



EUROPEAN MARITIME SAFETY AGENCY

SafeSeaNet system

SafeSeaNet

Procedures and guidelines for the
registration of new web server
certificates

Version 1.0
14-Sept-2004

Document Approval

	NAME	DATE	SIGNATURE
Prepared by:	Y. Hardy	01 Sept. 2003	

Distribution List

COMPANY	NAME	FUNCTION	FOR INFO / APPROVAL

Change Control History

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	01 Sept. 2003	Yves Hardy	First Draft
1.00	14 Sept. 2004	Y. Texier	

Table Of Contents

1. Interoperability

- 1.1 IDA PKI
- 1.2 SSL Protocol
- 1.3 Security Measures
- 1.4 The IDA PKI Implementation
- 1.5 The Actors

2. Procedure to obtain a server certificate

- 2.1 Here are some things you should do before starting enrolling
- 2.2 Obtaining a server certificate from Belgacom E-Trust CA
 - 2.2.1 Enabling your web browser to recognize Belgacom E-Trust as CA
 - 2.2.2 Enabling Belgacom E-Trust Root CA's certificates available on my Webserver/Website.
 - 2.2.3 Order Form and the General Terms and Conditions documents
- 2.3 Certificate Renewal Request

Annex:

- Certification services
- Data to be certified
- Letter of proof

1. Interoperability

This document applies to the TESTA Member States as well as the Internet Member States. In the past, only the Member States connected through TESTA backbone could request a server certificate via our own certificate authority which is represented by Belgacom E-Trust in Belgium.

Since a few weeks ago, the request is also valid for the Member States having decided to interconnect their local (national) web server through Internet in order to exchange the SafeSeaNet XML messages with the central SafeSeaNet web server.

For both types of connection, server certificates are free of charge for the Member States.

1.1 IDA PKI

PKI consists of organisational measures and technical tools that contribute to establishing and maintaining a secure and trustworthy environment for the exchange of information over computer networks.

1.2 SSL protocol

IDA PKI Secure Sockets Layer (SSL) can be implemented on the web server. SSL is a security protocol that:

- Ensures that data are transmitted in a private way;
- Ensures that data are not changed during transmission;
- Authenticate the web server This means the user is guaranteed that the web sever he is accessing is owned by the organisation it claims to be owned by;
- Authenticate the web server (optional) and this ensures the web browser has required access identification

An SSL protected site has to be accessed via the https protocol.

IDA PKI works as a normal PKI (making use of a key pair). The IDA PKI root Certificate Authority (CA) has been signed by a root CA on the Internet (BELGACOM e-TRUST).

A server certificate is there to acknowledge the server's identity (i.e. its domain name or IP address, in this case something **eu-admin.net** or 62.62.x.x), and this identity changes if the server is accessed through TESTA II or through the Internet.

For the exchange of XML messages between the Member States applications and the SafeSeaNet central system, authentication, confidentiality and integrity will be ensured by sending the XML messages using HTTPS and digital certificates (one digital certificate will be issued per Member State application).

From the different alternatives that have been analyzed (HTTPS, S/MIME over HTTP, XML Signature & Encryption), the first one (using HTTPS) has been chosen for its simplicity and cost-effectiveness.

1.3 Security Measures

- **Between the NCA web server and the Central SafeSeaNet Server:**

- ✓ It was decided by the SSN community to use the SSL protocol between the NCA application and the SafeSeaNet Central System.
- ✓ The Directorate Informatics (DI) of the European Commission (where the central SafeSeaNet server will be hosted) offers SSL as a standard solution. The implementation of SSL at the DI follows a set of strict rules.

These rules ensure that the implementation is standard, but it also brings some limitations, such as to end the SSL tunnel at the reverse proxy of the DI for the incoming traffic.

Consequently, simple SSL will be used for traffic between the NCA web server and the Central SafeSeaNet Server.

2-way SSL between the Central Index and the NCA for outgoing traffic.

In other words, this means that you have to configure your web server to work in 2-way SSL.

Please go to section 2.2.2 to get more details about how to deal with the SSL configuration of your web server.

- ✓ The IDA PKI will be used here to produce the NCA's certificate. There will be one IDA certificate for the SafeSeaNet central system for the SSL tunnel of the incoming and outgoing traffic, and there will be one IDA certificate for each NCA application connected to the SafeSeaNet server.

More information about SSL and PKI can be found in the document: "*SafeSeaNet Network & Security document*".

1.4 The IDA PKI Implementation

SafeSeaNet will use the IDA Public Key Infrastructure (PKI) to improve the security of the transactions by mean of SSL tunnels. IDA PKI will provide a generic PKI for the SafeSeaNet Closed User Group (CUG) solving issues related to the certificates interoperability and simplifying their management.

The PKI solution is based on the E-Trust infrastructure of Belgacom and is providing Soft certificates. The PKI service provided by the Commission is only accessible for the Member States connected through the TESTA network.

A certificate will be delivered for the SafeSeaNet Central System in order to permit SSL tunnelling for the incoming traffic from the NCA's application to the SafeSeaNet server.

A certificate will also be delivered for each NCA application of the Member States in order to permit SSL tunnelling for the outgoing traffic from the SafeSeaNet system to the NCA application.

1.5 The Actors

The components in the IDA PKI for SafeSeaNet are:

- The **users**, which request the certificates. *Each Member State should designate a local (national) administrator in charge of requesting, installing and managing the server certificate at national level.*
- The **Local Registration Authority (LRA)** that collects the requests for certifications, and orders the creation of certificates to the CA. It is represented by the **Local Registration Authority Officer (LRAO)**.

In the framework of the SafeSeaNet project, the LRAO will be represented by **Yannick Texier** within the EMSA.

- The **Certification Authority (CA)** that produces certificates, and handles the revocations. The CA of the IDA PKI is the E-Trust infrastructure of Belgacom
- A **Suspension and Revocation Authority Officer (SRAO)**. He will be responsible for all the revocation requests of the CUG users. This will be done by one person of the EMSA

2. Procedure to obtain a server certificate

Web server certificates are digital credentials that reside on a server and set up connection between that server and a client or another server. This secure connection is called a Secure Socket Layer (SSL) session.

With an SSL session established any information sent to or from that web server is encrypted. The web server certificate provides the identity of the web site owner because the Subject name in a server certificate is the DNS name of the server.

Server certificates are designed to protect you and visitors to your site. Installing a server certificate on your server lets you:

- **Authenticate your site.**

A digital certificate on your server automatically communicates your site's authenticity to visitors' web browsers, confirming that the visitor is actually communicating with you, and not with a fraudulent site stealing personal information

- **Keep private communication private.**

Digital certificates encrypt the data visitors that exchange with your site to keep it safe from interception or tampering using SSL technology.

2.1 Here are things you should do before starting enrolling

- **Install a Web Server software**

On your local (national) site, a web server must be up and running prior to launching the procedure for requesting a server certificate. Belgacom E-Trust (also known as Certificate Authority – CA) delivers server certificates for any server compatible with the **X509 v3** standard digital certificates and that are able to make a PKCS # 10 (PEM encoded) electronic certificate request. This covers most of the recent web servers available nowadays.

- **Your Web Server must support the SSL protocol**

The web server must be compatible with the **X509 v3** protocol that enables secure end-to-end electronic data exchange.

- **The DNS domain name must be registered**

Your web server should have a DNS domain name registered in its configuration file. During the generation of the certificate request, you will be prompted to enter some specific information about your server.

This information is very important since it will be the one that will be certified by Belgacom E-Trust CA. The most important part to enter correctly is the name of your server (CN). **It MUST correspond to the registered Web site server name you will protect.**

Indeed, if the real server name does not match the name in the certificate, you will never be able to start your SSL Web Server sessions.

For the Member States connected through TESTA backbone, it has been decided that the full DNS domain name should be registered as follows on the web server of the NCA:

SSN.<Country_Code>.EU-ADMIN.NET

<Country_Code> is composed of two characters of your country (i.e. Belgium: **BE**, Netherlands: **NL**, ...).

For the Internet Member States, you have to make sure that your DNS domain name is well registered and recognised officially on the Internet.

2.2 Obtaining a server certificate from Belgacom E-Trust CA

2.2.1 Enabling your web browser to recognize Belgacom CA

You need to have a browser that enables you to install the Belgacom E-Trust Root CA's certificates. That's why you need at least Netscape Navigator 3.x or higher, Netscape Communicator, or Microsoft 3.0x or higher.

Some parts of this site are secure and Belgacom E-Trust has certified the keys to encrypt the data between this server and your browser.

In order to enable your browser to recognize Belgacom E-Trust as a valid Certification Authority, please choose to accept Belgacom E-Trust as a valid Certification Authority.

<http://www.e-trust.belgacom.be/page.asp?lang=en&s=274>

In the current html page of the E-Trust site (see url above), you have to click on the following hyperlinks:

- Accept the Belgacom Qualified CA Certificate
- Accept the Belgacom Normalised CA Certificate

Two files should be downloaded on your local hard disk. Upon receiving those files, you should click on the hyperlink called: "[Certificate Installation Guide](#)" so that both downloaded files can be installed on your local web browser.

This hyperlink will guide you through a tutorial for the installation of your certificates.

If you encounter any difficulties at this stage of the installation, please do not hesitate to post your queries to the SafeSeaNet Interest Group located on our Circa web site. In the newsgroup, there is a special topic called: PKI for all these open issues.

2.2.2 Enabling Belgacom E-Trust CA's certificates available on my webserver/website

You have to click on the following hyperlink below:

[Http://www.e-trust.belgacom.be/page.asp?lang=en&s=399&ss=129](http://www.e-trust.belgacom.be/page.asp?lang=en&s=399&ss=129)

There, you should read the section called: “***Tested and Recommended Servers***”. On this page, examples are only given for the following web servers:

- ✓ Netscape Enterprise Servers
- ✓ Internet Information Server
- ✓ Apache

If your web server is not listed, please refer to the Internet site of your supplier in order to know how to deal with the installation and the configuration of the SSL protocol. Most recent web servers support the SSL protocol.

The rules remain the same for any kind of web server available on the market.

1. Before being able to use your web server with SSL, you need to generate a private key for it and to require a certificate for your server's public-key.

For this, you will have to generate a (RSA) 1024-bit private key stored in the file “*server.key*” encrypted by a given pass phrase using the triple-des encryption algorithm (des3 option).

2. Then, you will have to generate the certificate request file. You will use the “*server.key*” file generated above and generates the “*server.csr*” file certificate request that has to be copied on a diskette and then sent out by post with the other official documents to the LRAO (Yannick Texier).

Please see section 2.2.3 below to know the information that must be returned to the LRAO and by what means.

Last but not least, after receiving this “*server.csr*” file, Belgacom E-Trust will generate your web server certificate. (Obviously after all the necessary positive verification).

You should receive by the LRAO a file called “*server.crt*” in PEM format which represents your web certificate. Once received, the next step will consist of copying it in the right directory of your web server so that it can enable the use of the SSL protocol for establishing SSL connections.

I would like to draw your attention on the fact that the server certificate that will be generated by Belgacom E-Trust (our Certificate Authority) will only operate on the machine where you have generated the “server.csr” file. The key is unique per server and cannot be copied or even reused on other machines.

2.2.3 Order Form and the General Terms and Conditions

In order to validate your request of server certificate, you have to return to the authorized LRA (Yannick Texier) the following information, namely:

- ❑ Firstly, read the General Terms and Conditions (Object Identification, Number OID: 0.3.2062.9.6.2.4.2.4) that form an integral part hereof and is available on the following Internet site:

<http://195.13.1.46/en/uploads/Q&Ncps-uk-20011101.pdf>
- ❑ The duly completed and signed Order Form, see file called: *server_cert_order_form.doc* enclosed with this document.
- ❑ A signed copy of both sides of your identity card, passport or similarly valid official document
- ❑ A copy of the electronic certificate application on a diskette, since the key pair will have been generated by you (see section 2.2.2 for more details).
- ❑ A copy of the current official memorandum and articles of association of the company/organisation you officially represent, or failing this, an excerpt from the register of companies or any other valid official documents, including the relevant excerpt or a similar document.
- ❑ If the person signs the order form is acting on behalf of the legal representative, the Customer shall submit proof of fact that this person is duly authorized to sign for the legal representative.
- ❑ Proof that the server domain name for the business (see *server_cert_order_form.doc* file where it is referred to as “The Organization”) has been registered and is therefore unique

Important:

All those official documents must be returned to EMSA either by post or they will be handed over by hand during one of the next SafeSeaNet meetings.

If you decide to return the documents by post, you have to send them to the following post address:

**European Maritime Safety Agency
Mr. Yannick Texier
Rue de Geneve, 12
BE 1049 Brussels
Belgium**

Be careful, they cannot be sent to me by email. This way is not valid

2.3 Certificate Renewal Request

A certificate has an expiry date (end of validity). From that date, the certificate should not be accepted any more.

The certificate holder must therefore request renewal of his certificate. The CA reminds him, before the date of expiry, that he will have to issue that request. The subsequent procedure is very similar to the initial request of a certificate.

The lifetime of a certificate is typically one year

CERTIFICATION SERVICES
Certipost (E-Trust)

Standard Certipost (E-Trust) certificate
Web Server Order Form
Version 4.0, Automated Local Registration Authority Operator (LRAO)

Reserved for the Local Registration Authority (LRA)

Customer name:.....

LRA operator (LRAO):

Contract number:

Date of receipt:

Place where the copy of the registration documents is held in safekeeping:

.....

Hereby certifies that this Order Form and the appendixes hereto are duly authenticated and validated.

1 URL

2 URLs

3 URLs

Server certificate

Wildcard server certificate

Signature of the LRAO:

The data that follows shall form an integral part of your digital certificate. Some fields are optional, which means that you are not obliged to have this data certified. Where this is the case, you do not have to fill in the fields concerned. The certificate will have the same probative value regardless of whether these optional fields are filled in.

[illegible]

Information for checking your identity⁵

[illegible]

5

Agreement and signature

I hereby confirm having cognizance of the General Terms and Conditions (OID: 0.3.2062.9.6.2.4.2.4) for Certipost Qualified and Standard E-Trust Certificates, and in particular of my obligations thereunder, and confirm my acceptance thereof by signing this Order Form.

I likewise acknowledge that the authorized LRAs are required, by law, to ask for suspension or revocation of certificates they have issued should there be any indication that: they were issued on the basis of information that is inaccurate or falsified; the information no longer reflects the reality; or the reliability of the data relating to the signature created can no longer be guaranteed.

I hereby confirm that the information given on this Order Form or appended hereto and provided to the LRA, is true, accurate and complete.

Date: City:

Last name and first name(s):

Signature:

LETTER OF PROOF

Ministry of ... + full address
Country X

Date :

Subject : Request for server certificates – SafeSeaNet System – EMSA

.....

I, the undersigned, on behalf of the Organisation (e.g. Ministry of) owning the registration of the server domain name : for which a server certificate is requested, authorise by the present letter Mr. **Yannick Texier** to present himself to the Certipost Certificate Authority located in Brussels – Belgium and to sign the order form on behalf the duly authorised representative of the Organisation (e.g. Ministry of)

Signed,

.....

Stamp of your Organisation (or Ministry)