



Elia B2B E-nomination system - Certificate

Installation guide

Summary	This documents explains what is a Certificate and how to download this certificate for the BRP's using a specific system to connect to Elia B2B E-nomination system
Version	1.0
Date	15/06/2023

Contents

1.	Context: Certificates: Public key – Private key	3
2.	Use of certificates on the Elia B2B E-Nomination system	3
3.	Elia B2B E-Nomination Certificate validity.	4
4.	Get the certificates for your client.....	4
5.	Procedure to create the public certificate file on your server.....	5

The Elia B2B E-Nomination system uses certificates to prove to the Client that he connects to a system that really is the one from Elia.

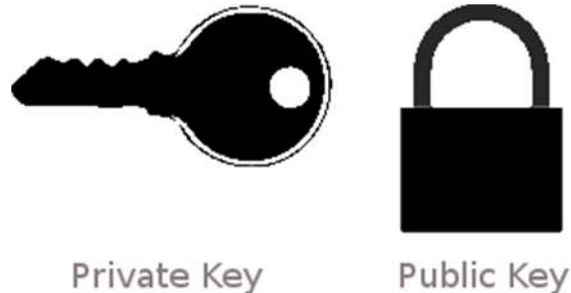
The Client does not need to provide a certificate to Elia. Only Elia has a certificate whose “public” part is used by the Client.

1. Context: Certificates: Public key – Private key

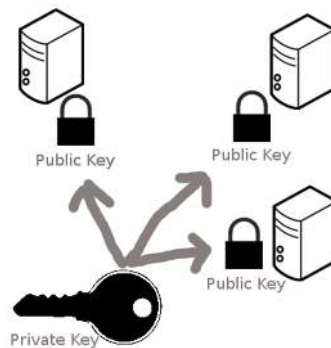
The certificate of the Elia B2B E-Nomination system implements the concept of public and private key

- A public key can be viewed as a lock device.
- A private key can be viewed as an actual key. This is the device used to open the ‘lock’ (Public key) that is stored on the other machine.

Like a regular key, the private key must be kept secret, safe, and out of the wrong hands.



Just like a real-life key system, it is not a problem if there are hundreds of the same ‘lock’ on many systems if the private key stays ... private.



Private and public key on computers

2. Use of certificates on the Elia B2B E-Nomination system

The private key is kept on the Elia B2B E-Nomination system.

But the public key can be distributed anywhere: The Client presents the public key to the Elia B2B E-Nomination system and checks if this private key from the Elia B2B E-Nomination system may “open” this public key.

Because only Elia has this private key, you can be certain that you have a connection with the real Elia B2B E-Nomination system.

The next step is to prove that this set of keys is “trustable”. Your client must request to a “trusting” company that guarantee that you can trust the “Keys”.

In the case of Elia B2B E-nomination system, this “trust” is given by the Company *DigiCert*

(<https://www.digicert.com/>)

3. Elia B2B E-Nomination Certificate validity.

The Elia B2B E-Nomination certificate is valid for 1 year and is normally replaced in March each year.

The exact date of end of validity of the current certificat can be displayed in your browser.µ

4. Get the certificates for your client.

When you are using a web browser to connect to Elia B2C E-Nomination system or Elia B2B E-Nomination system, you have nothing to do: your Web browser automatically verifies this “trust”.

However, if you are using an application running on an isolated server on your local network, this one may not have the right to download the public certificates (the “lock”).

Why?

This is a general rule that servers running on local network are very limited to access to the Internet and download data.

The IT Security department of your enterprise defines this rule:

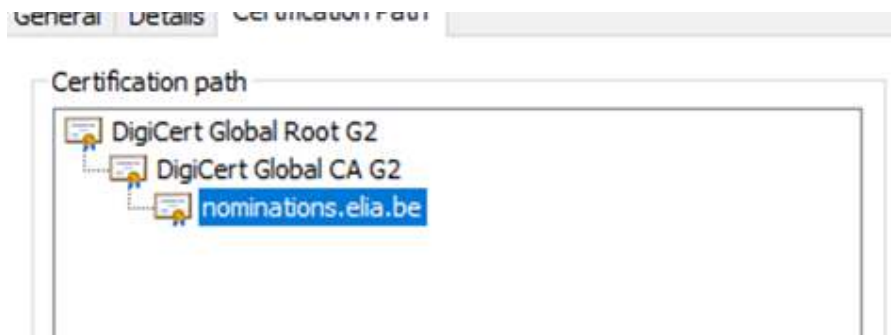
Please ask therefore to your IT Security department.

In this case, when the Elia E-Nomination system certificate is no longer valid and your local server may not get the new certificate, then your server will refuse to contact the Elia B2B E-Nomination system.

To avoid this case, your IT department must install itself the new certificate(s). The certificates are available on:

- the latest certificate from Elia B2B E-Nomination system can be downloaded via the following webpage: <https://nedi1.elia.be/namespaces/public/scheduling/nominations.elia.be.txt>
- The intermediate certificate (Global CA): <https://nedi1.elia.be/namespaces/public/scheduling/DigiCert%20Global%20G2%20TLS%20RSA%20SHA256%202020%20CA1.txt>
- The Global Root DigiCert certificate : <https://nedi1.elia.be/namespaces/public/scheduling/DigiCert%20Global%20Root%20G2.txt>

They respect following hierarchy of certification or “trust”:



You can of course download the certificates DigiCert from the web site of DigiCert ([SSL Digital Certificate Authority - Encryption & Authentication \(digicert.com\)](https://www.digicert.com))

5. Procedure to create the public certificate file on your server.

A certificate is practically a text file with a file extension as “.cer”.

However, many systems refuse to download “.cer” files for security reasons.

Therefore, the Elia public certificates are presented as text files. To get the certificate, you must:

- Click on the address given here above
- Your browser presents a long list of characters or proposes to download this list as a text file: whatever the case, you must have a text file with only this list of characters.
- When you have created this text file on your local network, rename it with the file extension “.cer”.
- Check with your IT security team where to place this file