security actions or when working in the realm of a general corporate security policy it can be the case that a security policy statement put forward in the list becomes superfluous. However, it should be noted that very commonly the interplay of several security measures is subtle. Often the accumulated effect of several security measures is necessary to implement a particular group of security policies and to countermeasure serious risks effectively.

It can very well be the case that on the basis of an appropriate risk-analysis that the gateway operator decides to take a well-considered risk with a vulnerability in the interconnection gateway. Perfect security can never be obtained; it is important to have a proper balance between threats and risks on the one hand and the value of assets associated with the gateway, the countermeasures that are in force and the general performance and availability of the gateway, on the other. Also a decision not to comply with a particular security policy statement should be explicitly documented.

The gateway operator is expected to check the implementation of the security policy statement against its abstract formulation in the security policy document. In the Security Evaluation Appendix an evaluation form is provided to check the implementation of the policy statements discussed above (See Security Policy Appendix for the complete listing.). The form also indicates what type of security measures are needed to answer to the particular policy statement. Three categories are identified: organisation & procedures, product supplied or configured, additional measures. Key words render some further direction regarding the expected compliance.

Use of the evaluation form in the appendix will support the filtering of the individual security policy statements and the subsequent selection of adequate security measures.

5.2 Certification against international standards

As a next step in the evaluation of the security of the gateway, a gateway operator may need, either due to company security policy or dictated by the business asset value, to have the OSS interconnection gateway certified against an international standard. Although the effort in time and expenses for evaluation are not ignorable, the benefits could be great:

- Independent approval of the security level of the system as meeting recognised security standards and subsequent branding.
- Justified confidence in the effectiveness of the security of the design and minimisation of the impact of threats.
- International recognition and third party endorsement enhancing potential market expansion.
- Leverage of the overall system quality and earlier detection of flaws and errors during the system development.

Various evaluation schemes are available today, e.g., TCSEC, ITSEC and the Common Criteria. As it seems that the Common Criteria will emerge as the de facto market standard and because of the wider legal scope, it is discussed here.

The ‘Common Criteria’-standard, officially known as Information technology – Security techniques: Evaluation criteria for IT security, ISO/IEC 15408, provides a touchstone for the evaluation of security of IT systems. It integrates and extends various existing evaluation standards, including the European ITSEC and the American TCSEC or Orange Book. One of the design goals

for the Common Criteria is the liability for convergence with operative national schemes for evaluation, certification and accreditation.

Starting point for an evaluation under the scheme of the Common Criteria is the so-called security target. In fact, the security target forms the basis of agreement between the system developer and the evaluator (but also towards the contractor or customers) as to what security is catered for by the system and regarding the context of evaluation. A security target consists of the security objectives and requirements of a concrete system. It specifies the security functions of the system and describes auxiliary measures used in the design and development of the system.

Categories of security functions within the Common Criteria are audit, cryptographic support, communications, user data protection, identification & authentication, security management, privacy, protection of security functions, resource utilisation, access and trusted paths & channels. For the auxiliary measures the Common Criteria distinguish: configuration & management, delivery & operation, maintenance of assurance, development, guidance documents, life cycle support, tests, vulnerability assessment. The standard provides a catalogue of generic security functions and general assurance policies from which appropriate security requirements can be selected and adapted to the particular application.

The Common Criteria also propose predefined sets of auxiliary measures that are referred to as evaluation assurance levels or EALs. These are internally consistent general-purpose assurance packages. Their levels, EAL1 up to EAL7 are backwardly compatible with earlier standards, in particular TCSEC (D up to A1) and ITSEC (E0 up to E6).

EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested and reviewed
EAL5	Semi-formally designed and tested
EAL6	Semi-formally verified design and tested
EAL7	Formally verified design and tested

An evaluation in accordance with Common Criteria is an assessment of the system against its security requirements. Not only the system itself, but also the security target is evaluated and judged on its un-ambiguity and consistency. The major portion of the evaluation constitutes the coverage of all security requirements by the design and implementation. The assessments of the security requirements may follow both a black-box approach or comprise investigations based on test reports, design documents and source code. The expected outcome of the security assessment is a confirmation that the security target is satisfied by the system, along with an account of the findings of the evaluation.

For more information on ITSEC see http://www.itsec.gov.uk. For more information on the Common Criteria see http://www.tno.nl/instit/fel/refs/cc.html.

6 Mutual Agreements

6.1 Introduction to Mutual Agreements

This section has been written to provide guidance to help reach mutual agreements between secure gateway operators. The first part of the document outlines the mutual security principles of high capacity gateways. It is important to note however, that small gateways and other architectures will have to interwork with high capacity gateways and with each other, so security implications still have to be understood and agreements made in those cases. Hence there will probably be no universally accepted way to reach agreements but by taking the high capacity gateways as the first case study, systematic means to reach agreements can be found to act as a role model for other instances. Appendix 5 lists a set of requirements, which are aimed at both parts of an interoperating relationship and the relationships between gateway operators and Trusted Third Parties (TTPs). The requirements are used to focus attention on security between operators and identifying equivalent relationships with third parties. Hence the requirements between operators will be reciprocal.

The over all aim of this section is to help in the early stages of producing a workable set of security focused, mutual terms and conditions for use between operators, and to explain how these have been derived. It also provides a draft framework for EURESCOM shareholders wishing to implement high capacity gateways.

6.2 Concepts

In the current economic, regulatory and technological environment, telecommunications operators and service providers need to implement electronic versions of processes like ordering, maintenance and billing in addition to new services like number portability and carrier pre-selection. These types of interconnection are usually called Electronic Bonding (EB) or more specifically **OSS Interconnection**.

The concept of a *gateway* is to provide translation functions and a common information model at a single point in an operator's organisation that is both physically and logically resilient. It becomes possible to have multiple protocols and network interfaces on the external side to suit a range of sizes and types of outside companies, and to have a well defined interface to the internal legacy OSS. It provides a single point where risks to the owner of the gateway can be assessed and where security features can be built in. It needs to be a **Trusted Entity**, which can be viewed by outsiders and regulators as a point of reference for electronic business transactions.

Secure gateways need to be set up with a profound understanding that there needs to be matching levels of trust and protocols to determine how to view the other party and vice versa. This is the **Principle of Reciprocity** that underpins the trust model of gateways. Without this, gateway operators and users would be taking unjustified risks with their business.

When a consensus has been reached between two or more parties regarding legally binding terms and conditions as well as unwritten social laws that are expected to be adhered to, then these parties have reached a **Mutual Agreement**. Private contracts are not specifically included since this is meant to be a public domain process.

Implicit in the formation of mutual agreements is that authorisation of actions within a companies network and OSS will be dependent on Trusted Third Parties rather than arranged by any more direct means. Hence there will be an environment of **Shared Governance** that will be foreign to current administrators. This will lead to some dissociation between the administration of gateways and security, which will be more automated.

In practical situations, there will inevitably be variations between gateway types, technologies, services, versions, etc. This however is the strength of the **Security Domain Matching** properties of gateways, which can manage risks in an environment where there is no overall control or accepted standards for secure behaviour. Making some common areas of agreement in how

otherwise mismatched organisations interoperate is vital to maintaining security of company's and individual user's assets.

More than one OSS gateway can exist in an organisation. Gateways will range from high value transaction processors for major services through to low value, high performance gateways, just above the network level, for providing QoS in interconnecting IP networks etc. Secure gateways will therefore act on key signalling information, especially where billing events occur. Each organisation will need to co-ordinate between its own gateway operations and this will put an emphasis on the role of **Secure Directories**. The integrity, availability and access control to data, of these directories must be assured. Associating directories with gateways is vital to maintain the integrity of the gateway and the e-commerce activities of the business that owns them. The role of these directories is fundamental to PKIs and hence the authentication services used in companies.

6.3 Drivers for a Gateway Mutual Agreements Security Model

To form an appropriate security model for gateways and how to arrive at mutual agreements, threats that need to be counter-measured need to be understood. These threats are derived from the list of threats given earlier, but are specific to the relationship between gateway operators. Some of the main threats are given below:

Fraud attacks

There are opportunities with gateways to carry out various forms of fraud. Included are: reconfiguration (via unsecured operator) to provide unpaid for service, slamming, unsubstantiated compensation claims etc.

Repudiation of actions

Disputing service delivered, service requests made, agreed prices etc. could be very damaging to either party (the Gateway Operator may both deliver and receive service).

Improper use of the Gateway Operator data obtained by another operator/SP

The misuse of data e.g. making private customer data public, that has been obtained by another operator (or an attacker of the other operator) from the Gateway Operator could be used to attack the Gateway Operator's interests.

Inter-operation with insecure operators

Any operators that do not conform to accepted security standards could cause confidentiality or other concerns to any other interconnecting operators. Likewise operators that cease trading or are in dispute with the Gateway Operator may use information to the detriment of the Gateway Operator.

Use of faulty or corrupt software

The gateway software could have security affecting faults or malicious functions (including viruses and trojans) that may be used to attack the Gateway Operator's interests. Such software may come in the form of upgrades or additional applications. Also any executable data that is propagated from a gateway operator, for example, to facilitate the use of gateway functions by small businesses, must contain no malicious code.

Failure of security software functions or hardware

Many of the security functions of gateways will use technology that could fail to work or behave as expected. For example, weaknesses in encryption algorithms may be discovered or the use of Smart Cards with weak physical security could lead to breaches.

Non-Recovery from failure or disaster

Suitable procedures need to be put in-place for cost effective business continuity plans. OSS interoperation has many interdependencies whereby a gateway becoming unavailable could adversely affect many other operators.

Deliberate unavailability of service

The inability to access services, as requested by the other operator could adversely affect its business, especially when this occurs at a critical time. The other operator could lose business or fail to meet the SLAs with its own customers due to such events, which could have been contrived to do so by the gateway operator.

Failure to supply or receive high integrity data

The Gateway Operator may fail to obtain usable data (i.e. high integrity data) within reasonable time limits due to the actions of another gateway operator. This could lead to the Gateway Operator/SP incurring SLA transgressions with its own customers. Likewise the Gateway Operator may fail to deliver such data to other operators.

Intentional overwhelming of the gateway by other operators

Other operators may, for malicious reasons, use means that they are authorised to use, to cause effective denial of service attack on other operators gateways. This could be by presenting large numbers of complex service requests, reconfiguration requests, etc. which could degrade the performance of the gateway targeted.

Failure of trust

If any operator is compromised then there would be a failure of trust leading to a breakdown of some security functions. A trusted third party being compromised would likewise cause disruption.

Poor key management

Secret keys, especially a root key of a CA, falling into the wrong hands or becoming unavailable (possibly even on system performance grounds) could result in major security breaches or unavailability problems.

6.4 Mutual Agreement areas

Many security functions of a gateway such as non-repudiation will rely on using agreed security mechanisms and trust services. Such areas need either bilateral or collective agreements. There are many barriers, some of which are political to obtaining such agreements. This section identifies most of the agreements needed for gateway interworking.

1. The security services used by gateways to counter the generic threats to commercial transactions and the assets of participating companies:

- Encryption Algorithms
- Digital Signature Standards
- Digital Certificate Standards
- Secure Communications Protocols
- PKI Implementations
- Security Software e.g. APIs
- Security Hardware e.g. Smart Cards

2. A fundamental necessity to security services using public key cryptography is the need for a Public Key Infrastructure (PKI):

- Certification Authorities
- Attribute Authorities
- Registration Authorities
- Validation Services
- Time Stamping Services

- Directory Services

3. Further Trusted Third Party services are needed to complete the trust environment:

- Key Recovery Services
- TTP Monitor
- Auditors
- Arbitration Services
- Recovery Services and CERT
- Security Technology Qualification and Common Criteria
- Software Escrow

4. Auxiliary agreements reflecting the business relationships between companies include:

- SLAs (Digitally signed)
- Terms & Conditions (Digitally Signed)
- Procedures for Verifying Compliance and dealing with non-compliance
- TTP Alert Protocol
- Ownership of Information
- Information Retention Policy
- Security Classification of Information
- Jurisdiction

All of these agreement areas need to be dealt with by parties wishing to interoperate. If these agreements are reached on a bilateral basis then there could be an enormous amount of effort needed to satisfy the requirements of a large market with hundreds of interoperating companies. Hence there is a great need to start finding areas that can be covered by common agreements resulting in great savings being made. Some of these areas could be dealt with by the European regulators, but others are more suited to private enterprise.

6.5 Security Environment and Ownership

The security environment in which mutual agreements are formed is influential in the formation of common agreements. The following factors need to be considered:

Ownership

Gateways act as a single point of contact with security and trust properties that are known to the external party. The individuals that either own or are managing directors of the operating company are ultimately responsible for the security of the gateway and as such some greater confidence can be placed by interoperating parties in such an auditable entity than an arbitrary mixture of distributed systems.

Common Framework

The need to protect assets, carry out risk analysis etc. is a common need for all interoperating parties. The value of assets at risk varies between companies. However, having little of value does not necessarily mean that security can be ignored or in contrast that security measures should be made too strict by larger companies to the detriment of smaller business.

Environment

Articles of state underpins the ideas of ownership, justice, crime etc. These factors can be seen as ‘the environment’ in which gateways work in. They represent a set of constraining factors, which cannot be altered (within the scope of EURESCOM), but must be taken into account when reaching mutual agreements.

Trust

Unfortunately there is no simple measure of trust or even what is a third party when competitors can also be suppliers, partners and involved in joint ventures. Isolating companies so that they are completely independent an hence a fully trustworthy and honest broker is possibly unobtainable, but reliance on technological defences and litigation, can be seen as the backdrop to the selection process for TTPs.

Trusted Third Parties

Trusted Third Parties are a vital component for the workings gateway mutual agreements including e-commerce aspects and the operation of PKIs. TTPs are vital for areas such as non-repudiation, issuing and revoking certificates, registration of users, independent auditing etc.

Signature Policy

The signature policy is a set of rules for the creation and verification of an electronic signature, under which the signature can be determined to be valid. In other words, specific semantics associated with an electronic signature that is implied by a legal or contractual framework.

6.6 Information security and the protection of assets

The nature of the assets to be protected in terms of their value, their properties and how can they be corrupted is central to the reasons to maintain security. Mutual agreements are needed to protect the assets on both sides of any transactions or communications accesses. Some fundamental security principles apply here when looking at data security such as encryption and digital signatures:

Encryption.

Encryption is needed to help fulfil a number of functions – confidentiality, authentication, integrity and non-repudiation.

It cannot protect users from:

- stolen encryption keys
- denial-of-service attacks
- Trojan encryption programs
- Insider attacks or mistakes

Privacy protection using a symmetric algorithm, such as Data Encryption Standard (DES) is relatively easy in small networks, requiring the exchange of secret encryption keys among each party. As a network proliferates, the secure exchange of secret keys becomes increasingly expensive and unwieldy. Consequently, this solution alone is impractical for even moderately sized networks.

Public key cryptography has been in use since around 1976 and is based on a well-established mathematical framework. Asymmetric cryptography is not usually used for encryption, as the process of encryption or decryption is slow. Instead, asymmetric encryption is mostly deployed to agree a symmetric session key, which in turn is used to encrypt the data.

Encryption strength

Cryptographic strength depends on many factors, not just key length:

- The secrecy of the key
- The difficulty of guessing the key called a ‘key search’ – In most cases, a 40-bit key is vulnerable to a key search attack.
- The difficulty of inverting the encryption algorithm without knowing the encryption key called ‘breaking the encryption algorithm’.
- The existence of ‘trapdoors’ or additional ways to decrypt the encrypted file.

- The ability to decrypt an encrypted message if one knows the way that a portion of it decrypts (called a known plain text attack).

Secure Communications

There are a number of protocols available for use in OSS gateway interconnection communications. Reducing the number of commonly used protocols can be advantageous. It is however important to have more than one protocol in case any major security flaws are exposed. Below are some recommended protocols that are favoured currently:

SSL: General-purpose cryptographic protocol for bi-directional communication channels. Commonly used with TCP/IP Internet protocol and popular web browsers (prefix 'https:'). Offers confidentiality through the use of user-specified encryption algorithms; integrity, through the use of user-defined cryptographic hash functions; authentication, through the use of X.509v3 public key certificates; non-repudiation, through the use of cryptographically signed messages. Very useful in the small user to gateway connections using web browsers.

IPsec and IPv6: Cryptographic protocols that provide end-to-end confidentiality for packets travelling over the Internet. IPSEC works with IPv4, the standard version of IP used on the Internet. IPv6 will include IPsec. The main use is as a multi-vendor protocol for creating virtual private networks (VPNs) over the Internet. The protocol has the functionality to provide authenticity, integrity and data confidentiality for all communications over the Internet, provided that vendors widely implement the protocol after some technical and key management issues are solved.

SSH: Secure shell provides cryptographically protected virtual terminal (Telnet) and file transfer operations. This could be popular with small business users running Linux.

Digital Signatures

Digital signatures provide analogous security functions for electronic documents that hand-written signatures do for printed documents. In addition, digital signatures provide for the integrity of documents. The signature is an un-forgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached and that the document has not been altered since the time it was signed. Verification of these properties is substantially different in the two cases. In the case of paper documents (i) only one copy or independently signed copies exist (ii) the difference between a forged signature and the natural variation in a genuine signature can be difficult to assess (iii) detection of any alterations will involve physical forensic analysis (iv) the time and date a signature was made can only be known if some notarisation has occurred, otherwise circumstantial evidence is needed.

A digital signature is a numerical device acting on numerical data which is infinitely reproducible and can be stored and transmitted in many forms. Digital signatures provide authentication of the sender, integrity of the data and non-repudiation of the content. The recipient of a digitally signed message can verify that the message originated from the person whose signature is attached, that the message has not been altered either intentionally or accidentally since it was signed and cannot claim that the signature was forged by someone else, especially if it as been time stamped.

There is an urgent need for a set of technologies, which can be used to provide a complete standards-based solution. The European Electronic Signature Standards Initiative (EESSI) mainly deals with the requirements for the qualified electronic signature. The EESSI requirement in this area states that a specification of one or more sets of components fulfilling the technical framework for Qualified Electronic Signatures is needed. They further recommend that the following sets of standards and mechanisms as a first set of components that can be used for qualified electronic signatures:

- Authentication framework using X.509 certificates [ISO/IEC 9548]
- X.509 PKI Certificate and CRL Profile [RFC 2459]
- Digital signatures using the RSA and DSA algorithms [ISO/IEC 14888-1,-3]
- Hash functions SHA-1 and RIPEMD-160 [ISO/IEC 10118-3]

- PKCS #7 Cryptographic Message Syntax [RFC 2315]
- Use of hardware tokens, such as smart cards [ISO/IEC 7816, PKCS#15], PCMCIA cards and Personal Digital Assistants (PDAs) for secure storage and usage of private keys

There are good reasons for choosing this set of technologies. These technologies are generally accepted, widely deployed and recognised at national and international level. Standards exist for the use of these technologies.

The requirements placed on the signer for the production of electronic signatures may not be sufficient for a verifier or an adjudicator as technical evidence to settle some disputes. Other enhancements are recommended, for example a time stamp linked to the signed information to prove that a certificate was not revoked at the time the signature was generated. This can be achieved through a Time Stamping Authority (TSA) that binds a timestamp to sign data. The TSA is considered to be an important component of electronic signature infrastructure for telecommunications gateways since bandwidth assets are measured in the time domain and cannot be recovered after disputes.

It is recognised that many current digital certificates do not contain enough information to cover many e-commerce, government or gateway applications. Certificates being issued by companies like Verisign, GTE and Thwate do not specify age, gender or show a photograph, limiting their use. This makes it difficult to do business. Requirements for extra information need to be identified, along with general requirements for digital certificates.

A need has been identified for standardised enhancements to the baseline requirements for general and qualified electronic signatures to address commonly recognised threats. The EESSI calls these 'enhanced electronic signatures'.

Digital Certificate Standards

It is expected that an X.509v3 certificate, with appropriate extensions will be able to contain the necessary information. The EESSI have made initial recommendations for addressing the requirements on the contents of Qualified Certificates, and the use of the X.509 version 3 standard certificate structure. An X.509v3 certificate verifies that a public key was signed by a particular Certification Authority (CA) and that trust can be placed in the certificate commensurate to the trust in the CA.

6.7 Administration and Authorisation

Most security thinking centres around ideas of control and hierarchical authorisation. In the interconnection environment however there is more commonly Shared Governance. What assets may be accessed and level of trust cannot come from direct influence such as in an employer to employee relationship but must be found in mutual agreements. There is technology being developed in the area of authorisation and with careful application this could be used in the gateway environments. Such technologies include role-based servers, OCSP and Extensions and Attribute Certificates.

Certificate policy

A certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements, e.g. as defined for X.509. A certificate policy provides a common reference for signer and verifiers. The rules are commonly defined as part of the practice statement of a CA, but can also be a collection of requirements issued by a recognised authority, to be fulfilled by a Certification Authority.

A certificate policy should ideally include:

- Undertakings by the certificate issuer (e.g. verification of subjects when registering, maintenance of audit logs, delays and means for the notification of revocation)
- Signer's obligations (e.g. maintaining secrecy of private keys).
- The requirement on relying parties in the proper use of certificates in validating signatures.

Managed Public Key Infrastructure

In order to authenticate an individual or group using a private key, a link is needed to connect their identity to their public key in a trustworthy way. CAs digitally sign the individual's or group's public key through the issuing of digital certificates. CAs along with other services, make up an infrastructure that is able to support electronic signatures and digital certificates. This framework is called a Public Key Infrastructure.

A PKI comprises of the following elements:

- Naming Authorities
- Registration Authorities
- Certification Authorities
- Notaries
- Key Recovery Services
- Time Stamping Services
- Auditors
- Directory Services and Certificate Revocation Lists
- Smart Card Issuers

Naming Authorities

Naming Authorities are used to allocate distinguished names that uniquely identify individuals. The digital certificate must contain more than just the individual's name to be able to distinguish that certificate. It must contain enough information to uniquely and legally identify that individual.

Registration Authorities

Registration Authorities verify that a person is who they say they are. For certain types of certificate, they require an applicants physical presence with the necessary documentation e.g. birth certificate. Once this has been done, the Registration Authority asks the Certificate Authority to issue a certificate. It does this and signs the certificate with its own private key. The Registration Authority is the most important link between the individual and their digital identity. It is however important to realise that business to business authentication can rely more on companies being linked strongly to the digital identities of its authorised users.

For low risk applications in low capacity gateways, PKIs can be established simply, by utilising managed PKI solutions from trust services suppliers. These may also be used in early implementations of high capacity gateways.

Certification Authorities

A certification authority is an organisation that issues public key certificates. The certificates issued are signed by the certification authority's own private key. The certificate attests that a particular public key belongs to a particular individual or organisation. To use the certificates issued by a CA, one needs to have a copy of the CA's public key. CA Public keys may be distributed in software packages e.g. web browsers or operating systems. Other CA public keys can often be added manually by the end user.

Notaries

Notarisation services are conducted by TTPs on behalf of a party wishing to send a digitally signed document or data. They act as a 'second signature' to the signer giving a form of non-repudiation that a CA can't give. This is equivalent to a signature by a referee (someone who knows you) on a document to be accepted by a party, which trusts the qualifications of the referee.

Key Recovery Service

In the case of encryption keys where the encrypted data is to be stored, the keys need to be made recoverable for eventualities where keys or media carrying keys are lost, stolen or damaged. It is

necessary to have some form of secure key duplication system or key escrow system to prevent total loss of encrypted data.

Time Stamping Services

A digital time-stamping service issues and can record time-stamped documents, which cryptographically bind a date and time with a digital document. The digital time-stamp, derived from a trusted clock, can be used at a later date to prove that an electronic document existed at the time stated on its time-stamp.

Secure Directories

Secure directories and network services are required to defend against some security threats. However this development must take place in the network standards arena and is not a gateway issue a such. Within gateways it is necessary to use directory services, since the gateway entity can be seen as a policy based network in its own right. How this is implemented in the gateway, is not of concern to the interoperating parties, it is just that it must be done securely.

TTP Key revocation

Any lost physical authentication token or disclosed password etc. should be reported across all gateways that have registered the user. This shall be only done via a TTP key revocation service.

There are many reasons why a Public Key may need to be revoked:

- The key holder's private key may be disclosed or compromised.
- The CA may discover that it issued the certificate to the wrong person or entity.
- The certificate may have been issued to grant access to a particular service, and the individual may have lost his authorisation for that service.
- The CA may have its systems compromised in such a way that someone has the ability to issue false certificates.

One solution is the X.509 version 2 Certificate Revocation Lists (CRL). A CRL is a list of every certificate that has been revoked by the CA that has not yet expired. A CRL is ideally issued at regular intervals. The CRL should also state for how long it will be valid and where to get the next CRL. Otherwise On-line Certificate Status Protocol can be used to check if a certificate has been revoked.

Smart Card Issuers

On receipt of the signature creation device, the user needs to be informed of the terms and conditions of its use (e.g. not writing down the PIN or password). This is usually specified in a contract that the user signs and returns to the issuing organisation.

6.8 Access Control and Authentication

The gateway acts as a trusted entity by all interconnecting systems. To obtain service through the gateway, authentication to the gateway itself is therefore needed. Once the user or system is connected to the gateway however, the gateway will usually be responsible for onwards access. This is a vital role in putting security in one trusted place, and being able to interwork with sometimes disparate legacy OSS. Self-authenticating messages will either terminate at the gateway for action, or will be logged and passed on to appropriate applications.

There are a wide range of authentication technologies:

- Password, pass-phrase or PIN
- Physically secure device: e.g. Smart card, USB devices, secure module etc.
- One time password system such as SKEY, Security Dynamics SecureID etc.
- Biometrics

6.9 Accountability

Gateways provide an accounting function for business-to-business transactions. Hence some reliance needs to be placed on the accountability of gateway operations. This serves the purposes of both the gateway owner and all parties using the gateway as a trusted entity.

Audit logs

Data recorded by gateways is most often used for the protection of the gateway owners interests. Some of this data however could be requested or used by interoperating parties. What data is recorded, how it is accessed and how its integrity is proven is subject to mutual agreement.

Roles

All users of gateways shall have critical actions logged. All users with a security critical role however will have greater scrutiny from the internal auditor. The internal auditor role has no other privileges than to read audit logs and to check that the data recorded meets security policies laid down by the gateway manager. The auditor cannot alter or delete audit data and cannot change any access rights.

TTP Monitor access

Although interoperating parties agree what data is to be logged under specific circumstances, it is usually inappropriate for them to have direct access to audit data. It is important therefore to ensure that there is access to relevant data made available to a TTP monitor. This TTP could be a regulator or any external body that can mediate between parties. Data could be obtained either from log files or monitored in real time in circumstances where subsequent actions of the gateway owner must be authorised in advance but where delays could be costly due to the activity taking place.

6.10 Implementation and Availability

A gateway may be viewed as a single logical entity but its physical nature could be very different. For instance, to maintain the availability of the gateway, there may be more than one geographical location used and several identical processors and storage units. Understanding the nature of an implementation is critical to the overall security and trust that can be placed in it by all parties.

Physical security

One of the critical aspects of trust in gateways is in the fact that they must be physically secure. This means that any physical access or influence on gateway equipment must be rigorously controlled. All electronic security systems have at some point a physically secure device or system. Gateways represent such an entity and must therefore be designed and managed to appropriate security standards.

Auditors

TTP auditors should be used to inspect the physical and procedural security of gateway installations. The auditing should be carried out periodically to ensure that security standards are being maintained.

Availability architecture

Protection against denial of service attacks is a major requirement for high capacity gateways. Availability is protected mainly by the design and management of gateway installations. Some of the protection against unavailability events includes: gateway firewall architecture, back-up processes, alternative sites, resilient network design, fast recovery procedures, technological diversity and the correct use of service pack updates. Claims made of availability of gateways must be justified and measured. The timing of unavailability events must also be monitored.

Signature creation environment

Currently the most common technology for securely carrying out digital signatures for individuals is the smart card. This is one of the most secure ways to protect private keys. A smart card has a microprocessor and can often create the public key and private key pair itself, so the private key,

used to produce digital signatures, never has to leave the physically secure device. A smart card can transmit the public key to external computers and has an amount of storage space for holding other public key certificates. If an operation is required to be carried out using the private key, then data, or a challenge must be transferred into the card, and then this will be processed (signed or decrypted etc.) inside the card and then the result is returned. Thus attackers can't use the private key unless they have possession of the smart card, and have successfully retrieved the private key from it (which is technically difficult and in most cases expensive). There are other forms of this technology and for high capacity gateways themselves, physically secure electronic modules would be more suitable due to their higher capacity. The main features of physically secure devices including smart cards are:

- Contains signature creation programme and data
- Protected by PIN
- Private key can't be read out without costly effort
- Critical data such as public key certificates cannot be altered
- A blocking function can prevent or inhibit exhaustive search
- Cannot be emulated (when appropriate protocols are used)

The main threat being countered by these devices is that attackers could access an individual's private key(s) or tamper with their most trusted public key certificates stored in the device. Physically secure devices are designed to not divulge secrets or allow access logically and to resist attempts to analyse them physically. It is however important to realise that the terminal being used to carry out signing is trusted i.e. the data being signed is that which is believed to be signed by the user. Security policies must ensure that terminal equipment can be trusted to carry out an individuals wishes faithfully. These issues can certainly be tackled as the technology is developed further but currently they should be treated as residual risks:

Verification of data to be signed

For manual signatures, the signer should be allowed to verify what is about to be signed. This happens in the non-digital world, one expects to be able to read anything that one is about to sign. The signer must be made aware of the implications of signing i.e. the rules being agreed to when signing. Explanatory text will be sufficient; this should be displayed, stored in an agreed place and itself signed at a higher level. There should be another level of security that confirms that the signature creation device is still in the hands of the original owner. This can be confirmed, to a degree, by the signer entering a PIN or password for every signature.

For automatic processes, the signing function will be carried out under predefined circumstances. Any changes to these circumstances or terms and conditions would have to be manually checked before re-launching automatic processes by the owner of the signing key.

The gateway security test model

Procedures for validation and testing gateway security against the standard European model. Before any gateway implementation is activated in the live environment, it could be tested against a 'dummy' gateway, which provides standard test routines to improve the chances of the live gateway functioning correctly. A common agreement could be formed to provide such a gateway with shared costs.

7 Conclusions

The existence of secure OSS interconnection gateways is vital if the telecommunications industry is to develop a dynamic trading environment. The gateway in this volume has been modelled as a trusted entity. The gateway is either owned by a trading company or a trusted third party, and must be designed and operated within appropriate security guidelines whereby risks to trading parties can be evaluated. This volume has been dedicated to this end. Being able to identify a trusted entity for carrying out transactions, which are free from, disclosure, alteration, impediments, repudiation etc. is not just a desirable goal but is probably vital to the functioning of high volume and automated commercial interoperation.

Authentication: It is essential to properly identify who is requesting access or to be sure that a transaction stems from the right person or business partner e.g. a high value transaction should always be digitally signed.

Authorisation: Actions that users are allowed to take must be controlled and any permission must be obtained in advance of access to the gateway. For management efficiency, roles with associated privileges can be ascribed to groups of users or security classes. Delegation of responsibility is also critical to gateway authorisation. This may be for the administration of users in an interconnecting operator or so that newly licensed operators can get access with the permission of the licensing authority.

Accountability: Detection and logging of actions is as much a deterrent to the abuse of systems as it is a means to bring perpetrators to justice. Also auditing and analysis of logs can be used to improve security or for gathering evidence for a third party such as a national regulator.

Availability: Protection against denial of service attacks is a major requirement for high capacity gateways. Availability needs to be protected by well designed authentication processes, gateway firewall architecture, accountability, back-up, alternative sites, resilient network design, fast recovery procedures, technological diversity, service pack updates, CERTs and industry wide protocol hardening.

Many security functions of a gateway such as non-repudiation will rely on using agreed security mechanisms and trust services. Such areas need either bilateral or collective agreements. There are many (some political) barriers to obtaining such agreements and this document indicates how to facilitate the resolution of problems. Although gateways use digital signatures etc., which are beginning to be recognised legally, the development of them is along e-commerce lines and this grows quicker when not fettered by government legislation. However the operation of gateways will probably be best served by taking the best of both approaches. Unregulated e-commerce activities when the market demands it and standard telecommunications based transactions between licensed operators with the full backing of the law, when serving regulator requirements.

Some problems inherent in PKI implementations are not yet solved, but the gateway concept helps with these issues anyway by being able to adapt incompatible systems to each other. That is, gateways offer ways to overcome the non-standardisation in PKI implementations and other security services used today.

Some allowance has had to be made within this project to the fact that the security technology supporting the implementation of trusted gateways is not fully mature or accepted. Hence the emphasis has been on delivering the means to achieve secure solutions in a real world trading environment rather than supplying arbitrary lists of technical solutions that solve a subset of the security questions. It is critical that a holistic view of security is taken rather that accepting products with security functionality built in as being a satisfactory solution. A proper adherence to the principles given in this volume should give the gateway operators many benefits including:

Single entity for risk analysis: Gateways offer a simpler solution to many security problems. A single trusted resilient entity is much easier to assess by risk analysis than a system of distributed elements connected together in an arbitrary way.

Open security standards: The use of common security services amongst operators will provide greater accessibility to good security. Security should never be used to exclude market players or

promote cartels. The gateway concept empowers more companies to participate fairly in the telecommunications services marketplace.

Standard models for mutual agreements: The business relationship between operators has a great impact on overall security and trust. Firm foundations in mutually assured security policies based on e-commerce best practice and simple means for new participants to enter the market are not just desirable but critical for the commercial growth of telecommunications services. Telecommunications regulators are expected to act in a pivotal mediation role in the early days.

Independent of legacy systems: Alternatively known as a 'security nightmare' legacy systems carry with them many earlier decisions on security policies that may not adapt to newer practices. They may be too permissive at the one extreme or too restrictive at the other. Gateways act as a buffer to legacy systems and can provide for instance Single Sign-On (SSO) for Gateway users, which would be infeasible with separate interfaces.

Reduced costs and development time: Security is 'built in' to the gateway concept. Use of common security standards and commercially available security functions can reduce costs and provide much better security within the industry than by depending on the vagaries of ad-hoc developments by participating companies.

Finally, this volume contains the guidance documents recommended by EURESCOM shareholders that will help in providing a secure environment for all participants that will serve to improve trading relationships across widely differing company types and national boundaries.

8 References

[1] BS7799–1:1999, Information security management, Part 1: Code of practice for information security management, British Standards Institute, London 1999

[2] SPRINT: Risk Analysis for Information Systems (User Guide), European Security Forum, London 1997

[3] Electronic Signature Formats, Draft ETSI ES 201 733 v1.1.4, ETSI, Sophia Antipolis 1999

[4] Common Criteria for Information Technology Security Evaluation, version 2.1, ISO/IEC 15408:1999, ISO 1999. See http://csrc.nist.gov/cc/

[5] The German BSI Safeguard Manual for Digital Signatures

[6] The American Bar Association PKI Evaluation Guidelines

[7] The Australian Government PKI Criteria for Accreditation of Certification Authorities

[8] The Government of Canada PKI Certificate Policies.

Appendix 1 Gateway Risk Analysis using SPRINT

From the European Security Forum, standard forms are available that support the risk analysis following the SPRINT method: Four one-page forms for the assessment of business impact (with respect to confidentiality, integrity and availability, and a summary form), three 2-3 page forms for the assessment of threats, vulnerabilities and controls (covering confidentiality, integrity and availability), and a one-page form for the action plan.

An indication of these forms when completed is given below for illustrating the risk analysis using SPRINT in an imaginary context of a generic OSS interconnection gateway. For the sake of presentation various details (e.g., explanation of business consequences and explanation of the threat and vulnerability factors) are suppressed. Also the Business Impact Assessment Summary form has been omitted. In the analysis it is assumed that the gateway operator does not act as a client to the gateway.

For the Business Impact Rating (BIR) the following scale is used: A Business Survival Threatened; B Serious Damage; C Significant Damage; D Minor Impact; E Negligible.

Confidentiality (Business Impact Assessment)

Business Consequences	BIR	Explanatory Comments
C1 Competitive Disadvantage	D	See item C5.
C2 Direct Loss of Business	E	
C3 Public Confidence	E	
C4 Additional Costs	D	See item C5.
C5 Legal Liability	C	Substantial violations of confidentiality agreements with gateway clients.
C6 Staff Morale	E	
C7 Fraud	E	
Overall Rating	D	

Integrity (Business Impact Assessment)

Business Consequences	BIR	Explanatory Comments
I1 Management Decisions	D	Incorrect allocation of administrative or maintenance resources.
I2 Direct Loss of Business	E	
I3 Fraud	D	Fraudulent new connections.
I4 Public Confidence	C	Service level of network operator may be perceived to be poor.
I5 Additional Costs	C	Restoration of data and recovery from other malicious actions.
I6 Legal Liability	E	Contractual obligation to support OLO at agreed service level.
I7 Staff Morale	E	
I8 Business Disruption	E	
Overall Rating	C	

The column on business impact rating, in the availability table to follow, is divided in 5 sub-columns with markings, from left to right, with respect to a duration of outage of an hour, a day, 2-3 days, a week, and a month, respectively.

Availability (Business Impact Assessment)						
Business Consequences	**Business Impact Rating**					**Explanatory Comments**
A1 Management Decisions	E	E	E	D	D	
A2 Direct Loss of Business	E	E	E	E	E	
A3 Public Confidence	E	E	E	D	B	Unavailability of a month unacceptable.
A4 Additional Costs	E	E	D	C	B	Interconnection should be taken over by other means.
A5 Legal Liability	E	E	D	C	B	Combination of A3 and A4.
A6 Recovery	E	D	D	C	C	Dependent upon the number of transactions handled by the gateway.
A7 Staff Morale	E	E	D	D	C	Month down-time does not fit with the corporate service level standard.
A8 Fraud	E	E	E	E	E	
A9 Business Disruption	E	E	E	E	E	
Overall Rating	E	E	D	C	B	
Overall Critical Timescale	2-3 days					

To the Vulnerability Rating (VR) the following scale applies: A Probable; B Highly Possible; C Possible; D Unlikely; E Impossible

Confidentiality (Threats, Vulnerabilities and Controls Assessment)			
Threat and vulnerability Factors	**VR**	**Comments**	**Controls Required**
TC.1 Outsiders gaining sight of print-outs and documents	E		
TC.2 Disclosure by employees of sensitive information to outsiders	E		
TC.3 Unauthorised entry into premises	E		
TC.4 Unauthorised Access to Data by Employees	B	Many legacy systems involved	Authentication and non-repudiation
TC.5 Unauthorised access to data by external personnel	B	Quasi open system at OLO-face	Authentication, logging, non-repudiation and data-separation.
TC.6 Confidentiality problems with connected systems	C	Through-logging should be prohibited	Disallow face-to-face connect.
TC.7 Interception of communication links	C	Encryption level to be dealt with in SLA	CLI, authentication, encryption

TC.8 Electronic emanations	D		
TC.9 Other threats to the confidentiality of system or data	E		

Integrity (Threats, Vulnerabilities and Controls Assessment)

Threat and vulnerability Factors	VR	Comments	Controls Required
TI.1 Input errors	B	Wide variety in OLOs.	Lexical analysis of input, training and userdocs, logging and non-repudiation.
TI.2 Program errors	E		
TI.3 Operator errors	C	Status of transaction should be clear.	
TI.4 Manipulation or suppression of input documents	E	See TI.1	
TI.5 Unauthorised use of transaction facilities	D		Authentication, logging, non-repudiation controls.
TI.6 Unauthorised modification of programs	E	Corporate security policy should sufficiently cover this.	
TI.7 Unauthorised modification of files	E	See TI.1	
TI.8 Manipulation of job streams	B	Difficult to handle. Gateway should be selected/configured carefully.	
TI.9 Manipulation of equipment or computer media	E	See TI.6	
TI.10 Integrity problems with feeder systems	B	Responsibility of OLO. Processing at legacy face is complicated. Should be clear conceptually.	
TI.11 Other threats to the integrity of system and data	E		

Availability (Threats, Vulnerabilities and Controls Assessment)

Threat and vulnerability Factors	VR	Comments	Controls Required
TA.1 Major disasters	D	As usual.	
TA.2 Inadequate IT contingency arrangements	D	Should be covered by corporate security policy.	
TA.3 Inadequate business continuity plans	D	*Idem.*	

TA.4 Day-to-day system outages	D	*Idem.*
TA.5 Degraded system performance	D	High performance required.
TA.6 Other threats to the availability of system and data	E	

SPRINT Action Plan

BIR	VR	Priority	Control Requirement
B	B	1	backup + 2 day replacement
B	C	2	face-to-face connect should be impossible
C	B	3	non-repudiation mechanism
C	B	4	logging
C	B	5	authentication OLO-face
C	B	6	authentication legacy-face
C	B	7	lexical analysis of input
C	C	8	encryption to be part of SLA
C	C	9	tracking and tracing of transactions
D	D	10	corporate security policy

Appendix 2 Security Policies

A2.1 General Policies

A2.1.1 National and International Legislation

The Gateway Operator managing directors and those appointed to roles of Gateway Manager and Gateway Security Manager, are personally responsible and accountable for ensuring compliance with the provisions of national or international: regulations, directives or laws, regarding data protection and interconnection. Data protection applies to all personal data that is held, processed or controlled by the Gateway Operator regardless of its origin or the system it is held on.

A2.1.2 Information Security Management

Unless otherwise stated BS7799 or equivalent shall be complied with.

A2.1.3 Gateway Security Policy Document

Gateway security policy document must be produced and owned by the gateway security manager.

A2.1.4 Gateway Manager's Responsibilities

Gateway managers are responsible for ensuring that all new gateway products and services are registered with an appointed gateway security manager. Additionally, they must ensure that:

- security statements are included in the gateway product & services business cases and supporting quality documentation
- the roles and responsibilities of the Security Manager and how to get in contact with him or her are stated in Quality documentation
- periodic reviews of the security documentation and the effectiveness of protection controls are completed
- the role of 'Security Manager' is assigned to an individual who will then ensure that security policies are implemented and maintained

A2.1.5 Assessment of Gateway Systems

System owners must assess their systems to determine security requirements with respect to the value of the system to the business. Estimates should be made of the loss to the company as a result of security breaches and unavailability. Appropriate controls and measures should be implemented to manage any security incidents and that any losses are effectively managed.

A2.1.6 Impact of Unauthorised Information Access

An assessment must be conducted to determine data assets at risk. It should be verified that only the required information within the OSS can be accessed e.g. if only name and address details are required then access to billing details should be prohibited. If access cannot be prohibited then the impact of this on the security of information shall be assessed and taken into account prior to signing any agreement.

A2.1.7 Responsibility for Fraud Risk Management

It is the responsibility of Gateway Managers, and other business process owners, to ensure that the risk of fraud is assessed. Also, appropriate controls and measures should be implemented to manage the fraud risks for gateway processes and that any losses are effectively managed.

A2.1.8 Trusted Third Parties

The use of Trusted Third Parties must be based on mutual agreements made with interconnecting SPs. Services supported would include:

- Certification Authorities
- Registration Authorities
- Security Monitors
- Security auditors
- Notaries
- Key Recovery Services
- Time Stamping Services
- Data Recovery Services

A2.1.9 Segregation of Environments

Development, test and live environments shall be segregated in order to minimise the risk of negligent or deliberate gateway system misuse and the propagation of errors between environments.

A2.1.10 Security Clauses in Service Level Agreements

Any agreements or supplementary agreements must contain the necessary security clauses to protect OSS information. The following will be included as appropriate:

- non-disclosure agreements to cover any OSS information shared with SPs
- what access to the Gateway Operator information is to be allowed and, if so, under what terms and constraints
- agreement to protect the Gateway Operator information to an equivalent standard as defined in BS7799 or equivalent
- provision for the Gateway Operator to check the security arrangements of the SP, if necessary, in order to verify the controls implemented to protect the Gateway Operator's information and *vice versa.*

A2.2 Information Security and the Protection of Assets

A2.2.1 Protection of Information

Gateway Manager shall ensure that:

- liability for protection failures are identified, specified and where appropriate, communicated to customers. This will be used in forming contractual agreements.
- all processes associated with the gateway will protect the confidentiality, integrity and availability of information whether it is the Gateway Operator's, SP's or service customer's
- identification and authentication requirements are specified for all users of the gateway, including those who support the gateway
- profiles are specified for access and authority levels for all users and people supporting the gateway
- critical functions within each process are protected against errors, missing information and unauthorised modification

- SP provided data can only be altered either at the SP's request or where the SP has agreed the alteration process
- only authorised people have access to the gateway or customer provided data in order to modify it
- accurate customer records, including charges, are maintained

A2.2.2 Privacy Markings on Electronic Information

All information held electronically must have a designated owner who is responsible for ensuring that the information clearly displays the appropriate privacy marking to reflect the impact of disclosure, alteration, incompleteness or unavailability of the information.

A2.2.3 Password Standard

Passwords are an important and simple means to authenticate users to systems by something they know. Passwords standards should be designed to reduce the risks associated with password: guessing, cracking, disclosure, etc.

A2.2.4 Encryption Key Management

The subject of key management is of critical importance in the security of Gateways. The components and architecture of the Public Key Infrastructure (PKI) implemented for key management purposes will be subject to mutual agreements. Procedures must be defined and followed for the management of all cryptographic keys (including secret and private keys). The Security Manager should ensure the secure back-up of keys for emergency purposes.

A2.2.5 Encryption Key Length

Gateway Operators must define the minimum key lengths needed to satisfy various information confidentiality levels or periods required. This applies to both symmetric and asymmetric cryptography and will be subject to mutual agreement and possible governmental control.

A2.2.6 Non-Repudiation

Where there is a requirement to prove the identity of the origin of data or messages, or to obtain 'proof of receipt', agreed cryptographic techniques or other similarly robust mechanisms must be used. The use of digital signature mechanisms and Trusted Third Parties will be the subject of mutual agreements.

A2.2.7 Transmission of Confidential Information

When confidential information is transmitted outside of the gateway, it must be encrypted to protect its confidentiality for a minimum time period.

A2.2.8 Message Integrity

Message integrity checks must be used where it is necessary to ensure that the transmitted data is not corrupted or subject to unauthorised changes.

A2.2.9 Data Input Validation

Data input validation must be used to maintain the integrity of the gateway. Procedures and supporting mechanisms must ensure that failed records are captured for subsequent correction.

A2.2.10 Internal Processing Validation

All gateway applications must be designed to minimise the risk of corruption caused by processing errors by building in validation checks, reconciliation checks, etc. on high integrity files, records and data items. Gateway software must:

- detect errors as soon as possible
- prevent unintended duplications being
- highlight any large value transactions made
- highlight any rare events specified as potential attacks

A2.2.11 Trusted Software

Gateway software shall not have any undocumented functionality. The software shall be authenticated and version managed.

A2.2.12 Change Control

All software must be subject to change control procedures. Vendor supplied software packages must not be modified outside of the scope recommended by the supplier. The procedures and supporting mechanisms must ensure that:

- all changes are notified to the Gateway Security Manager prior to authorisation in order to assess the security risk and to decide whether the security policies will remain valid
- changes are reviewed by the Gateway Security Manager prior to authorisation
- changes are properly tested and authorised prior to implementation
- all change requests are logged
- all associated documentation reflects the software change
- no unauthorised movement of code is permitted between the development, test and live environments
- any emergency changes are made under the supervision of the Gateway Security Manager.

A2.2.13 Access to Gateway Program Source Libraries

Access to gateway program source libraries must be controlled such that:

- code shall only be released on a strictly need to use basis
- code shall be subject to review before updating the source library
- old versions of code shall be archived

A2.2.14 Use of Authorised Software

Only authorised software shall be loaded onto gateway computers. This is to protect not only the fuctional integrity of the gateway but to avoid the loading of viruses or other malicious software. Implementation of this includes strict version management and integrity checking.

A2.2.15 Data Back-up for Recovery

Regular back-up copies of all essential data and software must be taken to facilitate recovery in times of failure and ensure minimal loss of data in the event of a major disaster. Back-up copies must be taken for all data, where the owner of that data believes it to be essential to the business, even if the system itself has not been deemed as requiring fallback.

A2.3 Authorisation & Administration

A2.3.1 Gateway Access Control Policy

The gateway system owner must ensure that an access control policy is defined which limits the access to data by users to the minimum required to perform their duties.

A2.3.2 Password Resets

Where password resets are required, these must be authorised by the Gateway Security Manager or through an electronic password reset system, which contains sufficient verification mechanisms (call back, local checks, knowledge of personal data etc.).

A2.3.3 Authorisation for Access to Gateway System Utilities

Permanent authorisation for access to gateway system utilities, e.g. editors and compilers, must only be allowed where absolutely necessary and restricted to the minimum number of authorised privilege users necessary. Access to software tools must be strictly controlled in the live environment.

A2.3.4 Segregation of Duties

Clear segregation of duties between the Gateway Operator is necessary to minimise the risk of negligent or deliberate system misuse. In particular segregation must be implemented between:

- Gateway Operator business use (the Gateway Operators own users)
- Service Provider users (SP)
- Gateway operations and maintenance
- Gateway system administration and Change management
- Gateway system development
- Security management
- Security audit

A2.3.5 User Id Authorisation

User IDs must be authorised through the appropriate business channel. This involves identifying the business need and to receive confirmation from authorising sources. All authorisations must be verified by an appropriate means and a record maintained of all valid authorisations for access.

A2.3.6 Management of User Profiles

User Ids that have powerful privileges associated with them must:

- only be provided and maintained by the Gateway Manager or an appointed Gateway System Administrator
- be set up with the minimum privilege and access required for the user to perform their duties
- only be allowed where there is a justifiable business need and no alternative mechanism is available
- only be authorised in response to an authorised change request (or a documented problem report and removed following completion of the work)
- be subject to audit

Templates used to set up User Ids must have no default privileges associated with them. Where it is necessary to provide privilege access authorisation on a permanent basis then a separate User Id must be allocated for performing normal work.

A2.3.7 Review of User Profiles

It is the responsibility of the Gateway Manager, in conjunction with the Gateway System Administrator, to periodically review user profiles and take appropriate action based on that review to reduce or remove access. Records of the review must be maintained.

A2.3.8 Authentication management and registration

A critical responsibility rests with the Gateway Manager for registering the users of the gateway both externally and internally. The SP gateways will also demand authentication, so provision of proper registration services will be necessary. For the registration of external users in particular, a Trusted Third Party may be used, subject to mutual agreement.

A2.3.9 Review of User Access

It is the responsibility of the gateway system administrator, to review the continuing need for access requirements and take appropriate action based on that review to reduce or remove access. Records of the review must be maintained.

A2.3.10 Authority to Interconnect

All interconnections must be authorised via an authority to connect process that has been approved by the gateway security manager. This will ensure:

- that an interconnect agreement is established between the domain owner and the other entity prior to the implementation of the interconnection
- compliance with technical and commercial security policies
- conformance with legal and regulatory conditions

A2.3.11 Gateway Security Penetration Testing

Any aggressive testing of security controls in a live gateway environment must be carried out strictly in accordance with a written schedule and the prior authorisation of the gateway manager and gateway security manager.

A2.3.12 Authorisation for Access to Audit/Monitoring Tools and Log Files

Access to audit/monitoring tools and data must be restricted on a need to use basis to members of the audit function or Trusted Third Parties. Updating access to the gateway log files and audit/monitoring tools must be strictly controlled via authorised change requests.

A2.4 Access Control & Authentication

A2.4.1 Gateway Access Control Policy

The Gateway Operator will establish detailed logical access control policies, standards and processes to limit the risk of unauthorised access by ensuring that:

- access to gateway services is via a secure log-on process
- access to electronic information is established and maintained at a level that is the minimum operationally required for an individual to discharge his/her responsibilities

- segregation of duties occurs to enhance security
- all legal and regulatory requirements are fulfilled

A2.4.2 Data Segregation and Access

Full consideration must be given to the segregation of data areas within the gateway so as to limit users' access to the minimum data necessary for them to perform their functions. This shall be enhanced by the use of transactions and transaction profiles (e.g. number of transactions per unit time) to which only certain User Ids have access.

A2.4.3 User or System Authentication

All connections to OSS interconnection gateway systems must use strong authentication (e.g. one-time password mechanism). Authentication should use a physical token e.g. a smart card, as well as something known such as a password.

System authentication will be assigned to a system owner who is responsible for the security of that system.

Means to provide authentication include:

- Something known
- Something possessed
- Biometrics
- Location
- Time
- Behaviour (or system response)

A2.4.4 Password Security

Owner/users of a User Id, must not disclose their password outside those people authorised to use it. Passwords must :

- not be written down or stored electronically, unless treated as appropriately privacy-marked information and protected in accordance with the highest privacy marking of the information which could be accessed if the password was compromised
- be stored in a one-way encrypted form away from the gateway system/application data files in a protected password file that is access controlled such that no users can read or copy the encrypted contents

Passwords are a primary means of authenticating users by something they know. Passwords are often adequate security in cases where assets at risk are not high or when there is good site security. Gateway systems must be designed in such a way as to verify as far as possible that the passwords entered are compliant with the Gateway Operator's Password Standard.

A2.4.5 Initial Password Use

When initial passwords are set, or after reset of passwords, the user must be forced to alter the password at the first logon using the new password.

A2.4.6 Password Changes

Forced password changes must occur periodically, with shorter periods for selected privileged User Ids. The facility must also be available to change them at any time (especially if a password compromise is suspected). On changing a password, the gateway system must ask for confirmation

to cater for typing errors. Reuse of passwords must not be permitted within a set period (e.g. 12 months).

A2.4.7 Pre-programming of Passwords

Passwords must not be included within any automated logon sequences, macros or function keys unless authorised by the gateway security manager. Where this is authorised the passwords must be stored using encryption according to the sensitivity of the data on the gateway system.

A2.4.8 Gateway Management Access Control

Gateway management ports must be specially protected by approved gateway access control mechanisms. These mechanisms must include strong authentication of users.

A2.4.9 Welcome Screens

Welcome screens presented prior to logon must contain only the minimum amount of information for access authorisation (i.e. a minimal prompt for User Id and password). OSS interconnection gateway system and application identifiers must not be displayed prior to logon.

A2.4.10 Validation of Log-on

User log-on must only be validated after all information has been input. If failure occurs during log-on, only anonymous help must be given. It must not be possible without further reference, to interpret the failure message to know what part of the log-on sequence has failed.

A2.4.11 Prescribed Warning Screen

A prescribed warning screen must be displayed immediately after a user successfully completes the logon sequence to any gateway system. The screen will require confirmation that the user has understood these requirements prior to proceeding. The prescribed warning screen could be worded as follows:

****

[OPERATOR NAME]

WARNING: You have accessed the [OSS INTERCONNECTION GATEWAY NAME] operated by [OPERATOR NAME]. You are required to have a personal authorisation from the gateway system administrator before you access the gateway system and you are strictly limited to the use set out in that written authorisation. Unauthorised access to or misuse of this gateway system is prohibited and constitutes an offence under the [LAW OF COUNTRY].

Are you authorised to access this OSS Interconnection Gateway as detailed above? (YES/NO)

****

A2.4.12 User Id Lockout or Disablement

After a preset number of consecutive unsuccessful attempts to log-on to a User Id, it must be disabled. Reset may be automatic, following a predefined time or time extending period. The data link must be dropped at the point where the User Id is disabled and a record shall be maintained by the gateway system of unsuccessful log-on attempts.

A2.4.13 Previous Session Information

On completion of successful log-on the date and time of previous successful log-on and details of any unsuccessful log-on attempts since the previous successful log-on must be displayed.

A2.4.14 Presentation of Options

After successful log-on to the OSS interconnection gateway system, users must only be presented with options for gateway systems/applications for which valid authorised User Ids are held.

A2.4.15 Terminal Identification

Where it is necessary to restrict access to gateway systems/applications, or restrict specific gateway transactions/profiles to specific terminals, then terminal identification or a similar method must be used.

A2.4.16 Temporary Access for Supplier Maintenance

Temporary links must:

- only be established from the Gateway Operator end after manual intervention
- have the ports disabled when not in use,
- have all remote diagnostic activity logged and audited
- have any User Ids allocated for this purpose disabled when not in use

A2.4.17 Remote Access for Supplier Maintenance/Repair

Remote access by gateway vendors for maintenance or diagnostics purposes to gateway hardware must be strictly controlled so as to protect the security of the gateway system. Maintenance must only be performed via the link at pre-arranged times as agreed with the Gateway Operator.

A2.4.18 Single Sign-on

Single sign-on mechanisms which are capable of password synchronisation across several systems must only do so if the single sign-on mechanism complies with the gateway access control policies. If there is any doubt regarding single sign-on mechanisms then it is safer to not enable them until properly evaluated.

A2.5 Accountability

A2.5.1 Gateway Accountability and Audit

The Gateway Manager shall ensure that:

- All processes, systems and data that require auditing are specified.
- The Gateway System Administrators are made accountable for their actions and audit trails of user and interconnected systems are maintained to ensure that unauthorised activity is detected.
- The gateway is security monitored by the Gateway Security Manager and detected events are acted on.
- Audit records are logged and can be analysed. The logs shall be checked periodically by the Gateway Security Manager to identify potential breaches of security and any such breaches must be investigated. The content or attributes of logs must not be modified until any

investigation is complete and must then be retained. Only authorised people shall have access to the logs.

A2.5.2 Unique User Id

Each user of the gateway must be uniquely identifiable to the gateway system by means of a unique User Id to allow for accountability and audit of actions. The owner of the User Id is personally responsible for any actions that take place using the User Id.

A2.5.3 Gateway Configuration Monitor

The Gateway Manager must ensure that the gateway configuration is checked at regular intervals to ensure that it has not been subverted or incorrectly set.

A2.5.4 Gateway Security Monitoring

Gateway security monitoring procedures must be implemented which ensure that audit data is inspected using appropriate tools and techniques. The procedures will include:

- Who is responsible for inspecting the audit data (i.e. the Security Manager and Security Auditor)
- Which events must be monitored
- How events will be monitored
- The frequency of monitoring
- What to do when suspicious activity is noted
- When to escalate and via what mechanism

A2.5.5 Security Alarms

Software security alarms should be provided to indicate to the systems security auditor when security breaches or attempted breaches occur. The logical access control policy for the gateway application or system should stipulate the circumstances/ conditions which will cause the alarm to be triggered.

A2.5.6 Access to Gateway System Utilities Logging

All use of powerful gateway system utilities must be logged and audited. Such logging may only be enabled or disabled by the Security Manager under strong authentication.

A2.5.7 Event Logging

In addition to any gateway system specific event logging requirements, the Gateway Security Manager must ensure that the following events are logged:

- Enabling and disabling of the audit process
- Any changes to the type of events logged by the audit trail
- Start up parameters and any changes to them
- Gateway system or gateway application start-up and shut-down
- Successful logins and login attempts (e.g. wrong User Id/password, and login patterns)
- Rejected access attempts because of insufficient authority
- All usage by privilege users (e.g. powerful access to gateway system utilities of gateway applications

- Use of selected gateway transaction
- Use of sensitive resources (e.g. access to confidential information)
- Changes to user privileges

A2.5.8 Unavailability of Audit Trail/Log Files

Where the gateway security audit trail or log files become unavailable for any reason the gateway system must continue to operate but an alarm must be triggered to the gateway system security manager.

A2.5.9 Retention of Journals and Audit Records

Audit records and journals must be retained in sufficient detail to allow for accountability and evidential purposes. Backup copies must also be maintained to protect against any accidental or deliberate erasure of data.

A2.5.10 Incident Management Procedures

Security incident management procedures must be drawn up by the Gateway Manager to ensure a quick and orderly approach to an incident. They should cover all types of security incident and cover or tie into (if separate) Fallback, Disaster Recovery and procedures for handling Viruses and Hacking. They should include the following:

- Collection and securing of important audit trails relating to the incident
- Immediate evaluation of problem severity
- All problems are allocated an owner (group or individual)
- Recording, reporting and review of emergency actions taken in response to the incident
- Analysis and identification of the cause of the incident
- Planning and implementation of remedies to prevent recurrence

A2.6 Implementation and Availability

A2.6.1 Gateway Configuration

Gateways must be configured so that:

- the nature of gateway internal systems and the structure of the Gateway Operator's internal network is not visible from external networks
- only explicitly addressed external traffic is routed onto external networks
- only authorised protocols are allowed to pass through to the gateway

A2.6.2 Gateway Design

Gateways must be designed to limit the effect of a component or link failure by providing alternative elements and routing. Single point of failure analysis should be conducted to minimise the effect of failure on gateway users. Gateways must be structured to limit the effect of any security breach.

A2.6.3 Communications Security, Interface Designs and Firewalls

Interface designs must include the capability to selectively deny access to certain types of data. Access from or to the Internet must be made via a suitable managed firewall. A managed firewall is also recommended, between the Gateway and the Gateway Operator's internal network.

A2.6.4 Logically and physically Secure LAN

The Gateway must only be connected to a secure LAN. The connection points for all LAN wiring, including ducts, risers and conduits, used to transport gateway information must be inspected on a regular basis to detect unauthorised access. The secure LAN must:

- be a separate security domain
- be restricted to users who have an operational need to access it
- have its direct access points within the Gateway Operator's secure premises
- only be connected to other networks via a secure firewall

A2.6.5 Physical Protection of the Gateway components

Risks to the physical security of the gateway servers must be addressed and appropriate counter measures implemented. As a minimum, these must include controls to prevent unauthorised access to the gateway components. At the outset, the planning process for a gateway installation must include security considerations regarding its physical siting and location. e.g.:

- accessibility of servers or other equipment
- civil unrest
- threats from incompatible neighbouring accommodation or work, both internal and external
- effects of natural disasters or burst water mains/tanks etc.

A2.6.6 Failures Prevention and Detection

Prevention and detection measures will be employed to prevent computer installation failure caused by interruption of essential services or other environmental influences.

A2.6.7 Hardware Maintenance and Failure Recovery

Hardware, both computer and network, shall be maintained regularly in accordance with manufacturers specifications. Where necessary, agreements shall be established with suppliers for recovery from failures within appropriate timescales to support the agreed service levels for the system.

A2.6.8 Master Consoles

Gateway master consoles must be:

- located in a physically secure environment
- sited such that their use cannot be overlooked by anyone who is not authorised
- cabled securely to prevent interception taking place

A2.6.9 Initial Password Conveyance

The conveyance of initial passwords to a user must be done in a secure manner and shall not be associated with the user ID. This is a critical implementation process to maintain adequate authentication.

Default Supplied Passwords

Any default or supplied passwords e.g. gateway manufacturer's supplied passwords, must be changed as soon as the gateway system/application is loaded within a gateway operator's environment.

A2.6.10 Gateway Software Verification

All gateway software must be tested prior to migration into the live environment to ensure that it:

- does not introduce security weaknesses
- functions according to requirements, especially security requirements
- does not adversely affect the operation of the OSS interconnection gateway system
- introduces no unauthorised system changes

A2.6.11 Software Maintenance and Failure Recovery

System and application software shall be maintained or upgraded as and when required in accordance with manufacturers and developers requirements. Where necessary agreements shall be established with suppliers for recovery from failures within appropriate timescales to support the agreed service levels for the system.

A2.6.12 Gateway Software and Data Back-ups

A back-up strategy must be defined and documented which ensures that the gateway can be recovered following failure (e.g. Hardware or Software, data corruption etc). This strategy must identify:

- the data/components which require back-up
- the frequency of the back-up, commensurate with the criticality and amount of change
- any specialist storage requirements

A2.6.13 Computer Media Labelling and Asset Registering

All computer media shall be electronically and physically labelled so that each item is individually identifiable both electronically and visibly. The use of descriptive labels other than privacy markings must be avoided. A register of assets shall be kept showing which computer the media belongs to, normally via an appropriate media management system. Care shall be taken in:

- computer media storage
- packaging and transportation
- erasure and destruction of computer media

A2.6.14 Contingency Planning for Gateways

Gateway manager must ensure that:

- procedures for the backing up of processes, systems, networks, applications and data are implemented and tested
- a business impact review is used to identify those processes, systems, networks, applications and data which will require rapid recovery in the event of a disaster
- a disaster recovery plan is established and maintained which allows recovery at a fallback site if necessary, within the required response time, and that the effectiveness of the plan is tested frequently through a fallback rehearsals programme

A2.6.15 Disaster Stores

Gateway manager must ensure that:

- Disaster Stores must be sited so that they are physically remote from, and cannot be affected by, any incident at the gateway installation.

- Alarms to detect unauthorised access and fire in disaster stores must be installed and connected back to a manned control position.
- The disaster store environment must be maintained in accordance with manufacturer recommendations for the storage of magnetic media.

Appendix 3 Security Requirements

(See Volume 2, Annex 1 for the complete list of gateway requirements.)

A3.1 General

ISEC 1 Products shall permit the gateway operator's security and policy to be enforced in the gateway. (R)

ISEC 2 Identification, authentication and encryption mechanisms used within the gateway must be fully documented and may need to be logged with the TTP. (R)

ISEC 3 Products must be capable of security evaluation to international standards by a third party in accordance with recognised standards. (R)

ISEC 4 Gateways must be capable of working with pre-existing and deployed firewalls. This may require specialist engineering to link any proprietary service/protocol to any required firewall inspection scripts. (R)

ISEC 5 Operating systems must be configured with the minimum set of applications necessary for functionality of the gateway. (R)

Frequently, vulnerabilities are discovered in operating systems and applications which may require remedial work, patches, or component replacement. (I)

ISEC 6 Suppliers shall state their approach to newly identified vulnerabilities, including any links they may have to agencies such as CERT, for the management of emergency software changes. (R).

ISEC 7 Secure operating procedures must be available. (R)

ISEC 8 The default security parameters associated with another Operator shall be configurable by TGO on a gateway wide basis. (R)

ISEC 9 Security relationships with individual Other Operators shall be configurable from the default on a contract-by-contract basis. (R)

A3.2 Architecture

Appropriate security technology and defence in depth can provide adequate protection against many of the threats that exist on open and insecure networks such as the Internet. Systems, which have functional separation across discrete physical devices, can provide a more formidable barrier to attackers. (I)

ISEC 10 The gateway must work with a simple browser or through an Other Operators OSS gateway. Suppliers must state how authentication and audit requirements are met. (R)

ISEC 11 There shall be functional and preferably physical separation between those components, which authenticate and interact with users and those components which process control logic. (R)

ISEC 12 It shall not be possible to access any management or control functionality on the Gateway via any interface utilised by Other Operators to access the gateway. (R)

ISEC 13 All devices, including routers, firewalls and servers etc., which form the gateway solution should be possible to be managed out of band. (R)

ISEC 14 Any connection to a public IP network must be via a Firewall device. (R)

ISEC 15 There shall be no direct IP connectivity end to end across the gateway. (R)

ISEC 16 Customer data shall not be held on the gateway. (R)

A3.3 Authentication/ access control

ISEC 17 Connections between TGO and Other Operators shall be strongly and mutually authenticated. (R)

ISEC 18 It shall be possible for the gateway to strongly and mutually authenticate itself to other equipment and to authenticate management connections. (R)

ISEC 19 The gateway shall authenticate (and log) each message as to its point of origin. (R)

ISEC 20 Tokens, keys, initial passwords and other access control material shall be issued by, and be under the control of the TTP. (R)

ISEC 21 It shall be possible for Other Operators to perform their own user management (create and delete users and assign permissions) within the agreed parameters set by TGO with that Operator. This would usually be a reciprocal relationship. (R)

ISEC 22 The method for how user IDs will be managed and distributed securely must be evaluated by the TTP. (R)

There is a possibility that keys can be lost, transactions records could be corrupted to remove evidence etc. (I)

ISEC 23 The Gateway TTP shall have key recovery techniques and procedures. (R)

ISEC 24 Authentication failures shall be logged and alerts generated if administrator configured thresholds are exceeded. If the gateway cannot authenticate a message the message shall not be processed. (R)

ISEC 25 It shall be possible to readily disable an account or accounts belonging to a single Other Operator by a Trusted Administrator (TA). Such an event shall be logged and the Registration Authority shall be alerted. (R)

ISEC 26 It shall be possible for TGO to extend or replace any functionality providing access control on any interface, be it customer facing, internal OSS facing, or management and administration. (R)

ISEC 27 The system must disable any account after three (or other predetermined number) failed authentication attempts. Any exceptions to this functionality on any part of the system must be stated. Suppliers must state how accounts are re-enabled and the audit process associated with this requirement. (R)

ISEC 28 The range of actions displayed to any user via any menu must be limited to those actions available in the users profile. (R)

ISEC 29 Mechanisms shall exist to protect against message replay attacks. (R)

ISEC 30 The system shall not allow any incoming Other Operator connection being routed to another Other Operator connection. (R)

ISEC 31 UNIX utilities (and similar), which allow network access to, provide information about, or connect to remote hosts, must be disabled or removed. (R)

ISEC 32 Systems shall be configured to ensure that system interfaces have the minimum set of services required for that interface. Systems shall be configured to ensure that all non-essential ports are disabled. (R)

ISEC 33 It shall be possible to assign users to one or more roles for the purpose of managing access-control. (R)

ISEC 34 The gateway shall control multiple levels of access to data for reading, writing, modifying, creating and deleting. It shall be possible to map these capabilities for specific resources (e.g. order PSTN line) onto roles. (R)

A3.4 Authorisation

ISEC 35 Each message received shall be authorised by the gateway before further processing in accordance with the rules below. (R)

ISEC 36 The services accessed and the transactions allowed for any Other Operator connecting to the Gateway shall be authorised in a Service Level Agreement and reflected in profiles stored by the Gateway.

ISEC 37 The gateway shall verify that the Other Operator is permitted to issue the particular transaction. (R)

ISEC 38 The gateway shall verify that the Other Operator is entitled to access the requested resources. (R)

ISEC 39 Authorisation failures shall be logged and alerts generated if administrator configured thresholds are exceeded. If the message cannot be authorised the message shall not be processed. (R)

A3.5 Validation

ISEC 40 Each incoming request from an Other Operator shall be validated to ensure internal message correctness and consistency and that it can be interpreted properly. (R)

ISEC 41 Each message destined for the Other Operator shall be validated to ensure the correct data is destined for the correct Other Operator. (R)

A3.6 Confidentiality

ISEC 42 All information communicated between the Gateway and the Other Operator shall be encrypted. (R)

ISEC 43 TGO must be able to deploy encryption developed or recommended by the supplier or any other scheme agreed with Other Operators. (R)

ISEC 44 Any cryptographic techniques or technology used by the Gateway used for the purposes of encryption, authentication, or signatures shall not contravene any national regulations and consequent restrictions. (R)

A3.7 Integrity

ISEC 45 Mechanisms shall exist to ensure integrity of data between the Gateway and the Other Operator. (R)

ISEC 46 The gateway shall support digital signatures for transactions. (R)

ISEC 47 Unauthorised changes and corruption of files must be detected and reported to the system administrator. (R)

A3.8 Availability

Devices connected to publicly accessible networks may be subject to attack to deny service to legitimate users of the device. (I)

ISEC 48 The gateway must be resistant to attack from SYN flood attacks, sustained Ping attacks, and other commonly understood denial of service methods. (R)

A3.9 Data separation

ISEC 49 All information flows within the gateway must be explicitly defined. (R). The Separation of each Other Operators data within the Gateway is clearly important. (I)

ISEC 50 Suppliers must state the mechanisms and techniques that are used to achieve such separation. (R)

ISEC 51 All IP connections between physical devices, which comprise the total gateway solution, shall depend upon static configuration of routes, not dynamic routing. (R)

A3.10 Audit

ISEC 52 I It shall be possible for TGO to identify individually identifiable accounts (User IDs or Functional Entities) for Other Operators which have been opened by a trusted administrator (R)

ISEC 53 Records of interchange between TGO and the Other Operator shall be maintained to protect TGO against repudiation of instructions. These records will include the following (R):

- Date and time using a trusted time source
- SP and SP end user reference
- Transaction number
- Transaction details

ISEC 54 A TTP read only monitor and audit log shall be available on each gateway – This is for resolving disputes and for law enforcement purposes.

ISEC 55 Immediate reference path must be established to a TTP in the event that an Other Operator has been detected by TGO to have been compromised.

The requirement for audit extends to the end-to-end solution. In multi-tier architectures, with audit logs kept on each platform it can be a complex and time consuming task to analyse a single transaction and determine its complete history and propagation. (I)

ISEC 56 The gateway shall support standard ways of identifying specific audit transactions to provide simpler reconciliation. (R)

ISEC 57 As a minimum the following events shall be logged: (R)

- Logon and logoff (by UserID)
- User and Group management
- Security policy changes
- Restart, shutdown and specified system events
- Order placement
- CDR transactions

ISEC 58 Analysis tools to examine audit logs shall be available to determine patterns of activity that would indicate misuse or attack. The capabilities of such tools shall be subject to standardisation and conformance testing in their own right. (R)

ISEC 59 When transactions occur as a consequence of previous transactions then they shall be correlated in the logs before proceeding beyond initialisation. (R)

It may be necessary to use audit information in a court of law. (I)

ISEC 60 Use of audit records as evidence requires the proof of a properly operating computing platform together with a case that the audit logs are a true and accurate reflection of what happened on the system at that place and time, and that the logs have not been subsequently tampered with. (R)

ISEC 61 Logging shall prove when a transaction was received, processed and responded to by both the Other Operator and the TGO sides of the gateway. The trusted clock mechanism shall not produce any sequence errors or timing disputes.(R)

ISEC 62 Logs of messages shall support certification of performance and response times. (R)

ISEC 63 Logs of messages shall support trouble reporting and resolution. In some cases, gateway operation may be suspended until critical faults have been cleared. (R)

ISEC 64 The audit trail shall provide functionality to support audit functions related to OSS access such as security, backup and recovery, interface compliance and proof of equivalence. (R)

ISEC 65 Logging shall be TGO configurable to support multiple levels of logging for traceability, debugging, performance monitoring and on an *ad hoc* basis. (R)

ISEC 66 The gateway shall allow TGO to configure log sizes for both alarm and maximum levels. (R)

ISEC 67 Alarms shall be generated if log sizes reach the size configured by TGO. It shall be possible for logging and service to continue until the maximum defined size is reached, when service could be disabled automatically. (R)

ISEC 68 Logs shall contain the complete message to which an entry relates. (R)

ISEC 69 The gateway shall allow for the viewing of the audit data of a transaction by the originating SP or a third party at the discretion of TGO. (R)

ISEC 70 The gateway shall allow TGO to configure archiving methods within standard guidelines. (R)

ISEC 71 The gateway shall support management of the logs. It shall be possible to increase log file size and perform log file archiving without loss of service. (R)

ISEC 72 An Other Operator shall not be allowed to view the log data of another Other Operator. (R)

A3.11 Fraud management

ISEC 73 It shall be possible to establish rules that limit the size, nature and frequency of orders according to a pre-determined profile. These rules will be managed by TGO administrators. (R)

As TGO establishes increasing trust with an Other Operator the rule profile may be relaxed. (I)

ISEC 74 The Gateway must provide mechanisms to enforce non-repudiation of transactions on the interface to the Other Operator. (R)

ISEC 75 Non-Repudiation mechanisms shall apply in both directions. (R)

It is possible that unscrupulous Other Operators may attempt to consecutively seek through records held on TGOs OSS, or alternatively, to regularly poll TGO's OSS. (I)

ISEC 76 It shall be possible to restrict transaction volumes on a per Other Operator Basis. (R)

ISEC 77 The gateway shall support the restoration of normal security after a breach is detected. The supplier must state the recovery processes that would be required from trusted sources in the event of a breach and recovery times. (R)

ISEC 78 Should the operation of the gateway suffer a catastrophic failure, the gateway shall not permit "pass through" access to TGO internal OSS by Other Operators. (R)

Appendix 4 Evaluation of Detailed Policy Statements

This appendix provides guidance for the informal evaluation of a specific OSS interconnection gateway implementation with respect to the security policy statements as reported above. Below all individual policy statements in the Security Policies Appendix are referred to by number and accompanied by a selection of categories, which are relevant to the implementation of the policy statement. The following categories are identified:

- Organisation and Procedures (O&P)
- Product Supplied or Configured (PSC)
- Additional Measures (AM)

If the category 'Organisation and Procedures' is mentioned along with a security policy statement, then the policy statement can be –partially or fully– implemented by measures within the organisational structure, by the establishment of procedures or by contractual arrangements. If the category 'Product Supplied or Configured' accompanies a security policy statement, then the policy statement can be realised by off-the-shelf functionality or capability of the interconnection gateway product itself or of a peripheral device connected to the gateway. The category 'Product Supplied or Configured' is also referred to in the situation where the gateway can be configured or when additional functionality has been developed for the gateway to implement a particular security policy. In cases when the category 'Additional Measures' is listed it is possible that the security policy statement at hand is realised –possibly in part– using equipment, procedures or arrangements that are falling outside the scope of the organisational structure, for instance where mutual agreements are needed, and that are not directly supported by the interconnection gateway system. When applicable a further qualification of the aspects of the security policy statements that fall in a certain category is added. In many situations more then one category applies.

A4.1 General Policies

1.1.1	O&P	Legal advise in particular regarding protection and dissimination of personal data that is processed by the gateway
1.1.2	O&P	Corporate security scheme or else the BS7799-standard (available from the Britisch Standards Institute)
1.1.3	O&P	Definition of roles and their responsibilities, including 'gateway manager', 'gateway operator managing director', and 'security manager'
1.1.4	O&P	Documentation on service levels, instantiation of roles, periodic review of security documentation
1.1.5	AM	Assessment of the threats to the gateway
1.1.6	AM	Risk analysis and audit of data assets
1.1.7	O&P	Assessment and control of fraud risk
1.1.8	O&P	Mutual agreements regarding TTPs with interconnecting SPs
1.1.9	–	(O&P or PSC) dependent on the gateway product
1.1.10	O&P	Nondisclosure agreements, agreements on access and protection of gateway operator's information

A4.2 Information Security and the Protection of Assets

1.2.1	O&P PSC AM	Liability, gateway processes, identification and authentication, profiles, protection of critical functions, alteration of SP data, authorisation to modify Gateway processes, profiles, protection of critical functions, alteration of SP data, authorisation to modify, customer records Customer records
1.2.2	O&P PSC	Designated owner of information Privacy marking
1.2.3	–	(O&P or PSC) password life-cycle management
1.2.4	O&P PSC	Mutual agreements, procedures for key management Realisation of key menagement
1.2.5	O&P PSC	Selection of key length Deployment of selected key length
1.2.6	O&P PSC AM	Mutual agreements Support for digital signatures Trusted third party services
1.2.7	O&P	Encryption of outbound information
1.2.8	PSC	Mechanisms to check integrity of data
1.2.9	–	(O&P or PSC) mechanisms for validation of data
1.2.10	O&P PSC	Identification of corruption risks Error detection, duplication prevention, highlighting
1.2.11	O&P PSC	Documentation of functionality Software authentication, version control
1.2.12	O&P PSC AM	Change control procedures, documentation, supervision of emergency changes Authorisation of software updates, supervised emergency changes Testing, logging, authorisation
1.2.13	O&P	Restricted release, review, archiving
1.2.14	O&P PSC AM	Authorisation of software Version management, integrity checking Version management, integrity checking
1.2.15	–	(O&P or PSC) procedures and facilities for back-up

A4.3 Authorisation & Administration

1.3.1	O&P	Access control policy document
1.3.2	–	(O&P or PSC) procedures and conditions for password resets
1.3.3	–	(O&P or PSC) caution with respect to availability of software tools in live environment
1.3.4	O&P	Policy, documentation and deployment
1.3.5	O&P	Out of band security
1.3.6	O&P	Control of user profiles with special privileges
1.3.7	O&P	Responsibility of gateway manager and gateway operator managing director

1.3.8	O&P AM	Registration of internal and external users trusted third party
1.3.9	O&P	Access rights should be kept as minimal as possible
1.3.10	O&P PSC	Interconnection agreement, legal and regulatory conditions Authorisation of interconnection
1.3.11	O&P	Approval by gateway security manager
1.3.12	–	(O&P or PSC) access restricted to need to know basis

A4.4 Access Control & Authentication

1.4.1	O&P	Gateway operator to establish detail policy and procedures
1.4.2	O&P	Access to data as restricted as possible
1.4.3	–	(O&P, PSC or AM) multiple way authentication
1.4.4	–	(PSC or AM) no passwords in clear text on the gateway
1.4.5	PSC	Forced alteration of password
1.4.6	PSC	Based on clear policy
1.4.7	–	(O&P or PSC) protection of password communication
1.4.8	O&P	Transparent view on port traffic
1.4.9	PSC	No disclosure of the identity of the gateway
1.4.10	PSC	No disclosure of login information
1.4.11	PSC	Legal matter
1.4.12	PSC	Anti-hacker measure
1.4.13	PSC	To alert possible misuse
1.4.14	PSC	Minimal functionality
1.4.15	–	(O&P or PSC) authentication of location
1.4.16	–	(O&P or PSC) minimise vulnerability to attack
1.4.17	–	(O&P or PSC) out of band security
1.4.18	O&P	Prevent mismatch of rights obtained form single sign-on server and gateway access control policy

A4.5 Accountability

1.5.1	O&P PSC AM	Specification of auditing, accountability, event handling Monitoring Analysis of audit logs
1.5.2	O&P	It should be possible to trace actions back to individual user
1.5.3	O&P	Regular checks
1.5.4	O&P	Inspection of logfiles
1.5.5	PSC	Based on access control policy
1.5.6	PSC	Important source for sharpening of security measures on the gateway
1.5.7	–	(O&P & PSC) to make logging useful
1.5.8	PSC	Alarm on lack of logging facilities

1.5.9	AM	Backups of logs should be kept sufficiently long
1.5.10	O&P	Documented and timely reaction to incidents

A4.6 Implementation and Availability

1.6.1	PSC	Prevent hacking as much as possible
1.6.2	PSC	Fault-tolerant architecture
1.6.3	–	(PSC or AM) firewalls and other mechanism to reject data
1.6.4	O&P	Regular assessment of the security of the local network
1.6.5	AM	Physical security of the gateway should be in balance with its business value
1.6.6	AM	Emergency power and network connectivity
1.6.7	AM	Regular inspection
1.6.8	AM	At safe place
1.6.9	O&P	Clear and documented procedures
1.6.10	O&P	Surprisingly frequent security breach
1.6.11	AM	Testing and validation of software and its effect on the security of the gateway
1.6.12	AM	Maintenance and upgrade according to supplier guidelines
1.6.13	O&P	To facility a quick recovery
1.6.14	AM	Simple and effective security measure
1.6.15	O&P	Responsibility of the gateway manager
1.6.16	O&P	Dependent on the assets of the gateway

Appendix 5 Requirements for Mutual Agreements

In this appendix, the generic requirements for mutual agreements are listed so that a complete set of bilateral or collective security relationships can be mapped out by any gateway owner. This set of requirements cannot be complete due to there being a large number of differing circumstances regarding gateway operation, but it is aimed at being a sound starting point.

A5.1 Security environment and Ownership

[MA1.1] The owners of gateways shall be the individuals that either own or are managing directors of the operating company. Delegation of responsibility for the management of gateways shall not obscure the direct link between ownership and responsibility.

[MA 1.2] Interoperating Parties shall conform to BS7799 or equivalent.

[MA 1.3] Commonly accepted codes of practice or standards for the management of information security (e.g. BS7799) shall be used as the basis for auditing gateway security.

[MA 1.4] Standard practices for the identification of security risks, as well as the application of appropriate controls to manage those risks for gateways, shall be used. There shall be a correspondence between the risk analysis methods used by interconnecting parties whereby shared governance risks can be identified. A recommended approach can be found in the section on risk analysis in this volume.

[MA 1.5] Self-certification against EURESCOM or other codes of practice may be recognised by either of the interoperating parties where risk analysis shows that there are limited potential impacts or suitable grounds for trust in the self-certifying party.

[MA 1.6] Companies and, for the benefit of employers, individuals, shall be held liable for any damage caused by the disclosure of authentication data (passwords, private keys etc.) without urgent revocation. This should engender greater responsibility in the holder of authentication data.

[MA 1.7] A signature policy shall be clearly defined. This shall be based on EESSI and RFC 2527 shall act as the default framework for Certificate policy requirements.

[MA 1.8] Each gateway operator may act as a separate CA (it is very likely that companies will use and issue certificates internally). In providing certificates for interoperation however, the same certificate policy requirements as for a TTP shall apply. Using a common body to issue certificates would however help to simplify security risk analysis but it is possibly unrealistic to expect this to happen in the near future.

[MA 1.9] Signing parties shall be able to read all data that is signed.

[MA 1.10] The implications of signing data shall be clear, agreed in advance and unalterable. Any changes made to signing procedures, conditions, technology etc. shall be clearly notified to signing parties, explicitly state any changes in meaning and be accepted by them. Such ‘small print’ may be uniquely referenced outside of the data being signed.

TTPs

[MA 1.11] TTPs shall be agreed between interoperating parties. The functions of TTPs covering the security needs of gateways include:

- Naming Authorities
- Certification Authorities
- Registration Authorities
- Directory and Domain name services
- Validators
- Notaries

- Time Stamping Authorities
- Key recovery services
- Monitors (e.g. Regulators)
- Mediators (e.g. Regulators)
- Card Issuers
- Auditors
- Auditors & Monitors of other TTPs

[MA 1.12] Each of the TTP functions must be separated as far as possible. Any of the functions that are combined shall be subject to risk analysis by participating service customers.

[MA 1.13] An audit of gateway implementations and management systems shall be carried out using a recognised independent auditor.

[MA 1.14] Where high value transactions are signed, they shall also be time stamped by a TTP for the purposes of non-repudiation.

[MA 1.15] A TTP for notarisation of business critical transactions shall be appointed.

[MA 1.16] For business critical digital signatures, notaries shall be used.

[MA 1.17] A TTP for signature verification shall be appointed.

[MA 1.18] TTPs shall follow standard guidelines for security management (e.g. BS7799).

[MA 1.19] TTPs shall operate trustworthy systems that are open to the scrutiny of public bodies e.g. reporting of hacker attacks.

[MA 1.20] TTPs shall be members of CERT if appropriate.

[MA 1.21] Technical profiles of TTPs such as computer platforms, performance, resilience, access routes etc. shall be defined and documented. This information will be useful in the procurement of TTP services.

[MA 1.22] A TTP needs to show that it uses trustworthy systems and products in its operation. This can be achieved through risk assessment and security certification along similar lines to the EURESCOM security assessment for Gateways (note: A set of requirements for each of the TTPs are not covered by P908).

[MA 1.23] In part some of the security issues regarding TTPs can be dealt with by an auditing and monitoring service provided by another TTP that can be appointed by interoperating parties. The decision to take this route shall be subject to risk analysis.

[MA 1.24] TTP mediation results shall be made available, where appropriate to improving security practices, to other interconnecting parties using the same TTP.

[MA 1.25] Auditors of TTPs shall be used rather than direct auditing by gateway operators. This is to prevent security weaknesses of TTPs being exposed by many audits being made by parties, which have no recognised auditing or reporting standards. Compliance will be checked against appropriate standards.

[MA 1.26] Re-certification of TTPs should be carried out if major changes occur in the certification criteria, major security failures occur, or if the security requirements of operators alter e.g. in response to new attacks.

[MA 1.27] TTP audits carried out prior to mutual agreements being arrived at may be accepted.

A5.2 Information security and the protection of assets

[MA 2.1] Public Key technology shall be used for digital signatures and authentication.

[MA 2.2] Time Stamping Services shall be used when non-repudiation of actions is required.

[MA 2.3] Digital signatures without notarisation such as via a time stamping authority shall be accepted as proof of actions of either party where mediation or litigation would be unnecessary or excessive regarding assets at risk.

[MA 2.4] Cryptography shall be used to provide security functions such as confidentiality, authentication, integrity and non-repudiation.

[MA 2.5] Authentication data shall be stored in secure directories.

[MA 2.6] Certificate Standards shall be compliant with current European Standards where legal protection is required.

[MA 2.7] A risk analysis shall be carried out prior to forming mutual agreements.

[MA 2.8] New functions, policies, systems or network components connected to or built into gateways shall be subject to a risk analysis.

[MA 2.9] Directory information shall be stored in the gateway or in equally secure and managed entities elsewhere.

[MA 2.10] Encryption keys used to maintain privacy of stored data may be stored by a TTP escrowing agent where necessary. Any data that is encrypted without escrow shall not adversely affect interconnecting parties if it is lost.

[MA 2.11] Digital certificate standards shall be identified along with extensions.

[MA 2.12] X509v3 shall be the default standard for public key certificates. This shall be reviewed regularly.

[MA 2.13] The integrity of gateway software builds shall be protected.

[MA 2.14] All software builds in gateways, including source code, shall be subject to escrow. This is to ensure that any malicious code built-in, could be identified if undocumented behaviour is suspected by any gateway operators or users, utilising the software.

[MA 2.15] Any encryption technique or technology used by the Gateway for the purposes of encryption shall not contravene any national regulations or other restrictions.

[MA 2.16] Encryption key strength shall be used as a criterion to set security levels between gateways.

TTPs

[MA 2.17] Registration Authorities shall provide full details of what procedures, processes and data sources are used to link identity to a real person and how this information is securely conveyed to a CA. These requirements may be set by CAs and agreed to by operators. The registration authority will need to be trusted to not permit fraudulent activity regarding PKIs e.g. processes shall be used to prevent users obtaining more than one identity.

[MA 2.18] Algorithms and key lengths for the signing of certificates by CAs shall conform with current practices: e.g. the DSA and RSA algorithm used with 1024 bit keys. For higher assurance, 2048 bit keys may be necessary. For hashing data, the SHA-1 and RIPEMD-160 algorithms shall be used since they are widely recognised as being of acceptable strength. This requirement should be reviewed regularly.

[MA 2.19] CAs must provide an available and secure certificate directory and a secure and immediate revocation service.

[MA 2.20] A directory of Registration Authorities must be maintained by CAs.

[MA 2.21] A digital notary may be appointed to guarantee a transaction ahead of completion. The signer shall be known by the notary and the receiver of the signed data shall trust the notary. The notaries on either side shall trust each other when bi-directional signed transactions are used.

[MA 2.22] TTP Time Stamping Services shall use trusted clocks and valid certificates.

[MA 2.23] Digital hashes may be time-stamped if privacy of communications needs to be enhanced.

[MA 2.24] The private key(s) of a Time Stamping Authority must be kept secure for its active lifetime.

[MA 2.25] The date and time must come from a trusted clock which is physically secure and which cannot be set back in time to before the last time stamp was made.

[MA 2.26] The uncertainty in clock time shall be maintained within specified limits so that many independent trusted clocks can be used for transactions without introducing logical errors.

[MA 2.27] A Time Stamping Authority's Public Key Certificate shall have an expiry date after the end of any contract or document validity period that has been time stamped using it. Note: hash tree technology, secure archiving etc. could be used as substitutes for this requirement.

A5.3 Administration and Authorisation

[MA 3.1] Unique naming shall be achieved based on unique numbers generated by interconnecting businesses. Any mergers between such businesses could cause the need to revoke numbers if any collide.

[MA 3.2] Public Key Certificate Class shall be used to identify levels of privilege

[MA 3.3] Site Audit Accreditation Classes shall be used to publicise compliance with standard security practices

[MA 3.4] Authentication levels shall correspond between gateways. Users accessing resources via gateways shall be able to use differing forms of credentials including: private authentication keys, passwords and anonymous. The control of access for each level of authentication shall be appropriate to the assurance given by the technology applied.

[MA 3.5] The disclosure of private keys used for digital signatures or authentication shall trigger an appropriate response from the key owner and lead to key revocation if necessary. This shall be supported by facilities made available by the gateway administrators and shall be fast acting in the cases of keys with a high security status.

[MA 3.6] Disclosed encryption keys shall be replaced and the impact on other operators of loss of privacy shall be assessed.

[MA 3.7] There shall be appropriate means of key recovery. This could include key escrow or keys being encrypted with a key from an independent TTP that is then escrowed.

[MA 3.8] Cryptographic algorithms used in the gateway must be fully documented and may need to be logged with a Trusted Third Party.

[MA 3.9] User roles shall be matched to access rights and privileges

[MA 3.10] Multiple gateway access technologies shall be supported and user credentials and access rights shall be appropriate to the nature of the technology. Types of access technology that should be supported include dial-in, Internet (via an ISP) and mobile devices.

[MA 3.11] Policy enforcement shall be transferable between gateways.

[MA 3.12] Individual users may have more than one role. Each role enacted by an individual user will have a unique identifier but also a bonding to the user's identity. Authentication credentials may vary between roles. Concurrent sessions by an individual user shall be restricted by the lowest authentication level e.g. if a user is also logged on as an administrator, the administrator privileges shall be restricted to those of a user during the user session.

[MA 3.13] It shall be possible to revoke authentication credentials from: the user, the users administrator, the gateway administrator or a TTP, by the appropriate authorising body.

[MA 3.14] Short-term access credentials shall usually expire. It shall be possible to revoke short-term credentials and propagate this information across other domains in exceptional circumstances.

[MA 3.15] Certificates, user profiles, access profiles etc. shall be stored in directories. Transient data shall be stored in associated databases or volatile memory.

[MA 3.16] Directory schema will be advertised and standardised for gateways to facilitate ease of communications and security management.

[MA 3.17] All users accessing gateways shall have unique identifiers. Uniqueness shall be maintained across all gateways (e.g. by using common numbering scheme)

[MA 3.18] Gateways shall handle any agreed digital certificate profile. The handling of non-standard certificates shall be agreed taking into account, process costs and security risks (e.g. having data missing such as a unique identifier).

[MA 3.19] Gateway operator roles shall be defined to include:

- Gateway Owner
- Gateway Manager
- Trusted Administrators (Authorisers)
- System Administrators
- Internal Registrar
- Trusted External Registrar (other Gateways with anonymous users)
- Security Manager
- Internal Auditors

[MA 3.20] User IDs will be managed and distributed securely.

[MA 3.21] Trusted administrators shall be designated by each interoperating party, these shall digitally sign new accounts and hold electronic Ids of their own employees.

[MA 3.22] Attributes contained within digital certificates shall include unique identifiers for: company, individual, role etc.

TTPs

[MA 3.23] CAs shall inform the person applying for a certificate or their representative, of the precise terms and conditions for the use of the certificate, including limitations on the use of the certificate, the existence of a voluntary accreditation, procedures for complaints and dispute settlements etc.

[MA 3.24] Certificate revocation lists shall be maintained by CAs.

[MA 3.25] Any lost physical authentication token or disclosed password etc. should be reported across all gateways which have registered the user. This shall only be done via a TTP key revocation service.

[MA 3.26] Tokens (e.g. smart card), keys, initial passwords and other access control material shall be issued by, and be under the control of the issuing TTP (e.g. smart card issuer).

[MA 3.27] The CA must ensure the accuracy of the date and time that a certificate was issued or revoked.

[MA 3.28] The process of dealing with the disabling of accounts e.g. of a rogue operator, shall be defined. The CA and RA shall be informed via either the Gateway Operator or the Regulator.

A5.4 Access Control and Authentication

[MA 4.1] When the gateway is acting as a trusted entity, the mutual authentication of users or systems shall always take place with the gateway itself and not other interconnected systems.

[MA 4.2] Authentication levels shall be used, not only to protect the gateway from abuse, but also to protect the users from abuse of their accounts.

[MA 4.3] Authentication data shall be stored securely by gateways.

[MA 4.4] All users or systems that authenticate to the gateway for sessions, shall have authentication data translated for onwards authentication to systems owned by the gateway operator (OSS), downstream gateway operators or TTPs.

[MA 4.5] It should be possible to map authentication data consistently across multiple domains where common agreements have been reached, otherwise re-authentication shall be required.

[MA 4.6] Users shall be authenticated to a single trusted domain and the authenticated profile and translated authentication data shall be passed on to other mutually trusted domains (delegation of authentication).

[MA 4.7] Access control may depend on conditional events. If access is refused to otherwise validated credentials from another gateway, then the event shall be logged and data made available for inspection by a TTP.

[MA 4.8] Gateway session control shall be maintained between gateways.

[MA 4.9] User session control shall be maintained between gateways.

[MA 4.10] Common policies shall be specified for gateways. These will include: warning screen, password handling, presentation of personalisation data etc.

[MA 4.11] Common policies for gateways shall be enforced at the point of access.

[MA 4.12] Alternative authentication methods (passwords, one time passwords, signed challenge, iris scan etc.) shall trigger selection processes between alternative roles and access rights.

[MA 4.13] Authentication data may be tunnelled through the gateway to other systems where appropriate.

[MA 4.14] Self-contained messages passed to the gateway may be self-authenticating, e.g. digitally signed.

[MA 4.15] Self-authenticating messages will either terminate at the gateway for action, or will be logged and passed on to appropriate applications.

TTPs

[MA 4.16] All users or systems that authenticate to the TTPs, shall have authentication data translated for onwards authentication to gateways i.e. users can log on to either TTPs or gateways first.

[MA 4.17] All authentication requirements that apply to gateways shall apply to TTPs.

A5.5 Accountability

[MA 5.1] Gateways shall support standard ways of identifying specific auditable events to provide simpler reconciliation. Information logged should include: logon and logoff by user Id, user and group management, security policy changes, restart, shutdown and specified events, order placements.

[MA 5.2] Log files shall provide an accurate reflection of what happened on the system at that place and time.

[MA 5.3] The integrity of log files shall be protected so that it can be proven that the logs have not been tampered with subsequent to capture.

[MA 5.4] Gateway operators shall work together to protect assets of any party from attack (collective responsibility and co-operative defence).

[MA 5.5] Fraud management shall use co-operative means to detect external offenders and also use separate systems for internal or other gateway operator actions.

[MA 5.6] Log events captured to satisfy other gateway operators needs, regulator requirements or legal requirements shall be retained for specified periods before deletion.

[MA 5.7] Audit logs containing sensitive information shall be encrypted.

[MA 5.8] Version management of software builds shall be protected and audited.

TTPs

[MA 5.9] TTP read only monitor and audit log access shall be made available on each gateway for resolving disputes and for law enforcement purposes.

[MA 5.10] If a gateway operator suspects fraud or that another gateway has been compromised, the TTP mediator e.g. a regulator, shall be informed of the problem and if any action has been taken.

[MA 5.11] The interoperating parties shall identify the public hierarchy for traceable audit functions to be carried out.

[MA 5.12] Audits shall result in improvement plans if implementations or management systems fail to meet identified criteria.

[MA 5.13] All audit results and certifications shall carry an expiry date before which re-certification should take place.

A5.6 Implementation and Availability

[MA 6.1] Multiple gateway access and authentication technologies shall be supported by appropriate interfaces. Types of technology that should be supported include dial-in, Internet access (via an ISP) and mobile devices.

[MA 6.2] No party shall supply terminals, clients or secure devices such as smart cards to interconnecting parties. The procurement of trusted terminals shall be the responsibility of the participating company alone and security failures of such equipment shall be borne by the users.

[MA 6.3] Signature creation devices shall be protected against modification and ensure the technical and cryptographic security of the processes supported by them.

[MA 6.4] Critical data from transactions shall be backed up frequently.

[MA 6.5] Disaster recovery shall be available for critical gateway functions, which other gateways rely on.

TTPs

[MA 6.6] Issuing of smart cards or any other secure device shall be carried out by a TTP Issuer.

[MA 6.7] Conformity assessment for vendors wishing to produce and supply signature creation devices (voluntary certification/manufacturer’s declaration) shall be carried out by a TTP.

[MA 6.8] Recovery processes that would be required from trusted sources in the event of a security breach and the expected recovery times shall be defined.

[MA 6.9] Key recovery services shall only be required when data is stored in an encrypted form by one party, when other parties may need subsequent access to the data e.g. log files.

Under these circumstances a key recovery service, trusted by all parties that have a need to access the data, shall be used.

Appendix 6 Use-cases and Test designs

A6.1 Introduction

This appendix contains three proposals for use-cases and related test. The use-cases address the issues of authentication and authorisation (Use-case T4_UC01: Add authentic and authorised service provider), accountability and monitoring (Use-case T4_UC02: Add authentic and authorised service provider) and non-repudiation, digital signing and time-stamping (Use-case T4_UC03: High-value transaction). This are all essential ingredients for a secure operating of the description of the OSS Interconnection Gateway as envisioned within P908. The use-cases and test designs demonstrate an elemental deployment of the security principles. By combining these fundamental building blocks differently other security mechanism can be constructed. It is therefore crucial that –as an absolute minimum– the proposed test designs will be covered during the test phase of EURESCOM P908-compliant gateway products.

All but one of the vital security requirements (see Appendix 3 of this volume) are covered by the use-cases and test designs below, viz. ISEC 17, 19, 24, 27, 35, 39, 42, 52, 57 for use-case T4_UC01, ISEC 17, 19, 24, 27, 35, 39, 42, 52, 57 for use-case T4_UC02, and ISEC 46, 53, 57, 61, 68, 74, 75 for use-case T4_UC03. Not covered is requirement ISEC 48 on denial of service attacks. (A requirement as ISEC 48 can be verified by performing standard security testing. For most industrially deployed operating systems there are various software packages for this commercially available.)

A6.2 Use-cases, test designs and logical testmodels

Three use-cases and associated test designs are provided: 1) the addition of an authentic and authorised service provider, 2) the detection and killing of a transaction transgressing an SLA-agreed maximum, and 3) the issuing of a high-value transaction and related assurance of non-repudability.

A6.2.1 Add Authentic and Authorised Service Provider

Use Case Name	Add authentic and authorised service provider
Code	T4_UC01
Summary	This Use Case will demonstrate the addition of a new service provider
Roles	Service Provider (SP), Gateway Operator (TGO)
Preconditions	Fully operational gateway, new service provider in possession of a smart card and a public key attribute certificate
Begins When	New service provider contacts the gateway
Description	• Authentication of new SP • Validation of authority of new SP • Logging of relevant actions
Ends When	The new SP has been authenticated and authorised.
Postconditions	Update of logfile
Exceptions	Failure in authentication or authorisation
Traceability	ISEC 17, 19, 24, 27, 35, 39, 42, 52, 57

Use Case Ref: T4_UC04
Test Design ID: T4_TD01
Test Purpose Successful authentication of new service provider
Covered Requirements ISEC 17, 19, 24, 27, 35, 39, 42, 52, 57
Preconditions • Fully operational gateway (GW) • New service provider (SP) in possession of appropriate smart card (ISO7816) and public key attribute certificate (X.509 version 3)
Test Description • New SP connects to GW • New SP identifies himself • GW authenticates new SP using smart card • New SP presents his public key attribute certificate to GW • GW initialises new SP with user profile as indicated by the attribute certificate
Expected results • Authentication of new SP by GW succeeds • New SP obtains user profile as indicated by attribute certificate
Postconditions • New SP has been added to GW with user profile as indicated by attribute certificate • The logfile shows the essential steps in the authentication and authorisation of new SP

NOTE: Exception test designs for failing authentication and failing authorisation still to be developed.

A6.2.2 SLA Transgression Accountability

Use Case Name	SLA transgression accountability
Code	T4_UC02
Summary	A transaction causes an SLA-agreed maximum level to be exceeded. The Gateway Operator activates the TTP-monitor and kills the transaction.
Roles	Service Provider (SP), Gateway Operator (TGO), Trusted Third Party (TTP)
Preconditions	• Fully operational gateway • Connected service provider for which a user-profile has been set up
Begins When	Service provider issues the transaction
Description	• SP issues a transaction • The transaction exceeds the SLA-agreed maximum level • TGO activates the TTP-monitor

	• TGO activates logfile which registers abortion of transactions • TGO kills the transaction • Record of abortion is stored in the appropriate logfile
Ends When	The transaction has been killed.
Postconditions	• Standard logfile has been updated • Logfile which registers killed transactions contains a new record of abortion
Exceptions	N/A
Traceability	ISEC 54, 57, 60, 66, 68, 71, 73

Use Case Ref: T4_UC02

Test Design ID: T4_TD02

Test Purpose

To demonstrate the activation of the TTP-monitor and the particular logfile when a transaction causes a SLA-agreed maximum to exceed.

Covered Requirements

ISEC 54, 57, 60, 66, 68, 71, 73

Preconditions

- Fully operational gateway (GW)
- Connected service provider (SP) for which a user profile has been set up.

Test Description

- SP issues a transaction
- The transaction exceeds the SLA-agreed maximum level
- TGO activates the TTP-monitor
- TGO activates logfile which registrates abortion of transactions
- TGO kills the transaction
- A record of abortion is created and stored in a special logfile
- TGO deactivates the TTP-monitor
- TGO deactivates the special logfile

Expected results

- Transaction is killed
- TTP-monitor activated and deactivated
- Logging on special logfile activated and deactivated

Postconditions

- Regular logfile shows the essential steps in the handling of the transaction
- A record of abortion has been appended to a special logfile

A6.2.3 High-Value Transaction

Use Case Name	High-value transaction
Code	T4_UC03
Summary	A high-value transaction is issued by a service provider and acknowledged by the gateway. A protocol involving digital signatures and a trusted time-stamping service assures non-repudiation of the transaction.
Roles	Service Provider (SP), Gateway (GW), Trusted Time-Stamping Service (TTS)
Preconditions	• Fully operational gateway • Connected service provider • Interconnection between SP, GW and TTS
Begins When	Service provider issues the high-value transaction
Description	• SP issues a digitally signed, high-value transaction to TTS • TTS puts a time-stamp and forwards the transaction to GW • GW creates a digitally signed receipt and sends it to TTS • TTS puts a time-stamp and forwards the receipt to SP • SP responds with a digitally signed acknowledgement to TTS • TTS puts a time-stamp and forwards the acknowledgement to GW
Ends When	Acknowledgement of SP has been received by GW
Postconditions	• Standard logfile has been updated • Digitally signed and verified high-value transaction and acknowledgement ready to be forwarded to OSS
Exceptions	N/A
Traceability	ISEC 46, 53, 57, 61, 68, 74, 75

Use Case Ref: T4_UC03

Test Design ID: T4_TD03

Test Purpose

To demonstrate the usage of digital signature and the usage of a time-stamping service in the execution of a non-repudiation protocol for the handling of a high-value transactions.

Covered Requirements

ISEC 46, 53, 57, 61, 68, 74, 75

Preconditions

- Fully operational gateway (GW)
- Connected service provider (SP)
- User-profile of SP at GW admits processing of the high-value transaction
- Interconnection of SP, GW and TTS
- SP and GW in possession of their private signing key

- GW in possession of the public signature-validation keys of SP and TTS
- SP in possession of the public signature-validation keys of GW and TTS

Test Description

- SP digitally signs a high-value transaction
- SP sends digitally signed high-value transaction to TTS for time-stamping and forwarding to GW
- TTS puts a time-stamp on the transaction and forwards the time-stamped transaction to GW
- GW checks the signatures of SP and TTS on the transaction
- GW checks the transaction against the user-profile of SP
- GW creates a receipt and signs it digitally
- GW sends digitally signed receipt to TTS for time-stamping and forwarding to SP
- TTS puts a time-stamp on the receipt and forwards the time-stamped transaction to GW
- SP optionally checks the signatures of GW and TTS on the receipt
- SP creates an acknowledgement and signs it digitally
- SP sends digitally signed acknowledgement to TTS for time-stamping and forwarding to GW
- TTS puts a time-stamp on the acknowledgement and forwards the time-stamped acknowledgement to GW
- GW checks the signatures of SP and TTS on the acknowledgement
- GW prepares the digitally signed and time-stamped high-value transaction and acknowledgement for further processing

Expected results

- Successful three tier communication between SP and GW via TTS

Postconditions

- Update of logfile reflecting the handling of the high-value transaction
- Digitally signed and time-stamped high-value transaction and acknowledgement available on GW for further processing by OSS

A6.3 Physical Test Set-up and Logical Test models

This subsection provides an overview of the physical test set-up and logical test models for the use-cases and test designs described above. The physical test set-up provides the global map of the systems that are needed to illustrate the use-cases. The logical test models describe the architectural picture underlying the test designs. Also an overview is given of the various phases that are foreseen for the test cases based on the security test designs as described in the above mentioned project document.

A6.3.1 Physical Test Set-Up

In Figure 1 below the physical set-up of the test model concerning the test designs described above. The logical test model for the test designs are given in the next section, which can be based upon the concrete set-up.

The following components are distinguished:

- GW: The OSS Interconnection Gateway or gateway for short.
- Web Server: A web server acting as the client-side interface to the gateway. This can be also be realised as an integrated part of the gateway (dependent on the particular gateway product).
- Manager: The point of control for the gateway. This can be a PC connected to the gateway or the console of the gateway. It should visualise the transactions that are processed by the gateway and give possibility to terminate transaction.
- TTP Monitor & TTS: A PC on which information from the GW can be displayed (via a read-only monitor connection). Furthermore a time-stamping facility should be supported, that time-stamps and forwards messages from SP to GW and vice versa.
- SP: A PC functioning as server provider (or server provider gateway) with smart card reader for authentication and authorisation purposes.
- Smart card (not labelled in Figure 1).

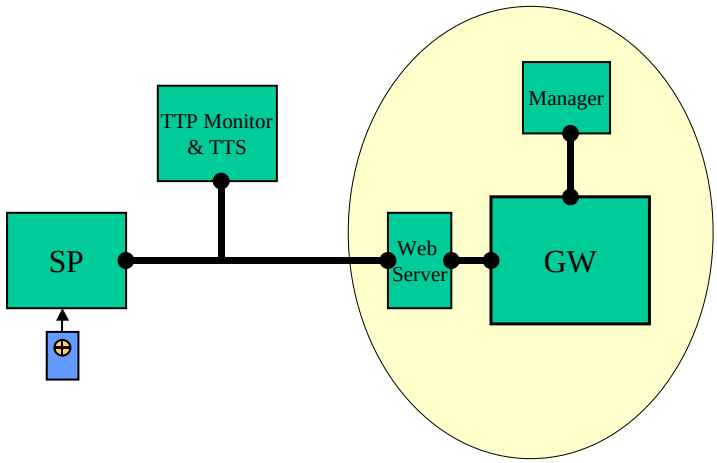


Figure 1 Physical Test Set-Up

The area indicated around Web Server, GW and Manager reflects the security perimeter of the gateway system. The connections used there are considered internal. The connections between SP, TTP Monitor & TTS and Web Server should support SSL, VPN and general messaging of transaction. (In principle this could simply be Ethernet).

A6.3.2 Logical Test models

We discuss the logical set-up for the three test designs related to security issue. The pictures below also illustrate the various phases that are foreseen for the test cases based on the proposed test designs.

A6.3.3 Add Authentic and Authorised Service Provider

In Figures 2 and 3 the following components are used:

- SP: Service provider
- GW: Gateway
- Manager: Console or display connected to gateway

SP and GW or web-interface of GW are connected via an SSL-connection. Manager is an integrated part of GW or connected to GW via a private link. In the authentication phase for test design T4_TD01 a ISO 7816 compliant smartcard is used; in the authorisation phase a ITU X.509 version 3 public key attribute certificate is used.

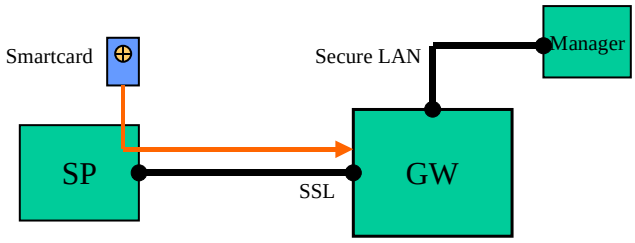


Figure 2 Authentication

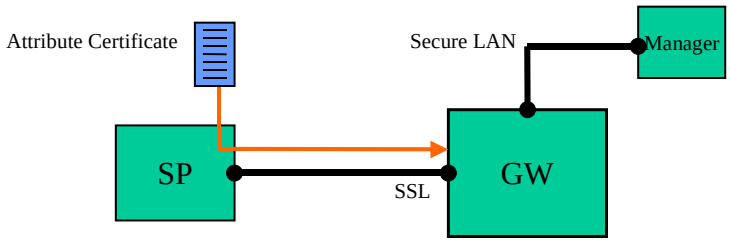


Figure 3 Authorisation

A6.3.4 SLA Transgression Accountability

In test design T4_TD02, as depicted in Figure 4, 5 and 6, a transaction is sent to the gateway. The transaction generates an alarm. Subsequently a monitor connection between GW and TTP is activated. Then the transaction is killed.

The following components are used in Figure 4, 5 and 6

- SP: Service provider
- GW: Gateway
- Manager: Console or display connected to gateway
- TTP Monitor: a read-only monitor connection for the trusted third party

SP and GW are connected via a VPN, as are GW and TTP Monitor. Manager and GW are connected via a private link. The arrow from SP to GW in Figure 4 indicates the transaction issued by SP. In Figure 5 the transaction has been received by GW, as indicated by the ellipse inside the GW-box. In Figure 6 the ellipse is crossed out, indicating the abortion of the transaction.

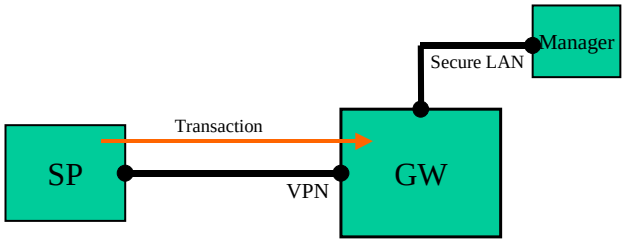


Figure 4 SP issues transaction

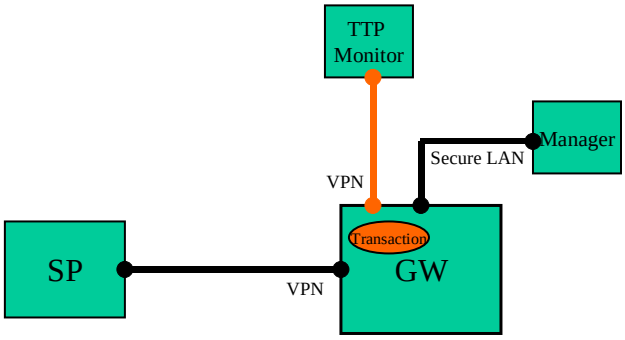


Figure 5 Transaction received, TTP Monitor activated

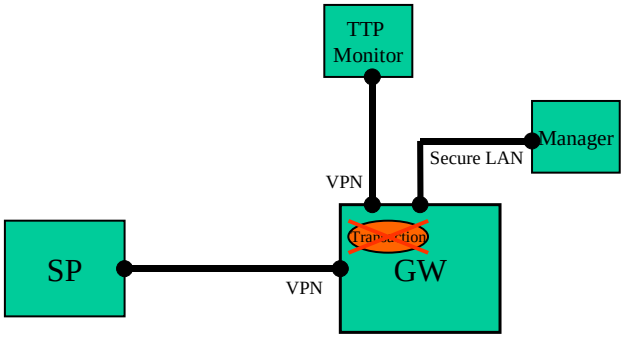


Figure 6: Transaction killed

A6.3.5 High-value transaction

The use-case on high-value transaction focuses on digital signatures and time-stamping (ETSI-standard ES 201 733 v1.14). Figure 7, 8 and 9 illustrate the three phases involved: issuing the transaction by a service provider, generating a receipt by the gateway, response with acknowledgement by the service provider.

The following components are used for the high-value transaction use-case:

- GW: Gateway
- Manager: Console or display connected to gateway
- SP: Service provider
- TTS: Trusted time-stamping service

SP and TTS on the one hand, and TTS and GW on the other hand, are connected via a VPN. The Manager is connected to GW via a private link. In Figure 7 the arrow labelled HVT indicates the issuing of a high-value transaction, the arrow labelled HVT+TS indicates the forwarding of the transaction with additional time-stamp by TTS. In Figure 8 the arrow labelled REC indicates the receipt that GW sends back, the arrow labelled REC+TS indicates the forwarding of the receipt with additional time-stamp by TTS. Finally, in Figure 9, the arrow labelled ACK indicates the sending of an acknowledgement by SP and the arrow labelled ACK+TS the forwarding of the time-stamped acknowledgement.

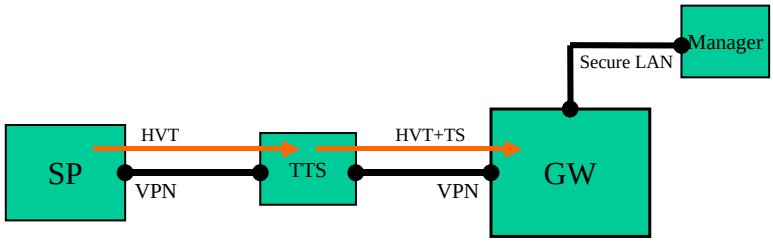


Figure 7: SP sends high-value transaction

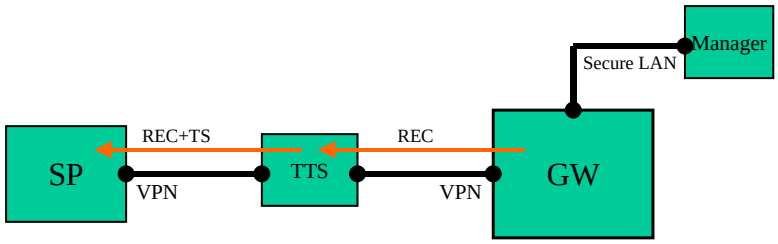


Figure 8: GW sends receipt

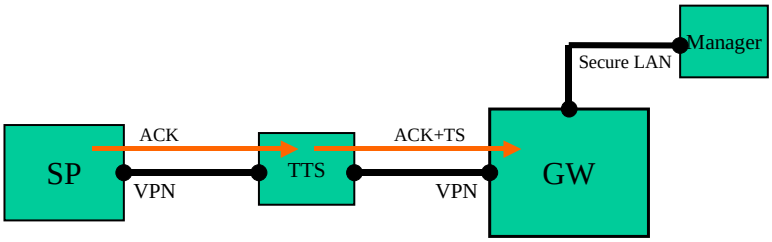


Figure 9: SP sends acknowledgement

