



IDENTITY VERIFICATION METHODS

Version 1.1

Valid from 01.10.2024

Version History		
Date	Version	Changes
27.10.2021	1.0	Initial Document
01.10.2024	1.1	Removal of the option for video identification via Agent.

Prior to the issuance of a Qualified Certificate for Electronic Signature or Electronic Seal, ADACOM verifies the identity of the Subscriber using one of the methods described below.

The required identification documents per qualified certificate type are described [here](#).

1. Identity verification with physical presence

The Subscriber's identity is verified with his/her physical presence either:

- by the Citizen's Service (KEP) or notary public
- by ADACOM's Local Registration Authority (LRA).

2. Remote identity verification with Qualified Certificate for Electronic Signature or Electronic Seal

If the Subscriber already has a valid Qualified Certificate for Electronic Signature or Electronic Seal, he/she can digitally sign the required identification documents and send them via email to lra@adacom.com or upload them through his/her profile on ADACOM's AQS portal.

The Subscriber must make sure that his/her Qualified Certificate has been initially issued based on physical identity verification.

Certificate renewal using this method is allowed only once. The Subscriber's identity will need to be re-verified by physical presence in the next certificate renewal.

3. Remote ID verification/proofing

The Subscriber's data is collected through an automated video call without the presence of an ADACOM agent; the agent checks this data at a later time. If the automated video call is unsuccessful for multiple times, the Subscriber has the option to be identified by physical presence either by the Citizen's Service (KEP) or notary public or by ADACOM's Local Registration Authority (LRA).

For more information about this method, please see [here](#).