

**REGULATION 28 EXPLANATIONS AND  
APPLICATION INSTRUCTIONS**

**ON THE INTEROPERABILITY OF  
COMMUNICATIONS NETWORKS AND  
SERVICES**

**CONTENTS**

<b>CONTENTS</b> .....	<b>1</b>
<b>1 LEGISLATION</b> .....	<b>3</b>
1.1 LEGISLATIVE BASIS FOR REGULATION .....	3
1.2 OTHER RELEVANT PROVISIONS .....	4
<b>2 PURPOSE AND VERSION HISTORY OF THE REGULATION</b> .....	<b>6</b>
2.1 PURPOSE OF THE REGULATION .....	6
2.2 KEY AMENDMENTS AND VERSION HISTORY .....	6
<b>3 SECTION 1: SCOPE OF APPLICATION</b> .....	<b>8</b>
<b>4 SECTION 2: DEFINITIONS</b> .....	<b>9</b>
4.1 CUSTOMER AND INTERCONNECTION INTERFACES .....	9
4.2 COMMUNICATIONS NETWORK OR SERVICE COMPONENT .....	9
4.3 COMMUNICATIONS SERVICE PROVIDED IN A TELEPHONE NETWORK .....	9
4.4 PREMIUM RATE SERVICE NUMBERS .....	9
4.5 CORPORATE SUBSCRIBER .....	9
<b>5 3 INTERCONNECTIVITY, INTEROPERABILITY AND INFORMATION SECURITY</b> .....	<b>10</b>
5.1 INTERFACE DESCRIPTIONS .....	10
5.2 PREVENTION OF DISTURBANCES IN OTHER NETWORKS AND SERVICES .....	11
5.3 PROTECTION OF NETWORK TO NETWORK AND USER TO NETWORK INTERFACE .....	12
5.4 BLOCKING OF UNNECESSARY SERVICES AND PROTOCOLS FROM DEVICES .....	13
5.5 RECOMMENDATIONS CONCERNING ETHERNET INTERFACE INFORMATION SECURITY .....	14
5.6 RECOMMENDATIONS FOR THE INTEROPERABILITY OF COMMUNICATIONS NETWORKS AND SERVICES .....	15
<b>6 SECTION 4, IP NETWORK TO NETWORK INTERFACE</b> .....	<b>15</b>
6.1 PREVENTION OF TRAFFIC COMPRISING FALSE SOURCE ADDRESSES .....	15
6.2 FILTERING FALSE ROUTE ADVERTISEMENTS .....	16
6.3 DOCUMENTATION OF IP ADDRESS BLOCKS .....	17
<b>7 SECTION 5: SIGNALLING</b> .....	<b>18</b>
7.1 TRANSFER OF INFORMATION REQUIRED BY THE OBLIGATORY FUNCTIONS IN THE NETWORK TO NETWORK INTERFACE .....	18
7.2 SIGNALLING POINT CODES USED IN FINLAND .....	19
<b>8 SECTION 6: TIMERS</b> .....	<b>19</b>
8.1 CALL SET-UP TIMERS .....	19
8.2 TIMERS FOR CALLS PLACED TO PREMIUM RATE SERVICE NUMBERS .....	20
<b>9 SECTION 7: TONES, ANNOUNCEMENTS AND RINGING SIGNALS</b> .....	<b>20</b>
9.1 STANDARD-COMPLIANT TONES, ANNOUNCEMENTS AND RINGING SIGNALS USED IN TELEPHONE SERVICES .....	20
9.2 OTHER TONES AND ANNOUNCEMENTS USED IN TELEPHONE SERVICES .....	21
9.3 USE OF MUSIC AND SIMILAR ALONGSIDE RINGING TONE .....	21
<b>10 SECTION 8: TRANSFER OF SUBSCRIPTION NUMBER</b> .....	<b>22</b>
10.1 TRANSFERRING A SUBSCRIPTION NUMBER IN THE NETWORK TO NETWORK INTERFACE .....	22
10.2 RECOMMENDATION FOR TRANSFER OF SUBSCRIPTION NUMBER IN SIP PROTOCOL .....	23
10.3 CHANGING A SUBSCRIPTION NUMBER .....	23
<b>11 SECTION 9: VALIDITY OF SUBSCRIPTION NUMBER</b> .....	<b>24</b>
11.1 ENSURING VALIDITY OF NUMBER .....	24
11.2 PROCEDURES WHEN RECEIVING ERRONEOUS NUMBERS .....	25
<b>12 SECTION 10: TRANSFER OF CALLING PARTY NUMBER IN USER TO NETWORK INTERFACE</b> .....	<b>26</b>
12.1 TRANSFER OF CALLING PARTY NUMBERS IN A FORMAT ENABLING CALLBACK .....	26
12.2 PROCEDURES IN THE CASE OF PREMIUM RATE SERVICE NUMBERS .....	26
<b>13 OTHER RECOMMENDATIONS REGARDING THE IMPLEMENTATION OF SIP SERVICES</b> .....	<b>27</b>
13.1 INTEROPERABILITY OF FAX SERVICES .....	27

13.2	CONNECTION OF SIP PBXs TO THE PUBLIC TELEPHONE NETWORK .....	27
13.3	ANONYMISATION OF SIP ADDRESSES IN THE CALL ITEMISATION OF A SUBSCRIBER BILL.....	28
<b>14</b>	<b>SECTION 11: ENTRY INTO FORCE AND TRANSITION PERIOD.....</b>	<b>28</b>
<b>15</b>	<b>REFERENCE LIST .....</b>	<b>28</b>
<b>16</b>	<b>LIST OF ACRONYMS .....</b>	<b>32</b>

## 1 LEGISLATION

The objective of this chapter is to provide regulation users with an overview of the statutes on which the regulation is based. Moreover, the chapter lists other appropriate legislation within this area.

### 1.1 Legislative basis for regulation

The Finnish Communications Regulatory Authority's (FICORA) regulation is based on [1] sections 47, 63 and 129 of the Communications Market Act (393/2003 with amendments, CMA) and on [2] sections 19 and 20 of the Act on the Protection of Privacy in Electronic Communications (516/2004 with amendments, PPEC).

The Communications Market Act entered into force on 25 July 2003, enforcing the Framework [3], Authorisation [4], Access [5] and Universal Service Directives [6] concerning electronic communications, approved by the EC in February 2002. The Act on the Protection of Privacy in Electronic Communications entered into force on 1 September 2004, enforcing the Directive on Privacy and Electronic Communications [7], approved by the EC in February 2002. The EU amended these directives on 25 November 2009, and the amendments must be enforced nationally by 25 May 2011. [8, 9] During the preparation of the regulation, no amendments to the legislation caused by directives that would impact on the content of this regulation were known.

*CMA, section 128 Quality requirements for communications networks and services.* The regulation is related to the requirements for communications networks and services laid down in the following sections, controlling the design, construction and maintenance of communications networks and services in such a manner that:

- 1) the technical quality of telecommunications is of a high standard;
- 2) the networks and services withstand normal, foreseeable climatic, mechanical, electromagnetic and other external interference;
- 4) the protection of privacy, information security and other rights of users and other persons are not endangered;
- 7) they are interoperable, and can be connected to other communications networks, if necessary and
- 10) Their charging mechanism is reliable and accurate.

*CMA, section 129 Orders on communications networks and services.* This regulation specifies the requirements in section 128 on the basis of the following paragraphs of section 129. According to these, FICORA's regulations may apply to:

- 4) interconnectivity, 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;
- 17) technical documentation and
- 20) standards to be complied with..

This regulation lays down the procedures promoting interoperability, elimination of disturbances and performance in telecom operators' communications networks and, in particular, between them and at the customer interface (communications network interface point). These also result in requirements concerning network management. Moreover, decrees are provided for the technical documentation of interfaces between telecom operators. Furthermore, the regulation provides for signalling and the information provided to the user concerning technical call success, in compliance with certain standards.

*CMA section 47 FICORA numbering regulation.* According to subsection 2 of this section, FICORA may lay down requirements for the type of numbers and identifiers that are permitted for use in telecommunications and to which purpose, as well as determine the geographical usage area for numbers and identifiers.

This regulation provides for the signalling point codes included in identifiers and for the manner in which numbers must be transferred in the interconnection traffic between telecom operators.

*CMA 63 § User's right to parallel use of a subscriber connection.* According to the provision, the user has the right to simultaneously connect a terminal to more than one subscription, and FICORA may issue more specific regulations regarding the technical measures required by the right.

This regulation provides for the handling of the calling party numbers conveyed from subscriptions connected to a Private Branch Exchange (PBX) to the general communications network.

*PPEC section 19, Obligation to ensure data security (subsections 1, 2 and 4)* Under the section's subsection 1, telecommunications operators must ensure the information security of their services, including the security of operations, communications, software, hardware and data material. Under subsection 4 of section 19 of the Act on the Protection of Privacy in Electronic Communications, FICORA may issue telecommunications companies with more detailed regulations concerning service information security as defined in the section.

This regulation provides for telecommunications companies' obligation to ensure that the components in their communications network and services do not create disturbances but can withstand malicious traffic. Telecommunications operator measures intended in the regulation can be related to telecommunications operators' software and hardware control. In the event that the requirements of the Act on the Protection of Privacy are fulfilled, the measures can also be related to the automatic analysis and filtering of messages, in which case these are the measures detailed in section 20 of the Act.

*PPEC section 20, Measures for implementing information security.* This section provides for the necessary actions that telecommunications operators, added-value-service providers, corporate subscribers, and anyone operating on their behalf have the right to take in order to ensure information security. Under section 5, FICORA may issue telecommunications companies with more detailed regulations concerning the technical prevention of information security violations or the elimination of information security disruptions, as defined in the section.

Section 4 of this regulation provides for the analysis and filtering of traffic at the address group level on the basis of public IP address blocks and the telecommunications company's IP address space.

## **1.2 Other relevant provisions**

### 1.2.1 Communications Market Act

*CMA Section 133, Provisions on terminal equipment.* In accordance with subsection 2 of this section, telecommunications operators must publish up-to-date technical specifications concerning the public communications network interfaces to which telecommunications terminals can be connected.

The customer premises equipment interface can be considered to be part of the customer interface described in this regulation.

#### Applications of the transfer of subscription number information

*CMA Section 45 Collection of telecommunications fees.* According to this section's subsection 2, the information of the subscription number of a subscription liable to payment must be transferred during the telecommunications connection. If this is not technically feasible, the telecommunications operator governed by the subscription contract will be obliged to provide the information required for invoicing to the other telecommunications operator or, if this is not possible, to collect the fees without compensation.

*CMA Section 64, User's right to tone dialling and calling line identification.* Any telecommunications operator operating in the telephone network must offer users tone dialling and a service that shows users the calling number before they answer the call (DTMF and A-id display).

*CMA Section 80, Itemisation in telecommunications bill.* This section provides for telecommunications bill itemisation, performed on the basis of call types. Bills must itemise, for instance, interna-

tional calls, long-distance calls, mobile calls, and fees incurred for use other than communications services (i.e. content services).

### 1.2.2 Act on the Protection of Privacy in Electronic Communications

*Act on the Protection of Privacy in Electronic Communications Section 2, Definitions.* According to subsection 11 of this section, *corporate subscriber* refers to a company or other organisation subscribing to communications or value added services that processes users' confidential messages, identification data or location data in their communications network. Companies maintaining their own PBX networks are one example of corporate subscribers.

*PPEC Section 19, Obligation to maintain information security (subsection 3)* Under this section's subsection 3, telecommunications operators are responsible to their subscribers and users for information security as defined in subsections 1 and 2, including with regard to third parties who partially or entirely carry out the network service, communications service, data storage, or added value service.

#### Applications of the transfer of subscription number information:

*PPEC Section 22, Subscriber connection identification.* A telecommunications operator providing a subscription identification service must offer the subscriber a user-friendly option of preventing:

- 1) identification of any or all of his or her subscriber connections;
- 2) identification of the subscriber connections of incoming calls;
- 3) reception of calls whose subscriber connection identification is barred, if this is technically possible without undue cost; and
- 4) identification of the subscriber connection to which incoming calls have been transferred.

*PPEC Section 24, Call itemisation of a bill.* In addition to what is specified with regard to itemisation in section 80 of the Communications Market Act, on request, telecommunications operators must provide call itemisation in bills, with the last three digits covered, or in some other manner that prevents identification of the other communicating party on the basis of the itemisation. On request, users must be provided with a call itemisation itemising in full the numbers and other ID data related to the communicating parties' subscriptions. FICORA may issue more specific regulations on the content and implementation of itemisation.

This regulation does not provide more specific requirements concerning the matter, but in chapter 13 of MPS FICORA provides interpretation guidelines for the anonymisation of SIP addresses in a call itemisation provided to the subscriber.

*Section 35, Disclosing information to emergency services authorities.* The obligation to disclose identification, subscription and location data to the Emergency Response Centre, Maritime Rescue Co-ordination Centre, the Maritime Rescue Subcentre, and the police.

*Section 36, Certain other authorities' right of access to information* This provision is related to the police authorities' right to access identification data when investigating certain crimes.

### 1.2.3 FICORA's technical regulations

The provided list represents the situation at the time of this memorandum's publication. All FICORA regulations are published on its website at [www.ficora.fi](http://www.ficora.fi).

*Regulation 11 on information security and functionality of e-mail services* [10]. This regulation determines the minimum requirements for e-mail service providers for ensuring the information security and functionality of their communications services.

*Regulation 13 on information security and functionality of Internet access services* [11]. This regulation applies to the provision of Internet access services provided in public communications networks, and the services, communications networks and communications services used by telecommunications operators for these functions. In this regulation, Internet access service refers to the transfer of Internet traffic. The regulation is applied for the provision of Internet access services in both online companies and service companies, as applicable.

*Regulation 35 on barring categories in telecommunications traffic* [12]. This regulation provides for telecommunications barring categories for public telecommunications network subscriptions and their technical implementation. According to the regulation, telecommunications traffic and short message traffic must be grouped into categories in accordance with the regulation, one of which is traffic to premium rate service numbers. The regulation includes the grouping of service numbers into service groups I to IV on the basis of numbers' first parts (public utility, commerce, entertainment and adult entertainment).

*Regulation 41 on documentation of communications network and service* [13]. Under the regulation, the general requirement for documentation is that the documentation related to communications networks and services must indicate how the interoperability of the networks and services is ensured. The regulation also specifies the accuracy level of the terminal device interface specifications required by section 133.2 of the Communications Market Act.<sup>1</sup>

## **2 PURPOSE AND VERSION HISTORY OF THE REGULATION**

The objective of this chapter is to provide regulation users with information on the goals and purpose of this regulation. The most significant amendments to the regulations and recommendations preceding this regulation are also detailed in this chapter.

### **2.1 Purpose of the regulation**

The purpose of this regulation is to promote the interconnectivity of various telecommunications operators' communications networks and services and the end-to-end interoperability of communications services. The objective is to prevent in advance any interconnectivity problems related to communications networks and services, thus promoting the implementation of new services. The purpose of the regulation is to ensure that telecommunications operators ensure the information security of their interconnection and customer interfaces, thus improving the operational reliability of communications networks and services.

The goal of the regulation and the accompanying recommendations is to promote solutions that are considered favourable by telecommunications operators, therefore facilitating the required matching and testing and providing cost savings.

Conveyance of subscribers' number information is discussed as its own special topic in the second chapter. Number information and its reliability is important, particularly with regard to charging, but also with regard to the call-back option, emergency authorities, the police, etc. The objective of the regulation is to safeguard the validity and unambiguity of the calling and forwarding subscription number, and the call-back capacity of numbers conveyed at the customer interface.

### **2.2 Key amendments and version history**

The FICORA 28 H/2010 M regulation comprises the requirements for the interoperability of communications networks and services that were previously distributed across two different regulations. This regulation replaces the following existing regulations:

- Regulation on interconnectivity, interoperability and signalling in communications networks (FICORA 28 G/2010 M)
- Regulation on transfer of subscriber's number information in communications networks (FICORA 49 D/2010 M)

Interoperability in communications networks and services has been selected as the name of the regulation, since interconnectivity, signaling and transfer of subscriber's number information are all geared towards the end-to-end interoperability of communications networks and services.

Numerous amendments to the requirements have been made. Virtually all the requirements, or at least their explanations and application guidelines, have been amended. Numerous PSTN/ISDN-based requirements have been removed, since they are no longer necessary. On the other hand, all-new requirements pertaining to communications networks and services have been added to the

---

<sup>1</sup> The requirements are based on Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

regulation. The regulation's scope of application has been expanded to comprehensively cover IP-based communications networks and services.

Passages pertaining to all IP-based communications networks and services have been transferred to the regulation from FICORA regulation 13 on information security and functionality of Internet access services. Insofar as sections 5 to 10 are concerned, the IP perspective is particularly related to the consideration of VoIP services.

#### Summary of key amendments:

A new general section (Section 3) on interconnectivity, interoperability and information security in communications networks and services has been added to the regulation. The regulation requires telecommunications operators to define interface descriptions in accordance with which other telecommunications operators can connect their communications networks or services to their network. This regulation replaces the general requirements for communications networks and services' conformance with standards, as described in section 4 of regulation 28 G/2010 M. The objective of the amendment is to facilitate the interconnectivity of communications networks and services.

Section 3 of this regulation also lays down new requirements for the information security and disruption tolerance and prevention related to customer and interconnection interfaces. The goal of these requirements is to improve the operational reliability of communications networks and services.

Requirements from regulation 13 have been moved to the regulation's new section 4, concerning IP interconnection interfaces. The goal of this amendment is to extend the application of the requirements for IP address hygiene/control to other services as well as the Internet access service. In addition, the requirements have been slightly altered, with the filtering requirements pertaining to private IP address space being the most significant change.

The requirements laid down in section 4 of regulation 49 D/2010 M are divided into two new sections: *Transfer of subscription number* (Section 8) and *Validity of subscription number* (Section 9). The most significant amendment with regard to this subject is the exception for corporate subscriptions, laid down in section 9, according to which a telecommunications operator can use, on certain conditions, a number received from a corporate subscription and not belonging to its own number space as the number of the calling subscription. The telecommunications operator must also ensure the reliability of charging in this event.

Section 5 of this regulation replaces the requirements for signalling laid down in sections 5 and 6 of regulation 28 G/2010 M. The requirements have been reworded in a more general manner, since the previous regulation's detailed specification was no longer required.

The requirements regarding the conveyance of a calling party number with international connections, provided in the previous regulation version (FICORA 49 D/2010 M, Section 5), have been omitted from the regulation. These requirements were omitted since this is no longer necessary, and there is also a desire to allow telecommunications operators to convey numbers at the connection interface in the international format.

The requirements regarding the attachment of identifiers to a calling party number, provided in the previous regulation version (FICORA 49 D/2010 M, Section 6), have been omitted from the regulation. These have been replaced with a new requirement stating that a calling party number must be conveyed to the called subscriber in a format that enables call-backs and the receipt of messages. This alteration was made to provide telecommunications operators with the opportunity to select their desired address format – within the limits imposed by terminal device support. The requirements stated in the section in question are no longer required for the prevention of misuse.

The requirements laid down in section 8 of regulation 28 G/2010 M regarding the music played alongside the call tone have also been simplified. According to the new regulation, the service user is no longer required to specify the subscribers to whom music is played. Similarly, the requirement for telecommunications operators to ensure that users are aware of the existence of the service has been omitted.

A new requirement has been added to section 10 of the regulation; according to this requirement, the calling party number display must be indicated as blocked for *calls from premium rate service numbers* belonging to the service groups II to IV.

Additionally, the requirements regarding the handling of a connected subscription's number, provided in the previous regulation version (FICORA 49 D/2010 M, Sections 7 and 8), have been omitted from the regulation. This requirement was omitted since the service in question is not in use.

A separate section on the application of standards is not included in the regulation. Standards are separately referenced in sections in which obligating or informative standard references are deemed necessary.

### **3 SECTION 1: SCOPE OF APPLICATION**

Section 1 provides for measures that telecommunications operators must undertake to promote interoperability, information security and general IP address hygiene between telecommunications operators' communications networks and services, and between the user and telecommunications operator. These general requirements are applied in a technology-neutral manner to all public communications networks and communications services. According to the definition in section 2 of the Communications Market Act, *a public communications network* is a communications network that is provided for an unrestricted group of users. According to section 2 of the Communications Market Act, *public authority network* refers to a communications network that has been created to ensure general safety and public order, or for the purposes of the rescue services or civil defence.

The regulation is now applied more extensively to public communications networks. Previously, regulation 28 applied to public communications networks only with regard to the distribution of targeted communication. Now, the general requirements in sections 3 and 4 apply to both targeted and public communications networks such as cable television or terrestrial digital television networks.

Section 2 of the regulation provides for various factors related to call set-up control and maintenance, the notices and signals provided for the user related to these, and number transfer and display during the connection. Section 2 of the regulation is only applied to *communications services provided in the public telephone network*. The requirements in section 2 are based on the previous regulation 49, the scope of application of which was specified as *telephone service provided in a public communications network*. The definitions are further discussed in the explanations in section 2.

This amendment also expands the scope of application of section 2 to unidirectional telephone services and messages transferred over the telephone network (including text messages and faxes). In this instance, the term public telephone network refers, in a technology-neutral manner, to all networks utilising E.164 numbers or a number determined by the domestic authorities such as a short message service number, or transferring communications even partially controlled by means of these numbers. Other identifiers can also be used in the terminal and network when calling and connecting calls; the regulation applies if an E.164 number is used for user or service identification in the network alongside other identifiers.

The requirements in the regulation's section 2 do not, therefore, apply to communications services using only name-format addresses that fall outside the scope of application described in the preceding chapter. The requirements for subscription number transfer and validity laid down in section 8 to 10 are not applied to these name-format addresses even where making and receiving calls with an E.164 is possible, since an insufficient amount of experience has been gained regarding the technical implementation of these for creating appropriate requirements. It should be noted that the definition of the regulation's scope of application only applies to the regulation's specified requirements, and does not restrict the scope of application of the Communications Market Act and the Act on the Protection of Privacy in Electronic Communications with regard to provisions concerning the accuracy of charges, for instance.

In a departure from the previous regulation 28, the interoperability, interconnectivity and signalling to the public communications network of communications networks *incorporated as a part of* the public communications network or *connected to* the new public communications network are mentioned in the regulation's scope of application. Networks connected to the public communica-

tions network refer to customers' own communications networks such as buildings' indoor wire networks and companies' own switching and data communications networks. These requirements will not be eliminated but rather included in the requirements regarding the public communications network's customer interfaces.

The regulation discusses interconnectivity in the technical sense, meaning the requirements apply to the interconnection of communications networks and services irrespective of the judicial background of the connection.

## **4 SECTION 2: DEFINITIONS**

This chapter describes the definitions employed in the regulation.

### **4.1 Customer and interconnection interfaces**

In this regulation, *customer interface* refers to an interface used for connecting a telecommunications operator's customer's communications network, terminal device or application to the public communications network. In English, the complete term is User to Network Interface (UNI).

In this regulation, *Network to Network Interface* refers to a connection interface between telecommunications operators' communications networks or services. In English, the complete term is Network to Network Interface (NNI).

### **4.2 Communications network or service component**

In this regulation, communications network or service component refers to a network element, device or information system comprising a communications network or service utilised by a communications networks or service. Communications network or service components include, e.g. a mobile switching centres, base station controllers, base stations, text message centres, DSLAMs, name servers, network access control servers, switches, routers, SIP application servers and intelligent network components. Communications network or service component does not refer to transmission links or network element parts such as mobile switching centre CPUs.

### **4.3 Communications service provided in a telephone network**

*Communications service provided in a telephone network* herein means a communications service enabling a user to make and receive calls by means of a number or numbers specified in the national or international numbering plan. The crucial part of this definition is that it is a connection made using an E.164 number or a number defined by a national authority, such as a short message service number, or a number in the routing of which these are used. Therefore, the definition also covers unidirectional call services as well as fax and text message services.

The definition is worded to avoid contradictions or overlap with the definitions and terms used in the law and directives. Hence, the term *telephone service* is not used, since it refers, on the basis of the Universal Service Directive's definition of a *publicly accessible telephone service*, to a service in which the same number can be used both for making and receiving calls. The definition of this regulation also covers VoIP services that are unidirectional with regard to numbering.

### **4.4 Premium rate service numbers**

Premium rate service numbers are numbers that can be used to provide services charged by means of the telephone bill. In accordance with FICORA regulation 35, premium rate service numbers are grouped into the groups I to IV (public utility, commerce, entertainment and adult entertainment services). Which service numbers fall into which group service is described in sections 1 and 2 of the regulation.

### **4.5 Corporate subscriber**

The definition of a *corporate or association subscriber* laid down in the Act on the Protection of Privacy in Electronic Communications (516/2004) is employed in the regulation. According to section 2 of this section, *corporate subscriber* refers to a company or other organisation subscribing to

communications or value added services that processes users' confidential messages, identification data or location data in their communications network.

## **Chapter 1, General requirements:**

### **5 3 INTERCONNECTIVITY, INTEROPERABILITY AND INFORMATION SECURITY**

This section lays down all the requirements regarding interconnectivity, interoperability and information security that are applied to all communications networks and services. These are basic requirements that telecommunications operators must implement in order to ensure the interoperability and information security of services regardless of the nature of the provided network service or communications service.

Since the requirements are applied to all communications networks and services, there is reason to give telecommunications operators the opportunity to select the mechanisms best suited to their own communications network or service. The essential thing, however, is that the telecommunications operator is able to fulfil the requirements laid down in the section using these mechanisms.

The requirements laid down in this section are basic requirements, the content of which will be further illuminated with examples later in this chapter.

#### **5.1 Interface descriptions**

The regulation requires telecommunications operators to define interface descriptions in accordance with which other telecommunications operators can connect their communications networks or services to their network.

##### Explanations

In order to provide end-to-end communications services, it is necessary for telecommunications operators to interconnect their public communications networks and services.

Interconnectivity and transfers of access rights between telecommunications operators are partially controlled by the Communications Market Act and the SMP decisions based on it, while also being partially based on commercial contracts that may be chargeable or free, especially with regard to IP interconnections. Telecommunications operators' interconnectivity obligations are laid down in section 39. This regulation does not indirectly comment on what type of interconnectivity obligations result from the legislation.

The goal of this regulation is to promote the technical implementation of interconnections, particularly in circumstances in which there are no established technical solutions and interconnection requires that the telecommunications operators select options enabling interconnectivity among the alternatives defined in the standards. Under section 2 of FICORA regulation 41, the general requirement for documentation is that the documentation related to communications networks and services must indicate that the interoperability of the networks and services is ensured. This requirement complements and specifies the general requirement. The definition of interface descriptions promotes practical interconnections between telecommunications operators, regardless of whether it is based on obligation or free will.

In accordance with subsection 2 of section 133 of the Telecommunications Market Act, telecommunications operators must publish up-to-date technical descriptions concerning the public communications network interfaces to which telecommunications terminals can be connected. This obligation is further specified in regulation 41.

##### Application

An interface or service description is a telecommunications operator's description of how a telecommunications operator requesting interconnection can connect to its network. Telecommunications operators must define the aforementioned interface description at a level of specificity which enables technical implementation of interconnection on the basis of that interface description. The more specific level depends on the interconnected services and the interconnection technology. Therefore, FICORA has deemed it appropriate to leave this matter to be decided by the telecom-

munications operators themselves. Below are a few examples of interconnection cases as well as of the minimum content of the interface descriptions appropriate to them:

- **Bitstream (operator DSL):** A network operator should determine in the interface description the technology, physical implementation of the interconnection and the available speed classes for both the User to Network and Network to Network Interfaces. Moreover, the interface description should indicate any possible restrictions concerning subscription use (e.g. the number of MAC addresses) and any other appropriate specifics related to the relevant technology dependent on the implementation such as the field used for customer identification (DHC option 8.2) and any possible information related to the compatibility of customer terminals.
- **Internet access service (IP transit and peering):** Insofar as the Internet access service is concerned, the interface description should determine, for instance, the used network technology, physical implementation of the interconnection interface, available speed classes and supported IP and routing protocols for the Network to Network Interface. In addition to these, the interface description should determine any other possible requirements, restrictions and other relevant details (e.g. AS number) defined for interconnections.
- **VoIP Network to Network Interface:** This example looks at a case in which the SIP protocol has been selected for interconnecting telephone services. In this event, at least the following should be determined in the interface description: the network technology implementation of the interconnection (e.g. interconnection over a separate IP connection, traffic exchange point, or the Internet), including more detailed technological specifications (c.f. the previous example), and the employed application protocol (SIP), along with the specifications required for interconnectivity and interoperability (SIP profile). Moreover, the interface description should determine the other requirements or restrictions possibly determined for interconnections.

In addition to the aforementioned details, the interface description should indicate the availability of the product as well as the applied delivery, fault recovery, maintenance and monitoring procedures, including the service level classes available to the telecommunications operator requesting interconnection.

If some centralised service (e.g. FICIX, [www.ficix.fi](http://www.ficix.fi)) is used for interconnection instead of a direct interconnection between two parties, this should be mentioned in the interface description. The requirements or guidelines possibly determined by the centralised service do not, however, have to be reiterated in the description.

#### Recommendation

FICORA recommends that telecommunications operators publish the interface descriptions on their websites, for instance, so as to make them available to telecommunications operators requesting interconnection.

## **5.2 Prevention of disturbances in other networks and services**

*Under the regulation, telecommunications operators must ensure that their communications networks or service components do not cause disturbances to other telecommunications operators' communications networks or services. Telecommunications operators must have the appropriate mechanisms to prevent such disturbances.*

#### Explanations

A telecommunications operator's network may not cause disturbances in another telecommunications operator's communications networks or services. The obligation laid down in the regulation obviously prohibits intentional interference, but the requirement is still primarily intended to prevent unintentional disturbances – caused by a configuration error, for instance – from spreading from one network to another. Disturbances spreading over a Network to Network Interface may create loops in the network, misdirect traffic or simply create congestion in some part of the network or service due to extra traffic. At worst, the service may be rendered altogether unavailable.

Since the impact of these disturbances can be great, it has been deemed necessary to oblige telecommunications operators to prevent their own network or service from causing interference in their connection partners' services. This has been decided despite the fact the telecommunications operators are obliged to protect from this type of interference under the following subsection.

Operations complying with this obligation should already be standard practice for telecommunications operators. Furthermore, the mechanisms mentioned in the section should already exist in the majority of devices, meaning the obligation should not result in significant costs to telecommunications operators.

#### Application

The obligation is not targeted at any one technology or protocol level, but rather the telecommunications operator must evaluate the threats caused by the technologies and services used in the Network to Network Interface, and subsequently implement all the protection mechanisms required for preventing disturbances from spreading.

Mechanisms that prevent loops from forming in the Network to Network Interface can be considered to represent this type of necessary protection mechanism. For instance, calls can be forwarded a maximum of five times in circuit-switched telephone services, after which the call will be disconnected. With regard to interconnection of Internet access services, this means the telecommunications operator not sending traffic over the same logical interface in the Network to Network Interface that it has already received over the interface in question.

### **5.3 Protection of Network to Network and User to Network Interface**

Under the regulation, *telecommunications operators must protect their own network from incoming malicious traffic from Network to Network and User to Network Interfaces by implementing the necessary protection mechanisms within its network.*

#### Explanations

The reasons for the protection of the Network to Network Interface between telecommunications operators have already been discussed in section 5.2. Compared to a Network to Network Interface between telecommunications operators, the User to Network Interface poses more varied threats. For instance, insofar as the Internet access service is concerned, the network operator must ensure, in addition to the prevention of threats mentioned in section 5.2, that customers are not able to eavesdrop on other customers' traffic or cause DoS attacks targeting these customers.

The nature and severity of the threats together with the required protection measures vary according to the service provided and the technology used. The application section provides an example of the protection of telephone services, for instance. With regard to email services, the matter is discussed in more detail in regulation 11 on information security and the functionality of e-mail services [10], and with regard to the Internet access service, in regulation 13 on the information security and functionality of Internet access services [11]. Some risks related to Ethernet technology and protection against these is discussed in section 5.5, Ethernet interface information security.

#### Application

Under the regulation, telecommunications operators must protect their own network from incoming malicious traffic from Network to Network and User to Network Interfaces by implementing the requisite protection mechanisms in its network. The closing of services unnecessary to the provided service is discussed in more detail in section 5.4.

The malicious traffic mentioned in the requirement refers to traffic harmful to the telecommunications operator's own communications network or service that may at worst jeopardise the functionality of the telecommunications operator's communications network or service.

The obligation is not targeted at any one technology or protocol level, but rather the telecommunications operator must evaluate the threats caused by the technologies and services used in the Network to Network Interface, and subsequently implement all the mechanisms required for pro-

tecting its communications network and service. These mechanisms include filters based on the source or target address, the protocol used, message content, or the number of messages.

The aforementioned protection mechanisms can also be implemented at the control level, in which case the filtering of messages is not necessary. It may therefore be sufficient, at least with regard to certain threats, for telecommunications operators to simply protect the control level of the devices processing the traffic in question in their network, while conveying traffic in the normal fashion via their network. If a telecommunications operator carries out protection at the control level instead of filtering, it must obviously implement the required mechanisms in all the necessary network elements.

Below are a few examples of threats and the protection measures required for them. It should be noted that the examples are not exclusive, and telecommunications operators must evaluate the required measures themselves.

- **Bitstream User to Network Interface:** This section discusses examples of the protective measures that network operators should implement in the User to Network Interface Ethernet DSLAM or the subsequent edge switch. Network operators should, for instance, filter the customer port's incoming and outgoing BPDU messages and manufacturer-specific L2-level control protocol messages.
- **VoIP Network to Network and User to Network Interfaces:** This section discusses examples of protective measures that telephone service providers should implement in order to protect their own networks. The problem is discussed in more detail in the RFC 5390 [14] and ID [15], for instance. Possibly necessary protective measures include restrictions based on source addresses or the amount of call attempts. The aforementioned mechanisms are easy to implement using SBC (RFC 5853) [16], for example.

#### 5.4 Blocking of unnecessary services and protocols from devices

*Under the regulation, a telecommunications operator must ensure that no unnecessary services or protocols with regard to the provided service are switched on in its Network to Network or User to Network Interface communications network or service components or their ports.*

##### Explanations

This requirement is related to the section's previous subsection in which telecommunications operators are obliged to implement any necessary protection mechanisms required for the protection of their own network. The switch-off of unnecessary services and protocols is one of the most crucial mechanisms of this type, and because of this it has been deemed necessary to present it as its own specifying requirement in addition to the other protection mechanisms deemed necessary by the telecommunications operator.

Switching off unnecessary services and protocols is crucial because when the communications network or service component is running less software, it also has less vulnerabilities of which potential attackers may utilise. Moreover, filtering unnecessary routing protocols or other control traffic in the management interfaces reduces the possibility of traffic distributed over the interface interfering with the operations of a telecommunications operator's network.

##### Application

This requirement is applied to communications network and service components in both the User to Network and Network to Network Interfaces. FICORA recommends that telecommunications operators apply the same practices to their other communications networks and service components, irrespective of their location.

The requirement is not targeted at any one technology or protocol level, but rather the telecommunications operator must evaluate unnecessary services on a device-specific - and possibly also port-specific - basis, and subsequently switch these off. In some devices this issue may have been taken into account in the default settings, or the device manufacturer may have provided commands that can be used to switch these types of services off all at once. Telecommunications operators must find out the correct procedure for each device, since this matter cannot be assumed

to be in order by default. Below are a few examples of the obligation's implementation in various network elements. It should be noted that the examples are not exclusive, and telecommunications operators must evaluate the required measures themselves.

- **Bitstream User to Network Interface (PE router):** This section discusses examples of the protective measures that service operators should implement in the User to Network Interface PE router. This means services such as FTP, HTTP, NTP, finger, or bootp not being switched on in the router's customer ports. Similarly, routing protocol or proxy arp messages from customer ports should not be processed at the control level. However, traffic can be distributed via the network.
- **Outgoing mail server (MSA):** The outgoing mail server is a device or virtual server in the User to Network Interface via which outgoing emails are sent from. This type of server does not handle routing or other network-level control protocols. In order to reduce vulnerability risks, no unnecessary services can be running in this network element. In MSA's case, these may potentially include FTP and HTTP servers.

## 5.5 Recommendations concerning Ethernet interface information security

This chapter discusses a few of the key information security problems related to Ethernet technology that impact on the operation of communications networks and services, while also providing examples of protection against these problems. The provided examples deal with situations in which the telecommunications operator network has been implemented using a conventional switch solution. The problems do not therefore primarily apply to networks using MPLS or pseudowire tunneling, for instance.

Even though no detailed obligations regarding the subject are laid down in this regulation, FICORA recommends that telecommunications operators also prepare for the threats mentioned in this chapter when implementing the necessary protection mechanisms.

### 5.5.1 Broadcast storms

A broadcast storm is created when too many multicast messages are sent to the network via the Network to Network Interface port. A broadcast storm may render the Network to Network Interface unusable, if the multicast messages fill up the interconnected network's capacity. Due to this, parties engaging in interconnection traffic must prepare for limiting the impact of broadcast storms. This can be done, for instance, by restricting the capacity allowed for distribution messages in the network.

FICORA recommends that only switches supporting so-called Storm-control filtering be used in interconnection traffic interfaces. Storm-control filtering enables you to reserve a specific portion of line capacity for unicast and broadcast traffic. Filter settings must be configured so as to prevent filtering from interfering with normal network traffic.

### 5.5.2 L2 control protocols

Operators can prevent loops from being created in their own L2 networks by utilising the Spanning Tree protocol (STP). The protocol may also lead to significant problems if misused. Many manufacturer-specific protocols such as the Cisco protocols CDP and VTP can also result in similar problems. At worst, a customer may intentionally or unintentionally crash the provided service or direct traffic via its own subscription without authorisation, which enables activities such as tapping and redirection of traffic. STP and manufacturer-specific protocols must be isolated by means of a control level.

### 5.5.3 VLAN hopping

Double Tag VLAN packets can be used to send Denial of Service traffic from a customer port via the switch's backbone network to VLANs behind other switches. This is possible since, in a native connection, the switch typically only removes the outermost VLAN identifier, in which event the other VLAN identifier is still left in the packet. Establishing a bidirectional connection is not possible, but this can be used to wage DoS attacks on the port of some other service or customer.

In order to avert the threat the network operator must ensure that only VLANs used by the subscriber are allowed in the trunk port of the subscriber switch. In the Network to Network Interface, network operators must only allow the VLAN area agreed with the service operator. It is also recommended to keep the number of switches between routing devices and the customer to a minimum.

#### 5.5.4 MAC address operation management and filtering

MAC address operation management and filtering are network protection methods that are necessary when protecting against interference of telecommunications traffic and errors caused by device failure. If a customer is able to fill the switch's MAC table, the switch will send all packets to every switch port, in which event every device connected to the switch will be able to view all customer traffic distributed via the switch. In switches and DSLAMs, the restricted size of the MAC table thus represents one of the known information security threats.

The severity of the above threat is, however, dependent on the technology used. A telecommunications operator may, for instance, reduce the risk of the above by utilising the Provider Backbone Bridging technology (802.1ah [17]). The problem can also be prevented by restricting the number of port-specific MAC addresses and by allowing traffic only to correct known MAC addresses. Preventing MAC tables from filling up from customer ports is not always possible in older or cheaper switches. The aforementioned problem also applies to the dimensioning of the Ethernet network between the terminating router and customer terminal. NOs and SOs should thus be able to manage the number of active MAC addresses in a port-specific manner (subscriber switch or Network to Network Interface).

### 5.6 Recommendations for the interoperability of communications networks and services

References to key national recommendations concerning the interoperability of communications networks and services are assembled under this chapter. The requirements and recommendations related to the interconnectivity of telephone services are detailed in chapters 10.2 and 13 of this memorandum.

Recommendations concerning Ethernet-based rental products are published in FICORA's working group report 3/2010 Ethernet-based rental products (available only in Finnish) [18].

The recommendation regarding Open Access networks and the interoperability of services provided in them are provided in FICORA's working group report 1/2010, Final report of Open Access pilot.

Recommendations concerning broadband connections' order and delivery processes have been published in FICORA's working group report 3/2006, Ordering and delivery processes for broadband connections.

## 6 SECTION 4, IP NETWORK TO NETWORK INTERFACE

This section provides for the basic requirements for the interconnection traffic of networks using the IP protocol.

### 6.1 Prevention of traffic comprising false source addresses

Under the regulation, *a telecommunications operator must prevent such IP traffic that is directed to its communications network where the sender's IP address set in the received IP packet*

- *belongs to the IP address space managed or advertised by the telecommunications operator itself, or*
- *belongs to the private IP address space, or*
- *does not belong to the routes advertised to other telecommunications operators by a telecommunications operator that delivers traffic.*

*However, traffic can be delivered if telecommunications operators have come to a separate agreement about it.*

### Explanations

IP packets directed to a telecommunications operator's network may include an erroneously defined source address, falsified either by mistake or on purpose. Receiving IP packets from another telecommunications operator using the telecommunications operator's own addresses or addresses belonging to a private IP address space as source addresses without a separate contract do not constitute a normal situation and entail significant information security risks.

Falsification of IP addresses (IP spoofing) is also often used in DoS attacks. In IP spoofing attacks, the attacker falsifies their own network address so that the target of the attack believes that the packets originate from a reliable source. Falsification of source addresses is used for concealing the attacker's identity. The lack of filtering of IP packets sent using a falsified sender address enables sabotage targeting other Internet users without the possibility of discovering the perpetrator's identity.

The requirements are intended to significantly reduce the problems caused by attacks using falsified IP source addresses and network failures.

### Application

Telecommunications operators must filter traffic directed to their network containing a source address that is erroneous in the above manner, unless otherwise agreed. Special filters should be installed in the routers, reducing the number of IP packets using falsified addresses sent to and from the network.

This requirement only applies to source addresses relevant to the telecommunications operator's network, meaning that the telecommunications operator does not need to check the other source addresses distributed with an IP packet's duty load in connection with VPN tunnelling, for instance.

Filtering procedures must be performed at the technically appropriate level of specificity in the Network to Network Interface. In some unusual situations, a telecommunications operator may make an agreement with another telecommunications operator concerning a part of the telecommunications operator's address space being temporarily routed from the other's network.

This procedure must be planned and executed with careful consideration, using methods suitable to the Network to Network Interface conditions. The solution options to be used and factors to be considered are detailed in the IETF specifications RFC 2827 (BCP 38) [21] and RFC 3704 (BCP 84) [22]. The primary responsibility for the prevention of traffic comprising false source addresses falls to the telecommunications operator distributing traffic.

## **6.2 Filtering false route advertisements**

*Under the regulation, of the route advertisements received at interconnection interfaces, a telecommunications operator must reject routes that belong to the operator's own networks or the networks of its customers, unless individual networks have been otherwise agreed upon.*

No telecommunications operator should advertise routes including network address blocks controlled by another telecommunications operator or its customer, or more specific sub-blocks without a separate agreement. For example, certain temporary multihoming solutions may require this type of agreement.

Unauthorised advertising may constitute intentional or unintentional activity to direct traffic to the attacker's system. In order to protect against risks associated with unauthorised advertising, a telecommunications operator receiving route advertising must filter out false advertising.

### 6.3 Documentation of IP address blocks

Under the regulation, *the telecommunications operator must ensure that the IP addresses allocated to it and advertised by it are properly documented in the database of the Internet address register that has granted the address space.*

#### Explanations

A telecommunications operator must carefully document the use of IP addresses allocated to and advertised by that operator by documenting the networks in the database of the Internet address register that has granted the address space. Documentation of the address spaces is important because telecommunications operators use this information for creating prefix lists. Prefix lists are used for ensuring that a telecommunications operator advertising routes only advertises the address spaces it manages.

Telecommunications operators must ensure that the WHOIS database of the Internet address register (IR) that has granted the address space includes appropriate information regarding the address spaces managed by the telecommunications operator or its customers, including abuse and irt contact information.

Appropriately documented IP network resources provide great assistance with concern to the maintenance of routing information as well as the resolving of information security violations.

#### Application

Telecommunications operators must report the networks managed by it to the database of the Internet address register (IR) that has granted the address space. This information is logged and maintained in accordance with the address register's valid guidelines. This information includes IP address space, the telecommunications operators' contact information, the administrator's contact information, abuse and IRT contact information and the network AS number, from which the IP addresses in question can be found.

The telecommunications operator must specifically ensure that the documentation of the IP networks used by that operator is up-to-date. If a telecommunications operator acts as the source of route advertising for PI network spaces controlled by other organisations, the veracity of the information related to the address spaces in question must be checked in connection with the activation of route advertising. Similarly, if a telecommunications operator maintains a Local Internet Registry, lending IP address space to third parties, the veracity of the information must be checked when the network address space is being registered.

In practical terms, this requirement means that telecommunications operators are not allowed to advertise undocumented IP address spaces to other telecommunications operators.

The European Local Internet Registry RIPE NCC has adopted a dedicated field, "IRT Object", for registering abuse contact information. Use of the IRT Object data field is documented in the RIPE NCC document "RIPE Database Update Reference Manual" [23]. Instructive examples for the adoption of IRT Objects are provided in the documents "RIPE IRT object - Technical HOW TO" [24] and "IRT FAQ" [25].

## **Chapter 2: Special requirements for communications services provided in a telephone network:**

### **7 SECTION 5: SIGNALLING**

This section determines the requirements for signalling in communications services provided in a telephone network.

#### **7.1 Transfer of information required by the obligatory functions in the Network to Network Interface**

Under the regulation, *the interconnection traffic between telecommunications operators must be arranged so that the information required by functions that are stated as obligatory in the provisions is transferred over the interconnection interface.*

##### Explanations

Certain requirements are laid down in the provisions for telecommunications operator functions whose appropriate implementation requires information to be transferred over the Network to Network Interface. These provisions are compiled under section 1.2. Some of the functions may also be implemented in a manner that does not require information to be transferred over the interface. In that event, this requirement will not apply.

The functions covered by the regulation include:

- Billing and the related itemisation in customer invoicing (if the telecommunications operators have agreed to use a billing method in which billing information is transferred over the Network to Network Interface).
- Functions related to the calling party's number information, including billing on the basis of the calling party's number, tracing of malicious calls, and positioning of caller and address search at emergency response centre.

This is a general requirement that requires adequate information transfer over the Network to Network Interface, regardless of interface implementation.

##### Application

In interconnection traffic negotiations, telecommunications companies must ensure that all the relevant information will be transferred over the adopted protocols determined by the telecommunications operators.

Presently, the ISUP user part of Common Channel Signalling is primarily used for interconnection, determined with regard to basic calls in the standards SFS 5779 (ISUP2) [26], SFS 5869 (ISUP3) [27] and SFS 5901 (ISUP4) [28], and with regard to additional services in the standards SFS 5778 [29], SFS 5868 [30] and SFS 5902 [31].

Some of the information transferred over the Network to Network Interface is included in the various prefixes of the number transferred in the called party's number field. With regard to these, the codes are determined in the FICORA working group report 5/2004 Number portability, fixed telephone network, technical network implementation [32].

If the telecommunications operators implement and start to use other signalling methods (e.g. SIP) in the Network to Network Interface, they must ensure that the information required by the obligatory functions can be transferred over the interface.

## 7.2 Signalling point codes used in Finland

Under the regulation, *communications network components connected to the public telephone network using a common channel signalling system and located within Finland must apply the signalling point codes granted by FICORA.*

### Explanations

Common Channelling Signalling system signalling point codes are used for identifying communications network components connected to the signalling network. By only using codes granted by FICORA in components connected to the public network it can be ensured that no two components have the same code and that signalling traffic to and from each component can be correctly channelled in the signalling network.

### Application

The principles for granting signalling point codes are determined in FICORA regulation 32 on numbering in a public telephone network [33].

Finland's national Common Channelling Signalling network forms a single unified network, which is made possible only by using codes allocated to the national network in the network indicator field of the signalling part MTP. This code, determined in section 14.2.2. of ITU-T recommendation Q.704 [34], is "Sub-service field Network indicator code 10 National network".

The structure of the international signalling point codes used in the international signalling network is determined in the ITU-T recommendation Q.708 [35].

## 8 SECTION 6: TIMERS

This section determines the requirements for timers in communications services provided in a telephone network.

### 8.1 Call set-up timers

Under the regulation, *telecommunications operators must implement, in an appropriate manner, the timers necessary for call set-up.*

### Explanations

Call set-up signalling reserves various resources in the network during call set-up. In circuit-switched networks the prevention of overlong resource reservations aids in network resource (e.g. voice channels) dimensioning, while preventing the likelihood of call barring. Overlong (non-disconnected) call attempts cause problems in VoIP networks too, if the memory reserved for maintenance of connection status is exceeded. Insofar as these are concerned, the timers must be short enough.

It is essential from the user's perspective that sufficient time has been reserved for call set-up in such a manner that call set-up is not unnecessarily prevented due to exceedingly short timers. Since the executor of the shortest timer in the call set-up chain determines the time reserved for call set-up, it is reasonable to determine minimum lengths for the timers.

### Application

Standard-compliant timers are implemented in the network components participating in call set-up, and these prevent resources from staying reserved in various cases of call-set up failure, while also preventing overly rapid call set-up interruption.

Necessary timers include at least the timer controlling the connection time and the timer controlling the called party's response time. The timer controlling the connection time in circuit-switched networks' ISUP signalling (T7) is 20 to 30 seconds (default value 30 seconds) and the timer controlling the called party's response time (T9) is 1.5 to 3 minutes (default value 3 minutes). Similar timers' rated values, observing their ranges, should be used in other networks.

As far as calls terminating in the mobile phone network are concerned, the timer controlling the called party's response time can, however, be set shorter than the determined minimum value. However, in this event it must be ensured that the timer is long enough to prevent the operation of any service from being blocked due to an overly short timer (e.g. a call does not have the time to be forwarded to voice mail if the timer is too short).

The SIP protocol does not determine the timers that are fully compatible with the aforementioned timers. In VoIP solutions utilising the SIP protocol, it is, however, possible to replace the timer controlling the connection time and the timer controlling the called party's response time with SIP protocol timer C (Proxy INVITE transaction timeout) [36].

In adoption situations, such as cases in which a VoIP service implemented using the SIP protocol is interconnected to the circuit-switched telephone network, each network operates in accordance with its own timers.

A set of other timers are also specified in the signalling standards and specifications. Some of these timers are related to resource management and some are necessary with regard to the functionality of signalling. Telecommunications operators must implement the timers necessary for the provided service.

## **8.2 Timers for calls placed to premium rate service numbers**

*Under the regulation, in the communications services provided in telephone networks, the telecommunications operator that implements the service must be prepared to implement timers for monitoring calls made to premium rate numbers.*

### Explanations

The regulation requires telecommunications operators providing public telephone connections to the service provider (telecommunications operator implementing the service) to be able to technically implement timers, but does not determine their length or when timers should be used. Functions and services related to the management of the user's call costs concerning call duration are covered within *self-regulation*.

This matter is discussed in more detail in the Basic Set of Norms for Providing Premium Telephone Services that can be found on the website of MAPEL, the Ethical Committee for Premium Rate Services ([www.mapel.fi](http://www.mapel.fi)) [37]. Section 24 of the set of norms, based on the sector's self-regulation, determines that the maximum service duration in premium rate telephone services is 30 minutes in call classes III and IV, unless the service duration is prolonged by the caller's action.

### Application

A timer is activated in communications networks upon activation of the answer signal when calling specifically determined premium rate service numbers. Expiry of the timer disconnects the call.

## **9 SECTION 7: TONES, ANNOUNCEMENTS AND RINGING SIGNALS**

### **9.1 Standard-compliant tones, announcements and ringing signals used in telephone services**

*Under the regulation, tones, announcements and ringing signals complying with standards SFS 5876 [38] and SFS 5749 [39] must be used in communications services provided in the telephone network in order to advise the user on different network modes related to call set-up.*

### Explanations

Providing advice for users regarding communications networks' various modes is beneficial for the network and user alike. When the user is advised on what is blocking call set-up, they can alter their course of action at the call attempt, for instance. For example, if they hear the announcement "the number you have dialled is not in service", they can check the number dialled. It is crucial to

users that the tones and announcements regarding network modes are consistent in as many situations as possible. It is also beneficial to the network that users do not burden the network with repeated erroneous call attempts.

#### Application

The standard SFS 5876 determines a set of situations and the tones used in those situations; similarly, SFS 5749 determines a set of situations along with the announcements used in them. Telecommunications operators must use the specified tones and announcements in the situations determined in the standards. The general principles of tone and announcement use are described in standard SFS 5749. Adaptation of SIP responses and ISUP cause codes is not included in the standard SFS 5749. Insofar as these parts are concerned, adaptation is determined in the national document GFI 0301 [40], based on ITU-T recommendation Q.1912.5 [41]. Recommendation Q.1912.5 determines the various SIP profiles (A, B and C) and the relevant adaptation of cause codes. IETF has determined similar adaptations in specification RFC 3398 [42].

The various ringing signals are determined in standard SFS 5876. In accordance with the standard, the ringing signals are sent from exchanges in case of fixed-network analogue subscriptions, making it necessary for them to be compliant with the standard. Insofar as ISDN subscriptions, mobile subscriptions and VoIP subscriptions are concerned, information of incoming calls is transferred to the terminal in signalling, and the terminal indicates incoming calls on the basis of this information. The terminal can indicate incoming calls in a number of ways, and the regulation does not impose any requirements on terminal operation.

### **9.2 Other tones and announcements used in telephone services**

Under the regulation, *other signals and announcements in accordance with subsection 1 related to call set-up must be unambiguous, clear and distinguishable from one another.*

#### Explanations

For instance, a telecommunications operator may deem it necessary to adopt a tone or announcement that is not determined in the standards in connection with the introduction of new services. In order to prevent these tones and announcements from being mistaken for standard-compliant tones and announcements or others adopted by the telecommunications operator, they must be unambiguous, clear and distinguishable from one another.

#### Application

When a telecommunications operator adopts a new tone or announcement that is not included in the standards, it must ensure, using such measures as user tests, that these will not be mistaken for other tones and announcements already in use.

### **9.3 Use of music and similar alongside ringing tone**

Under the regulation, *the telecommunications operator can offer its subscribers a service where, when calling a customer using the service, the calling party hears, in addition to the standard ringing tone, music or something similar selected by the subscriber of the service. The standard-compliant ringing tone must be clearly heard alongside other sounds.*

#### Explanations

New services are always being established in communications networks. Offering music or similar sounds to replace the ringing tone is one such service. The adoption of various types of new services in communications networks must be promoted, but in such a manner as not to cause problems to users. Users must have a clear understanding that they hear ringing tone related to the service and not, for instance, call queuing music. If ringing tones were only music, it would be impossible to differentiate between ringing tones and call queuing music.

### Application

A ringing tone complying with standard SFS 5876 [38], at the volume determined in the standard, must be used alongside music or similar sounds. The music must be adjusted to a volume ensuring that the standard-compliant ringing tone is clearly audible.

Such things as birdsong and a train whistle, for instance, also count as music and similar sounds. However, marketing content, etc is not allowed.

## **10 SECTION 8: TRANSFER OF SUBSCRIPTION NUMBER**

### **10.1 Transferring a subscription number in the Network to Network Interface**

*Under the regulation, the calling party number and in case of a redirected call, the redirecting number must be transferred in communications services provided in a telephone network between telecommunications operators.*

*Moreover, subsection 2, section 8 states that the calling party number and in case of a redirected call, the redirecting number must be transferred in an international format at the Network to Network Interface, unless the signalling can indicate whether the format of the number is a national (significant) number or an international number.*

### Explanations

Calling party numbers can be utilised in many communications network services (e.g. number display, charging) and many official functions are based on it (e.g. address search and positioning in emergency response centre with regard to emergency calls). In case of a redirected call, the transferred subscription number can be used for charging, for instance. Due to this, it must be required that the numbers are transferred between telecommunications operators, in which case they can be further transferred to the application using them. The transferred number should be as unambiguous as possible.

In the ISUP standards, the transfer method of the calling party number and in case of a redirected call the transfer method of redirecting number is defined. Subscription numbers can be transferred in their national or international formats, depending on the case.

The SIP protocol provides numerous alternative header fields for number information transfer, and the number can be displayed in different formats in the fields. Different parties may interpret the standards in a different fashion, in which event the recipient of number information may find it difficult to interpret in which header and format the information required for number transfer is presented. These practices must be unified in order to promote the adoption of VoIP technology.

### Application

Telecommunications operators must transfer the calling party number and, in case of a redirected call, the redirecting number in the telephone network, if these are available. Both numbers are, however, not always available in incoming calls from PBXs or abroad.

When using ISUP-based signalling, transfer of subscription numbers over the telecommunications operator interface is determined in the ISUP standards [26-31]. In accordance with the ISUP standards, the parameter "calling party number" is used and the parameter "redirecting number" is used with regard to redirected calls.

The calling party number and, in the case of a redirected call, the redirecting number must be transferred in an international format at the Network to Network Interface, unless the signalling can indicate whether the format of the number is a national (significant) number or an international number.

In order to ensure the validity and unambiguousness of a number, telecommunications operators must agree on the other details of subscription number transfer. With regard to the SIP protocol, this matter is discussed in more detail below in section 10.2.

## 10.2 Recommendation for transfer of subscription number in SIP protocol

With regard to VoIP interconnection, the transfer of subscription numbers, and by extension caller identities, is not unambiguously determined in the standards. Practices are starting to form, but they have not been standardised yet. Therefore, FICORA has deemed it necessary to provide the following recommendations, the purpose of which is to provide telecommunications operators a default value that should be followed, unless expressly otherwise agreed by telecommunications operators.

For instance, the SIP protocol together with its extensions determine several fields in which information on callers or call transferers can be transferred. The calling party number can be displayed in the From, P-Asserted-Identity and Remote-Party-ID header fields, for instance. With regards to this, however, a practice of transferring caller identities between telecommunications operators using the P-Asserted-Identity (PAId) field is becoming standard. FICORA recommends the transfer of calling party numbers in the PAId field in the SIP Network to Network Interface [43, 44].

With regard to redirecting numbers, the prevailing practice has been to transfer the number in the Diversion header field. IETF has determined another solution that is based on the History-Info field [45]. Thus, the transfer method for redirecting numbers has not yet been standardised. Telecommunications operators should therefore agree on a method to be applied. Adaptation between these to header fields is discussed in the document RFC 6044 [46].

Subscription numbers can either be transferred in the TEL URI [47] or SIP URI [36] format. FICORA recommends calling party and redirecting numbers to be transferred in the SIP URI format in the SIP Network to Network Interface, in accordance with the following example:  
(sip:+358969661234@example.fi;user=phone).

The domain part of SIP-URI must be unambiguous.

In the SIP Network to Network Interface, called party numbers can be transferred either in the SIP URI format or routing number format, using the Request-URI field. The routing number is transferred in the TEL URI format or the aforementioned SIP URI format using the npdi and rn parameters [48].

In the Network to Network Interface, the number identification barring is indicated by means of an ID parameter in the Privacy header field [49]. With regard to interconnection performed using the SIP protocol, the B-end operator is responsible for removing the PAId field. The call originating network operator is responsible for the anonymisation of any other fields possibly requiring modification. Many of these fields should already be anonymised in the caller terminal.

## 10.3 Changing a subscription number

*Under the regulation, the calling party number and the redirecting number must not, in principle, be changed when being transferred via the communications network.*

### Explanations

Validity of the calling party number and the redirecting number requires that the number must not be changed when being transferred via the communications network in signalling, excluding separately determined situations.

### Application

As a rule, the content of the calling party number field and redirecting number field is not changed with regard to network components in signalling. Exceptions include transfer of the calling party number to the customer subscription, in which case it can be altered in accordance with section 10, as well as various intelligent network solutions, including number portability, in which the directory number serves as the subscriber identifier, instead of the actual routing number that identifies the technical subscription. In some cases of adaptation, a number format conversion between international and national significant numbers can be performed in the network. Moreover, the calling party number can be changed to another number controlled by the telecommunications op-

erator in question and agreed with the customer in various types of number changing services and, for instance, the multi-SIM service.

## **11 SECTION 9: VALIDITY OF SUBSCRIPTION NUMBER**

### **11.1 Ensuring validity of number**

*Under the regulation, the telecommunications operator of the call originating network must ensure that the calling party number it transfers in call origination and in case of a redirected call, the re-directing number, is valid and unambiguous.*

Insofar as corporate subscriptions are concerned, this obligation is further specified in the section's subsection 2 as follows: *If the telecommunications operator of the call originating network uses in call origination a calling party number it has received from a corporate customer interface, and that number does not belong to the operator's number space, the telecommunications operator must ensure with the corporate customer or the telecommunications operator who administers the number that the number can unambiguously be associated with a certain subscription of the corporate customer in question. However, even in this case, the telecommunications operator must ensure the reliability of charging.*

#### Explanations

Due to the numerous applications of the calling party number and in case of a redirected call, the redirecting number, it is reasonable to require the number that is transferred over the telecommunications operator interface to be valid and unambiguous. In some cases, the valid number associated with charging and with call-back is different. In these cases, as a rule, the valid number with regard to charging should be transferred.

Telecommunications operators must ensure the validity of numbers received from the User to Network Interface. However, verification can be difficult with regard to corporate subscriptions. In this context, corporate subscription refers to a subscription used for connecting internal IP networks, PBX networks and similar to the public communications network.

Multinational companies, in particular, have transnational VoIP networks in which they wish to route calls to the public telephone network via a corporate subscription in the target country's public telephone network. Their goal may be, for instance, to save on international call costs, while also enabling call-back directly to the mobile phone instead of the PBX. Calls made from international numbers and domestic mobile phone numbers connected to a PBX may be directed from the corporate subscription to the public telephone network.

Regularly blocking number display or altering the calling party number into the PBX's call number would, however, contradict the user's interests, so the regulation adopts the supposition that a telecommunications operator may use a calling party number it has received from a corporate subscription in an unchanged form as a calling party number, if this number can be unambiguously connected to a certain subscription in that corporation/organisation. The telecommunications operator's various options for verifying the reliability of charging are discussed in the application instructions.

#### Application

A telecommunications operator receiving a number from another telecommunications operator cannot verify the validity of that number. Therefore, in practice the regulation requires for a telecommunications operator controlling a subscription to set the calling party number or redirecting number to signalling, while also being responsible for the validity of the number, in the case of calls and messages from the subscription. The telecommunications operator controlling the redirecting number is responsible for the validity of the redirecting number.

If the telecommunications operator uses in call origination a calling party number it has received from a corporate customer interface, and that number does not belong to the operator's number space, the telecommunications operator must ensure with the corporate customer or the telecommunications operator who controls the number that the number can unambiguously be associated with a certain subscription of the corporate customer in question.

If the telecommunications operator cannot guarantee the validity of the redirecting number received from a corporate subscription, it must regardless employ other methods to ensure that a calling party number that cannot potentially be billed or is otherwise erroneous does not endanger the reliability of charging. Telecommunications operators may ensure the reliability of charging by, for instance:

- Indicating the calling party number's display is blocked.
- Replacing the calling party number with the identifying number of the corporate subscription in question (switch call number in the case of PBXs).
- Indicating that the call is redirected and indicating the identifying number of the corporate subscription in question as the redirection number (switch call number in the case of PBXs).
- By indicating call payer in some other manner (e.g. using the P-Charge-Info field determined in the SIP protocol [50]).

The preceding versions of the regulation up to 28 G separately discussed an event in which a telecommunications terminal is connected to more than one telecommunications operators' communications network subscriptions (parallel use of call number). Previously, telecommunications operators were obliged to agree with one another whether numbers included in the other telecommunications operator's number space were used as calling party numbers. If a telecommunications operator can verify, in the aforementioned manner, that calling party numbers received from corporate subscriptions have been allocated to that corporation's numbers by a telecommunications operator, the telecommunications operator will no longer be required to agree on the use of these numbers with the telecommunications operator controlling the numbers.

In the case of calls redirected by a PBX, the PBX should transfer both the original calling party number and the switch number as the redirecting number. In the event the PBX is not able to transfer both numbers, it should only transfer the switch number. If, however, the PBX is able to signal that the call is being redirected, it can transfer the original calling party number as well.

### **11.2 Procedures when receiving erroneous numbers**

*Under the regulation, if the calling party numbers received by the telecommunications operator are regularly erroneous, the telecommunications operator must set, in call origination, the presentation of the calling party number restricted in the outgoing signalling irrespective of the default setting received by the exchange. In similar situations concerning text message and multimedia message services, the telecommunications operator of the call originating network must change the calling party number into a number to which calls cannot be returned and reply messages cannot be sent.*

#### Explanations

Due to the numerous applications of the calling party number and, in the case of a redirected call, the redirecting number, it is reasonable to require the number that is transferred over the telecommunications operator interface to be valid and unambiguous. If the number is regularly erroneous, the information indicating this must be transferred in signalling.

#### Application

The telecommunications operator sets the calling party number presentation restricted in signalling. If the telecommunications operator receives erroneous numbers from a shared PBX, the telecommunications operator may need to block the call attempt instead of simply indicating the calling party number representation restricted.

In some cases of calls received from abroad it has been observed that the received calling party numbers are regularly erroneous. As a rule, in these cases the national operator should resolve the matter in cooperation with the international operator, ensuring the validity of the received calling party numbers. If the operators are unable to resolve the matter, the only way to prevent erroneous numbers from reaching subscribers is to indicate their presentation as restricted.

If number presentation is set as restricted, the calling party number is transferred in telecommunications operator networks, but the number is not transferred over the User to Network Interface.

The only exception to this rule is the authorities receiving emergency calls; calling party numbers are transferred to them despite the value of the restriction indicator.

Number presentation cannot be indicated as restricted in text message and multimedia message services, so the telecommunications operator must change the calling party number into a number to which calls cannot be returned and reply messages cannot be sent.

## **12 SECTION 10: TRANSFER OF CALLING PARTY NUMBER IN USER TO NETWORK INTERFACE**

### **12.1 Transfer of calling party numbers in a format enabling callback**

Under the regulation, *in call services, calling party numbers must be transferred to the called party in a format enabling callback.*

#### Explanations

The basic idea of the CLIP supplementary service (calling line identification presentation), provided for called parties is for the called party being able to directly see the number in a manner enabling callback.

#### Application

The number transferred in the User to Network Interface may be different, depending on the call type and network. It may be possible to transfer the calling party number in the national or international format, with either the 00 or + prefix used for indicating the international format. In a SIP-based network it may be possible to transfer even name-format SIP addresses, provided that they enable callback or a response message to be sent.

There are therefore various options, and their usefulness is largely dependent on the used network solution and terminals' ability to handle addresses in various formats. Due to this, telecommunications operators have been given the opportunity to decide on the specific calling party transfer format, as long as this requirement is fulfilled.

### **12.2 Procedures in the case of premium rate service numbers**

Under the regulation, *the presentation of calling party numbers for calls originating from premium rate numbers must be indicated as restricted in the outgoing signalling of the originating network if the calling party number is a premium rate number belonging to the service groups II to IV.*

#### Explanations

In 2008, FICORA drafted the recommendation 313/2008 *Use of a premium rate service number as a calling party number* [51]. In the background were revealed cases in which premium rate numbers belonging to service groups II to IV were used as calling party numbers for advertising purposes. Customers had been called by means of, presumably, automatic calling systems in such a manner that the service numbers had been registered in the memory of the called party telephones. This was done to lure called parties to call back premium rate service numbers without them having ordered a service themselves. The aforementioned cases of misuse have not been seen with premium rate service numbers belonging to service group I.

Services, the nature of which would require the display of premium rate service numbers to called parties, do not exist in service groups II to IV. As a consequence, altering the previous recommendation into a requirement of the regulation is appropriate.

Service number holders have considered it important that subscription numbers corresponding to service numbers are not revealed to users. Subscription numbers could be used to call service numbers without the service fee associated with the service number. Due to this, service providers should have the opportunity to decide whether to restrict the presentation when using a subscription number.

### Application

In the case of calls originating from premium rate service numbers in service groups II to IV, the source end telecommunications operator may set either the subscription number or service number of the subscription in question as the calling party number. In the case of service numbers, the number presentation is always indicated as restricted in the case of subscription numbers, the number presentation is indicated as restricted when the service provider so wishes.

This regulation repeals FICORA's 2008 recommendation 313/2008, Use of a premium rate service number as a calling party number [51].

## **13 OTHER RECOMMENDATIONS REGARDING THE IMPLEMENTATION OF SIP SERVICES**

This chapter provides some recommendations regarding the implementation and interoperability of SIP services that are not directly related to any specific section of the regulation.

### **13.1 Interoperability of fax services**

Even though fax use has seen a marked decrease in the face of the new reality of communications, the fax is still a necessary communication tool in various contexts. In order to ensure the functionality of this service, fax performance in the IP network must be ensured.

The implementation of fax services in subscriptions using VoIP technology has proven challenging. Problems have been posed by insufficient support for devices in the transfer pathway as well as insufficient testing of products, device performance, and various problems relating to compatibility. The detected problems have been discussed in more detail in the problem description, drafted by the SIP Forum's<sup>2</sup> FoIP working group [52].

The SIP Forum FoIP working group has determined solutions aimed at eliminating the observed problems. Rectification and improvement proposals have been published in at least the following standards, published by ITU-T between 2009 and 2010:

- T.38 [53]
- V.152 [54]
- V.153 [55]

### Recommendation

It is recommended that telecommunications operators providing fax services pay attention to fax service support, interoperability and performance with regard to their equipment and software acquisitions. Telecommunications operators are advised to utilise products conforming to the aforementioned latest standards, where the rectification of the observed problems has been attempted.

### **13.2 Connection of SIP PBXs to the public telephone network**

The interface for SIP-based PBXs has not yet been standardised, leading to challenges regarding the interconnection of these PBXs to the public telephone network. Telecommunications operators have been forced to test the PBXs in order to be able to identify the PBXs compatible with the provided service. Even if a PBX has been found to be compatible, some adaptations may have still been required. It would benefit both customers and telecommunications operators if a shared interface that everyone could try to support were being used.

SIP Forum published its first recommendation on the PBX interface (SIPconnect 1.0 Technical Recommendation) in January 2008. Since then, work has continued, resulting in the latest interface version, SIPconnect 1.1 [56].

SIP Forum has also started SIPconnect compatibility testing for PBXs, and a group of manufacturers has already tested and added support for their products. Further information on this subject can be found on the SIP Forum website<sup>3</sup>.

---

<sup>2</sup> <http://www.sipforum.org/>

<sup>3</sup> <http://www.sipforum.org/content/view/289/246/>

### Recommendation

It is recommended that telecommunications operators provide their customers with a Network to Network Interface conforming to the SIPconnect specifications for interconnecting SIP-based PBXs to the public telephone network.

#### **13.3 Anonymisation of SIP addresses in the call itemisation of a subscriber bill**

This paragraph presents FICORA's recommendation regarding the anonymisation of SIP addresses in the bill itemisation provided for subscribers. The following is decreed in section 24 of the Protection of Privacy in Electronic Communications (Call itemisation of a bill) regarding the itemisation provided to subscribers:

*In addition to the provisions on itemisation in telecommunications bills in section 80 of the Telecommunications Market Act, a telecommunications operator shall release the call itemisation of the bill if the subscriber so requests. Such an itemisation shall be provided in a form where the last three digits of the phone number are obscured or the itemisation otherwise rendered such that the other party of the communication cannot be identified.*

Additionally, the section includes two exceptions to this rule. First, a subscription-specific itemisation may not include the identification data of free-of-charge services. If calling, for instance, other SIP addresses in the same network is free of charge, the itemisation may not include the identification data of these connections.

Second, it is stated in subsection 4 of section 24 of the Act on the Protection of Privacy in Electronic Communications:

*Notwithstanding the provisions of subsection 2, a telecommunications operator shall release to the subscriber an itemisation by service type for calls for which the subscriber incurs charges beyond those related to the use of the communications service.*

At the time of this recommendation's drafting, such services are not being provided from a SIP address, so FICORA has not considered it necessary to provide a separate recommendation concerning the subject.

Since the last three digits of SIP addresses cannot be obscured, telecommunications operators must otherwise ensure that the other communication party cannot be identified on the basis of the itemisation. In FICORA's opinion, a safe alternative would be to only indicate the connection's time, duration, charge and SIP address in a completely anonymised form in the itemisation provided to the subscriber. This means that the itemisation indicates that a SIP address has been called, but the user component and domain component of the SIP URI are both anonymised. A good starting point would be to not reveal even the length or domain part of the address.

Furthermore, FICORA recommends that this practice is explained to the party requesting call itemisation in, for instance, the itemisation, since this type of practice probably represents something new and unfamiliar to that party.

#### **14 SECTION 11: ENTRY INTO FORCE AND TRANSITION PERIOD**

This regulation will enter into force on 1 April 2011 and will remain in force until further notice.

#### **15 REFERENCE LIST**

[1] Communications Market Act (393/2003 with amendments, CMA), latest version: <http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>

[2] The Act on the Protection of Privacy in Electronic Communications (516/2004 with amendments), latest version: <http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>

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) of 7 March 2002,

<http://eur-lex.europa.eu/>

Directive 2002/20/EC of the European Parliament and of the Council on the authorisation of electronic communications networks and services (Authorisation Directive) of 7 March 2002,

<http://eur-lex.europa.eu/>

[5] Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) of 7 March 2002, <http://eur-lex.europa.eu/>

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) of 7 March 2002,

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) of 7 March 2002, <http://eur-lex.europa.eu/>

[8] Directive 2009/136/EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (amendment of the Universal Service Directive and Directive on Privacy and Electronic Communications) of 25 November 2009, <http://eur-lex.europa.eu/>

[9] Directive 2009/140/EC of the European Parliament and of the amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. (amendment of Framework, Access and Authorisation Directives), 25 November 2009, <http://eur-lex.europa.eu/>

[10] FICORA regulation 11 A/2008 M on information security and functionality of e-mail services, latest version: <http://www.ficora.fi/en/index/saadokset/maaraykset.html>

[11] FICORA regulation 13 A/2008 M on information security and functionality of Internet access services, <http://www.ficora.fi/en/index/saadokset/maaraykset.html>

[12] FICORA regulation 35 O/2010 M on barring categories in telecommunications, latest version: <http://www.ficora.fi/en/index/saadokset/maaraykset.html>

[13] FICORA regulation 41 D/2009 M on technical documentation of communications networks and services, latest version: <http://www.ficora.fi/en/index/saadokset/maaraykset.html>

[14] IETF RFC 5390 Requirements for Management of Overload in the Session Initiation Protocol, <http://datatracker.ietf.org/doc/rfc5390/>

[15] IETF SPEERMINT ID Security Threats and Suggested Countermeasures, <https://datatracker.ietf.org/doc/draft-ietf-speermint-voipthreats/>

[16] IETF, RFC 5853, Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments <http://datatracker.ietf.org/doc/rfc5853/>

[17] IEEE Standards Association, IEEE Std. 802.1ah - Provider Backbone Bridges, <http://www.ieee802.org/1/>

[18] FICORA, working group report 3/2010, Ethernet-pohjaiset vuokratuotteet, 20 December 2010, <http://www.ficora.fi/attachments/suomiry/5v7CD6Ac1/TRaportti032010.pdf>

- [19] FICORA, working group report 1/2010, Open Access -pilotin loppuraportti, 16 March 2010, <http://www.ficora.fi/attachments/suomiry/5oIN5b87E/TRaportti012010.pdf>
- [20] FICORA, working group report 3/2006, Operaattorien väliset toimintatavat laajakaistaprosesseissa, 7 March 2008, <http://www.ficora.fi/attachments/suomiry/1158858935467/TRaportti052005.pdf>
- [21] IETF RFC 2827 (BCP 38) Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, <http://datatracker.ietf.org/doc/rfc2827/>
- [22] IETF RFC 3704 (BCP 84) Ingress Filtering for Multihomed Networks, <http://datatracker.ietf.org/doc/rfc3704/>
- [23] RIPE NCC, RIPE Database Update Reference Manual, <http://www.ripe.net/db/support/update-reference-manual.pdf>
- [24] RIPE NCC, RIPE IRT Object- Technical HOW TO, <http://www.ripe.net/db/support/security/irt/irt-h2.html>
- [25] RIPE NCC, IRT Object FAQ, <http://www.ripe.net/db/support/security/irt/faq.html>
- [26] Finnish Standards Association SFS, SFS 5779 Signalling in the public switched network. ISDN User Part ISUP Version 2 of the national Signalling System No.7. Application of ITU-T recommendations Q.761-Q.764 and Q.766 in Finland 2nd edition 1996, <http://sales.sfs.fi/>
- [27] Finnish Standards Association SFS, SFS 5778 Signalling in the public switched network. ISDN User Part ISUP Version 2 of the national Signalling System No.7. Supplementary services. 2. 2nd edition 1997, <http://sales.sfs.fi/>
- [28] Finnish Standards Association SFS, SFS 5869 Signalling in the public switched network. ISDN User Part ISUP Version 3 of the national Signalling System No.7. Application of ITU-T recommendations Q.730 and Q.761-Q.766 in Finland. 2<sup>nd</sup> edition 2001, <http://sales.sfs.fi/>
- [29] Finnish Standards Association SFS, SFS 5868 Signalling in the public switched network. ISDN User Part ISUP Version 3 of the national Signalling System No.7. Supplementary services. 1999, <http://sales.sfs.fi/>
- [30] Finnish Standards Association SFS, SFS 5901 Signalling in the public switched network. ISDN User Part ISUP Version 4 of the national Signalling System No.7. Application of ITU-T recommendations Q.730 and Q.761-Q.766 in Finland. 2002, <http://sales.sfs.fi/>
- [31] Finnish Standards Association SFS, SFS 5902 Signalling in the public switched network. ISDN User Part ISUP Version 4 of the national Signalling System No.7. Supplementary services. 2002, <http://sales.sfs.fi/>
- [32] FICORA, working group report 5/2004 Puhelinnumeron siirrettävyys, kiinteä puhelinverkko, tekninen verkkototeutus, 8 December 2008, <http://www.ficora.fi/index/saadokset/tyoryhmaraportit.html>
- [33] FICORA regulation 32 O/2010 M On numbering in a public telephone network, latest version: <http://www.ficora.fi/en/index/saadokset/maaraykset.html>
- [34] ITU-T recommendation Q.704 (07/1996): Switching and Signalling; Specifications of Signalling System No. 7 – Message transfer part: Signalling network functions and messages, <http://www.itu.int/ITU-T/index.html>
- [35] ITU-T recommendation Q.708 (03/1999): Switching and Signalling; Specifications of Signalling System No. 7 – Message transfer part: Assignment procedures for international signalling point codes, <http://www.itu.int/ITU-T/index.html>
- [36] IETF, RFC 3261 SIP: Session Initiation Protocol, <http://datatracker.ietf.org/doc/rfc3261/>

- [37] MAPEL, Basic Set of Norms for Providing Premium Electronic Services, <http://www.mapel.fi/normisto/>
- [38] Finnish Standards Association SFS, SFS 5876 Telecommunications network exchanges. Tones and ringing signals, 9.5.2000, <http://sales.sfs.fi/>
- [39] Finnish Standards Association SFS, SFS 5749 Signalling in the public switched network. Handling of cause information related to call failure, 20 August 2001, <http://sales.sfs.fi/>
- [40] FICORA, GFI 0301: Guidelines for Implementation; ISUP-SIP Interworking Profile C, latest version: <http://www.ficora.fi/en/index/saadokset/ohjeet/teletoiminta.html>
- [41] ITU-T recommendation Q.1912.5 (03/2004): Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part, <http://www.itu.int/ITU-T/index.html>
- [42] IETF RFC 3398 Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping, <http://datatracker.ietf.org/doc/rfc3398/>
- [43] IETF RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, <http://datatracker.ietf.org/doc/rfc3325/>
- [44] IETF RFC 876 Updates to Asserted Identity in the Session Initiation Protocol (SIP), <http://datatracker.ietf.org/doc/rfc5876/>
- [45] IETF RFC 4244 An Extension to the Session Initiation Protocol (SIP) for Request History Information, <http://datatracker.ietf.org/doc/rfc4244/>
- [46] IETF RFC 6044 Mapping and interworking of Diversion information Between Diversion and History-Info Headers in the Session Initiation Protocol (SIP), <http://datatracker.ietf.org/doc/rfc6044/>
- [47] IETF RFC 3966 The tel URI for Telephone Numbers, <http://datatracker.ietf.org/doc/rfc3966/>
- [48] RFC 4694 Number Portability Parameters for the "tel" URI, <http://datatracker.ietf.org/doc/rfc4694/>
- [49] IETF RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP), <http://datatracker.ietf.org/doc/rfc3323/>
- [50] IETF ID P-Charge-Info - A Private Header (P-Header) Extension to the Session Initiation Protocol (SIP), <https://datatracker.ietf.org/doc/draft-york-sipping-p-charge-info/>
- This regulation repeals FICORA's 2008 recommendation 313/2008 S, Lisämaksullisen palvelunumeron käyttö kutsuvan liittymän numerona, <http://www.ficora.fi/attachments/suomiry/5vHi1e9ec/Suositus3132008S.pdf>
- [52] SIP Forum, Fax Over IP Task Group Problem Statement – V1.0, 23 July 2009 [http://www.sipforum.org/component/option,com\\_docman/task,doc\\_download/gid,303/Itemid,261/](http://www.sipforum.org/component/option,com_docman/task,doc_download/gid,303/Itemid,261/)
- [53] ITU-T recommendation T.38 (09/10): Procedures for real-time Group 3 facsimile communication over IP networks, <http://www.itu.int/ITU-T/index.html>
- [54] ITU-T recommendation V.152 (09/10): Procedures for supporting voice-band data over IP networks, <http://www.itu.int/ITU-T/index.html>
- [55] ITU-T recommendation V.153 (12/09): Interworking between T.38 and V.152 using IP peering for realtime facsimile services, <http://www.itu.int/ITU-T/index.html>
- [56] SIP Forum, SIPconnect 1.1 (draft version), [http://www.sipforum.org/component/option,com\\_docman/task,cat\\_view/gid,84/Itemid,75/](http://www.sipforum.org/component/option,com_docman/task,cat_view/gid,84/Itemid,75/)

**16 LIST OF ACRONYMS**

AS	Autonomous System
ASCII	American Standard Code for Information Interchange
BCP	Best Current Practice
BPDU	Bridge Protocol Data Unit
CDP	Cisco Discovery Protocol
CLIP	Calling Line Identification Presentation
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTMF	Dual-tone multi-frequency
E.164	ITU standard for national and international telephone numbers
EU	European Union
FICIX	Finnish Communication and Internet Exchange
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
L2	OSI model Layer 2 (Data link)
MAC	Media Access Control
REA	Regulation explanations and application
MSA	Mail Submission Agent
MTP	Message Transfer Part
NTP	Network Time Protocol
PE	Provider Edge
PI	Provider Independent
SO	Service operator
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RFC	Request for Comments
RIPE	Réseaux IP Européens
SBC	Session Border Controller
SFS	Finnish Standards Association
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
PPEC	Act on the Protection of Privacy in Electronic Communications
URI	Uniform Resource Identifier
VLAN	Virtual Local Area Network
CMA	Communications Market Act
NO	Network operator
VoIP	Voice over IP
VTP	VLAN Trunk Protocol