

QuoVadis Advanced Plus Certificate Application Form

For readability please complete this form online and print and sign it (if signed with a pen-ink signature)

Type of certificate required		USB token		HSM
Duration of certificate (1 / 2 / 3 year)				

1.1 Applicant/Certificate Holder Details

First Name(s)	
Last Name	
Title (Mr, Mrs, Dr)	
e-Mail Address	
Organisation	
Organisation Unit (Optional)	
Pseudonym (Optional)	
Home address of Certificate Holder	
Direct Number for Certificate Holder	
Mobile Number	
Nationality	
Passport/Driving Licence Number	
Passport/Driving Licence Country of Issue	
Year of Birth	
Company Address	
Company Switchboard Number	
Company Registration Number	

All data will be handled and stored as highly confidential according to the requirements of relevant Data Protection laws.

By accepting this certificate I confirm that:

- all declarations made in relation to the information contained in the certificate are true and accurate;
- reasonable measures will be taken to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate;
- the certificate will be used strictly in compliance with the QuoVadis certificate policy (CP/CPS) and Certificate Holder Agreement;
- the certificate will immediately be declared invalid if the certificate details are no longer correct or the private key is lost, stolen, or potentially compromised;
- I agree with the publication of the certificate;
- I accept the QuoVadis Certificate Holder Agreement and "General Conditions for use of QuoVadis Certificates" below; and
- I have read the University of Queensland Privacy Statement on page 4 of this form.

Name of Applicant/Certificate Holder	Signature of Applicant	Date
--------------------------------------	------------------------	------

Confirmation of ID for the Certificate Application

Important Note:

This "Confirmation of the ID for the Certificate Application" form should be completed and signed by an authorised Sub-LRA Agent Administrator, AusCERT Administrator, Justice of the Peace, Public Notary, solicitor or other authority acceptable to QuoVadis. The notarising party confirms that:

- the applicant personally appeared to verify his/her identity
- the personal details correspond with the presented ID (passport, driving licence or Government ID card)
- the attached copy of the passport or Government ID card is identical to the original document

Note: This form is ONLY to be completed by the Person confirming the ID (sub-LRA Agent Administrator / AusCERT Administrator / Solicitor / Justice of the Peace, Public Notary)

For readability please complete this form online and print and sign it (if signed with a pen-ink signature)

Name of Certificate Applicant _____

ID reference number of Certificate Applicant
(eg. Passport/driving licence number) _____

Name of Person confirming ID _____

Tel. number of Person confirming ID _____

Organisation of Person confirming ID _____

Job Title of Person confirming ID _____

Stamp of Person confirming ID (if applicable) _____

Signature of Person confirming ID _____

Date and Time _____

Send the completed Certificate Application Form and the notarised copies of the ID to AusCERT in a secure fashion. We recommend putting a strong password on the PDF and using Cloudstor (<https://cloudstor.aarnet.edu.au/sender/>) to securely upload the file to AusCERT, using cs@auscert.org.au to receive the notification. Contact AusCERT out of band on +61 7 3365 4417 to provide the password. Delete the PDF from Cloudstor when the file is downloaded.

Instructions

Suitability

QV Advanced Plus Certificates are in the Adobe Approved Trust List and are suitable for digitally signing PDFs and providing a high level of assurance to relying parties that the PDF content is authentic. QV Advanced Plus Certificates can only be issued on to an approved Secure Signature Creation Device, such as a cryptographic USB token (such as SafeNet iKey 4000 or above).

Certificate Application documents

The following documents are required:

- Application form signed by the Certificate Applicant (page 1)
- Form called 'Confirmation of ID for the Certificate Application' (page 2)
- Copy of passport or Driving Licence of the Applicant/Certificate holder

General Naming Conventions

The name must clearly identify the certificate holder in humanly understandable form. Certificates may only be issued in the correct name of the certificate holder. Anonymous certificates are not allowed. The name of the certificate holder must be conclusive. A name may only be used multiple times if the certificate holder has multiple certificates with different key usages. In the allocation of pseudonyms, similarities with a natural or legal person or organizational unit must be excluded. Allowed characters are: a-z A-Z 0-9 / space.

Naming Conventions for Natural Persons

Titles can only be used if they are stated in an official identification document that includes photograph (i.e., Dr. Peter R. Smith).

Naming Conventions for Legal Persons and Organizations

Legal persons or organizations can only be represented by a natural person.

Pseudonyms

The common name of a Pseudonym begins with the word PSEUDONYM (i.e. cn = PSEUDONYM : Accounting).

Certificate Acceptance

A certificate is accepted by the certificate holder if the certificate is used, or no report is made to QuoVadis within 10 days of issuance. Incorrectly issued certificates must be reported to QuoVadis without delay.

Revocation

Certificates may be revoked via email, telephone, or in handwriting to QuoVadis in accordance with the CP/CPS and Certificate Holder Agreement. Suspensions are not allowed (as per the CP/CPS). Once declared invalid, certificates cannot be renewed or extended.

Obligations of the Certificate Holder

The Certificate Holder agrees to the obligations documented in the QuoVadis Certificate Holder Agreement which is available from: <http://www.quovadisglobal.com/repository>

Additional Information

The QuoVadis website (www.quovadisglobal.com) provides additional information and documents relating to users' rights and obligations, including:

- QuoVadis Certification Policy CP/CPS
- QuoVadis Relying Party Agreement
- QuoVadis Certificate Holder Agreement

Send the completed Certificate Application Form and the notarised copies of the ID to AusCERT in a secure fashion.

We recommend putting a strong password on the PDF and using Cloudstor (<https://cloudstor.aarnet.edu.au/sender/>) to securely upload the file to AusCERT, using cs@auscert.org.au to receive the notification. Contact AusCERT out of band on +61 7 3365 4417 to provide the password. Delete the PDF from Cloudstor when the file is downloaded.

Further Assistance, revocation service (7x24x365), Support

QuoVadis Online Security Ltd, Rhoades Mill, Main Road, Sibsey, Boston, Lincolnshire, PE22 0TW

www.quovadisglobal.co.uk <https://support.quovadisglobal.com>

Tel. +44 (0) 333 666 2000 au.support@quovadisglobal.com

Fax +44 (0) 333 666 3000

The University of Queensland Privacy Statement

Your Personal Information and Personal Information regarding the Applicant's relevant employees, agents and contractors, is being collected for the purpose of administering and performing (including providing services in relation to) the contracts and arrangements related to this form ('Purpose').

For this Purpose, this Personal Information may be shared with and used by The University of Queensland (trading as AusCERT), QuoVadis and their related entities, contractors and affiliates and PKI infrastructure auditors. Some of these persons are likely to be outside of Australia and your information may be disclosed to and used and stored by them outside of Australia. Because The University of Queensland is a statutory body, your Personal Information may also be shared with Queensland Government departments or agencies, Queensland Government Bodies, Non-Government Organisations and/or Commonwealth, States or Territories in connection with the Purpose. Third parties may have access to this Personal Information where it is required to be used or disclosed in, or relation to the use of, digital certificates and/or the services associated with providing and/or using digital certificates. Personal Information will not be otherwise used or disclosed without consent, except where and as permitted or required by law.

For further information please consult the UQ Privacy Management Policy at:

<http://www.uq.edu.au/hupp/index.html?page=24999>.