TRAFICOM
Finnish Transport and Communications Agency

Registrar's guide

Guidance and requirements for becoming a registrar

Finnish Transport and Communications Agency

Version history

Version	Date	Description/change	Author
1.0	25/10/2018	Version 1	Ari-Matti Husa
1.1.	21/12/2018	version 1.1	Ari-Matti Husa
1.2	6/9/2021	version 1.2	Sami Salmensuo

TRAFICOM
Finnish Transport and Communications Agency

Content

1 Registrar's tasks and obligations 5

1.1 Registrar's service obligations 5
1.1.1 Registration and renewal fees 5

1.2 Duty to advise customers 6
1.2.1 Minimum level of guidance 6

1.3 Correct and updated information 7
1.3.1 Updating contact details 8
1.3.2 Statutory address for service and other email addresses 8

1.4 Renewing domain names 9
1.4.1 Registrar's duties upon expiry of a domain name 9

1.5 Removing domain names from the register 9
1.5.1 Problems in removals from register 10

1.6 Transferring domain names to a new holder 10
1.6.1 Right to request domain name transfer 10
1.6.2 Domain name transfer time 11

1.7 Changing registrars 11
1.7.1 Registrar transfer key 12
1.7.2 Domain names without a registrar 12
1.7.3 If problems arise 12

1.8 Terminating registrar's operations 12
1.8.1 Notification of Traficom's prohibition decision 13
1.8.2 Closing of prepaid account 13

2 Information security in registrar's operations 13

2.1 Information security in practice 14
2.1.1 Areas of information security 15

2.2 Risk management 16

2.3 Information material 17
2.3.1 Classification and processing of the material 18
2.3.2 Information material documentation 18

2.4 Information security control 18
2.4.1 Identifying threats 19
2.4.2 Prevention of threats 19
2.4.3 Monitoring documentation 19

2.5 Management of threats and incidents 20
2.5.1 Purpose of procedural guidelines 20

2.6 Change management 20
2.6.1 Planning changes 20
2.6.2 Documenting changes 21

2.7 Data protection in domain name services 21

TRAFICOM
Finnish Transport and Communications Agency

2.7.1 Collection of personal data in domain name services 22
2.7.2 Purpose and nature of processing personal data 22
2.7.3 Registrar's obligations as a data processor 23
2.7.4 Domain name holder's rights 25
2.8 Obligation to notify information security incidents 25
2.8.1 Information security incidents must be reported immediately . 26
2.8.2 Significant violations of information security 26
2.9 Name servers 28
2.9.1 Name server configurations 29
2.9.2 Domain Name System Security Extensions (DNSSEC) 30
2.9.3 Name server test 32
2.10 Technical interfaces 32
2.10.1 Browser-based user interface 32
2.10.2 EPP interface 33
2.10.3 RFC standards 33
2.10.4 KATAKRI requirements in the use of EPP interface 33
2.10.5 EPP sandbox environment 34
2.10.6 Whois service for fi-domain names 35
2.10.7 Domain Availability Service (DAS) 35
2.10.8 OData 35
2.11 Registration as a registrar 36
2.11.1 Statutory address for service and other email addresses 36
2.11.2 Resellers' operations 36
2.12 PGP keys 37

Finnish Transport and Communications Agency

1 Registrar's tasks and obligations

1.1 Registrar's service obligations

Registrars assist and advise their customers in all issues related to fi-domain names. Registrars enter fi-domain names in the domain name register and perform any related changes requested by their customers.

Domain name holders contact their own registrar in all issues related to fi-domain names. Under the Act on Electronic Communications Services (ECSA), registrars are responsible for ensuring the holders' rights and providing them with sufficient information on fi-domain names and any changes in the registrars' operations.

At the request of their customers, registrars

- enter domain names in the domain name register maintained by the Transport and Communications Agency (Traficom)
- update related details
- renew domain names
- transfer domain names from one registrar to another
- transfer domain names from one holder to another
- remove domain names from the domain name register.

Registrars must also provide their customers with

- general guidance related to fi-domain names
- information in case the registrar has terminated its operations or Traficom has issued a prohibition decision concerning the registrar.

1.1.1 Registration and renewal fees

Registrars pay Traficom for registering and renewing their customers' domain names via the registrar's technical interface. Registration and renewal fees are based on the registration period:

- 1 year EUR 9
- 2 years EUR 18
- 3 years EUR 27
- 4 years EUR 36
- 5 years EUR 45

Fees related to the registration and renewal of domain names are charged to registrars' prepaid accounts. Registrars must make a deposit to the prepaid account in advance to have sufficient funds for the transactions. The fees paid by registrars are based on Decree 660/2016 of the Ministry of Transport and Communications.

Traficom does not refund any fees to registrars even if a registrar had accidentally registered a domain name incorrectly or Traficom removed a domain name from the register based on its decision.

1.2 Duty to advise customers

Before registering fi-domain names, registrars must provide guidance to their customers at least about the domain name's form, content and compliance with law.

Registrars must provide their customers with information on the requirements related to fi-domain names before registering a domain name. The guidance should be easy and detailed. This obligation is limited to providing information. Domain name holders bear the ultimate responsibility for ensuring that their domain name is lawful.

The information must be available for both existing and future domain name holders regardless of whether the customers already have a contract with the registrar or not.

Registrars must actively contribute to ensuring that domain name registrations comply with law. Customers should be particularly aware of requirements concerning protected names and trademarks already before they register a domain name. The purpose of the duty to give advice is to avoid incorrect and illegal domain name registrations, which may even lead to the domain name being cancelled.

1.2.1 Minimum level of guidance

Registrars may choose themselves how they will fulfil the duty to give advice, but in terms of content, registrars must provide their customers information on at least the following issues related to the content and form of the domain name:

What is a protected name or trademark?

- Under the ECSA, protected names and trademarks include:
- names or trademarks that have been entered into the trade register or into the registers of trademarks, associations, foundations, or political parties in Finland
- names of public bodies, unincorporated state enterprises, independent public corporations, public associations, or diplomatic missions of a foreign state or their bodies
- established names, secondary marks or trademarks referred to in the Business Names Act or Trademarks Act
- EU trademarks entered into the EUIPO trademark register.

How can domain name holders check whether a name or trademark is protected?

Registrars must provide their customers with links to public registers of the Finnish Patent and Registration Office (business information system, register of associations, register of trademarks) and the EU trademark register of the European Union Intellectual Property Office (EUIPO).

What does a lawful domain name mean?

At the time of registration, a domain name must not be:

- based on a protected name or trademark owned by another party, unless the domain name holder can present a good, acceptable reason for registering the domain name
- similar to a protected name or trademark owned by another party, if the clear intent of registering the domain name is to benefit from it or to cause damage.

Allowed characters in a domain name

Registrars must advise their customers on characters allowed in a domain name, which are the letters from a to z and the numbers from 0 to 9. In addition, allowed characters include native language characters å, ä and ö as well as characters in the Saami languages spoken in Finland and the hyphen-minus.

In marketing and registering domain names, registrars must pay attention to the restrictions concerning domain names containing native language characters. Customers applying for a domain name or planning to do so must be aware of the technical restrictions related to domain names containing native language characters.

In particular, customers may have to apply for a domain name containing native language characters and an equivalent domain name without native language characters, for example ääkkönen.fi and aakkonen.fi.

Punycode, also called ACE (ASCII Compatible Encoding), enables the use of characters outside the Latin alphabet. The domain name system can read a domain name consisting of native language characters, if it is technically defined as an ACE string.

For example, the ACE string of ääkkönen.fi is xn--kknen-fraa=0m.fi.

Several websites, including Traficom, provide IDN conversion tools.

1.3 Correct and updated information

Registrars must ensure that their customers' details in the fi-domain name register are up to date at the time of registration and later on if the details change.

An fi-domain name must always be registered in the name of its actual holder. For example, it is not allowed to register a customer's fi-domain

name in the registrar's name. If Traficom needs to investigate any unclear issues or settle disputes related to fi-domain names, the rights of the party registered as the domain name holder are compared to the rights of other parties.

It is very important for the legal protection of the customers that the holder entry is accurate and the domain name has been registered to the correct party.

The information in the domain name register must remain correct and up to date also after the registration. If customers request registrars to modify their domain name, registrars are obliged to:

- update domain name holders' contact details
- remove domain names from the register
- transfer domain names from one holder to another
- transfer domain names from one registrar to another
- renew domain names.

1.3.1 Updating contact details

Registrars must keep the contact details of their customers up to date. Registrars must update contact details at the request of their customers and also in other cases, if necessary.

Registrars are responsible for making sure that the notified details are correct and they are kept up to date. If a domain name holder (customer) suffers damage due to a registrar's negligence, the holder can claim for compensation.

1.3.2 Statutory address for service and other email addresses

Traficom uses the email entered in the domain name register for hearings and service of notices, which means that documents or decisions related to domain names may always be issued by email. This 'address for service' has major legal importance, and it is mandatory to notify such address to Traficom.

The address for service enables Traficom to quickly issue its binding decisions, since a decision or other document is deemed to have been received on the third day from sending the message.

It is crucial that domain name holders' addresses for service are correct. This is very important for the legal protection of registrars, too. Registrars are responsible for entering domain name holders' addresses for service to the register and keeping them up to date.

Registrars may also enter other email addresses in Traficom's electronic system if it is necessary to keep email addresses intended for processing

Finnish Transport and Communications Agency

everyday technical issues related to the domain name separate from the mandatory address for service.

1.4 Renewing domain names

Registrars inform fi-domain name holders when their domain names are about to expire.

A domain name registered in the domain name register is valid from one to five years. Registrars may renew domain names for one, two, three, four or five years at a time.

1.4.1 Registrar's duties upon expiry of a domain name

When an fi-domain name is about to expire, registrars:

- inform the holder about the expiry well in advance
- instruct the holder on how to submit a renewal request
- provide the holder information about the consequences of not renewing the domain name.

Registrars and domain name holders (customers) may conclude an agreement on renewing domain names. Such agreement may state, for instance, that the registrar automatically ensures the validity of the customer's domain name and renews the domain name annually without informing the customer on the expiry.

Traficom does not control agreements between domain name holders and registrars or settle any contractual disputes.

1.5 Removing domain names from the register

Fi-domain name holders can request registrars to remove their domain name from Traficom's register before its expiry.

Registrars remove domain names from the fi-domain name register and the fi-root at the request of the holder.

Registrars are responsible for ensuring that

- domain names are removed from the register only at the request of the domain name holder or the holder's authorised representative
- no third party can intentionally or unintentionally remove domain names from the register
- if the domain name holder is an organisation, the person requesting the removal is authorised to do so (e.g. authorised to sign for the company as set out in the Trade Register).

Finnish Transport and Communications Agency

1.5.1 Problems in removals from register

Removing a domain name falsely from the register may have significant financial effects. A registrar may even be held liable for false removal.

Legislation on domain names does not lay down provisions on the contractual relationship between domain name holders and registrars, and contract, damages or consumer law issues arising from removals are resolved under other legislation.

1.6 Transferring domain names to a new holder

Registrars can transfer fi-domain names to a new holder after confirming that the party requesting the transfer has the right to do so.

A domain name holder may decide to transfer a valid domain name to another holder. After receiving a transfer request, a registrar:

- ensures that the requesting party has the right to transfer the domain name
- sends a holder transfer key to the domain name holder. Registrars cannot see the content of the key.
- transfers the domain name to the new holder within five working days of receiving the holder transfer key.

The domain name holder must authorise a registrar to perform the transfer by giving the holder transfer key to the registrar. This procedure ensures that the domain name holder has consented to the transfer and the registrar cannot transfer the domain name without the holder's consent.

Holders can authorise either their own registrar or the registrar of the new holder to perform the transfer. The registrar of the new holder can only perform the transfer if, in addition to the holder transfer key, the registrar has received a registrar transfer key, which enables the registrar to start hosting the domain name.

The holder transfer key is a code created by Traficom and registrars cannot see it. Registrars always send the holder transfer key to the current holder of the domain name and the holder must then forward the key to the registrar for the transfer.

1.6.1 Right to request domain name transfer

Registrars must ensure that the party requesting the transfer is the domain name holder or the holder's authorised representative. The transfer of a domain name may affect the holder’s legal protection and therefore registrars must perform the transfer with due care. As a rule, the party receiving the domain name (new holder) has the right to trust that there are legal grounds for the transfer.

If any other party than the domain name holder requests a transfer, registrars must request the holder's authorisation showing that the party requesting the transfer is authorised to act on the holder's behalf.

1.6.2 Domain name transfer time

Registrars must perform the technical transfer of a domain name within five working days of receiving the holder transfer key and details of the new holder from the current holder. The transfer time is a statutory service level requirement.

1.7 Changing registrars

In case an fi-domain name holder wants to change registrars, the current registrar must be involved in the process by creating a registrar transfer key and providing it to the holder or directly to the gaining registrar.

A domain name holder may change registrars any time without any special reason.

Stages of changing registrars

1. If a domain name holder wishes to change registrars, the holder must either

   - authorise the gaining registrar to request a registrar transfer key from the current registrar or
   - request the registrar transfer key from the current registrar and then forward it to the gaining registrar.
   - The holder must send the request for changing registrars to a registrar in writing to make it possible to determine the time limit for providing the key or to clarify any unclear issues in retrospect.

2. The current registrar must ensure that the holder or the gaining registrar has the right to request the registrar transfer key and provide it to the requesting party within five working days of an authorised request.

   The current registrar must check it carefully that the party requesting the transfer is the domain name holder. If the request is made by some other party, the requesting party must provide an appropriate authorisation. Registrars may, for example, contact the holder to confirm that the authorisation is valid.

3. Depending on the process chosen, the gaining registrar receives the registrar transfer key either from the current registrar or the holder, after which the gaining registrar can start hosting the domain name.

TRAFICOM
Finnish Transport and Communications Agency

1.7.1 Registrar transfer key

A registrar transfer key means a code that enables the administration of a domain name to be transferred from one registrar to another. The current registrar creates the code in the domain name system. The system does not send to code to the gaining registrar. Instead, the current registrar provides it, e.g. by telephone or email. The current registrar means the registrar giving up the administration of a domain name and the gaining registrar means the registrar assuming the administration of a domain name.

1.7.2 Domain names without a registrar

A registrar transfer key is also needed in case of orphan domains, that is, domain names without a registrar. In such cases, domain name holders have to request the code from Traficom. After receiving the code, holders send it to the registrar of their choice and the registrar can start hosting the domain name.

1.7.3 If problems arise

After the domain name holder has informed its current registrar of its intention to change registrars, the registrar must take the necessary steps within a reasonable time (five working days) and contribute to a successful change of registrars.

If the current registrar does not provide the registrar transfer key to the gaining registrar or holder within the specified time despite repeated requests, the gaining registrar may request Traficom to provide the registrar transfer key to the holder.

The contractual relationship between domain name holders and registrars is not governed by domain name legislation, and contract or consumer law issues arising from the change of registrars are resolved under other legislation.

1.8 Terminating registrar's operations

Registrars must notify their customers and Traficom in case they terminate their operations. Registrars must also inform their customers of any prohibition decisions issued by Traficom.

If registrars terminate their operations, they must inform Traficom and their customers no less than two weeks in advance to give their customers (fi-domain name holders) the chance to keep their domain names operable and to ensure that they have enough time to change name server administrators before the registrar terminates its operations.

Registrars must inform each customer separately about the termination of operations. For instance, publishing the information only on the registrar’s

website is not adequate although it is recommended to use the website as a secondary means of communication. Email is an efficient way of communicating to customers but Traficom recommends contacting them also by telephone.

Traficom recommends registrars to inform each of their customers about terminating or temporarily suspending operations well in advance.

1.8.1 Notification of Traficom's prohibition decision

Traficom monitors that registrars' operations comply with law and if necessary, issues a note of any violations. Traficom may decide to temporarily suspend a registrar's operations if the registrar does not remedy its defect or neglect despite of Traficom's notes.

If Traficom issues a prohibition decision concerning a registrar's operations, the registrar must notify its customers about this immediately since the customers may have to search for a new registrar in such cases.

Traficom implements the prohibition decision by shutting down the technical interface so that

- the registrar is prevented from registering new domain names or
- the registrar is also prevented from managing its customers' existing domain names.

1.8.2 Closing of prepaid account

Registrars that have terminated their operations can request Traficom to return the funds on their prepaid account that have not been used to register or renew domain names.

2 Information security in registrar's operations

Registrars must ensure the information security of their operations by preparing against threats and addressing irregularities. The minimum requirements for information security are intended to protect both registrars' operations and domain name holders' rights.

Registrars must pay attention to the different areas of information security in all phases of their operations: when planning, maintaining and terminating operations. To make information security an everyday routine, registrars must create processes and practices.

Documented contingency plan

Registrars are obliged to prepare detailed instructions for handling information security threats. Registrars must ensure that

- events that are relevant for information security will not go unnoticed

TRAFICOM
Finnish Transport and Communications Agency

- problems and irregularities identified in information security are addressed.

In order to develop and manage information security, registrars must have up-to-date documentation of their information security plans. The documentation also helps Traficom to verify, where appropriate, that registrars meet their obligations regarding information security. The documentation policy of information security issues depends on the scale of the company's operations.

Minimum requirements laid down for information security

Under section 3(1)(28) of the ECSA, information security means the administrative and technical measures taken to ensure the confidentiality, integrity and availability of data. These measures ensure that

- data and information systems can be used only by those who are entitled to use them
- data can only be modified only by those who are entitled to do so.

Traficom's Domain Name Regulation 68 describes the minimum requirements for information security management that all registrars must meet in their operations. The purpose of the requirements is

- to ensure the basic level of information security in domain name services.
- to minimise the harmful impact of information security risks on the domain name services and on fi-domain name holders.

2.1 Information security in practice

Registrars must document and maintain an up-to-date description of how they take various areas of information security into consideration in their operations.

There are several aspects to be considered in implementing and documenting information security measures. These aspects are listed in Traficom's Regulation 68. The Regulation does not specify how information security should be ensured in practice, since relevant measures may vary from company to company depending, for example, on services offered.

The essential requirement is that registrars identify the information security requirements relevant for their operations and the practices that best serve their implementation in the operations.

Traficom requires that registrars have updated documents on how they implement information security measures in their operations. Traficom does not specify the documents and leaves them to the discretion of the registrar. The most important issue is that the documentation is updated

Finnish Transport and Communications Agency

and proves that all the areas of information security listed in the section have been taken into account in the operations.

2.1.1 Areas of information security

Through all stages of fi-domain name services, registrars must pay attention to the following areas of information security:

Administrative information security

- information security guidance documents (typical examples include information security policy and architecture) with which the management of the organisation proves its determination to ensure information security, the general principles of information security and its commitment to information security matters
- processes and their management
- management of risks and business continuity (see section 15 of Traficom's Regulation 68)
- documentation practices and systems
- auditing and rehearsing procedures.

Personnel security

- personnel's information security responsibilities and obligations
- personnel's information security skills and skills development
- personnel's background investigations
- key employee risks
- prevention of risky combinations of responsibilities and tasks
- job rotation to detect irregularities
- procedures to be followed when employment is terminated
- misconduct and non-compliance of personnel

Security of hardware, software and data communications

- vulnerability management
- detection of information security violations (see sections 17 and 18 of Regulation 68)
- change management (see section 19 of Regulation 68)
- security of information material and usage
- safeguarding of confidentiality, integrity and availability of information
- classification of information material and treatment according to the classification (see section 16 of Regulation 68)
- responsibilities related to the maintenance of a user rights register: awarding, amending and cancelling user rights
- prevention of the accumulation of user rights
- prevention of unauthorised access to the administration and configuration data related to the provision of domain name registration services and to the invoicing, account and log data of the customers of the domain name registrar
- data storage and deletion.

Finnish Transport and Communications Agency

Physical security

- location of facilities and the security of the surroundings
- access control
- structural protection.

Traficom has the right to audit the operations of a registrar, if necessary.

Traficom's regulations are available on Traficom’s website.

2.2 Risk management

Registrars must identify the functions, information and systems that are critical for the continuity of its operations and regularly evaluate and address any information security risks that they may be exposed to and the management of such risks. The risk management processes and results must be documented.

A security risk refers to the likelihood of an injury or damage and its consequences. An information security risk means an accidental or deliberate event that compromises the confidentiality, integrity or availability of domain name services. The difference between an information security risk and an information security threat is that the likelihood and consequences of a risk have been assessed.

Information security risks may arise from the following:

- human error
- gaps in or non-compliance with instructions provided to the personnel
- theft or vandalism
- flaws and malfunctions of equipment, systems or software
- malware spread
- destruction of data
- fire or water damage
- errors and neglect on the part of a subcontractor or a member of a partner network.

Objectives of risk management

Risk management is a process that aims at identifying risks, reducing their likelihood and/or impact to an acceptable level and maintaining the achieved level. The purpose of risk management is to protect the organisation and its ability to perform its operations, taking into account economic factors.

The objective of risk management requirements is to ensure that registrars are aware of the consequences of a potential realisation of the risks and know whether the risk-mitigating measures are adequate.

The objectives of risk management include:

Finnish Transport and Communications Agency

- speeding up recovery after information security incidents
- reducing the costs and damage caused by information security incidents
- helping in allocating investments that improve the information security of domain name services
- improving the quality and productivity of domain name services
- optimising, in terms of finances, the management of risks related to domain name services and preventing the realisation of risks.

Identifying and addressing risks

Examples of standards and publications addressing risk management include the following:

- ISO/IEC 27005
- NIST 800- 30 Risk Management Guide
- OCTAVE

Traficom does not require compliance with a particular standard. Risk management models vary from company to company, and there is no single model that would suit every purpose.

Traficom requires registrars to identify the risks related to their operations and their continuity, and how to address such risks. Addressing the risks means that registrars determine an acceptable risk level to their operations and take appropriate measures (often called controls) to reach this level. This means that in practice, risk management requires allocating responsibilities and scheduling. In addition, the implementation and impact of risk management measures should be monitored.

Traficom also requires that risk management is regular, i.e. that risks and the measures to manage them are evaluated on a regular basis. Registrars are free to determine the appropriate monitoring cycle. Typically, companies run risk management

- regularly on an annual basis
- whenever new services or functions are being established
- every time after a potential risk is realised.

Documentation of the process and its results

Traficom supervises registrars' operations and registrars must document their established risk management process and results to monitor the compliance with the risk management requirements.

2.3 Information material

Registrars must have a classification system for any information material that is critical for their operations and a procedure for processing information material related to the classification system.

The classification system and procedure for processing information material ensure that important information related to domain name services is only available to those who have the right to access it. The classification criteria and processing procedures must be documented and maintained in a timely manner.

2.3.1 Classification and processing of the material

Registrars must determine a set of information material classification criteria that is appropriate for their own operations. Material may be classified, for example, as follows:

- public
- confidential
- secret.

Furthermore, registrars must determine how they process (protect) the materials belonging to the different classes.

2.3.2 Information material documentation

The classification and the related processing guidelines must be documented. The classification and its documentation must include the following:

- general principles in assessing the security class and confidentiality of information material and in keeping material secret
- rights to process and alter material and the distribution of the rights to access and alter information material
- determination of the confidentiality class
- publicity of data or documents, including the right to speak publicly of the matter concerned
- document properties: paper, watermark and other marks
- storage and encryption
- printing and copying
- backup copies
- sending and receiving, distributing and moving
- documentation of the processing of data and documents
- archiving and processing of documents, or the termination of such processing rights,
- destruction of data and documents.

2.4 Information security control

Registrars must continuously monitor their operations to either identify or prevent events that interfere or threaten the operations.

Registrars must ensure that events that are significant to information security are identified. In order to monitor the operations, registrars must be able to identify information security violations and threats related to the

operations. In practice, this means that registrars must maintain a management system for their services.

2.4.1 Identifying threats

Registrars' proactive and prompt actions are crucial in identifying incidents. If registrars are well equipped to identify incidents, the measures to detect, control and remedy information security incidents can be initiated quickly, without having to wait until customers complain.

Registrars shall monitor constantly the state of information security in their operations. The monitoring must be carried using a management mechanism suitable for the operations which identifies any events affecting the state of information security as soon as possible. Such events include

- denial-of-service attacks
- data leaks
- attempted hacking
- excessive user authorisations.

2.4.2 Prevention of threats

The prevention of information security incidents aims at identifying even the smallest signs of emerging problems as early as possible. Through prevention, their impact on domain name services may be minimised. In the best scenario, there is no visible impact at all.

Registrars must attempt to identify events that are developing into problems using their service management mechanisms. Such mechanisms may include:

- software alerts and service quality metrics that indicate deviations from normal operations even when an immediate incident is not detected. Registrars are responsible for determining appropriate alerts and metrics.
- alerts of identified hardware or software vulnerabilities predicting information security incidents.

2.4.3 Monitoring documentation

Registrars must prepare and maintain up-to-date documentation of the management mechanisms for their operations to be able to demonstrate, when necessary, how they meet the requirements.

Systems and procedures used for receiving and analysing various alerts and notifications must be documented and the documentation must be kept up to date. In other words, registrars must have a description of the technical systems and measures they use to process information and notifications on the state of their services.

TRAFICOM
Finnish Transport and Communications Agency

2.5 Management of threats and incidents

Registrars must prepare guidelines in case of events that disturb or threaten the information security of their operations. The guidelines are used both to minimise and to address such events.

Registrars must prepare in advance clear procedural guidelines for addressing events that disturb or threaten the information security of their operations. The guidelines are used to minimise the impacts of such events without undue delay.

The guidelines must specify

- how to organise information security management
- who are responsible for information security
- how these responsible operators may be contacted.

The guidelines must be documented and kept up to date.

2.5.1 Purpose of procedural guidelines

The most important objective of the guidelines is to enable identifying the cause of an information security incident as quickly as possible and minimising the impact of the event. The guidelines also have practical importance, for example, in training new personnel.

The guidelines must also take into account any special instructions concerning the corrective measures in case of major incidents. Such special instructions may concern, for example, on-call or deputy arrangements.

Typically, the organisation of information security management is described in a company's internal information security policy, which is a set of documents describing the measures and targets of information security that has been approved by the company management.

2.6 Change management

Registrars must organise changes, maintenance and updates so that they disturb their operations as little as possible.

Registrars must perform changes to the network, software, hardware, configuration, interface and equipment rooms in a controlled and systematic manner. The changes must disturb domain name services as little as possible.

2.6.1 Planning changes

Registrars must reserve sufficient amount of time for changes, maintenance and updates in order to perform them in a controlled manner. Registrars must define and document the underlying processes and practices.

Finnish Transport and Communications Agency

Any disturbances arising from the changes, such as downtime, must be minimised. As downtime cannot sometimes be avoided and it should be possible to carry out planned changes with as few errors as possible, when estimating the required downtime, not only the service needs but also the realistic time needed for carrying out the changes carefully should be considered.

To manage changes and minimise damage, registrars must, before taking any actions

- plan the phases of the changes
- determine the required resources
- estimate the impact and length of the changes
- plan the measures to be taken if the changes do not turn out as planned.

For example, when the software of a device is replaced with another or its configuration is changed, it may be a good idea to simulate the impact of such changes in advance as far as possible to enable identifying and fixing errors before they materialise.

2.6.2 Documenting changes

Registrars must prepare and document the underlying processes and practices related to the changes to enable a systematic and predictable approach.

For each change, maintenance or update, registrars must, on a case-by-case basis and according to its established processes and practices, estimate and reserve adequate time for completing the change, maintenance or update.

2.7 Data protection in domain name services

Registrars collect personal data from domain name holders for registering domain names. Registrars enter the data into Traficom's domain name register and keep the data up to date. Registrars' operations are governed by the EU General Data Protection Regulation (GDPR), Finnish law and Traficom's Regulation.

Traficom does not conclude contracts with registrars on personal data processing. When registrars start acting as fi-domain name registrars approved by Traficom, they commit to complying with the obligations laid down for registrars in Finnish law and Traficom's Regulation.

The Act on Electronic Communications Services (917/2014, ECSA) and Traficom's Regulation 68 constitute a legal basis referred to in the GDPR for registrars to process the personal data of domain name holders for domain name registration purposes, in other words to provide domain name services.

Traficom’s statutory obligations include management of the country code .fi and maintenance of the fi-domain name register. In accordance with the GDPR, Traficom acts as the data controller of personal data entered into the domain name register, and registrars act as processors of personal data on Traficom's behalf.

2.7.1 Collection of personal data in domain name services

Under law, personal data on domain name holders collected in domain name services include:

- name
- personal identity code / other identifier
- postal address
- telephone number
- contact person and phone number of contact person (legal persons)
- email address (electronic address for service)
- Registrars are responsible for ensuring that these details are up to date

If a registrar collects non-statutory data on a domain name holder, the registrar acts as the data controller of that non-statutory data.

2.7.2 Purpose and nature of processing personal data

Domain name services refer to the entering of domain names into the fi-domain name register and the administration of the register entries. Only service providers i.e. registrars that have made a domain name notification to Traficom can make entries to the domain name register.

Domain names must be registered in the name of a domain name holder, and registrars must enter the holder’s correct, up-to-date and identifying information, and the email address to be used for hearing and for service of notices, into the domain name register.

Registrars are responsible for ensuring that the details are correct and up to date.

Domain name services refer to all actions taken by a registrar to maintain the domain name related information entered into the domain name register. Administration refers to updating contact details, renewal of domain dames, transfers of domain names from one registrar to another, and changing of registrars.

Domain name services also involve obligations related to notifications and the provision of advice.

If a registrar sets name servers for a domain name, the registrar is responsible for ensuring that the name servers function in accordance with Traficom's Regulation. Registrars are fully responsible that their

Finnish Transport and Communications Agency

subcontractors, third service providers or other personal data processors (for example resellers) fulfil the obligations in relation to Traficom.

The administration of a domain name also means the ability to enter data into the domain name register using the technical systems prescribed by Traficom and the ability to ensure the information security of operations.

Registrars process personal data in accordance with the GDPR, Finnish law and Traficom's Regulation.

If registrars provide non-statutory services to a domain name holder (for example web hosting or email services, server space, etc.) and collect personal data on the holder for that purpose, these registrars acts as data controllers of that data, and must have legal grounds for processing the data in accordance with the GDPR.

Subject and duration of data processing

Registrars may process the personal data they have entered into and maintained in the domain name register only for as long as they host the domain name in question and/or as long as the domain name is valid, grace period included. Registrars are responsible for deleting the personal data of domain name holders from its systems.

2.7.3 Registrar’s obligations as a data processor

When processing the personal data of domain name holders in the provision of domain name services, registrars must comply with the obligations of a processor laid down in article 28 of the GDPR.

If a registrar uses resellers for service provision, it must enter the details of the resellers into Traficom’s domain name register and ensure that the details remain up to date. Registrars are fully responsible for the resellers’ performance (Article 28(2) of the GDPR).

Registrars may only process the personal data of domain name holders in accordance with the provisions of the ECSA and Traficom's Regulation 68. The Explanatory Notes to the Domain Name Regulation (68/2014M) document provide more concrete information on the practical application of the Regulation.

Registrars may not disclose personal data from Traficom's domain name register without legal grounds.

Traficom maintains a search engine for public information in the domain name register.

Finnish Transport and Communications Agency

Registrars must submit any requests for information from the domain name register concerning non-public information to Traficom (Article 28(3)(e) of the GDPR).

If a registrar discloses personal data from Traficom's domain name register on the basis of other applicable legislation, the registrar must notify Traficom of such legal grounds prior to the disclosure of the information, unless that law prohibits such information on important grounds of public interest (Article 28(3) of the GDPR).

Employees of registrars must be committed to confidentiality with regard to the personal data they process (Article 28(3)(b) of the GDPR).

Registrars must ensure the information security of their operations. The statutory obligation for registrars to ensure the information security of their operations is provided in section 170(1)/6) of the ECSA and Article 32 of the GDPR. Under section 3(1)(28) of the ECSA, information security means the administrative and technical measures taken to ensure the confidentiality, integrity and availability of data. Chapter 4 of Traficom's Domain Name Regulation 68 describes the minimum requirements for information security management that all registrars must meet in their operations.

The Explanatory Notes to the Regulation provide more concrete information on the practical application of the Regulation.

Registrars are obliged to assist Traficom in compliance with the obligations laid down in the GDPR (Article 28(3)(f) of the GDPR).

Registrars must delete the personal data of a domain name holder from their systems after the holder ceases to be their customer or after a domain name expires, grace period included (Article 28(3)(g) of the GDPR).

Traficom monitors registrars and conducts audits as a supervisory measure. Registrars must allow for audits conducted by Traficom (Article 28(3)(h) of the GDPR).

Registrars must notify Traficom immediately if they assess that Traficom's guidelines are in violation of the rules of the GDPR (Article 28(3)(h) of the GDPR).

If a registrar infringes the GDPR by determining the purposes and means of processing domain name holders' personal data, the registrar is considered to be a controller in respect of that processing (Article 28(10) of the GDPR).

Registrars must keep the domain name holders' personal data accurate and up to date.

Registrars must notify Traficom immediately of any information security incidents concerning personal data.

Finnish Transport and Communications Agency

Registrars must maintain a privacy policy of their processing activities (Article 30(2) of the GDPR).

2.7.4 Domain name holder's rights

Domain name holders have the right:

1. to know who uses their personal data

Registrars and Traficom process the personal data of a domain name holder. Registrars can use subcontractors (resellers) in the provision of domain name services and registrars take full responsibility of their actions.

2. to know the purpose for using their personal data

The personal data of a domain name holder is used for registering and managing domain names, and for resolving disputes related to fi-domain names. Registrars register and manage domain names. Traficom administers the domain name register for the .fi domain and resolves disputes on fi-domain names at the request of right holders.

3. to review and correct their personal data.

There is an electronic form for reviewing personal data on Traficom's website.

Read more about the processing of personal data on Traficom's website.

2.8 Obligation to notify information security incidents

Registrars must report any threats to or violations of information security immediately.

Registrars must notify Traficom immediately if they detect in their operations

- significant violations of information security
- threats of significant violations of information security or events that essentially prevent or disturb their operations.

The notification must specify the incident or related threat in terms of

- estimated duration
- impacts
- corrective measures
- measures to prevent such incident from reoccurring.

The notification on a significant information security incident submitted to Traficom should also include, where possible, information about the cause of the incident or threat and how it emerged.

Finnish Transport and Communications Agency

2.8.1 Information security incidents must be reported immediately

The notification must be made within 24 hours of the registrar becoming aware of the incident.

For example, if a registrar's system has been hacked, it is crucial that the supervising authority is notified immediately. There is a risk that the hacker may be able to freely alter the details of the domain names managed by the registrar, such as name servers. Depending on the registrar's customer base, the threat may concern a large amount of customers.

Registrars can report incidents by form.

If some information is lacking and the event needs further examination, the registrar should make a so-called preliminary notification within 24 hours, which can then be complemented as soon as possible but no later than three (3) days after the preliminary notification.

If, in spite of examinations, the registrar cannot provide all information within three days of the preliminary notification, the information that has become available before this deadline must be notified, along with reasons why the rest of the information will be notified after the deadline.

2.8.2 Significant violations of information security

Registrars must notify significant information security violations in their operations to Traficom.

Violations of information security may affect the confidentiality, integrity or availability of data or information systems.

Confidentiality: Only authorised parties know the data and the authentication data related to user IDs.

Integrity: Unauthorised alteration of data is not possible. Third parties are not able to tamper with information systems.

Availability: The service and the data contained are available to those who are authorised to access them.

Assessment of the significance of information security violations

When assessing the significance of an information security violation or another incident, the adverse effects of the incident or the severity of the information security threat must be examined. The following should always be protected, and any information security incidents in them are to be considered significant:

- services provided by registrars, as well as the information and communication systems employed in providing the services

Finnish Transport and Communications Agency

- information security, protection of personal data and business secrets of the registrars' customers
- the Finnish fi-root administered by Traficom (following a violation of information security that directly or indirectly affects a registrar).

Repeated, exceptionally lengthy or obviously deliberate action with a negative impact on registrars' ability to ensure the information security of their operations is also to be considered significant. In addition, an incident is to be considered significant if it cannot be eliminated through actions taken by registrars only.

Information security violations that must be notified

The list of information security violation types below is not exhaustive. Its purpose is to clarify the severity level of the reporting threshold. Minor information security violations and threats of such violations may also be notified to Traficom if it is considered necessary.

Significant information security incidents that should be notified to Traficom include the following:

- hacking of the information systems of registrars
- unauthorised access to the systems of registrars
- vulnerability or configuration error in the systems of registrars that compromises information security
- accidental disclosure of logins to third parties
- logins to Traficom's systems falling into the hands of third parties.

Unauthorised alterations

- an opportunity to make unauthorised changes to domain names administered by a registrar
- unauthorised changes made by the staff of a registrar to Traficom's domain name register
- unauthorised access to the self-service portal provided by a registrar to its customers, intended for enabling customers to maintain the information related to their domain names.

Denial-of-service attacks

- if a registrar's system is paralysed and/or customer access to the system is prevented; or
- the system failure affects the operation of Traficom's system.

Recommended voluntary notifications

Traficom recommends that, at their discretion, registrars notify Traficom also about minor violations of information security and threats of such violations. Such knowledge may be relevant in carrying out Traficom's other information security duties.

Traficom has the right to undertake the necessary measures in order to detect, prevent, investigate and commit to pre-trial investigation any significant information security violations aimed at public communications networks or services using fi-domain names or their holders. Traficom may undertake these measures without consulting domain name holders.

The necessary measures carried out by Traficom may be actions targeted at root .fi name server data and may include the following:

- preventing and restricting traffic to domain names
- rerouting traffic to domain names to another domain name address
- any other comparable technical measures.

Furthermore, Traficom's duties include:

- promoting the functionality, freedom from interference and security of electronic communications
- collecting information on violations of and threats to information security in respect of network services, communications services and added value services as well as on defects and interference situations in communications networks and services
- disseminating information security matters as well as communications network and service matters
- investigating violations of and threats to information security in respect of network services, communications services and added-value services.

2.9 Name servers

Registrars are responsible for ensuring that fi-domain names provided for customers are configured in accordance with relevant technical requirements.

Fi-domain names may be registered either using functioning name servers or completely without name servers. However, if name servers are provided, all of them must be functioning. If a domain name holder wishes later to keep the domain name without any associated services (so-called parking), such as email or a website, the name servers must be removed from the fi-root.

Name server requirements

As provided in Traficom’s Regulation 68/2014 M, at least two and at the most ten name servers that are independent of one another must be configured to serve the domain name. This helps to ensure the functioning of the domain name in case of a failure of one of the name servers.

Name servers are independent of each other if they have

- different server devices
- different IP addresses

Finnish Transport and Communications Agency

- separate internet connections.

Furthermore, all name servers must

- be connected to the internet
- have the name server configurations available to be verified by name server queries made by Traficom.

Traficom verifies the functionality of all name servers regularly. If one or more name servers are out of operation or the name server configurations are not correct, Traficom sends a notification email to the registrar or to the email address of the name server administrator indicated by the registrar.

The name server test tool at Traficom's website allow users to check the configurations.

Information security recommendations for name servers

Traficom recommends that third parties are prevented from transferring domain name information (AXFR, DNS zone transfer protocol). Furthermore, name servers should not return a correct value if the software version is inquired. If the correct software version is returned, information security may be compromised in cases where the name server software version has a known information security issue.

2.9.1 Name server configurations

Name servers must meet the requirements set for them. It is recommended to use standard serial numbers and timers of SOA records.

Name servers must be equipped with NS records (Name Server) indicating all name servers added to a domain name. The NS records must point to servers, for which an IP address has been configured using either an A record or an AAAA record (or both) in the DNS. The NS records may only be name servers that have actually been configured for the domain name. The NS records must be consistent with the information configured in the fi-root.

Requirements and recommendations for SOA record

The SOA record (Start of Authority) that defines the configuration of the name server of the domain name must comply with the following:

the MNAME (Master Name) field must contain the name of the primary name server of the domain name

the RNAME (Responsible Name) field must contain a working email address that belongs to the administrator of the name servers. The email address must be configured without the @ symbol, which is replaced by a dot. For

example: hostmaster.domain.fi. The best practice is to configure the hostmaster address in the RNAME field in accordance with RFC 2142.

Traficom recommends that the serial numbers and timers of SOA records should not differ essentially from published internet standards and recommendations. Traficom recommends the following:

```
fi.example. 3600 SOA dns.fi.example. hostmaster.fi.example. (
2018090401 ; serial YYYYMMDDnn
86400 ; refresh ( 24 hours)
7200 ; retry ( 2 hours)
3600000 ; expire (1000 hours)
172800 ) ; minimum ( 2 days)
```

Serial number

The recommended form of the serial number is YYYYMMDDnn, where YYYY is the year, MM is the month, DD is the day and nn is a running number that increases by one at each update. The number of the first version of the day is 01. The serial number helps to verify that the zone records of all domain name servers are the same. The serial number must not be zero (0).

Refresh and retry

The refresh and retry values determine how often secondary name servers check whether the domain name server information on the primary name server has been changed. The retry value determines the time of a new attempt to retrieve the name server information if the previous attempt was unsuccessful.

Expire

The expire value indicates how long the name server keeps the old zone record if a new record cannot be retrieved.

TTL

The minimum TTL (time to live) value determines a default TTL for resource records (RR). In certain situations, it is justified to set the TTL value lower than the recommendations, for example when name servers are changed.

2.9.2 Domain Name System Security Extensions (DNSSEC)

DNSSEC is a service improving the information security of the DNS. DNSSEC can be set up for an fi-domain name, too.

DNSSEC is an extension to the DNS, which can be used to ensure the reliable origin and integrity of the information obtained from the name server.

Finnish Transport and Communications Agency

When DNSSEC is enabled for an fi-domain name, responses to name service queries are electronically signed. DNSSEC ensures that responses to DNS queries come from the right sender and that the response information has not been modified. This way, those visiting a website connected to the domain name can be confident that they are directed to the right website.

For DNSSEC to work, the DNS resolver used must support the validation of DNNSEC signatures. Otherwise, the security of the DNNSEC chain of trust cannot be confirmed.

Provision of DNSSEC to customers

Registrars can enable DNSSEC by signing the domain name data, after which they can add DS records to the domain name. Registrars can manage DS records via the EPP interface and the browser-based interface. Key exchange can be automated using the EPP interface.

Creating an electronic signature requires

- a private key that is kept secret and the holder alone has access to it; and
- a public key published in its own record in the name system.

The electronic signature can be verified by using the public key corresponding with the private key. Resolver name servers perform the validation on behalf of the user.

The public keys of the fi zone are published in the root zone. Registrars maintaining resolver name servers are recommended to configure a trust anchor for the root zone in their name servers. The trust anchor is available on IANA's DNSSEC site.

Traficom’s DNSSEC brochure describes and gives examples on how DNSSEC works. The brochure is available on Traficom’s website.

Parameters used in the DNSSEC signature of the fi-zone

- hash function: SHA-256
- signature algorithm: RSA
- NSEC3
- Opt-Out
- Zone Signing Key (ZSK): RSA 1024-bit (replaced by 2048-bit key in the near future)
- Key Signing Key (KSK): RSA 2048-bit.

The zone's DNSKEY record group only is signed with the KSK key. The ZSK key is used for signing the zone's other name system records, such as the DS records of the signed sub-zones and the authoritative records of the fi

zone. The life span of a ZSK key is one month and that of a KSK key is 12 months.

Inquiries:

For more information about the DNSSEC information security extension, contact us by email:

fi-domain-tech@traficom.fi.

2.9.3 Name server test

The name server test tools at Traficom's website allow you to check the functionality of the name services of a domain name.

The name server test helps you to check

- whether the fi-domain name is configured to name servers in accordance with Traficom's requirements
- whether the name services of the fi-domain name are functioning properly
- whether DNSSEC is enabled for the domain name.

If you have received an email from Traficom about name servers that are not functioning, you can use the name server test to get more information about the problem.

You can also check the functionality of the name servers before registering a domain name. If you are about to change a name server, you can check whether the new name servers comply with Traficom's requirements.

2.10 Technical interfaces

Registrars may use either a browser-based user interface or an EPP interface defined by Traficom as the technical interface to the fi-domain name register.

2.10.1 Browser-based user interface

Registrars may log in to Traficom's fi-domain name register via the browser-based user interface. Registrars log in using two-factor authentication

Two-factor authentication means that the login requires a one-time password in addition to a user ID and password. The one-time password is an eight-digit password that is valid for only one login session. It is sent to registrars by text message.

In order to be able to log in, registrars must already be registered with Traficom.

Finnish Transport and Communications Agency

2.10.2 EPP interface

EPP (Extensible Provisioning Protocol) is an XML-based technical interface. Registrars can connect to the interface by using their own client software.

Traficom does not provide ready-made client software and it is the registrar's responsibility to programme or acquire the client software.

Registrars do not have to start using the EPP interface. Using both interfaces is also possible.

Registrars' EPP client software must be compatible with Traficom's EPP interface description. It specifies the restrictions and extensions of interfaces based on the RFC documents.

Before a registrar can start using Traficom's EPP interface, the registrar's own client software must be tested in Traficom's EPP sandbox environment.

The EPP interface is available at

`https://epp.domain.fi` (port 700).

2.10.3 RFC standards

Traficom's EPP interface is mainly based on the following RFC standards:

- RFC 4310 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 5730 Extensible Provisioning Protocol (EPP)
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC 5910 Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).

2.10.4 KATAKRI requirements in the use of EPP interface

Katakri is an auditing tool for authorities that can be used to assess the target organisation's ability to protect an authority's classified information.

If a registrar uses Traficom's EPP interface as the technical interface, the registrar must meet the criteria derived from the requirements of protection level (IV) of subdivision I, information assurance, of the currently valid version of Katakri with respect to the following:

1. communications security
2. system security.

The Katakri audit tool brings together the minimum requirements based on national legislation and international obligations. Katakri, as such, does not set mandatory requirements on information security; instead, the

requirements included in Katakri are based on legislation in force and international information security obligations binding on Finland. To ensure transparency, a source reference is always given in connection with the requirements presented in Katakri.

Subdivisions of requirements

The requirements in Katakri are divided into three subdivisions:

- The subdivision on security management (T) aims to ensure that the organisation has sufficient security management abilities and skills.
- The subdivision on physical security (F) describes the security requirements for the physical environment of processing classified information.
- The subdivision on information assurance (I) describes the security requirements for the IT environment. This subdivision is further divided into three protection levels on the basis of the information handled (ST IV, ST III, ST II).

Registrars using Traficom's EPP interface must meet the requirements in the subdivision of information assurance in terms of communications security and system security.

The requirements apply to domain name services. Registrars are responsible for meeting the above-mentioned requirements. If necessary, Traficom may audit registrars' operations.

If the party engaged in domain name services also carries out other operations, the requirements do not apply to such operations.

Traficom's regulation refers to the currently valid version of the criteria. The valid version of Katakri is available on the website of the Ministry of Defence.

If a registrar uses Traficom's EPP interface as the technical interface, the registrar must meet the criteria derived from the requirements of protection level (IV) of subdivision I, information assurance, of the currently valid version of Katakri (information security audit tool) with respect to the following:

1. communications security
2. system security.

2.10.5 EPP sandbox environment

Registrars that use an EPP interface must have their own client software which is compatible with Traficom's EPP interface. The registrars' client software must pass tests required by Traficom.

If a registrar uses Traficom's EPP interface, the client software of the registrar must be consistent Traficom's EPP interface description.

Before a registrar can start using Traficom's EPP interface, the registrar's own client software must be tested in Traficom's EPP sandbox environment.

The following documents on Traficom's website provide advice for the testing:

- EPP test instructions
- EPP interface description
- XML schemas

If you have questions about testing, contact us by email: fi-domain-tech@traficom.fi.

2.10.6 Whois service for fi-domain names

Registrars may use Traficom's whois service so that their customers are able to check whether a certain fi-domain name is available.

The whois service for fi-domain names is at whois.fi. To use the service, registrars need the whois client program that is included in most Unix and Linux operating systems.

2.10.7 Domain Availability Service (DAS)

Traficom's DAS (Domain Availability Service) is designed for fast fi-domain name availability queries. The service only shows if a domain name is available for registration. It does not retrieve data on the domain name holder or detailed domain status information.

The service is available at

`das.domain.fi` (port 715/UDP)

The service description of the DAS is available at Traficom's website.

2.10.8 OData

The OData interface in the domain name system provides information about domain names registered by organisations and associations (Domains). It also contains name service data (NameServers) and contact details of the domain name administrators.

Please note that in principle, the interface does not provide information about domain names registered by private persons. Therefore, the interface cannot be used to check whether a certain domain name is available. This restriction should be noted in other queries, too. In practice, the data covers roughly 80% of domain names.

Finnish Transport and Communications Agency

The data provided by the OData service are updated once a day.

The service description of the OData is available at Traficom's website.

2.11 Registration as a registrar

Those intending to start acting as an fi-domain name registrar should examine all obligations laid down by law before registering with Traficom.

The operations of fi-domain name registrars are governed by the provisions in the ECSA. Those intending to start acting as a registrar should consider in advance whether they will be able to meet all of the registrars' statutory obligations, including information security requirements.

There is an electronic registration form for registrars on Traficom's website. Any changes in the submitted information must be notified to Traficom without delay. Traficom recommends that registrars update any changed information in Traficom's domain name register within three days.

Registrars can use the fi-registrar logo in their operations as an fi-domain name registrar. The official versions of the logo are available on Traficom's website.

2.11.1 Statutory address for service and other email addresses

Traficom uses the email address entered in the domain name register for all hearings and service of notices related to fi-domain names, which means that documents or decisions related to domain names may always be issued by email. This 'address for service' has major legal importance, and it is mandatory to notify such address to Traficom.

The address for service enables Traficom to quickly issue its binding decisions, since a decision or other document is deemed to have been received on the third day from sending the message.

It is crucial that a registrar has a correct address for service, and it is very important for the legal protection of the registrar to keep it up to date. Registrars are also responsible for entering the domain name holders' addresses for service in the register and keeping them up to date.

Registrars may also enter other email addresses in Traficom's electronic system if it is necessary to keep email addresses intended for processing everyday technical issues related to the domain name separate from the mandatory address for service.

2.11.2 Resellers' operations

Traficom monitors registrars' operations. If a registrar uses resellers in its operations, it always bears the responsibility for its resellers' activities. A reseller may, for instance, offer customer support and invoicing services. If a registrar adds the details of its reseller in the fi-domain name register,

the details appear in the whois information of fi-domain names under "Reseller".

The provisions of the ECSA oblige specifically the party that is registered as a registrar with Traficom. Registrars are also responsible for ensuring that their resellers meet the requirements for fi-domain name operations.

2.12 PGP keys

Some of Traficom's emails related to fi-domain names are signed using role keys, i.e. PGP keys.

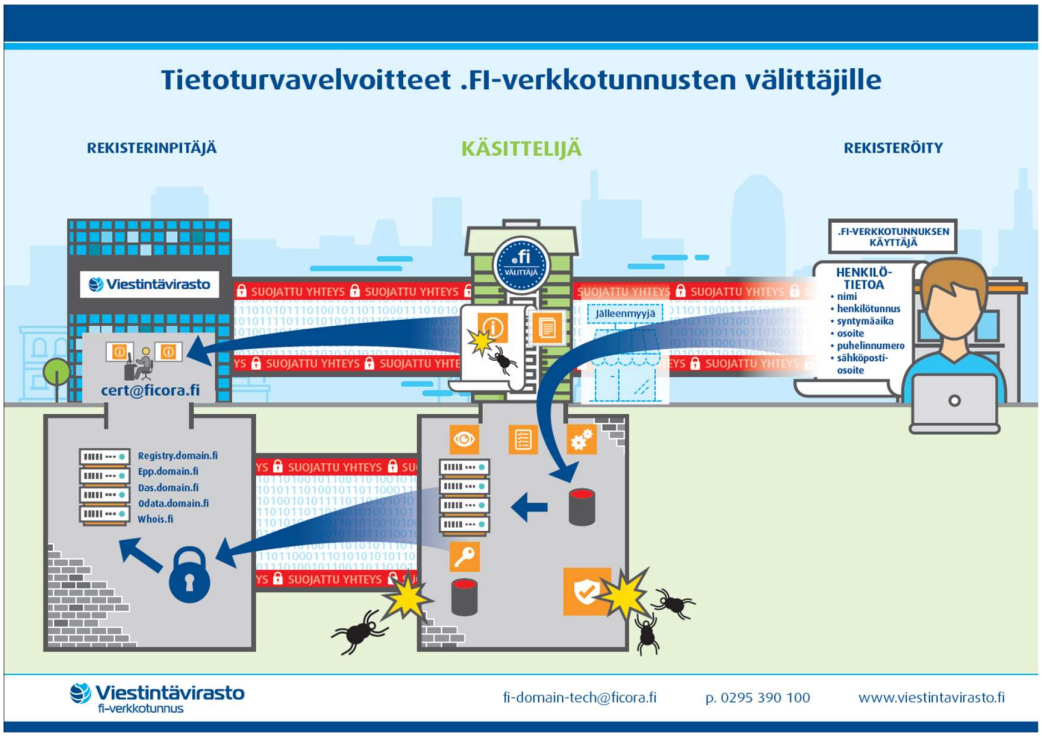
The PGP is used for encrypting or signing emails. The programme is based on public-key encryption.

An email is signed with the sender's private key.

The signed email can be verified with the sender's public key. The sender's public key can be used for checking whether the message is sent by the right party.

The PGP keys used by Traficom are available on Traficom's website.

TRAFICOM
Finnish Transport and Communications Agency



Miksi tietoturvaa?

- *Varmistutaan siitä, että merkittävät tietoturvaloukkaukset havaitaan ja hoidetaan ajoissa, mieluummin taki ennen asiakkaiden valituksia.*
- *Asiakkaat haluavat valita luotettavan välittäjän, joka pitää hyvää huolta heidän liiketoiminnastaan ja henkilötiedoistaan.*
- *Luvaton pääsy verkkotunnusrekisteriin käyttäen välittäjältä varastettuja tunnuksia vahingoittaa sekä välittäjän että verkkotunnusjärjestelmän toimintaa.*
- *Tietoturvahäiriöiden välttäminen johtaa parempaan toimintavarmuuteen, ja auttaa välttämään myös häiriöiden aiheuttamia odottamattomia kuluja.*

Tietoliikenne- ja tietojärjestelmäturvallisuus

- Suomen laki ja Viestintäviraston määräys edellyttävät, että verkkotunnusvälittäjä huolehtii järjestelmänsä tietoturvasta Viestintäviraston ohjeistamalla tavalla.
- Jos välittäjä käyttää EPP-rajapintaa, järjestelmän on myös toteutettava KATAKRI:n (tason IV) tietoliikenne- ja tietojärjestelmävaatimusosuudet. (Ajantasainen versio KATAKRI 2015, sivut 30-52) http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille.
- Jos välittäjä käyttää selainkäyttöliittymää, tietoturvavelvoitteet ovat vastaavat, mutta KATAKRI:n noudattaminen ei ole pakollista. Suosittelemme silti kaikille välittäjille KATAKRI:in perehtymistä.

Turvallisuusdokumentit

1. Riskienhallinnan prosessit ja tulokset

- Riskien määrittäminen ja toimenpiteet niiden huomioimiseksi on osa normaalia liiketoimintaa erityisesti silloin kun turvalliset ja luotettavat yhteydet ovat välittäjien liiketoiminnan ytimessä. Välittäjä: ovathan riskienhallinnan dokumenttinne ajan tasalla? Valmistautukaa perustelemaan valitsemanne toimenpiteet.

2. Luokittelukriteerit ja arkaluonteisten aineistojen käsittely

- Henkilötiedot ovat arkaluonteista aineistoa. Kuinka säilytätte ja suojelette sitä?
- Pääsytunnukset EPP-rajapintaan tai selainkäyttöliittymään on suojattava huolella.

3. Valvontamekanismit

- Olkaa tietoisia siitä mitä tapahtuu omassa järjestelmässänne, jotta pystytte reagoimaan ajallaan. Ovatko tunkeutumisesto- ja havainnointijärjestelmänne ajan tasalla?

4. Tietoturvaloukkausten käsittely

- Kuinka tietoturvaloukkaukset havaitaan?
- Kuinka tietoturvaloukkauksista toivutaan?
- Tietoturvaloukkauksista ilmoitetaan vapaamuotoisella sähköpostilla osoitteeseen cert@ficora.fi tai Viestintäviraston asiointilomakkeella. Ilmoittamisprosessien tulee olla ohjeistettu henkilökunnalle.

Ilmoitus tietoturvaloukkauksesta

- Arvioitu kesto
- Vaikutukset
- Korjaustoimenpiteet
- Tilanteen toistumisen ennaltaehkäisevät toimenpiteet

5. Muutostenhallinnan prosessit

- Muutostöiden tulee olla suunniteltuja ja huoltoikkunoiden tarpeeksi pitkiä.

Muistettavaa

- Suomen lain edellyttämä välitystoiminnan tietoturva -ohjeistus "Välitystoiminnan tietoturva" on osoitteessa https://www.viestintavirasto.fi/fiverkkotunnus.html.
- Uuden tietosuojalain vuoksi saatatte joutua muuttamaan toimintatapojanne, hankkimaan uusia ohjelmistoja tai laitteita.
- Viestintävirasto tulee kysymään teiltä yksityiskohtaisempia kysymyksiä valitsemistanne tietoturvatoimenpiteistä, joten pitäkää dokumenttinne ajan tasalla.
- Haluamme olla avuksi! Lähetämme teille sähköpostia tulevista muutoksista. Lisäohjeita ja oppaita on tulossa tietoturvavaatimuksista.

Viestintävirasto
fi-verkkotunnus
fi-domain-tech@ficora.fi
p. 0295 390 100
www.viestintavirasto.fi

TRAFICOM
Finnish Transport and Communications Agency