

**THE EXPLANATORY NOTE OF REGULATION 11**

MPS 11

Contents

**1 LEGISLATION ..... 2**

1.1 LEGISLATIVE BASIS FOR THE REGULATION ..... 2

1.2 OTHER RELATED PROVISIONS ..... 3

**2 OBJECTIVE OF REGULATION AND CHANGES MADE TO IT ..... 3**

2.1 THE OBJECTIVE OF THE REGULATION ..... 3

2.2 KEY CHANGES AND CHANGES MADE IN THE PAST ..... 4

**3 SECTION-SPECIFIC BASIS AND GUIDELINES FOR APPLICATION ..... 4**

3.1 SECTION 1 SCOPE OF APPLICATION ..... 4

3.2 SECTION 2 DEFINITIONS ..... 4

3.2.1 *E-mail service* ..... 4

3.2.2 *E-mail transfer service* ..... 5

3.2.3 *Secondary e-mail transfer service* ..... 5

3.2.4 *Open mail relay* ..... 6

3.2.5 *Malicious e-mail traffic* ..... 6

3.2.6 *Filtering* ..... 6

3.3 SECTION 3 OPEN RELAYS FOR E-MAIL ..... 6

3.4 SECTION 4 HANDLING OF INCOMING E-MAIL TRAFFIC ..... 7

3.4.1 *Identification of malicious e-mail traffic* ..... 7

3.4.2 *Filtering and marking of e-mail traffic* ..... 10

3.4.3 *Notifying of the filtering principles for incoming e-mail traffic* ..... 11

3.5 SECTION 5 HANDLING OF OUTGOING E-MAIL TRAFFIC ..... 12

3.6 SECTION 6 CONNECTION BETWEEN CUSTOMER AND E-MAIL SERVER ..... 13

3.7 SECTION 7 MONITORING OF FUNCTIONALITY AND QUALITY OF E-MAIL SERVICES ..... 13

3.8 SECTION 8 MANAGEMENT OF E-MAIL ADDRESSES ..... 15

3.8.1 *Description of e-mail address management to customers* ..... 15

3.8.2 *Reuse of e-mail addresses relinquished from customers* ..... 15

3.8.3 *Management of problem situations of misleading e-mail addresses* ..... 16

3.9 SECTION 9 CONTACT DETAILS OF AN E-MAIL ADDRESS PROVIDER ..... 16

3.10 SECTION 10 TRANSITIONAL PROVISIONS AND ENTRY INTO FORCE ..... 16

**4 OTHER RECOMMENDATIONS ..... 16**

4.1.1 *Protection of connections between servers* ..... 16

**5 REFERENCES ..... 17**

**6 ABBREVIATIONS ..... 18**

## 1 LEGISLATION

The aim of this chapter is to give the user of the regulation a general overview of the provisions this regulation is based on. The chapter also provides other essentially related provisions.

### 1.1 Legislative basis for the regulation

FICORA's regulation is based on sections 128 and 129 of the Communications Market Act [1] and sections 19 and 20 of the Act on the Protection of Privacy in Electronic Communications [2]. The Act, which entered into force on 25 July 2003, gave, for its part, effect to the directives within the electronic communications sector adopted by the EC in February 2002, i.e. the Framework Directive [3], the Authorisation Directive [4], the Access Directive [5] and the Universal Service Directive [6]. The Act on the Protection of Privacy in Electronic Communications, which entered into force on 1 September 2004, gave, for its part effect to the *Directive on privacy and electronic communications* [7] adopted by the EC in July 2002.

FICORA may, pursuant to section 19(4) of the Act on the Protection of Privacy in Electronic Communications, issue further regulations to a telecommunications operator on the information security of services referred to in subsections 1 to 3. According to subsection 1, a telecommunications operator must maintain the information security of its services. According to subsection 2, the obligation to see to information security also concerns the data handling needed for the implementation of the obligation to retain identification data referred to in the Act. According to subsection 3, a telecommunications operator is responsible to subscribers and users for the information security referred to in subsections 1 and 2 also on behalf of any third party that wholly or in part provides a network service, communications service, data storage or value added service.

The Finnish Communications Regulatory Authority (FICORA) may, under section 20 of the Act on the Protection of Privacy in Electronic Communications, issue further regulations to a telecommunications operator on the technical measures for combating information security incidents of the service and the removal of information security disruptions referred to in the section. According to the section, a telecommunications and value-added service provider has the right to undertake immediate measures in order to ensure information security referred to in section 19.

The regulation relates to the requirements provided in section 128 (1), (4), (5), (7) and (12) of the Communications Market Act, which state that public communications networks and communications services, and the communications networks and communications services connected to them must be planned, built and maintained in such a manner that:

- 1) the technical quality of telecommunications is of a high standard;
- 4) the protection of privacy, information security and other rights of users and other persons are not endangered;
- 5) the health and assets of users or other persons are not put at risk;
- 7) they function together and can, if necessary, be connected to another communications network;
- 12) a telecommunications operator is also otherwise able to meet the obligations it has or those imposed under this Act.

This regulation specifies the above mentioned technical requirements by virtue of section 129 (2 to 5), (10), (15 to 16) and (20 to 21), according to which FICORA's regulations may cover:

- 2) the structure of a communications network;
- 3) the performance capacity of a communications network and communications service;
- 4) interconnection, interoperability and signalling;
- 5) the technical characteristics of communications network termination points;
- 10) communications network security and minimizing interference;
- 15) services provided for users;
- 16) performance maintenance and monitoring and network management;
- 20) standards to be complied with.
- 21) other comparable technical requirements set for a communications network or communications service.

## 1.2 Other related provisions

This paragraph describes other regulations issued by FICORA whose subject matter relates to this regulation. The purpose of the paragraph is to give the user of the regulation a better possibility to have a general view of the obligations concerning communications networks and services.

Regulation 9 on obligation to report information security incidents and faults and disturbances in telecommunications networks and services [8]. The regulation is applied to operators' public telecommunications operations and the telecommunications devices used in it. The regulation is also applied to telecommunications operations in public authority networks and devices used in them.

Regulation 13 on information security and functionality of internet access services [9]. The regulation applies to the production of Internet access services provided in public communications networks and related systems, communications networks and communications services used by telecommunications operators to provide these services. In the regulation, Internet access service means transmission of Internet traffic. The regulation applies, as applicable, also to the production of Internet access services both for network operators and service operators.

Regulation 47 on information security of telecommunications operators [10]. The regulation applies to operations relating to the implementation of public communications services of telecommunications operators as well as systems, communications networks and communications services used by telecommunications operators for public telecommunications. It prescribes how operators must tend to information security related issues.

Regulation 53 on the obligation to retain identification data [11]. The regulation prescribes certain telecommunications operators the obligation to retain identification data. The regulation is not used for imposing telecommunications operators an obligation to retain any new data, but the purpose is to extend the current storage period of the data they have retained for own use.

Regulation 54 on priority rating, redundancy, power supply and physical protection of communications networks and services [12]. The purpose of the regulation is to ensure the reliability of communications networks and services, protection of privacy and information security under normal circumstances, in fault situations in normal circumstances and in state of emergency. Therefore, the regulation imposes telecommunications operators minimum obligations of e.g. ensuring power supply of devices used for the implementation of communications networks and services, the physical protection of devices and ensuring that devices and connections are effective.

The list corresponds to the situation at the time this document was published. All FICORA Regulations can be found at [www.ficora.fi](http://www.ficora.fi).

## 2 OBJECTIVE OF REGULATION AND CHANGES MADE TO IT

The aim of this chapter is to give the user of the regulation information on the objectives and aims of the regulation. This chapter also includes the most important changes made to the obligations and recommendations preceding the regulation.

### 2.1 The objective of the regulation

The objective of the regulation is to impose minimum obligations on e-mail service providers in order to ensure the information security and functionality of a communications service.

The aim of the regulation is to ensure that the e-mail services used by consumers are effective. It is difficult for consumers to assess the information security and functionality of communications services. Because consumers scarcely have a chance to affect the functionality of communications services, it is best to see to the functionality by way of a regulation by imposing minimum obligations regarding the key technical characteristics of an e-mail service on e-mail service providers.

The significance of e-mail service is also more relevant for the entire society. Therefore, the regulation imposes obligations on the handling of e-mail communications, management of e-mail servers and addresses and service quality control on service providers.

## **2.2 Key changes and changes made in the past**

Compared to the previous version of the regulation, the roles of an e-mail service provider and Internet access service provider have been separated, as far as their responsibilities regarding e-mail services are concerned. This regulation focuses on the obligations and responsibilities concerning an e-mail service provider. The requirements and recommendations concerning those providing Internet access services or subscriptions have been transferred to regulation 13 (regulation on information security and functionality of internet access services).

The structure of the paragraphs in the regulation has been renewed. The requirements concerning e-mail service providers included in section 5 of the previous regulation (directing and routing of e-mail traffic to a consumer subscription), in section 6 (directing and routing of outgoing e-mail traffic from a consumer subscription) and in section 7 (detecting and filtering of malicious software traffic) have, in this regulation, been compiled under two paragraphs (section 4, handling of incoming e-mail traffic and section 5, handling of outgoing e-mail traffic). The purpose of the change is to clarify the content and subjects of the regulation.

In section 6 of the regulation, a new obligation has been issued on e-mail service providers on the provision of protected connections as a primarily connection between the customer and the e-mail store and between the customer and the mail submission agent.

Another novelty in the regulation is the management of e-mail addresses as referred to in section 8. The purpose of the section is to harmonize the various practices service providers have for managing e-mail addresses. Also service providers are obliged to provide consumers with information on how they manage e-mail addresses. The obligations on ensuring the usability of an e-mail service have been placed under other sections and the regulation on network management, which is under revision.

## **3 SECTION-SPECIFIC BASIS AND GUIDELINES FOR APPLICATION**

This chapter examines the basis for each section and the guidelines for their application.

### **3.1 Section 1 Scope of application**

The scope of application of the regulation comprises the provision of services of submitting, transferring or delivering e-mail messages provided in public communications networks to consumer and business customers, as well as related systems. The regulation applies to the provision of e-mail services regardless of the mode of operation. Thus, the regulation is also applicable for a service provided by a public organisation or an association to all willing users of the service. Respectively the regulation is not applicable to e-mail services provided to a set of users that is subject to prior restriction e.g. an e-mail service provided by a company or municipality for their employees.

The regulation also applies to the redirecting services of messages counted as transfer services. Sections 5 and 6 of this regulation do not, however, apply to these services.

E-mail service and a transfer service of e-mail are defined in more detail in section 3.2. Definitions (sections 3.2.1, 3.2.2 and 3.2.3).

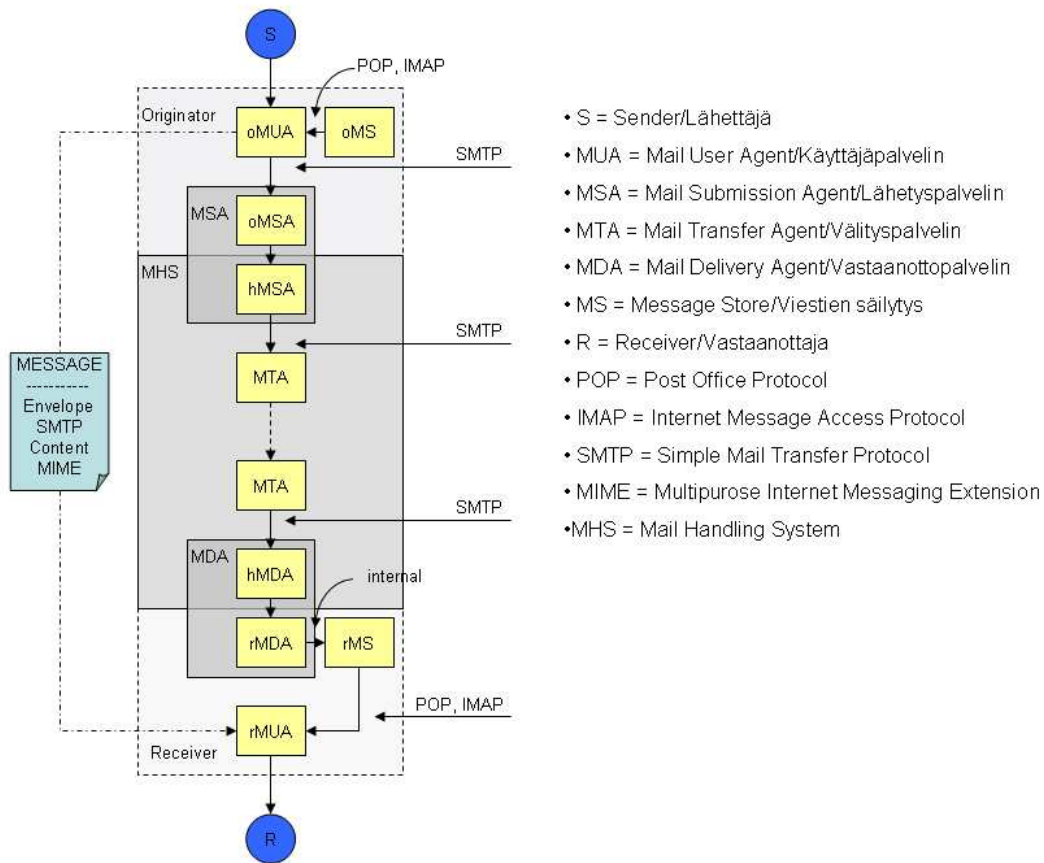
### **3.2 Section 2 Definitions**

This section explores the definitions used for the regulation.

#### **3.2.1 E-mail service**

In this regulation, "e-mail service" means submission, transfer or delivery service of e-mail messages. The principle of an e-mail service, various functions and protocols used between functions are shown in figure 1. An e-mail submission service means a service where the customer sends a message via a service provider's mail submission agent (MSA). Transfer service means a service where e-mail messages are received, (handled) and forwarded to the target agreed upon with the

customer. Delivery service means service where the customer's e-mail messages are accepted by a mail delivery agent (MDA) and delivered to the customer's e-mail store.



**Figure 1: Principle of e-mail service**

In this regulation, outgoing e-mail traffic means e-mail messages sent by the customers of e-mail service providers and transferred via the service provider's mail submission agents to the e-mail system's mail transfer agent (MTA).

In this regulation, incoming e-mail traffic means e-mail messages sent to the customers of e-mail service providers and transferred via the service provider's mail delivery agents to the customers' message stores (MS).

The functionality of an e-mail system means the quality of service with which the submission, transfer and delivery of legitimate e-mail messages functions without significant delays or interruptions in use and legitimate e-mail messages are delivered to recipients.

The usability of e-mail service means how the users of an e-mail service have experienced the quality and functionality of the service. E.g. service breakdowns and the volume of malicious e-mail messages may affect the usability of the service.

### 3.2.2 E-mail transfer service

In this regulation, "e-mail transfer service" means a service provided by an e-mail service provider for the purpose of transferring or redirecting messages via its e-mail servers.

### 3.2.3 Secondary e-mail transfer service

In this regulation, secondary e-mail transfer server means an e-mail transfer agent backing the customer's own e-mail service. In the service, the customer's e-mail server or servers have been determined as the primary mx record or records. Thus, the incoming e-mail traffic of the customer

is not transferred via the service provider's secondary e-mail transfer agents unless the customer's servers are inaccessible.

#### 3.2.4 Open mail relay

In this regulation, "open mail relay" means message transfer system a third party may unlawfully use for transferring e-mail messages. In the regulation, a transfer system means e.g. an e-mail server, a www proxy or software installed on a www-server used for the purpose of transferring e-mail messages.

#### 3.2.5 Malicious e-mail traffic

In this regulation, malicious e-mail traffic means such e-mail traffic that may endanger the information security of a communications network or service. Information security of a service means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it (Functionality), that data can only be modified by those who are entitled to do so (Confidentiality), and that data and information systems can be used by those who are entitled to use them (Usability). In this regulation, malicious e-mail traffic also means such e-mail traffic that causes harm to the information security of the receiver's terminal equipment. It is unavoidable to regard this sort of traffic as malicious, because the information security threats directed at the terminal equipment of the communications parties indirectly endanger the information security of a communications service provided by a telecommunications operator, too.

The maliciousness of e-mail traffic must be examined both from the e-mail service provider's and customer's viewpoints. In practice, this means that the usability of a communications service may require measures both in order to ensure the transfer ability of the service provided by the e-mail service provider and to maintain the quality of service transferred to the user. In theory, the majority of information security threats directed at an e-mail service could be solved by increasing the transfer capacity available for an e-mail service. Measures such as these do not, however, directly affect the usability of the service from the viewpoint of an e-mail service user, because the service can, in practice, be blocked e.g. due to large spam volumes.

When assessing e-mail traffic regarded as malicious, it is essential whether an e-mail message is determined as malicious by widely-used identification and filtering mechanisms of malicious e-mail.

#### 3.2.6 Filtering

In this regulation, filtering means the rejection of transfer or delivery of e-mail messages, removal of such malicious software from the messages that endanger information security, or other related technical measures.

### **3.3 Section 3 Open relays for e-mail**

Open mail relays are widely used for transferring malicious e-mail traffic. It is possible to reduce the volume of malicious e-mail traffic by identifying open e-mail relays and preventing the use of third parties' e-mail servers for transferring e-mail messages.

An e-mail service provider must ensure that the e-mail systems under its administration do not function as open mail relays. Test measures in connection with the introduction and modification of systems and services and careful definition of settings are examples of measures taken in order to ensure the safe use of electronic mail systems.

An e-mail service operator must, at regular intervals, test all electronic mail systems under its administration to ensure that the systems do not operate as open mail relays. Unless a company has acquired a testing system, it can use the public services for testing widely available on the Internet.

For the e-mail transfer agent belonging to the Internet access provider's Internet subscription, this obligation means that it is only possible to send e-mail without identification from the network of the ISP in question.

### **3.4 Section 4 Handling of incoming e-mail traffic**

In this regulation, the handling of incoming e-mail traffic means measures which can be implemented to incoming e-mail messages customers receive via mail delivery agents of e-mail service providers or mail transfer agents. These measures are: identification of malicious sources of e-mail traffic and malicious e-mail traffic, filtering and marking measures made to traffic identified as malicious and the delivery of traffic to customers.

#### **3.4.1 Identification of malicious e-mail traffic**

A major part of the known, authorized e-mail sources and authorized sources of malicious e-mail messages can be identified on the basis of e-mail traffic sources. If authorized sources can be identified, it is possible to avoid the filtering of legitimate e-mail traffic on the basis of a false identification. If the sources of malicious e-mail traffic are identified, it is possible to prevent the delivery of messages received from these sources to the e-mail store or an e-mail message can be marked as malicious before delivering it to the customer's mail store.

Identification of e-mail sources can be based on the identification of authorized senders, unauthorized senders or both. The identification can be made, for example, on the basis of the network address, domain name or e-mail server of the sender. Determination of maliciousness is based on information received or collected in advance from messages transferred via the source or the analysis of the message content.

#### **Reasons**

A major part of e-mail traffic is received from implicit network addresses or e-mail servers. On the basis of experience, monitoring and external compilation of statistics, some of them can be identified as sources of malicious e-mail traffic as early as when the SMTP connection is being opened. Similarly, a major part of the legitimate e-mail traffic is repeatedly received from previously-known and used authorized e-mail sources, which can be identified as early as the connection is opened. If the sources of malicious e-mail traffic are identified as early as possible when a connection is opened, it enables that an e-mail service provider must not even accept the traffic in question. This reduces the load on an e-mail service and improves the delivery of legitimate e-mail messages to customers.

The identification of malicious e-mail traffic is a necessity for all the filtering and marking measures made by e-mail service providers. An e-mail service provider can, however, detect only part of the malicious e-mail traffic on the basis of the e-mail sources. Therefore, a service provider must also have other mechanisms for detecting malicious e-mail traffic.

Many of the mechanisms can, however, incur significant expenses to the e-mail service provider. A more strict set of identification criteria is more susceptible to incorrect interpretations. By using the basic identification mechanisms, an e-mail service provider can diminish the effects of malicious e-mail traffic, and improve the information security and functionality of the service, and how the users experience the service quality and usability. Due to the above-mentioned reasons, an e-mail service provider has been allowed to select the identification mechanisms best suitable for identifying malicious e-mail traffic with regard to the service it provides.

#### **Application**

An e-mail service provider must have up-to-date and reliable mechanisms in order to identify the sources of e-mail traffic and determine maliciousness in e-mail traffic. An e-mail service provider may select the mechanisms to be used in its system out of several alternatives so that a significant amount of incoming malicious e-mail traffic will be identified and thus puts the delivery of legitimate messages at minimal risk. In addition to the basic identification mechanisms fulfilling the above-mentioned criteria, which are available for all customers, an e-mail service provider may provide its customers with more sophisticated and tailored identification and handling mechanisms of malicious traffic e.g. on a separate agreement.

When the filtering mechanisms for e-mail traffic are used at the stage when an SMTP connection, is being opened an e-mail service provider must have an efficient mechanism for identifying the most important, implicit, legitimate e-mail sources. At the time of the publication of the regulation, this means the use of access lists.

There are several alternatives for identifying e-mail sources and determining maliciousness. It is possible to identify a significant part of malicious e-mail traffic by using one method only. The results of identifying malicious traffic will, however, often improve if several methods complementary to one another are used simultaneously. Each method offers their advantages in comparison with other methods, but unfortunately each method is also connected with a problem. An e-mail service provider must be aware of the advantages and disadvantages of the methods it uses, and assess their effects prior to the introduction of the methods.

### Black lists

Connections and e-mail messages received from implicit unauthorized e-mail sources can be identified and filtered by black lists. A black list generally means a database of known malicious e-mail sources often consisting of network addresses. The list can also consist of individual e-mail addresses, domain names or e-mail servers used for sending spam. A black list can be maintained by an e-mail service provider, a third party or user herself or himself.

E-mail systems usually use centralized black lists maintained by a third party. Special care should be taken when using and selecting black lists in order to avoid incorrect interpretations. Static black lists are often unreliable because the sources of malicious e-mail traffic change often and the eventual static, false information on the black list blocks legitimate e-mail traffic on a long-term basis. If information is removed from a static black list, it must be hand picked. Dynamically maintained black lists, on the other hand, are updated fast and incorrect listings are typically removed from the list regularly.

It is not normally sensible to build one's own black list because of the constantly changing information content. When black lists are used, it is worth avoiding black lists listing certain large network ranges on the basis of individual users' measures. This makes sure that the usability of the e-mail service is secured. In addition, such black lists should be avoided where the reasons for ending up on the list are unclear, there are no clear procedures for getting out of the list, or which large service providers are not recommended to use.

When an e-mail service provider is selecting a black list maintained by a third party, it should pay special attention to the following characteristics of the list:

- Publication of listing principles
- It is simple to remove from the list and there are guidelines for that
- The contact details for the maintainer of the list are public
- The listing is not based on a single incorrect message
- The list is updated regularly

When using black lists, it should be kept in mind that the lists may contain incorrect information and therefore prevent legitimate e-mail traffic. A list maintained by a third party must be followed regularly. Different lists usually contain various sources, so the simultaneous use of several lists often gives the best result. The recognition percentage of malicious traffic sent from various sources to the e-mail delivery agent increases when different lists identify different malicious sources. Black lists can also be used as part of the rating of the maliciousness of an e-mail source in heuristic filtering. Then, a single incorrect listing will not initiate the filtering of a legitimate message.

When an e-mail service provider uses black lists, it must use a mechanism for identifying the implicit, most important legitimate e-mail sources. At the time of the publication of the regulation, this means the use of access lists. An e-mail service provider must, to minimise the consequences of possible errors caused by the list, list its key cooperation partners and trustworthy national service providers on a list to bypass the blacklisting (whitelist) in the e-mail system.

### Whitelisting

The delivery of messages is marked as permitted on the whitelist, if they have been received via certain network addresses, e-mail servers or e-mail addresses widely known as trustworthy senders of legitimate messages. These can be e.g. implicit e-mail service providers and cooperation partners.

Use of whitelists is, in practice unavoidable when using other block or filtering methods based on an e-mail source. Whitelists can help to ensure the delivery of messages from trustworthy sources, if messages would otherwise be filtered as a result of an incorrect black list, for example.

When the whitelist is used, it must be kept in mind that malicious e-mail traffic can also be sent via trustworthy sources, so sources on the whitelist cannot either be unconditionally trusted. For example forged whitelisted addresses can also be included in malicious e-mail service messages in order to promote the delivery of malicious e-mail traffic. In order to avoid problems, the content of messages sent from the sources on the whitelist must be monitored.

The whitelist is often a very static list of network addresses. The service provider must see to that the information on the list is up-to-date in order to avoid the problems caused by dated information. FICORA's CERT-FI maintains a centralized whitelist of the e-mail servers of Finnish players. E-mail service providers send their modified server information to CERT-FI, which forwards the updated list regularly to users. If a company wants to have the white list of CERT-FI or have its name on the list, they must contact CERT-FI. Another alternative of a centralized whitelist is e.g. DNS Whitelist (<http://www.dnswl.org/>).

#### Greylisting

Greylisting is based on the activities of software sending malicious e-mail traffic. Unlike normal e-mail system, this software does not attempt to resend the message, although the delivery of a message had failed. In greylisting, certain parameters can be automatically recorded (the IP address /C class of the address of the sender of the incoming e-mail, SMTP sender and SMTP receiver) or a hash table including these. A message from an unknown sender or containing certain parameters will be blocked. When the source tries to resend the message, after a delay, the delivery will be accepted. In the future, messages from the source in question will be received without delay.

The challenge of greylisting is that it causes delay for legitimate e-mail messages arriving from previously unknown sources. In addition, greylisting is based on the senders' principle of sending the malicious message only once. If senders of malicious traffic begin resending messages in order to evade greylisting, greylisting is not successful. In addition, resending e-mail messages generates more e-mail traffic which burdens both networks and e-mail servers.

#### Reputation systems

Reputation systems are based on the former delivery history of the source of the message. Messages sent by e-mail sources (e.g. sender's IP address and SMTP sender) are monitored, statistics are compiled of them and they are compared to the previous message history. The focus of the compilation of statistics and comparison is whether a source sends legitimate e-mail messages or malicious e-mail messages. E-mail sources can also be monitored on the basis of the number of messages sent from the server. The data are used in order that the reputation class of an e-mail source can be determined on the basis of the sender's prior delivery and message history. The reputation class determines whether the message from the source is delivered to the recipient in a matter-of-fact way, message is delivered to the recipient on a lower priority or the message delivery is blocked.

The advantage of reputation systems is that they exploit the monitoring of long-term sources, and messages are not filtered on the basis of single illegitimate messages. Reputation systems support other filtering systems well and as part of the heuristic filtering, they decrease the faults made by other sets of criteria. When using reputation systems, it should be borne in mind that the classification of the system does not necessarily have the time to react to the fast flow of malicious traffic.

Reputation systems maintained by third parties gather the information needed for the classification from their customers. The information received from several sources is compiled into a common database in order that the reputation classification can be made. An example of a reputation system implementation maintained by a third party is TrustedSource (<http://www.trustedsource.org/>) and reputation system supporting single identification systems is spamassassin AWL (<http://wiki.apache.org/spamassassin/AutoWhitelist>).

### Heuristic analysis

An e-mail service provider can implement the determination and filtering of the maliciousness of messages also on an analysis based on the content of an e-mail message, or use these methods to reinforce the methods used for identifying e-mail sources in the filtering of e-mail messages.

Generally, the content of malicious e-mail messages fulfils the criteria formerly known. Filtering based on the content of a message can be made for example by comparing the checksum calculated from the message with known checksums of malicious messages or by searching for signs of malicious elements, such as certain strings, formulations, attachments, images or links. It is also possible to search an e-mail message for features of an illegitimate e-mail message. The filtering methods based on black lists may be combined with content filtering, for example. When several mechanisms are combined, each method either increases or decreases the classification of messages. The final classification given for the message determines whether the message is malicious or not. On the basis of the analysis made, the filtering software rejects or discards the message, marks it likely to be malicious or forwards it as such.

### Other mechanisms

In addition to the above-mentioned mechanisms, an e-mail service provider can choose several other methods for the identification of e-mail sources and new methods are introduced steadily. Newcomers are e.g. Sender Policy Framework (SPF) [13] and Domain Keys Identified Mail (DKIM) [14], which identifies that an e-mail message has been sent from the e-mail server revealed by the e-mail address. Similar to other control methods for malicious e-mail traffic, these mechanisms have many weaknesses to be taken into consideration when the methods are introduced. A description of the case is available in RFC 4686 [15]. Because e.g. e-mail transfer services, electronic postcards and ISPs' MSAs violate the operations of these mechanisms, the mechanisms are best suited for the positive identification of the source only.

Before the new mechanisms are introduced, an e-mail service provider must carefully study the operating principles and risks of the method in order to the filtering of incorrect, legitimate e-mail messages. Often the accuracy of single mechanisms is insecure, if the interpretation "authorized/unauthorized" given by the mechanism is unconditionally trusted. Instead, the simultaneous use of several mechanisms as part of the classification system may well give very accurate filtering results with little margin of error.

### **Recommendations**

E-mail service providers are recommended to run the identification of malicious e-mail traffic already when an SMTP connection is being opened. Thus, a great part of the malicious e-mail traffic can be blocked even before it can access the e-mail system. The procedure diminishes significantly the burden caused by malicious e-mail traffic.

Several methods are recommended to be used simultaneously in order that malicious e-mail traffic is identified. Thus, the identification accuracy of malicious e-mail traffic can be improved and thus, for example, tighter filtering criteria can be used.

The use of access lists is recommended in order to avoid false interpretations in situations where an e-mail service provider has block and filtering methods in use. E-mail service providers are recommended to take into use e.g. the access list maintained by FICORA's CERT-FI or equivalent.

#### 3.4.2 Filtering and marking of e-mail traffic

The filtering of incoming e-mail traffic means that the access of identified, malicious e-mail traffic sent to customers is denied to customers' e-mail box. By filtering malicious e-mail messages, it is possible to lessen the burden of e-mail servers and the number of malicious e-mail messages ending up in customers' e-mail boxes, and accordingly, ease the checking of legitimate messages. At the same time, the effects of malicious e-mail messages are prevented e.g. when customers open attachment files included in their e-mail messages or when they click a link in a message and get transferred to a site containing a malware. The filtering of e-mail traffic can improve the service quality and information security of the service experienced by customers.

**Reasons**

A significant part of incoming e-mail traffic can currently be interpreted as malicious e-mail traffic. Malicious e-mail messages that have been identified and filtered at the earliest possible stage decrease the burden of an e-mail system and the delivery of legitimate messages improves. If the access of malicious e-mail traffic is denied to e-mail servers, it is possible to prevent the malicious effects directed at the system in the case of denial-of-service attacks, for example. The information security and functionality of the service improve if malicious e-mail messages are filtered.

By filtering malicious e-mail messages, the access of content, which is malicious for the information security of the customer and communications networks, is denied to the customer's e-mail store. This also prevents any further handling of e-mail messages. Also, the volume of incoming e-mail messages in the customer's e-mail store drops if malicious e-mail traffic is filtered. The handling of e-mail messages becomes easier for the customer when legitimate messages need not to be separated from malicious ones. At the same time, the service quality and usability experienced by the customer improves.

The filtering of e-mail messages can be based on the identification mechanisms of malicious e-mail sources and/or heuristic filtering methods. Because some e-mail service customers want to make sure themselves that no incorrect filtering happens, e-mail service providers have been given an opportunity to mark traffic as malicious instead of filtering it. At the request of the customer and by a separate agreement, an e-mail service provider can also choose not to mark.

**Application**

An e-mail service provider must mark or filter such e-mail traffic from incoming e-mail traffic that it has determined as malicious on the basis of the identification mechanisms for malicious e-mail traffic or the sources of it. Instead of automatically filtering traffic that has been identified as malicious, an e-mail service provider may also e.g. direct part or all of the messages it has found and marked as malicious in the filtering procedure to a separate folder in the user's mailbox, where for example a certain amount of messages may be stored for a certain time to be inspected by the user. An e-mail service provider can also remove the content identified as malicious from the messages before the message is delivered to a customer.

The opportunity given to a service provider to separately agree with the customer that traffic found malicious will not be filtered or marked as malicious means that a separate agreement is made with the customer. An e-mail service provider cannot thus include this alternative in its standard agreements.

However, despite of all the above-mentioned exceptions, an e-mail service provider must always filter such e-mail traffic that is identified as malicious and endangers the functionality of the systems used for producing an e-mail service.

### 3.4.3 Notifying of the filtering principles for incoming e-mail traffic

The identification, filtering or marking malicious e-mail traffic is necessary in order to ensure the functionality and usability of an e-mail service. Misunderstandings and unnecessary customer complaints can be avoided by notifying customers about the available basic principles of filtering e-mail traffic.

**Reasons**

The customer has the right to receive information about the features of the service provided to her or him and thus about the filtering principles used by an e-mail service provider. In addition, the filtering of incoming e-mail traffic made by an e-mail service provider often brings about that customers present inquiries to the service provider if legitimate e-mail messages are incorrectly filtered or the amount of malicious e-mail traffic delivered to the customer's e-mail store increases significantly.

**Application**

When an e-mail service provider filters the e-mail traffic of its customers, it must describe its general principles of filtering to the customer. The purpose of the description is to inform the customers, at a general level, of the filtering methods used and their effect on the customer's communication. The description of the filtering principles to the customer must not endanger the informa-

tion security of the communication service, i.e. the description needs not to be unnecessarily detailed and describe precise grounds why, for example, a single e-mail message is interpreted as malicious.

For example, if black lists are used, an e-mail service provider need not list the black lists used in the filtering in detail, because the lists used may vary depending on the situation.

### **3.5 Section 5 Handling of outgoing e-mail traffic**

In this regulation, handling of outgoing e-mail traffic means measures that can be made to e-mail messages sent via the outgoing mail submission agent (MSA). These are the identification of authorized senders and filtering of e-mail traffic submitted via an MSA and identified as malicious.

#### **Reasons**

The objective of the handling of outgoing e-mail traffic is to reduce malicious e-mail traffic submitted via the servers of an e-mail service provider, the volume of spam, and improve the reputation of e-mail servers of an e-mail service provider, as well as promote the delivery of legitimate e-mail messages of the service provider's customers. The service quality experienced by users is also promoted.

The effects of malicious e-mail traffic can be considerably cut if malicious e-mail messages are identified and their delivery is blocked at the earliest possible stage. Therefore, an e-mail service provider must restrict the right to send e-mail to persons authorized to do that and filter the e-mail traffic identified as malicious before malicious e-mail messages burden information networks and mail delivery agents.

By using these methods, an e-mail service provider can reduce the number of malicious e-mail messages sent from its servers, and thus improve its reputation from the viewpoint of message recipients, and promote the transmission and delivery of legitimate messages sent by authorized users of e-mail service providers.

In addition, if malicious traffic is identified and the source of the traffic is found, the customer of a service provider can be notified of the malware in the customer's computer. Also, the customer can be advised on how to remove the malware and thus prevent the delivery of malicious messages from the customer's computer in the future.

#### **Application**

An e-mail service provider must have up-to-date and reliable mechanisms for identifying and filtering malicious outgoing e-mail traffic. The identification of malicious e-mail traffic can be based on the identification of an unauthorized source, virus scan of outgoing traffic, exceptional volume of outgoing e-mail traffic from the user's computer, or verifying whether the subject field of the message is in accordance with the Internet standards.

An e-mail service provider may select the mechanisms used in its system out of several alternatives so that a significant amount of outgoing malicious e-mail traffic will be identified and thus puts the delivery of legitimate messages at minimal risk.

If an e-mail service provider finds that the terminal device of an authorized user is used for the delivery of malicious e-mail traffic, an e-mail service provider must filter the e-mail traffic sent from the customer, or block the customer's e-mail traffic and contact the customer, if necessary.

#### Exceptional traffic volume

An e-mail service provider should set the limits for normal use in order to identify exceptional traffic volumes. If the volume of outgoing traffic exceeds the transmission limit defined as normal, an e-mail service provider can block the customer's e-mail traffic temporarily. In addition, an e-mail service provider must, if possible, contact the customer so that the customer is able to take the necessary measures in order to clean the contaminated computer and remedy the situation.

#### Notice for customers

An e-mail service provider must describe the general principles of filtering outgoing e-mail traffic to customers. The operating principles described in section 3.4.3 apply to the communications of filtering principles.

### **3.6 Section 6 Connection between customer and e-mail server**

In this regulation, connection between the customer and an e-mail server means connection between the mail user agent (MUA) and the mail server (MS), and mail user agent (MUA) and mail server agent (MSA).

The protection of the connection between the customer and e-mail server, and customer and e-mail box means that the customer is identified, as well as the encryption of the traffic between the customer and service.

#### **Reasons**

User names and passwords are transferred between the customer and e-mail server. If the connections between the customer and server are protected, it is possible to prevent this information from ending up in the hands of a third party, and prevent the misuse of the service and improve the information security of the service. In addition, by protecting the connection between the customer and server, it is possible to ensure that messages remain confidential in the traffic between the customer and server. In addition to protecting the connection, customers can be provided a safe manner of using the e-mail service independently of the connection network, and to improve the confidentiality of the service experienced by customers.

Customers should be informed that the protection of the connection between the customer and server will not, however, always ensure the confidentiality of the connection from one end of the communication episode to another, i.e. from the sender to the receiver.

It is justified that connections are always protected because of the typical uses of web-based e-mail services (webmail).

#### **Application**

An e-mail service provider must provide, as the primary alternative, the customers with a protected connection between the customer and an e-mail box, and the customer and the outgoing e-mail server. The obligation also applies to other than web-based e-mail services.

This obligation means that a telecommunications operator must provide all its e-mail service customers a possibility to use protected connections, and that customers will be advised, in the instructions passed to them and available for them, that the use of protected connections is either the primary or the only alternative.

In order to identify authorized users and open a protected customer connection, it is recommended that a SMTP-AUTH [16] protocol is used for the client mail transfer agent.

IMAP or POP connections (IMAPS/POPS [17], [18]) protected by SSL/TLS protocol can, for example, be used for this purpose between the customer and e-mail box server.

The customer connections of web-based e-mail services must always be protected. At the time this note is being written, the recommended protection method is the HTTPS protocol [19].

### **3.7 Section 7 Monitoring of functionality and quality of e-mail services**

#### **Reasons**

E-mail service has developed into a communications service important for the entire society's functions. It is necessary to ensure that e-mail services are effective. It is necessary to continuously follow the functionality and quality of the service in order that problem situations can be detected and tackled at an early stage.

A telecommunications operator must continuously monitor the quality and reliability of its services in production of general e-mail services and transmission of e-mail. The procedures for monitoring the functionality and quality of services are primarily intended for supporting the maintenance and development of the services and ensuring the functionality of services.

**Application**

An e-mail service provider must continuously monitor the quality and reliability of the general operations related to an e-mail service. Monitoring includes the monitoring of the functionality and quality of the service and long-term compilation of statistics.

Continuous monitoring of the quality and service reliability of operations

An e-mail service provider must have the appropriate and sufficient mechanisms for detecting significant problems affecting the functionality of the service and for reacting to them. These problems mean situations where the availability or information security of an e-mail service is endangered for example due to exceptionally high e-mail traffic volume or fault in software or equipment.

An e-mail service provider with over 10,000 customers must have these mechanisms in use around the clock. Problem situations must, however, always be responded to without unnecessary delay taking the seriousness of the problem into consideration. In this regulation, the response to problem situations means, for example, implementation of the filtering methods listed in this recommendation, use of automatic control mechanisms in systems producing e-mail services and re-direction of e-mail traffic in cases of congestion in communication or disturbance in services.

Examples of permanent indicators suitable for detecting the above-mentioned problems are for example delay of an e-mail message and load and message queues in e-mail service.

Transmission delay of an e-mail message

The monitoring of a transmission delay of an e-mail message in the service provider's own system means the measuring of the time needed for the transmission of a message within the service provider's own systems. For outgoing e-mail traffic the delay may be measured from the moment the message is accepted for delivery from the consumer subscription or e-mail application, as webmail, to the moment when efforts are made for further transmission. The message cannot be delivered further for example in cases where the receiving e-mail server is temporarily congested and asks the sending server to try again later.

For incoming e-mail traffic, the transmission delay may be measured from the moment when an external e-mail system transmits a message to the telecommunications operator's incoming e-mail system to the moment when the message has been delivered to the recipient's mailbox in the operator's own system or the message is being relayed to a recipient outside the system. In the operator's own systems, the message may pass even through several servers, for example through an e-mail server for incoming traffic from an outside system to a mailbox server. The transmission delay may be monitored as a total delay of the system or as an internal delay of a single server component.

Load and message queues in e-mail service

The monitoring of system load and message queues means monitoring of the situational data pertaining to the load of the server systems and message queues of e-mail traffic. The monitoring of system load means, for example, monitoring of the resources at the operating system level from the systems used for the production of e-mail services. The monitoring of message queues means, for example, automatic monitoring of message queues in systems used for the production of an e-mail service in order that fault situations can be detected fast and the situation can be tackled.

Statistics

In order to develop e-mail service, ensure the functionality of the service and for the purposes of authorities, an e-mail service provider must monitor and compile statistics of the following parameters at least:

- the volume of e-mail traffic identified, listed and filtered as malicious
- the volume of e-mail traffic sent and received
- the network load of an e-mail service
- customer volume

### Monitoring of filtering mechanisms

Monitoring how the filtering mechanisms used function means the monitoring of the filters used, such as black lists or content filtering, with regard to the operation of the mechanism and the traffic volume filtered. The monitoring enables that a telecommunications operator can ensure that the mechanisms function, the reasons for filtering in unclear cases and monitor the volume of traffic filtered within a certain period.

It is possible to monitor how filtering mechanisms function, for example, by reporting the messages rejected by blacklists in the e-mail log, by logging the messages marked or rejected based on content filtering and by monitoring statistics made of these values. The filters may also be tested by sending test messages including malicious components through systems protected by filtering mechanisms. The volume of traffic filtered may be monitored for example by compiling statistics classifying the traffic as malware, otherwise malicious or normal traffic. Regarding malware, a telecommunications operator can, for example, compile statistics summing up the frequency of occurrence of different types of malware in e-mail traffic. The number of disconnected subscriptions can be gathered, for example, by monitoring the transaction log collected by systems that automatically interfere with deviating traffic. On the basis of the monitoring, an operator may take further measures, if necessary, to introduce enhanced filtering methods, for example.

## **3.8 Section 8 Management of e-mail addresses**

Management of e-mail addresses is part of the functionality and availability of e-mail service. Various management practices of e-mail addresses, similar and/or misleading e-mail addresses and e-mail addresses removed from service and the reintroduction of removed e-mail addresses have caused problem situations. By uniting the practices of different service providers and describing the management of e-mail addresses to customers, it is possible to prevent the problem situations such as these experienced by customers. Ready-made operations models can, on the other hand, accelerate the solving of problem situations.

### 3.8.1 Description of e-mail address management to customers

#### **Reasons**

The management of e-mail addresses vary from service provider to service provider. In addition, problem situations are interpreted in different ways depending on the service provider. It is possible to avoid misunderstandings and accelerate the solving of problem situations by determining common management practices and describing them to customers.

#### **Application**

An e-mail service provider must determine and describe the practices regarding the administration of e-mail addresses to customers. The description must help the customer to find out how she or he can have a new e-mail address, modify the settings of the e-mail service and remove an e-mail address. Accordingly, an e-mail service provider must describe its customers the operations models and restrictions related to resembling and misleading e-mail addresses.

### 3.8.2 Reuse of e-mail addresses relinquished from customers

#### **Reasons**

Messages are often sent to an e-mail address after it has been closed. If the relinquished address has immediately or soon after the closing been given to another customer, the new customer may begin receiving e-mail messages meant for the former customer. In order to prevent the misuse of confidentiality of e-mail messages and e-mail addresses, an e-mail address that has been terminated must be put in quarantine before it can be set free for reuse.

#### **Application**

An e-mail service provider must not transfer an e-mail address a customer has relinquished to another customer until three months has passed since the e-mail address has become vacant. If the former holder of an e-mail address wishes to have his or her old e-mail address back within three months since she or he has given up on it, the customer has the right to have it back, unless the customer relationship has been terminated. The right to resume an e-mail address does not, however, in itself oblige a service provider to retain the e-mail messages in the e-mail account after

the account has been terminated. However, a mutual agreement between the parties may lead to an obligation such as this.

### 3.8.3 Management of problem situations of misleading e-mail addresses

#### **Reasons**

Misleading e-mail addresses are created in order to mislead the other party to think that the holder of the address is another person or organisation. Misleading e-mail address means e-mail address registered, for example, in another person's or company's name, business ID or widely-known maintenance address (e.g. postmaster, webmaster or customer service). Operations models that have been established in advance accelerate and clarify the handling of cases.

#### **Application**

If an e-mail service provider finds out or is informed of a misleading e-mail address registered for its domain name, it must tackle the problem. An e-mail service provider has the right to terminate addresses which have been obtained with the purpose to mislead. An e-mail address may also be another person's personal data. The accuracy requirement and the related obligation to rectify personal data in accordance with the Personal Data Act apply personal data. Using another person's personal data with the intention of obtaining benefit can also be punishable as a criminal offence.

FICORA recommends that e-mail service providers do not grant their customers misleading e-mail addresses or their Finnish equivalents with regard to the domain name of the e-mail service provider, referred to in RFC 2142 [20].

### **3.9 Section 9 Contact details of an e-mail address provider**

An e-mail service provider must ensure that its domain names and those used for providing e-mail services have postmaster and abuse addresses, and that incoming messages are regularly monitored.

This requirement is necessary to ensure that a telecommunications operator has a contact point so that eventual disruption or malfunction can be reported to it regardless of the location of the informant.

Due to the large diffusion of the postmaster and abuse addresses, they often attract illegitimate communication. Therefore, a telecommunications operator should arrange the monitoring of the address in such a way that the handling of legitimate messages is not delayed because of the great volume of malicious e-mail traffic. If a telecommunications operator has a large number of domain names, it is reasonable to direct the messages arriving at the postmaster and abuse addresses of domain names to applicable contact points. A telecommunications operator can also transfer the monitoring of contacts to the party responsible for the domain name.

### **3.10 Section 10 Transitional provisions and entry into force**

This Regulation enters into force on 1 November 2008.

If the implementation of the obligation (on provision of protected connections) issued in section 6 of the regulation requires that the e-mail service providers' information systems and customer communications is modified, this obligation has been issued a transition period until 1 March 2009.

## **4 OTHER RECOMMENDATIONS**

This section examines the other non-obliging recommendations issued to e-mail service providers, which are not directly related to any of the paragraphs of this regulation.

### 4.1.1 Protection of connections between servers

The protection of the connections between the mail submission, transfer and delivery agents promotes the information security and reliability of an e-mail service. When a protected connection is used between the servers, they identify one another at the stage when the connection is made. The other party of communications can be found to be reliable on the basis of the identification.

The protection of connections between the servers can also prevent e-mail addresses from ending up in the hands of a third party.

E-mail service providers and users must, however, take into consideration that not all connections between servers are protected.

### **Recommendation**

In order to ensure the safety of e-mail communication, it is recommended that, if the e-mail server (MSA, MTA or MDA) supports the use of a protected connection, this characteristic is taken into use where possible.

## **5 REFERENCES**

- [1] Communications Market Act (393/2003):  
<http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf> (amendments up to 2004 included)
- [2] Act on the Protection of Privacy in Electronic Communications (516/2004):  
<http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf> (no amendments included)
- [3] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), 7 March 2002.  
[http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexplus!prod!DocNumber&type\\_doc=Directive&an\\_doc=2002&nu\\_doc=21&lq=en](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=Directive&an_doc=2002&nu_doc=21&lq=en)
- [4] Directive 2002/20/EC of the European Parliament and of the Council on the authorisation of electronic communications networks and services (Authorisation Directive), 7 March 2002.  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:EN:NOT>
- [5] Directive 2002/19/EC of the European Parliament and of the Council on access to, and inter-connection of, electronic communications networks and associated facilities (Access Directive), 7 March 2002. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:NOT>
- [6] Directive 2002/22/EC of the European Parliament and of the Council on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), 7 March 2002.  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:NOT>
- [7] Directive 2002/58/EC of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 7 March 2002.  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT>
- [8] Regulation on obligation to report information security incidents and faults and disturbances in public telecommunications (FICORA 9 B/2004 M),  
<http://www.ficora.fi/attachments/englanti/1156489108198/Files/CurrentFile/FICORA09B2004M.pdf>
- [9] FICORA Regulation 13 A/2008 M on information security and functionality of Internet access services  
<http://www.ficora.fi/attachments/englanti/5B37hthyt/Files/CurrentFile/FICORA13A2008M.pdf>
- [10] FICORA Regulation 47 B/2004 M on information security of telecommunications operators,  
<http://www.ficora.fi/attachments/englanti/1156489119589/Files/CurrentFile/FICORA47B2004M.pdf>
- [11] FICORA Regulation 53/2008 M on the obligation to retain identification data (Viestintävirasto 53 F/2008 M),  
<http://www.ficora.fi/attachments/englanti/5ynhW3rwX/Files/CurrentFile/FICORA532008M.pdf>
- [12] FICORA Regulation 54/2008 M on priority rating, redundancy, power supply and physical protection of communications networks and services,  
<http://www.ficora.fi/attachments/englanti/5wJbOLb5P/Files/CurrentFile/FICORA542008.pdf>

[13] RFC 4408, Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, <http://www.ietf.org/rfc/rfc4408.txt>

[14] RFC 4871, DomainKeys Identified Mail (DKIM) Signatures, <http://www.ietf.org/rfc/rfc4871.txt>

[15] RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail (DKIM), <http://www.ietf.org/rfc/rfc4686.txt>

[16] RFC 2554, SMTP Service Extension for Authentication, <http://www.ietf.org/rfc/rfc2554.txt>

[17] RFC 2595, Using TLS with IMAP, POP3 and ACAP, <http://www.ietf.org/rfc/rfc2595.txt>

[18] RFC 4616, The PLAIN Simple Authentication and Security Layer (SASL) Mechanism, <http://www.ietf.org/rfc/rfc4616.txt>

[19] RFC 2818, HTTP Over TLS, <http://www.ietf.org/rfc/rfc2818.txt>

[20] RFC 2142 Mailbox names for Common Services, Roles and Functions, <http://www.ietf.org/rfc/rfc2142.txt>

## 6 ABBREVIATIONS

|           |  |
|-----------|--|
| CERT-FI   | Computer Emergency Response Team - Finland |
| DNS       | Domain Name Server                         |
| IMAP      | Internet Message Access Protocol           |
| IMAPS     | Secure IMAP                                |
| IP        | Internet Protocol                          |
| ISP       | Internet Service Provider                  |
| MDA       | Message Delivery Agent                     |
| MSA       | Message Submission Agent                   |
| MTA       | Mail Transfer Agent                        |
| MX        | mail exchange                              |
| POP       | Post Office Protocol                       |
| POPS      | Secure POP                                 |
| RFC       | Request for Comments                       |
| SMTP      | Simple Mail Transfer Protocol              |
| SMTP-AUTH | SMTP Authentication                        |
| SSL       | Secure Socket Layer                        |
| TLS       | Transport Layer Security                   |