digicert + QuoVadis

Face-to-Face Identity Verification by 3rd Party

Important Note:

If the certificate request is for a personal/organisation certificate and the application is performed remotely (i.e. the applicant will not present themselves in person at a DigiCert + QuoVadis office) then this "**Face-to-face Identity Verifcation by 3rd Party**" form should be completed and signed by (tick which one applies):

☐ A Public Notary (including a Notary stamp on this form)

☐ A Qualified Solicitor/Lawyer (cross-check in the relevant Solicitor/Lawyer database)

The 3rd Party confirms that:

- the applicant personally appeared to verify his/her identity.
- the personal details presented below correspond with the presented ID (passport or Government issued ID card)
- the attached copy of the passport or Government ID card is identical to the original document and has been notarised accordingly.
- the 3rd party accepts that DigiCert + QuoVadis will perform a cross-check by phone/e-mail to verify the authenticity of the notaries stamp/signature, and to contact the 3rd party via email for confirmation of the notarized form's authenticity. The 3rd party agrees to actively cooperate in this verification process before this document can be relied upon.
- any security features present on the ID document and supporting documents shall be thoroughly examined and validated in accordance with the applicable regulations and standards.
- the 3rd party hereby confirms that the following requirements, as specified in ETSI TS 119 461 (see Appendix A for details), have been met during the identity validation process.
- the 3rd party further confirms that the type of ID validated aligns with the ID types deemed acceptable per the provided source.
  Please refer to "Acceptable Sources for QuoVadis Authentication of Identity v1.3"
  https://www.quovadisglobal.com/repository/

Note: This form is ONLY to be completed by a public notary or a qualified solicitor/lawyer.

Name of Applicant (as it appears on ID document):	
Type of Identification Document:	☐ Government issued ID card ☐ Passport
Identification Document number of applicant:	
Nationality:	
Issuance Date of ID:	
Expiry Date of ID:	
Issuing Authority of ID:	
Issuing Country of ID:	

ACKNOWLEDGMENT

Stamp Here (If applicable)

I hereby certify that the person above personally appeared before me to verify their identity. The personal details presented correspond with the presented ID and I confirm that the attached copy of the passport or Government ID card is identical to the original document.

Witness by .
Verifier Signs Here

Date: __/_____/_____ Time: :_____ AM/PM

Print Name	Organization / Employer
Telephone	Email:
Address:	Membership/qualified number:

Appendix A: ETSI TS 119 461 Requirements

VAL-8.3.1-09	*The authenticity and integrity of the evidence shall be verified.*
VAL-8.3.1-10	*If the evidence has explicit security features/elements these elements shall be verified.* *NOTE 2: This need not be all security elements of e.g. a physical identity document. A selection of elements sufficient for assessing that the evidence is genuine can be applied.*
BIN-8.4.1-01	*The identity proofing process shall verify that the applicant is the legitimate evidence holder.*
BIN-8.4.1-02	*The identity proofing process shall verify that the evidence is in the possession of the applicant.* *NOTE 1: For the evidence types existing eID means and existing digital signature means, no specific binding requirements are needed since the validation of the evidence also verifies the binding. This is under the assumption that only the applicant can use the eID means or digital signature means.* *NOTE 2: For the supplementary evidence types trusted register, proof of access, and documents and attestations, no specific binding requirements are needed. If the binding of the authoritative evidence (identity document, eID means, or digital signature means) to the applicant is successful, and the supplementary evidence is validated and identifies the same person, the supplementary evidence is considered bound to the applicant.*
BIN-8.4.4-01	*The registration officer shall compare the face photo obtained from the applicant's identity document with the applicant's physical appearance, either from the applicant's the physical presence or from a video sequence.*
BIN-8.4.4-03	*The registration officer shall perform a morphological analysis according to a defined feature list. EXAMPLE 2: As recommended by the FISWG Facial Comparison Overview and Methodology Guidelines [i.20] and the corresponding checklist in [i.21].*
BIN-8.4.4-04	*The registration officer shall be allowed to spend sufficient time for the face comparison. NOTE 1: In general, an assessment according to the FISWG Facial Comparison Overview and Methodology Guidelines [i.20] can be sufficient, while a review according to the same document can be required at least for remote identity proofing.*
BIN-8.4.4-05	*The registration officer shall have tools available to magnify images to view details.* *NOTE 2: With physical presence and physical identity document, this can be a magnifying glass to use for the face image printed on the document. If face images are used, computerized tools are assumed.*
VAL-8.3.3-16 [CONDITONAL]	*If validation of identity documents is done manually, and the process is performed with physical presentation of the document, the registration officer should have available tools to enhance the reliability of the validation. EXAMPLE 5: Magnifying glass and ultraviolet lamp.*
VAL-8.3.3-17 [CONDITONAL]	*If validation of identity documents is done manually, and the document is used in a remote identity proofing process, the registration officer shall have available tools to enhance the reliability of the validation. EXAMPLE 6: Computerized tool to zoom in on details of the document.*
VAL-8.3.8-03	*If a document or attestation is in physical form or digital form rendered for human validation, the identity proofing process shall verify that the document presented is visually equal to the expected visual appearance.*

VAL-8.3.8-04	*If a document or attestation is in physical form and the document type contains security elements, these security elements shall be verified to the extent required by the identity proofing context.*

This form should be sent together with the completed Certificate Application Form and the copies of the ID to QuoVadis TrustLink B.V.

Address: **QuoVadis TrustLink B.V.**
Nevelgaarde 56 noord
3436 ZZ Nieuwegein
The Netherlands

e-Mail: nl.validation@digicert.com
Tel: +31 (0) 30 232 4320

digicert + QuoVadis