HAPPI
HEALTHY AGEING
PUBLIC PROCUREMENT OF INNOVATIONS

SUPPLIERS INFORMATION

What is an electronic certificate and how to get yours to bid the HAPPI tender electronically.

To bid a call for tender electronically, rather than by postal way, an electronic certificate is required to sign the offer. The submission of an offer within a “formalized” procedure, as HAPPI, needs the authentication and signature of a responsible person able to engage the company.

The electronic certificate is a digital identity. It’s nominative and as such belongs to a member of a company. The electronic certificate is constituted by three (3) inseparable elements:

1. The information regarding the identity of the holder (name, surname, position, department, email…), its organization (company, association or administration…), the validity period of the certificate, the identity of the certifying authority which generated it, the purpose and scope of the certificate, a link to access to the policy certification of the authority and a link to find the list of the revoked certificates;
2. The private key;
3. The public key.

The GSR (General Security Referential) defines 3 security levels for electronic signatures: * (the less restrictive level), ** and *** (the most secure level). The main differences between these levels concern the required qualification levels for security products used to sign and check digital signatures:

- The elementary level for security level *
- The standard level for security level **
- The reinforced level for security level ***

With regards to the signature application (which computes the hash of the document) and the signature checking module, the GSR recommends a qualification at the standard level for security levels ** and ***.
For levels ** and ***, the signing key is stored in a hardware cryptographic device (for instance, a smart card or a USB key), whereas, for security level *, the key can be stored in a software module.

This certification is provided by a “certifying authority”. The certifying authority is a service provider which creates certificates for users. The certifying authority signs certificates and guarantee their integrity and the information they contain. The authority also ensures the link between certificates and their users as well as the veracity of the enquirer’s information, by doing an examination of the identity documents provided and a “face-to-face” meeting, in certain cases.

To be sure that an electronic certificate is usable to bid on public procurement, you have to choose a certification service provider classified in a trusted list of a member state from the European Union. The European Commission updates a “list of lists” which gives you access to the lists of the other member states. **The certificates delivered by a service provider from a trusted list of a member state are acceptable in all the other countries of the European Union.**

→ Here is the link to find the EU Trusted Lists of Certification Service Providers:
https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

The validity duration of an electronic certificate is two or three years. Its annual cost depends on the associated services, usually it's between 70 Euros and 130 Euros.

It takes between two weeks and one month to get a digital signature certificate, sometimes more. So we recommend you anticipate this procedure. Moreover, it's recommended to order an electronic certificate with high level security to make sure that it will be acceptable by the most public procurement authorities.