TRAFICOM
Finnish Transport and Communications Agency

RECOMMENDATION TO TELECOMMUNICATIONS OPERATORS ON DETECTING AND PREVENTING CALLER ID SPOOFING

Traficom Publications

5/2022

Contents

1 Introduction

The spoofing of calling party numbers in international calls terminating in Finland has become a major problem. This global phenomenon became more common in Finland in 2020, and in 2021 the volumes of spoofed calls and their share of the total volume of international call termination increased significantly.

Caller ID spoofing or spoofing a calling party number means disguising the number where the call originates as a Finnish number. This technique is widely used by criminals to increase the likelihood of victims answering international scam calls. The following are examples of commonly used fraud schemes:

- technical support scams
- customer support calls from banks
- investment scams
- business service scams (e.g. callers 'selling' a company's own domain name back to the company by threatening to make it available for the company's competitors).

The Finnish National Bureau of Investigation has reported receiving numerous reports about scam calls like the above in 2020 and 2021. In the cases reported, caller ID spoofing to disguise the calling party number as a Finnish one has been a key element of the scam. The method is commonly used in other countries as well, and it is part of highly organised international crime.

This Recommendation issued by the Finnish Transport and Communications Agency Traficom presents models for analysis and action to detect the following basic cases of caller ID spoofing:

- in international call termination, calls in which the calling party number does not belong to the active Finnish numbering space
- in international call termination, calls in which the calling party number is fraudulently presented as a number belonging to the Finnish numbering space allocated to telecommunications areas in fixed telephone networks or to the numbering space allocated to nationwide subscriber or service numbers
- in international call termination, calls in which the calling party number is fraudulently presented as a number belonging to the numbering space allocated to Finnish mobile networks (mobile number)
- in international call termination, calls in which the field for the calling party number is empty or the calling line identity (CLI) in the field does not comply with the syntax.

When caller ID spoofing has been detected, the call attempt should be addressed by taking the measures specified in this Recommendation.

The models for analysis and action presented in this Recommendation to enable the detection of basic cases of caller ID spoofing only apply to Finnish telephone numbers and Finnish telephone subscriptions. Foreign mobile network subscriber connections roaming in Finnish mobile networks are excluded from the scope of this Recommendation.

This Recommendation has been prepared in cooperation with telecommunications operators in a Traficom working group.

In addition to telecommunications operators, the measures presented in this Recommendation may also be applied by other communications providers.

2 Use of Finnish numbers in international call termination

This chapter discusses the recommended action regarding calls that are terminated via an interconnection interface for international traffic (international interface) and where the calling party number is a Finnish telephone number other than a mobile number referred to in Chapter 3. Such other numbers include, for example, subscriber numbers within telecommunications areas, nationwide subscriber and service numbers and numbers included in the reserve of numbers.

This chapter also presents a model for a safe way of using Finnish telephone numbers as calling party numbers from abroad.

Implementing the recommended action will affect the parallel use of numbers in several networks. Telecommunications operators should take these effects into account and provide their customers with relevant instructions.

2.1 Blocking the use of Finnish numbers in international call termination

At present, when calls are terminated in Finland via the interconnection interface for international traffic, the receiving telecommunications operator has practically no way of identifying the caller or knowing whether the caller has the right to use the calling party number indicated.

In the working group's view, it would be justified to prohibit the use of Finnish telephone numbers as calling party numbers abroad. This should be done by way of a regulation issued by Traficom. This would allow numbers to be unambiguously considered spoofed when calls from these numbers are received via the interconnection interface for international traffic.

Traficom recommends that telecommunications operators block calls terminating from the international interface when the calling party number is a Finnish telephone number other than a mobile network subscriber number (mobile number) referred to in Chapter 3. Mobile numbers are subject to the rules specified in Chapter 3.

The procedure described here also applies to **the termination of forwarded calls from the international interface when the calling party number is a Finnish telephone number**. **Traficom recommends that telecommunications operators:**

- activate **calling line identification restriction** for **calls forwarded from an international telephone number**
- **block** calls **forwarded from a Finnish telephone number**. However, calls **may be forwarded** when the forwarding number is a Finnish mobile number that has been **successfully validated in accordance with Chapter 3**.

This Recommendation does not apply to calls in which the called party number is a Finnish mobile station roaming number (MSRN). Mobile station roaming number refers to an identification number that a Finnish mobile operator gives to a customer with an international subscription roaming in Finland. When the called party number is a mobile station roaming number given by a Finnish

mobile operator, the calling party number is not validated. Instead, the call is directed directly to the destination network.

The following MSRN number spaces are currently in use:

- 04099, 0457011, 0457601, 0457605, 0508710, 0508711, 0508712, 0508713, 0508761 and 050879

This Recommendation does not apply to VoLTE roaming (S8HR) calls, because in these calls telecommunications operators can identify users and verify their right to use numbers.

Call blocking measures are discussed in more detail in Chapter 4.

2.2 Direct customers are considered national traffic

In accordance with the FICORA Regulation 28 on the interoperability of communications networks and services, the telecommunications operator of the call originating network is responsible for ensuring that the numbers in call origination are valid and unambiguous. This is an important obligation because only the operator of the originating network can ensure that the number used by its customer is valid.

In this context, it is irrelevant whether the customer is physically located in Finland or abroad. The originating telecommunications operator can identify the customer and validate the number in both cases. Therefore, in this regard, there is no need to apply the prohibition on using Finnish telephone numbers abroad, as referred to in Chapter 2.1. These cases are considered national traffic.

Thus, for example, corporate switchboards and call centres may be physically located abroad and still use Finnish telephone numbers as long as the traffic is directed to Finland via a dedicated traffic route so that a customer or telecommunications operator using Finnish numbers can be identified and the telecommunications operator of the originating network can comply with Regulation 28.

3 Use of mobile numbers in international call termination

Finnish mobile network customers and their subscriptions cannot be immediately identified at the interface for international call termination.

This chapter discusses models for analysis and action recommended for international call termination when the calling party number is a Finnish mobile number. Two possible implementation methods are presented.

In this Recommendation, mobile numbers refer to:

- Finnish mobile network subscriber numbers (currently subscriber numbers beginning with 04 and 050)
- subscriber numbers beginning with 0299.

By way of derogation from the above, a calling line identification restriction is imposed on the number range 0435.

General rules concerning the use of Finnish numbers abroad are specified in Chapter 2 of this Recommendation.

3.1 Validation of incoming calls between telecommunications operators

When a telecommunications operator receives from the international interface calls in which the calling party number is a Finnish mobile number, the operator should ensure that:

- the number belongs to a customer of a telecommunications operator with telecommunications operations in Finland; and
- the customer in question is abroad and can therefore be assumed to be making the call in question.

The transfer, analysis and decision-making models recommended for this validation are illustrated in Figure 1.

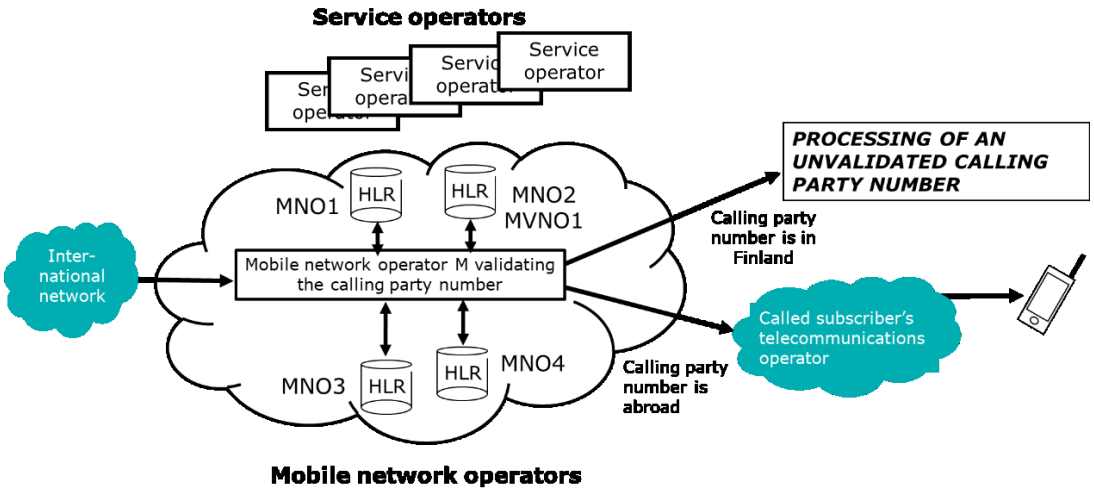

Figure 1. Validation of Finnish mobile numbers in international call termination

The telecommunications operator receiving a call at the international interface is responsible for ensuring that the number is valid and that the call is connected forward only after successful validation.

1) The receiving telecommunications operator terminating international calls in which the calling party number is a Finnish mobile number performs a number portability query concerning the calling party number.

2) If the query in step 1 is successful, the telecommunications operator checks where the calling subscriber is located at the time.

3) Based on the above checks, the telecommunications operator decides whether the call can be connected to the called subscriber. If the checks are successful and the calling subscriber is abroad, the call can, as a rule, be connected to the called subscriber without other measures. In other cases, the call must undergo the measures specified in Chapter 4.

Notwithstanding the above, the receiving telecommunications operator terminating international calls may also subcontract these measures to another telecommunications operator. The receiving telecommunications operator may agree with another telecommunications operator that the other operator performs the above-mentioned number portability query and checks the current location of the Finnish mobile subscription. In such a case, the receiving telecommunications operator is itself responsible for further measures. Alternatively, the receiving telecommunications operator may make an arrangement where it directs the call

to another telecommunications operator that takes all the measures described above.

If the telecommunications operator cannot perform the validation, it must take the measures required when a validation fails. These are discussed in Chapter 4.

3.2 Validation of incoming calls using a proxy server

Incoming calls can be validated by using a 'proxy server model' in which a proxy server relays the validation requests and responses. In this case, the telecommunications operator receiving calls at the international interface sends validation requests to the proxy server for those calls where the calling party number is a Finnish mobile number.

1) Information on the calling party number is sent to the proxy server. The telecommunications operator sending the request does not need to know the mobile network operator or service operator whose customer the subscriber is.

2) The proxy server forwards the request to the correct mobile network operator that responds to the request by sending the subscriber's current roaming status to the proxy server.

3) The proxy server forwards the response to the telecommunications operator that made the original request. Based on the information contained in the response, the operator decides whether it can connect the call to the called subscriber.

Traficom recommends that telecommunications operators establish a proxy server because when operators use a proxy server, there is no need to open mobile network signalling interfaces between different telecommunications operators or send customers' status details between different telecommunications operators. A proxy server also makes it possible to provide a query interface that is network technology neutral.

Being technology neutral means that a proxy server can carry out protocol conversions without the query interface being tied to a specific technology used in mobile networks and can provide different alternatives for sending both requests and responses (e.g. MAP (ATI), SIP, HTTPS, RADIUS and DIAMETER).

Traficom recommends logging proxy server transactions. Traficom also recommends compiling statistics on the logs in accordance with Chapter 4.3.

4 Further processing of call attempts

This Chapters gives recommendations on the further processing of call attempts. If it is uncertain whether the caller's number is valid, the main rule is call blocking, which is discussed in Chapter 4.1. As an exception to the main rule, calling line identification of a Finnish calling party number is restricted when forwarded calls are terminated from the international interface if the forwarding number is an international telephone number.

4.1 Call blocking

This chapter concerns call termination situations in which a telecommunications operator blocks incoming calls from the international interface in accordance with Chapter 2 or the validation of the calling subscriber's number at the international interface has failed and the number has been determined spoofed.

Traficom recommends that such calls may not be directed to the called subscriber. The telecommunications operator can, for example:

1) release the call or
2) direct the call attempt to an indication device that transmits ringing tone on the voice channel.

4.2 Voice termination rate

Commission Delegated Regulation (EU) 2021/654 [1] determines maximum termination rates. However, according to recital 15 "*operators would not be bound to apply Union-wide termination rates to termination of calls if the CLI is missing, invalid or fraudulent*".

This allows telecommunications operators to apply termination rates of their choice to calls in which the calling party number is missing, invalid or fraudulent. However, as noted in Chapter 4.1 above, this Recommendation recommends blocking calls from fraudulent calling party numbers. Telecommunications operators may use pricing as a tool to address other cases, such as calls in which the calling party number is missing or invalid.

4.3 Statistics

Traficom recommends that telecommunications operators compile statistics on call attempts and the related further processing measures taken when the calling subscriber's number of a terminating call cannot be validated at the international interface. This will enable the monitoring of the effectiveness and proportionality of the measures.

Traficom recommends that telecommunications operators compile monthly statistics on the following information regarding the use of Finnish calling party numbers at the international interface:

- the number of blocked calls indicated separately for the following categories: mobile numbers and other numbers
- for forwarded calls in accordance with Chapter 2.1, the number of calls in which calling line identification restriction is activated because the forwarding number is an international telephone number
- the total number of calls
- the number of calls from mobile numbers that have passed validation.

Traficom will ask for these statistics as part of its measures to supervise compliance with obligations and for their possible further development.

5 Legislation and regulations

5.1 Telecommunications operators' obligation to ensure the validity of calling party numbers

According to FICORA Regulation 28, 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 forwarded (redirected) call, the forwarding number is valid and unambiguous.

According to the Regulation, if the calling party numbers received by the telecommunications operator are regularly incorrect, 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 such a number to which calls cannot be returned and reply messages cannot be sent.

Under the Regulation, the telecommunications operator of the call originating network is responsible for validating the right to use a number, but all telecommunications operators must take action if the calling party numbers they receive are regularly incorrect.

5.2 Processing traffic data to verify the validity of numbers and to validate numbers

In call termination, verifying that numbers are valid and validating mobile numbers require the processing of traffic data. The processing of traffic data is governed by the Act on Electronic Communications Services (917/2014).

According to section 138, subsection 1 of the Act, messages and traffic data may only be processed to the extent necessary for the conveyance of communications, performance of the agreed service, and for the purpose of ensuring information security as provided in section 272.

When mobile numbers are validated, traffic data is processed by the telecommunications operator initiating the validation ('validating operator') and the telecommunications operator of the alleged calling party number ('assisting operator'), if the subscriber is not the validating operator's own customer. Validating a mobile number requires the disclosure of traffic data to the assisting operator.

According to section 272, subsection 1 of the Act on Electronic Communications Services, a communications provider has the right to undertake necessary measures referred to in subsection 2 of the same section to ensure information security in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services and information systems.

The processing of traffic data is justified if it is necessary to ensure information security, such as communications security, in a communications network. The concept of information security covers, for example, ensuring the integrity of data, monitoring the origin of telecommunications traffic (government proposals HE 221/2013 vp, p. 91 and HE 125/2003 vp, p. 48) and having sufficient authentication procedures.

Pursuant to section 137, subsection 1 of the Act on Electronic Communications Services, processing electronic communications and traffic data is only allowed to the extent necessary for the purpose of such processing, and must not limit the confidentiality of communications or the protection of privacy any more than is necessary. In other words, traffic data should never be processed if it is possible to achieve the objective of processing in any other way that is less intrusive of the confidentiality of communications. Moreover, processing may not be disproportionate to the objective. The processing of traffic data for validation purposes is justified if there is no other way reasonably available to prevent calls with spoofed calling line identity.

Firstly, Traficom is of the view that, in order to ensure the information security of a communications network, the validating operator can be considered to have a ground to verify that the origin of a call terminating on its network

corresponds to the calling party number associated with the call so that the number is not spoofed.

Secondly, the disclosure of traffic data between telecommunications operators makes it possible to validate Finnish mobile numbers. Such a reciprocal process between the participating mobile network operators can be considered necessary to enable each operator to ensure the information security of its communications network with regard to the origin of international calls terminating on the network.[1] The disclosure of traffic data by the assisting operator may also be considered necessary for the operator to ensure the information security of its own service: to prevent foreign parties from posing as its subscribers, to prevent the misuse of its numbering space and to ensure that its customers do not receive incorrect call-backs or face other consequences because of number spoofing.

Telecommunications operators must ensure that the processing of traffic date does not limit the protection of subscribers' and users' privacy any more than is necessary to ensure information security. The processing must be proportionate to the severity of the information security threat being prevented, and it must be impossible to achieve the objective in some other way that is less intrusive of privacy. Because the processing of traffic data must be limited to what is absolutely necessary, telecommunications operators must introduce the measures reasonably available to them to limit the disclosed traffic data to the absolutely necessary. The proxy server model enables the disclosed traffic data to be processed so that it only includes the data that is strictly necessary to validate a mobile number. The validating operator must in any case destroy all unnecessary traffic data. Before the proxy server model is taken in use, mobile numbers may be validated if the benefits of validation are estimated to be materially greater than any adverse effect on the protection of users' privacy.

Implementing information security measures

Pursuant to section 272, subsection 2 of the Act on Electronic Communications Services, measures taken to implement information security may include the automatic prevention or limitation of the transmission or reception of communications. Based on this ground, a telecommunications operator may, for example, release a call if it is necessary to ensure information security.

Section 272, subsection 4 of the Act requires, among other things, that the telecommunications operator implements the measures with care and that they are commensurate with the seriousness of the disruption being combated. Such measures shall not limit freedom of speech, the confidentiality of communications or the protection of privacy any more than is necessary for the purpose of attaining the goals referred to in subsection 1 of the same section. The telecommunications operator must try to implement the measures so that wanted calls are not blocked, the data obtained in the validation process is not used for unlawful purposes and the procedure does not cause new, unmanageable information security risks for the telecommunications operator or users.

Purpose limitation of processing and destruction of traffic data

Pursuant to section 137, subsection 1 of the Act on Electronic Communications Services, processing electronic communications and traffic data is only allowed to the extent necessary for the purpose of such processing and must not limit the confidentiality of communications or the protection of privacy any more than is necessary. Under subsection 3, traffic data must, after processing, be destroyed or rendered such that it cannot be associated with the subscriber or user involved, unless otherwise provided by law.

[1] The preparatory material of the repealed Act on the Protection of Privacy in Electronic Communications noted that the implementation of information security measures may require cooperation between telecommunications operators (Government proposal to Parliament on the Act on the Protection of Privacy in Electronic Communications and on certain related acts, HE 125/2003 vp, p. 11). The disclosure of traffic data between different parties may be necessary in situations that concern several networks and require joint measures (government proposal HE 125/2003 vp, p. 62 as regards cases of misuse).

Once traffic data is no longer needed for ensuring the validity of or validating a number, the data must be destroyed or rendered anonymous. This does not prevent telecommunications operators from compiling statistics on call attempts and measures for their further processing as referred to in Chapter 4.3 above.

Informing users

Under section 138, subsection 2 of the Act on Electronic Communications Services, communications providers must inform subscribers or users about what traffic data is processed and how long the processing will last. Telecommunications operators must describe the validation process to the extent necessary, including possible disclosure of traffic data.

Processing of personal data

Traffic data constitutes personal data, and its processing is therefore also subject to the provisions of the General Data Protection Regulation [2] and the Data Protection Act (1050/2018) insofar as the Act on Electronic Communications Services does not contain any specific provisions on the matter. Telecommunications operators must ensure compliance with the above-mentioned legislation in addition to the Act on Electronic Communications Services.

6 References

[1] Commission Delegated Regulation (EU) 2021/654 of 18 December 2020 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council by setting a single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32021R0654

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Finnish Transport and Communications Agency Traficom

PO Box 320, FI-00059 TRAFICOM, Finland
tel. +358 29 534 5000

traficom.fi

ISBN 978-952-311-781-5
ISSN 2669-8757 (online)

TRAFICOM
Finnish Transport and Communications Agency