



Interreg
Hungary – Slovakia



Co-funded by
the European Union

Guide to digital signatures

Interreg Hungary – Slovakia Programme

Version: 1.10
Publication date: 15/05/2024



History of changes

Version	Date of publishing	Changes
1.00	15/05/2024	Initial version

Content

History of changes	2
Content	3
Introduction	4
The use of electronic signatures	4
Where and how to get electronic signatures?	5
Certificates for electronic signatures	5
Trust service providers	5
The use of trust services.....	6
How to preserve electronically signed documents?	8
Contact details of national trust service providers.....	9
Hungary	9
Slovakia	10

This comprehensive guide is tailored specifically for the lead partners of the Interreg VI-A Hungary-Slovakia Programme. Within its pages, you'll find invaluable legal insights and practical advice regarding the trustworthiness of digital signatures and associated services within the cross-border program. Additionally, discover essential contact information for trusted service providers operating in both Hungary and Slovakia.

Introduction

The European Union encourages its Member States to digitise their public administration processes, enabling citizens to sign official documents electronically. To bring these practices to an international level, the European Union established its own legislative context, providing a framework for the uniform, cross-border use of digital signatures, the verification of their authenticity and the issuance of certificates by authorised trust service providers.

The EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and the Commission Implementing Decision (EU) 2015/1506 provide the legal framework for e-signatures. eIDAS has developed standards regarding e-signatures, qualified digital certificates, electronic seals, timestamps and further authentication mechanisms allowing electronic transactions to be conducted with the same legal standing as paper-based transactions¹ in the European Union. Together with the national electronic identification schemes of the Member States, eIDAS ensures the legal, secure and seamless cross-border interoperability of electronic interactions between citizens, businesses and public authorities.

The use of electronic signatures

Digital (or electronic) signatures are the electronic correspondent of handwritten signatures. However, they shall not be mistaken for handwritten signatures applied to electronic interfaces (e.g., the hand-written signature made on a screen when receiving postal packages). The main idea of electronic signatures is that the signatory is able to change the structure of a document by encrypting it, thus providing its authenticity.

Electronic signatures (e-signatures) are most often based on public key cryptography, which means that each user owns a public key and a private key. The public key is globally unique and serves as an identifier of its user, while the private key is encrypted and can exclusively be used to create digital signatures. The public key can be shared with any other party; however, the private key must be under the sole control of the user (signatory) often presented in a physical form such as a special USB pendrive, usually called eToken. The public key is granted in certificates, which serve as a trustworthy binding to the user's private key.

¹ Article 25 of eIDAS states, that qualified electronic signatures shall have explicitly equivalent legal effect of a handwritten signatures across all EU Member States.



Where and how to get electronic signatures?

Certificates for electronic signatures

In terms of cross-border applicability, two types of e-signatures are acceptable in the EU: the advanced electronic signatures (AdES) and qualified electronic signatures (QES).

As defined in the eIDAS, an advanced electronic signature is an electronic signature which is

- uniquely linked to and capable of identifying the signatory;
- created in a way that allows the signatory to retain control;
- linked to the document in a way that any subsequent change of the data is detectable.

The most commonly used technology able to provide these requirements relies on the use of a public-key infrastructure (PKI), which involves the use of certificates and cryptographic keys.

In the meantime, a qualified electronic signature is an advanced electronic signature, which is:

- created by a qualified signature creation device (QSCD);
- and is based on a qualified certificate for electronic signatures.

Although both types of e-signatures are accepted in the EU, it is highly recommended to use qualified electronic signatures, since qualified e-signature certificates are more secure, offer longer validity periods and are legally acceptable in all EU countries.

In order to sign documents as a natural person, a certificate for electronic signatures is needed. On the one hand, a certificate for electronic signatures is an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. This way, the certificate, usually linked to the signed document, can be used to verify the identity of the signatory and whether the document has been signed using the corresponding private key. On the other hand, qualified certificates for electronic signatures, by following stricter requirements laid down in eIDAS, provide higher guarantees regarding the identity of the signatory and therefore higher legal certainty regarding the created electronic signatures.

Electronic signature certificates are issued to natural persons and legal entities, usually having 2 to 3 years of validity (depending on the provider and the type of certificate). There are three concepts that are key to understanding the eIDAS regulation and its benefits:

- electronic signatures are legal in the EU, regardless of their underlying technology,
- eIDAS defines multiple electronic signature types for use in the EU,
- each type is useful when using e-signature across your business.

Trust service providers

Trust services are electronic services offered by trust service providers, responsible for the creation, verification, validation, authentication and preservation of electronic signatures, seals, time stamps and most importantly, the certificates for electronic signatures.

The certificates for electronic signatures are issued by national trust service providers. Trust service providers are natural persons or legal entities providing digital trust services for natural persons, private companies and public law bodies, assuring integrity of electronic identification

for signatories and services. These service providers are also responsible for storing, signing and issuing digital (electronic) certificates.

The EU-recommended way to comply with eIDAS and minimise the legal risk for businesses is the following of the EU technical standards. In order to ensure that every possible legal and practical precaution has been taken, there are few key aspects which require special attention.

Qualified trust service providers (QTSP) are providers authorised to issue qualified certificates for electronic services and their qualified status is granted by a national competent, supervisory authority.

Member States of the European Union and European Economic Area are responsible for publishing their national Trusted Lists of the national qualified trust service providers. These lists and the QTSPs listed in it, can be browsed in a user-friendly way using the so-called EU Trusted List Browser [Accessible: <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home>].

The Trusted List Browser is helping potential customers to choose the right service provider. A trust service provider is not entitled to provide qualified trust services if they are not on the EU's List of Trusted Lists.

The list of qualified trust service providers operating in Hungary and Slovakia accessible via the following links:

Hungary: <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/HU>

Slovakia: <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/SK>

The contact details of the available trust service providers are included in Chapter 'Contact details of national trust service providers'.

The use of trust services

Once the suitable trust service provider has been chosen, consumers shall request for the selected services, then they will receive a private key for electronic signing and access to the provider's authentication system, through which electronic signature certificates will be generated.

If there is any form of trust service already in use, the validity of the trust service – i.e. qualified /advanced e-signature, timestamp etc. – should also be checked through the eIDAS Dashboard.

Trust services and providers can be checked in three ways:

1. by country as where the providers' headquarters are located, or
2. by the type of trust service,



DIGITAL eSignature / eIDAS Dashboard / Browse / Trusted Lists / Search by type of service

What type of service are you looking for? step 1/2

☐ Check all

Qualified trust services

<input type="checkbox"/> Qualified certificate for electronic signature	<input type="checkbox"/> Qualified certificate for electronic seal	<input type="checkbox"/> Qualified certificate for website authentication
<input type="checkbox"/> Qualified validation service for qualified electronic signature	<input type="checkbox"/> Qualified preservation service for qualified electronic signature	<input type="checkbox"/> Qualified validation service for qualified electronic seal
<input type="checkbox"/> Qualified preservation service for qualified electronic seal	<input type="checkbox"/> Qualified time stamp	<input type="checkbox"/> Qualified electronic registered delivery service


Non-qualified trust services

<input type="checkbox"/> Certificate for electronic signature	<input type="checkbox"/> Certificate for electronic seal	<input type="checkbox"/> Certificate for website authentication
<input type="checkbox"/> Validation service for electronic signature	<input type="checkbox"/> Generation service for electronic signature	<input type="checkbox"/> Preservation service for electronic signature
<input type="checkbox"/> Validation service for electronic seal	<input type="checkbox"/> Generation service for electronic seal	<input type="checkbox"/> Preservation service for electronic seal
<input type="checkbox"/> Time stamp service	<input type="checkbox"/> Electronic registered delivery service	<input type="checkbox"/> Non-regulatory, nationally defined trust service
<input type="checkbox"/> Undefined type		

3. or through uploading an electronically signed document or a certificate.

DIGITAL eSignature / eIDAS Dashboard / Browse / Trusted Lists / Search with signed file

Upload a file (either a signed file or a certificate file)



Drag file here or click to [select file to upload](#).

Maximum upload file size: 10 Mo.

The search does not perform signature(s) or trusted list(s) validation. This feature only retrieves the trust service(s) associated to the signature(s) on the signed file.

In order to validate the signature(s), a signature validation feature is proposed by the [DSS Demonstration WebApp](#).

After contracting a trust service provider, the process of e-signing documents can be started in a few days at the most. Depending on the agreed service package, signature can be created through the trust service provider's signature creation device such as an application, or a special webpage, or a physical device (eToken) or a combination of those. When the document has been electronically signed, the document is usually stored in ASiCe data container file, but other formats including CAdES, XAdES and PAdES are also acceptable.

As previously mentioned, every e-signature certificate has a validity of no more than 3 years. Most types of certificates are validated to the time of validation (i.e., for the present time), electronic signature certificates are validated to the time when the electronic signature was created. To determine the time of when an e-signature was created on a document easily and safely, timestamps are recommended, otherwise controlling and monitoring certificate revocation statuses might prove complicated.

How to preserve electronically signed documents?

The long-term validity of electronically signed documents is also an important factor.

A time stamp is a trusted third-party confirmation that the document existed at a given time i.e. when document was signed. It is important to validate the signing certificate up to the time of the signature creation (as it has to be valid only at the time of the signature creation). Therefore, when using electronic signatures, it is highly important to use timestamps – ideally qualified timestamps.

By using (qualified) timestamps the long-term preservation process (over 3 years) of e-signed documents can also be prepared sufficiently. There are two ways to preserve the electronically signed documents before the end date of the validity period:

1. certificate renewal,
2. archiving.

Renewal can only be considered before the expiry date of the certificate. The expiry date could be elongated by another 2-3 years after refreshing the certificate. However the process of renewal will possibly have to be repeated in case of longer project implementation period.

The easiest and safest way of preserving e-signed documents is through electronic archiving. Without going into technical details, archiving means that electronically signed documents are preserved on a protected cloud run by a trust service provider and automatically receive long-term archiving timestamps ensuring the validity of a signed document for as many years as needed. The cloud can be accessed by the user after authentication, this way signed documents can be up- or downloaded in easy and safe way.

Finally trust service providers are also offering solutions to the **delicate situation of expired certificates**. Keeping in mind that **after the expiry date the certificate loses its validity**, there are ways to check if the signed document has been modified. However, these processes are expensive in general, especially when multiple documents are concerned.

Contact details of national trust service providers²

In this chapter, the trust service providers relevant from the point of the view of lead partners are listed.

Hungary

In Hungary, the supervisory body responsible for the list of qualified trust service providers is the National Media and Infocommunications Authority (NMHH).

Microsec

Microsec Micro Software Engineering & Consulting Company Limited by Shares is a qualified trust service provider actively operating in Hungary, providing the following trust services:

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified preservation service for qualified electronic signature
- Qualified preservation service for qualified electronic seal
- Qualified time stamp
- Certificate for electronic signature
- Certificate for electronic seal
- Certificate for website authentication
- Time stamp service
- Non-regulatory, nationally defined trust service.

Contact details:

- Address: 13 Ángel Sanz Briz Road, Budapest, HU
- Telephone: +36 1 505 4444
- E-mail: info@microsec.com
- Customer Service Hours: Monday-Friday: 8:30AM-4:30PM
- Website: <https://www.microsec.hu/>

NETLOCK

NETLOCK Informatics and Network Privacy services Limited Company is the second qualified trust service provider operating in Hungary.

NETLOCK provides the following trust services:

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified preservation service for qualified electronic signature
- Qualified preservation service for qualified electronic seal
- Qualified time stamp

² Please note that the list of providers may be subject to updates. You are kindly asked to visit the links provided in chapter 'Trust service providers' in your country.

- Certificate for electronic signature
- Certificate for electronic seal
- Certificate for website authentication
- Time stamp service
- Non-regulatory, nationally defined trust service

Contact details:

- Address: 17. Hungária krt., 1143 Budapest, HU
- Mailing address: 1439 Budapest, Pf. 663
- E-mail addresses: kerelmek@netlock.hu, Product support: support@netlock.hu, Sales: ajanlat@netlock.hu
- Website: <https://netlock.hu/>

Slovakia

The Slovak National Security Authority is responsible for the protection of classified information, cryptographic services, trust services and cyber security.

Ardaco, a.s.

Ardaco provides the following trust services:

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified validation service for qualified electronic signature
- Qualified validation service for qualified electronic seal
- Qualified time stamp

Contact details:

- Address: Polianky 5, Bratislava, SK
- E-mail address: support@ardaco.com
- Website: <https://tsp.ardaco.com/en>

Brainit.sk, s.r.o.

Brainit provides the following trust services:

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified preservation service for qualified electronic signature
- Qualified preservation service for qualified electronic seal
- Qualified time stamp

Contact details:

- Address: Veľký Diel 3323, Žilina, SK
- E-mail address: info@brainit.sk
- Website: <https://brainit.sk/en/home/>

Disig, a.s.

Disig provides the following trust services:

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified preservation service for qualified electronic signature
- Qualified preservation service for qualified electronic seal
- Qualified validation service for qualified electronic signature
- Qualified validation service for qualified electronic seal
- Qualified time stamp

Contact details:

- Address: Zahradnicka 151, Bratislava, SK
- E-mail address: disig@disig.sk
- Website: <http://eidas.disig.sk/en/>

Viasec, s.r.o.

Viasec provides the following trust services:

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified time stamp

Contact details:

- Address: Borska 6, Bratislava, SK
- E-mail address: support@psca.sk
- Website: <http://www.pscs.sk/>