Subscriber Guide

Trust/Link Enterprise

https://tl.quovadisglobal.com
Version 2.2

Contents

Notes

QuoVadis has made efforts to ensure the accuracy and completeness of the information in this Guide. However, QuoVadis makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. QuoVadis assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained in this document.

Further, QuoVadis assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner.

This document may describe Trust/Link Enterprise features and/or functionality that are not present in your specific service agreement. QuoVadis reserves the right to make changes to any information herein without further notice.

Version Control

This is version 2.2 of this document. Major changes introduced in this version of Trust/Link Enterprise include:

- For SSL certificates, Trust/Link automatically duplicates the Common Name Subject DN field (CN) in the first DnsName SAN field (DnsName).
- Trust/Link enforces re-validation timeframes for Subject information for Business SSL (39 months) and EV SSL (13 months).
- Trust/Link supports the phase out of SSL certificates with internal server names and Reserved IP addresses by November 1, 2015.
- Trust/Link enforces a minimum key size of 2048 bits.

Access and Support

Trust/Link Enterprise is a managed PKI that allows organisations to easily issue and manage SSL and End User digital certificates. The system uses templates and automated workflows to ensure proper authentication of users and certificate content.

New SSL Subscribers must be invited by an Administrator to work with specific Organisations on the Trust/Link Enterprise Account.

Existing Subscribers may access their customised *Subscriber Services* Account using their password at https://tl.quovadisglobal.com/.

Important Note: A Subscriber e-mail address may only be associated with a single Account on Trust/Link. If a Subscriber requires access to multiple Accounts (for example, an external consultant working for different Trust/Link customers), then separate email addresses or aliases must be used.

Support

QuoVadis provides support for the Trust/Link application, validation of new Organisations or Domains, as well as assistance with the installation of SSL certificates on servers.

Subscriber questions relating to the processing of individual SSL certificates should be directed to an Administrator on the Account. QuoVadis Support will not intervene in individual certificate requests.

For assistance, we recommend that you use the Support form at *Support* → *Contact Support* or file a ticket at the QuoVadis support website at http://support.quovadisglobal.com/.

You may also contact our local support desks for assistance in local business hours:

Bermuda:	+1-441-278-2810
Netherlands:	+31 (0) 30 232-43-20
Switzerland:	+41-71-272-6060
UK:	+44 (0) 333 666 2000

You may also review our Support Knowledgebase at http://support.quovadisglobal.com/ for detailed instructions on how to generate CSRs or install SSL certificates on various platforms.

PKI Widgets

Useful SSL tools may be found at https://pkiwidgets.quovadisglobal.com/. These include:

- *Verify SSL Installation* – Confirm that the correct and valid SSL certificate is installed and properly trusted on your server.
- *Generate CSR* – Create a test Certificate Signing Request.
- *Decode CSR* – Read any Certificate Signing Request.
- *Decode Certificate* – Read any PEM-formatted digital certificate so you can view its contents.
- *Convert Certificate Format* – Convert your digital certificates to different formats such as PEM, DER, and P7B.
- *Match Certificate & CSR* – Confirm if your CSR matches your SSL certificate.
- *CSR Command Tools* – Wizards to create command lines to generate CSRs in Java, Microsoft Exchange, and OpenSSL.

Introduction

You have been given responsibility to act as a Subscriber on QuoVadis' Trust/Link.

A Subscriber is the person who submits SSL Certificate Requests to the Trust/Link system, and later installs the approved SSL certificate. Subscribers have password access to a personalised *Subscriber Services* webpage where they can submit new Certificate Requests as well as manage existing SSL certificates associated with them.

When a Subscriber submits a Certificate Request, it is automatically routed to the appointed Administrator for processing. Trust/Link uses pre-validated filters for the various Organisations and Domains on the Account, and Administrators have the ability to modify the incoming Certificate Requests during the approval process.

Subscriber Responsibilities

A Subscriber (aka Certificate Holder) has certain responsibilities under the QuoVadis user agreements including, but not limited to:

- The Certificate Holder has provided/will provide accurate and complete information, both in the Certificate Request and as otherwise requested by QuoVadis. The Certificate Holder consents to QuoVadis retaining such registration information in accordance with the QuoVadis data retention policy;
- The Certificate Holder will take all reasonable measures necessary 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(s) (and any associated access information or device – e.g., password or token);
- The Certificate Holder will not install and use the certificate(s) until it has reviewed and verified the accuracy of the data in each certificate;
- The Certificate Holder will install the certificate only on the server accessible at the domain name listed on the certificate, and/or to use the certificate solely in compliance with all applicable laws, and solely in accordance with this Certificate Holder Agreement;
- If the certificate requires the use of a Secure Signature Creation Device (SSCD), the Certificate Holder will only use the certificate with such a device that has either been supplied by or approved by QuoVadis;
- If the Certificate Holder generates their keys, then they will generate them in a secure manner in accordance with industry leading practices;
- The Certificate Holder will promptly cease using a certificate and its associated Private Key, and promptly request that QuoVadis revoke the certificate, in the event that: (a) any information in the certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Certificate Holder's Private Key associated with the Public Key listed in the certificate;

- The Certificate Holder will promptly cease all use of the Private Key corresponding to the Public Key listed in a certificate upon expiration or revocation of that certificate.

The QuoVadis Certificate Holder Agreement and other important policy documents may be found at http://www.quovadisglobal.com/repository.

Setting up a Subscriber Account

Subscribers must be invited by an Administrator to have access to request SSL certificates in the name of one or more Organisations on an Account.

When you receive a Trust/Link invitation by email, you will be required to select a secure password that will enable you to access *Subscriber Services* on an ongoing basis at https://tl.quovadisglobal.com/.

Trust/Link Subscriber invitations expire after 7 days. Your Administrator (named in the invitation email) can reinvite you at any time.

Important Note: Administrators may add or remove Organisations from your Subscriber Services Account on an ongoing basis.

Your Account shows certificates that have been assigned to you, even if you no longer have access to issue new certificates for the corresponding Organisation.

Your Administrator may also assign certificates created by you to another Subscriber, in which case they will no longer appear in your Account.

Changing Passwords

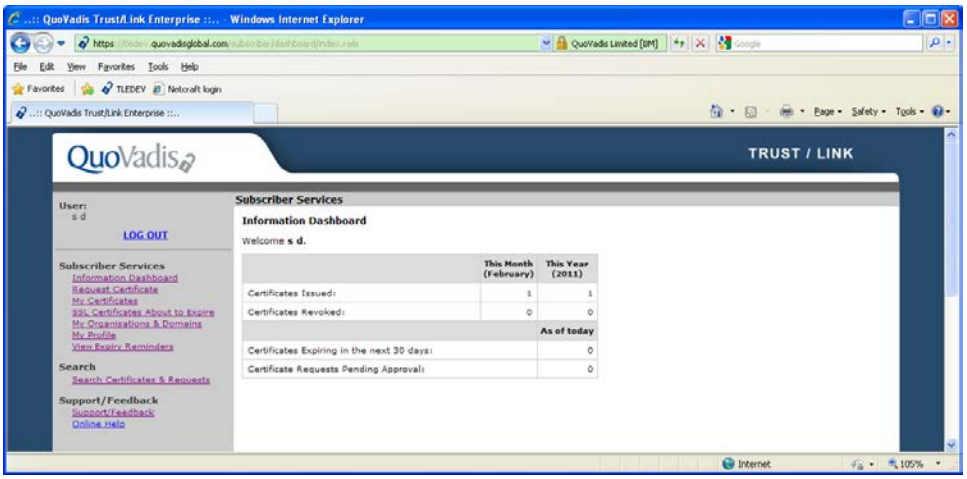
You may change your password at any time by selecting *My Profile*.

Important Note: If you forget your password, you may select the "Forgotten your Password?" link on the login page. Trust/Link will send a notification to your registered email address allowing you to reset your password. Alternatively, you may contact an Administrator for your Account to reset your password for you.

Using Subscriber Services

Once authenticated in *Subscriber Services*, you will see the "information dashboard" featuring an overview of your:

- SSL certificates issued and revoked (this month and this year)
- Certificates expiring in the next 30 days
- Certificate Requests pending approval



Request Certificates

To request a new SSL certificate use the *Request Certificates* section of Trust/Link.

- From the first pulldown menu, select the Organisation for which you would like to request an SSL certificate.
- Then, using the second pulldown menu, select the Policy Template you would like to request.
- Finally complete the Certificate Request form including the Certificate Signing Request (CSR) that you have created on your web server or device.

When you hit submit, Trust/Link will show the details of the CSR that you submitted and allow you to make changes or add additional SAN fields.

Once your Certificate Request is complete, it will be automatically sent to the appropriate Administrators on your Account for approval.

Important Note: Trust/Link will accept Certificate Requests for Domains that have not been pre-validated for the Account. However, these orders may not be approved until an Administrator has requested that QuoVadis validate and enable the Domain.

Important Note: Trust/Link uses pre-approved templates for Organisation details that are included in SSL certificates. Therefore, the information in your final SSL certificate may differ from the CSR you originally submitted.

Trust/Link sends automated email notifications to confirm that the Certificate Request has been received, and to advise of changes in its approval status.

Important Note: QuoVadis provides support for the Trust/Link application, validation of new Organisations or Domains, as well as assistance with the installation of SSL certificates on servers. Subscriber questions relating to the processing of individual SSL certificates should be directed to an Administrator on the Account. QuoVadis Support will not intervene in individual certificate requests.

IP Addresses and Internal Hostnames

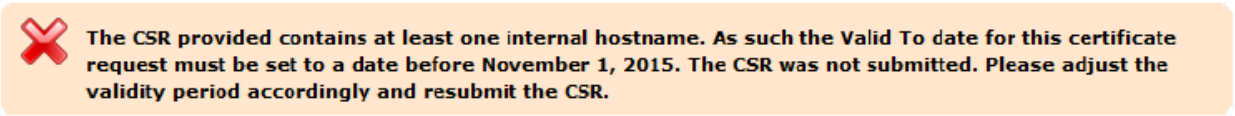
The CA/Browser Forum Baseline Requirements (section 9.2.1) deprecates the use of “non-unique names” in publicly-trusted SSL. There are growing concerns that this practice may create vulnerabilities which allow attackers to perform "man in the middle" attacks and eavesdrop on secure connections. QuoVadis recommends the use of Fully Qualified Domain Names (FQDNs) which are unique to the Account/Organisation in SSL certificates.

Important Note: IP addresses and Internal Server Names may only be included in Business SSL certificates; their use is not allowed in EV SSL or End User certificates.

Trust/Link will not allow Business SSL to be issued/renewed including Reserved IP addresses or Internal Server Names with validity after November 1, 2015.

Internal Server Names and External IP addresses must be specifically approved in Trust/Link. Private IP Network addresses are automatically processed by the system.

If a Subscriber submits a certificate request including Internal Server Names or Reserved IP addresses for a validity period extending beyond November 1, 2015. Trust/Link provides an alert and requests that the user amend the “Valid To” date.



EV Status

For an extended Validation SSL to be issued, both the Organisation and Domain must be approved for EV use. This is noted by the tag “[EV]” after the applicable entities on your *My Organisations and Domains* page.

SSL Key Sizes

The security of information protected by cryptography depends on the strength of the keys. In accordance with leading industry practices and standards, all QuoVadis Extended Validation (EV) SSL and QuoVadis Business SSL certificates MUST be generated using a 2048 bit key size. The QuoVadis Trust/Link Enterprise

application will automatically reject any Certificate Requests for these policies where the key size is less than 2048 bits.

SAN Fields

You may add or delete SAN (SubjAltName) fields to the certificate, even if they are not included in the CSR you submit.

- Remember that, if you use the SAN fields, you must repeat the initial Common Name as a SAN.
- Only DnsName and Rfc822Name entries may be used.
- All SAN entries are subject to the same Domain filters as the Common Name.

Important Note: Trust/Link automatically repeats the value of the Common Name Subject DN field (CN) in the first DnsName SAN field (DnsName) for all SSL certificates. (If this is already included in the submitted Certificate Request, Trust/Link simply moves the repeated value to the first DnsName field).

Confirmation Messages

Whenever actions are committed to Trust/Link, the system provides immediate onscreen feedback on the success of the action. In addition, for most actions the system provides confirmation/notification emails to the affected users.

Action was successful.

Action was completed but requires attention from a superior user on the Account. For example, when a Certificate Request is submitted for an unapproved Domain, Trust/Link accepts the order. However, the order may not be processed until the order is amended or that Domain has been approved.

Action was unsuccessful. Trust/Link provides a reason for the error to allow you to make corrections.

CSR and SSL Installation Help

QuoVadis provides detailed instructions on how to generate CSRs or install SSL certificates on various platforms at http://support.quovadisglobal.com/. You may also contact our local support desks for assistance in local business hours.

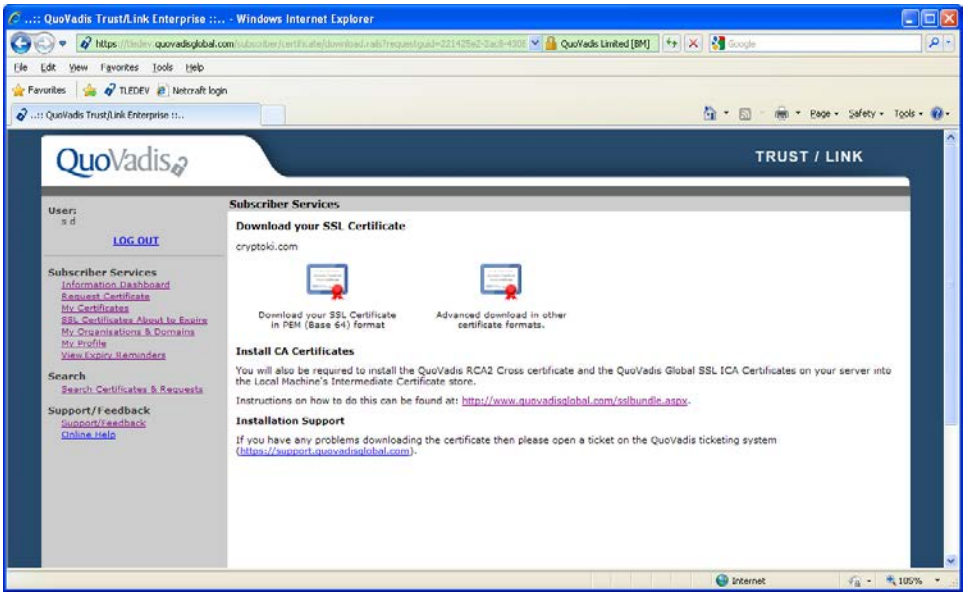
Other Navigation

- The *My Certificates* section shows a list of all your pending Certificate Requests and currently valid certificates.
    - When notified by email, you may log into *Subscriber Services* to download your certificates, as well as to perform lifecycle management (such as renewal and revocation).
- The *Certificates About to Expire* section provides a listing of all your SSL certificates that are due to expire in the next 30 days, with a link to commence renewal.
- The *My Organisations and Domains* section shows the Organisations and associated Domains that have been assigned for your use.
- The *My Profile* section allows you to update your Subscriber details and change passwords.
- The *View Expiry Reminders* section allows you to enter information about an existing certificate (not issued by Trust/Link) so that the system will remind you before expiry. This is useful when transitioning existing SSL to QuoVadis.
- The *Search Certificates & Requests* section allows you to review your larger pool of certificates including those that have previously expired or been revoked.

Picking up an SSL Certificate

When a Certificate Request has been approved, Trust/Link will send an email to you. Follow the link and enter your standard Account password to download the certificate from *Subscriber Services*.

In addition, the Subscriber may visit *Subscriber Services* → *My Certificates* to view and manage all certificates for which they are responsible.



Once logged in, you have the option of downloading the certificate in the following formats:

- PEM (base64 encoded)
- PEM with Chain
- DER (binary encoded)
- PKCS #7 (P7C format)

You may download an SSL certificate up to 25 times, after which Trust/Link disables the download.

Revoking an SSL Certificate

Your Organisation has the authority and responsibility to revoke SSL certificates when necessary. Both Administrators and Subscribers may revoke certificates using Trust/Link. Reasons for revocation include, but are not limited to:

- The Certificate Holder or Certificate Owner requests revocation of its certificate;
- The Certificate Holder indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
- QuoVadis obtains reasonable evidence that the Certificate Holder's Private Key (corresponding to the Public Key in the certificate) has been compromised, or that the certificate has otherwise been misused;
- QuoVadis receives notice or otherwise become aware that a Certificate Holder violates any of its material obligations under the Certificate Holder Agreement;
- The Certificate Holder fails or refuses to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity;
- QuoVadis determines, in its sole discretion, that the Private Key corresponding to the certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content that is harmful, malicious, hostile or downloaded onto a user's system without their consent;
- QuoVadis receives notice or otherwise become aware that a court or arbitrator has revoked a Certificate Holder's right to use the domain name or other information listed in the certificate.
- QuoVadis receives notice or otherwise becomes aware of a material change in the information contained in the certificate or if QuoVadis determines that any of the information appearing in the certificate is not accurate;
- A determination, in QuoVadis' sole discretion, that the certificate was not issued in accordance with the terms and conditions of the CP/CPS;
- QuoVadis' right to issue certificates by law, regulation, or policy expires or is revoked or terminated;
- QuoVadis' Private Key for that certificate has been compromised;
- Such additional revocation events as QuoVadis publishes in its CP/CPS or deems appropriate based on the circumstances of the event; or
- QuoVadis receives notice or otherwise becomes aware that a Certificate Holder has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of QuoVadis' jurisdiction of operation.

Revocation Steps

You may revoke certificates you requested directly from *Subscriber Services → My Certificates*.

1. Select the certificate you wish to revoke
2. Select the Revoke button
3. Select the reason for the revocation (from the standard list) and complete the revocation.

Alternatively, you may request an Administrator who manages the Organisation for which the certificate was issued do the revocation for you.

In some cases, your Account may be configured for "second authorisation", in which case your revocation will not complete until it has been approved by an Administrator.

Searching for your Certificates

Your *My Certificates* page shows only your current pending Certificate Requests and valid SSL certificates.

You may view all the certificates assigned to you – including expired and revoked certificates – using *Subscriber Services → Search.*

Important Note: Administrators on the Trust/Link system have expanded Search and reporting capabilities across the Account, including the ability to view audit logs associated with user and certificate activity.

As some Subscribers using Trust/Link may have many certificates, the system provides sortable tables. If you select column headings that are underlined, you may sort the table based on that column, either in ascending or descending order.

Subject ▲	Date	Organisation	Authorisation

Renewing an SSL Certificate

Trust/Link will send you reminder emails leading up to the expiry of your SSL certificate. These emails are sent 30 days, 14 day, and 1 day before expiry.

The *SSL Certificates Expiring* section provides a listing of all your SSL certificates that are due to expire in the next 30 days, with a link to commence renewal.

If you renew a certificate early, the remaining validity period for the existing certificate will be added to the replacement certificate's validity period.

With the renew functionality, the contents of the previous certificate is copied onto the renewal Certificate Request for your convenience.

All renewals of QuoVadis certificates require that a new CSR be submitted.

Important Note: Trust/Link enforces periodic revalidation of Organisation and Domain details for SSL certificates in compliance with the CA/B Forum Baseline Requirements. For Business SSL, Organisation details and Domain control must be revalidated within 39 months of initial approval, and for EV SSL within 13 months of initial approval.

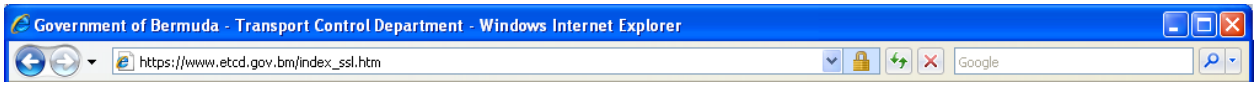
If you submit a certificate request whose details require validation, Trust/Link will accept the order but it will only be approved when revalidation is complete.

Adding Expiry Reminders

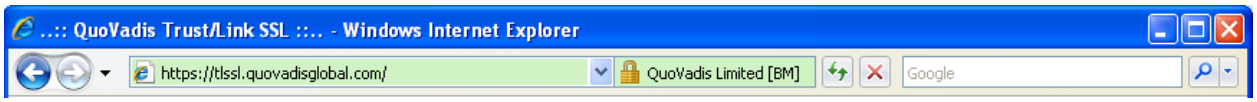
Using *View Expiry Reminders* you can enter the expiration dates of existing SSL certificates issued by any CA so that Trust/Link notifies you 30 days before expiry. This function is useful when transitioning existing certificates to QuoVadis.

SSL Background

Trust/Link may be used to issue the following SSL certificate classes according to the relevant QuoVadis CP/CPS.



Business SSL follow standard "Organisation validated" policies. They are suitable for a wide range of authentication and encryption needs. Business SSL may include fully qualified Domain names, internal server names, or Reserved IP addresses. They are available in 1, 2, or 3 year validity periods.



Extended Validation SSL follow the "EV Guidelines" promulgated by the CA/B Forum. EV certificates follow more detailed verification procedures and are suitable for high-profile web sites where authentication is important. EV certificates include Fully Qualified Domain Names only. EV certificates trigger the special EV indicators in browsers that support EV. EV certificates are available in 1 or 2 year validity periods.

All QuoVadis SSL support the use of SAN fields.

Glossary of Terms

Account

The Account is the company or organisation that has contracted with QuoVadis to use Trust/Link.

Administrator

Additional Administrators may be designated by Organisation within the Account. In addition, various permissions may be assigned allowing work balancing and control.

Domain

A registered Domain Name that includes the labels of all superior nodes in the Internet Domain Name System (DNS). For example: example.quovadisglobal.com. Within Accounts enabled for SSL, Domains may be pre-validated for use with specific Organisations. If EV SSL certificates are desired, QuoVadis must conduct additional vetting and flag those Domains as "EV eligible".

Internal Server Name

A Server Name (which may or may not include an unregistered Domain Name) that is not resolvable using the public DNS. For example: mail, exchange, exch01, example.local, or localhost.

Organisation

Within the Account, multiple Organisations may be defined representing companies, subsidiaries, or locations. Trust/Link allows Organisations to be pre-validated to allow efficient processing of Certificate Requests, and accurate use of organisational details in certificates.

Primary Administrator

The Primary Administrator is specifically identified in the Trust/Link services agreement for an Account and is the first user set up in the Account. The Primary Administrator must occupy a position of corporate responsibility appropriate to the role, and may delegate their authority by adding additional users to the Account. The Primary Administrator enjoys universal roles and permissions on the Account.

Reserved IP Address

IANA assigns the following IP blocks as Reserved IP addresses for private networks. SSL certificate requests including Reserved IP addresses are automatically processed for validity periods ending before November 1, 2013. All external IP addresses as well as Internal Server Names must be specifically approved by QuoVadis.

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Subscriber

A Subscriber is the person who submits Certificate Requests to the Trust/Link system, and later installs the approved SSL certificate.

Validation

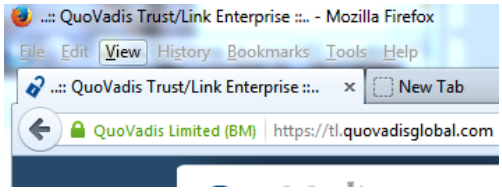
Certificate Authorities have a responsibility to ensure that 1) personnel involved in issuing an SSL certificate are authorised to act on behalf of the Organisation named in the certificate, 2) that the Organisation has the right to use the Domain in the certificate, and 3) that any Organisational details in the certificate are correct. Trust/Link uses a combination of workflows and templates to ensure this validation occurs.

Appendix 1: AusCERT Certificate Policies

The following certificate policies are available to organisations (Sub-LRAs) which use the AusCERT Certificate Service provided by QuoVadis.

SSL Certificate Policies:

1) QV Business SSL 10 SAN G2 – this is an organisation-validated certificate (QuoVadis term them Business SSL) with up to 10 SAN (Subject Alternative Name) fields. Most certificates are for a single DNS name (e.g. www.auscert.org.au) but some will require additional DNS fields. An example could be a single certificate covering www.auscert.org.au plus auscert.org.au. A second example could include www.auscert.org.au plus auscert.org.au plus secure.auscert.org.au plus remote.auscert.org.au.
2) QV Business SSL 20 SAN G2 – this is an organisation-validated certificate with up to 20 SAN fields. No wildcards can be included in the SAN.
3) QV Business SSL 50 SAN G2 – this is an organisation-validated certificate with up to 50 SAN fields. No wildcards can be included in the SAN.[1]
4) QV Business SSL Wildcard G2 – this is an organisation-validated wildcard certificate. An example would be *.auscert.org.au. In this example the certificate could be applied to any sub-domain for example www.auscert.org.au, secure.auscert.org.au, remote.auscert.org.au. But a certificate for *.auscert.org.au can't be used on a server with the domain smtp.mail.auscert.org.au. With a wildcard certificate you can install it onto multiple servers if you wish.
5) EV SSL 10 SAN G2 – this is an Extended Validation SSL certificate with up to 10 SAN (Subject Alternative Name) fields. No wildcards can be included in the SAN. The EV SSL certificate displays the name of the organisation that the certificate represents in green next to the address bar. EV SSL certificates are the best certificate to use for sites where you want users to be confident in the legitimacy of the website. See example below:



6) EV SSL 20 SAN G2 – this is an Extended Validation SSL certificate with up to 20 SAN fields. No wildcards can be included in the SAN.
7) AusCERT Grid Server – this is a special Grid Server certificate (EU Grid PMA), which are publicly trusted and IGTF accredited. These should only be used in specific circumstances related to grid

[1] If you require a certificate with more than 50 SANs and up to 100 SANS, this can be arranged by sending an email to au.support@quovadisglobal.com.

computing and are not for general use. The certificates have special fields that are specific to Grid resources.

Certificate issuing process for all SSL certificates

Steps 1 and 2 only need to be done where the subscriber who needs to obtain an SSL certificate is not already registered with TrustLink as a subscriber for your organisation.

1) The Agent Administrator logs into Trust/Link and clicks on Invite Subscriber and completes the form to invite the Subscriber to register on TrustLink.
2) Once a Subscriber has registered themselves on TrustLink, the Subscriber can then follow the following process to request/obtain SSL certificates below.
3) The Subscriber logs into the Trust/Link portal and clicks on 'Request Certificate'
4) They complete the request form ensuring they select the correct type of certificate and the duration that they require. They paste their CSR (Certificate Signing Request) into the online form. Typically, this is a text file generated by the webserver for the site they require the certificate for. For more details about generating CSRs, refer to the QV Knowledgebase: https://support.quovadisglobal.com/KB/c7/csr-generation.aspx
5) The Subscriber goes through a validation check where the CSR is decoded and they confirm the details that they require in the certificate. They can add SAN fields at this time. They then submit the request.
6) All of Agent Administrators for the Subscriber's organisation (the Sub-LRA) which have notifications enabled are notified by eMail that a Certificate Request is pending from the Subscriber.
7) One of the Agent Administrators will login to the Trust/Link portal and go to the Process Certificate Requests tab (or click on the link in the eMail notification sent to them.
8) The Agent Administrator will be able to view the details of the certificate. Options available are 'Update' if changes need to be made to the request or 'Approve'. There is also an option to 'Reject' the Certificate Request. If the certificate request is for a domain that has not been added or approved to the TrustLink system this will generate a warning error. In which case, you will need to add the domain and wait until it is approved before proceeding to approve the certificate request. If you encounter problems with getting the domain approved, submit a support request to QuoVadis https://support.quovadisglobal.com/
9) If the request is approved by an Agent Administrator for the Subscriber's organisation[2], the certificate will be issued by QuoVadis and the Subscriber will be notified by eMail that their certificate is ready to download.

[2] Your account has been set up by default to require only one Agent Administrator to approve each SSL certificate request. It can be configured to require at least two Agent Administrators to approve each SSL certificate request. Please contact cs@auscert.org.au, if you require this change.

End User Certificate Policies:

Under the QuoVadis TrustLink system End Users are also called Registrants.

1) Codesigning cert – this is a Code Signing certificate. These are certificates which are used to secure code by applying a digital signature.
2) AusCERT grid end user – these are individual authentication certificates issued to users who are accessing Grid resources. The have special fields in specific to Grid resources and should not be used for general use. Before these certificates can be issued, the organisation (Sub-LRA) Agent Administrator must have a face-to-face meeting with the Certificate Applicant to verify their identity and identity documents. There is an application form for this type of certificates which must be completed **before the Invite End User/Registrant form is submitted.** The completed form, which is available for download from http://cs.auscert.org.au/ must be sent to QuoVadis by submitting a ticket online to https://support.quovadisglobal.com/Main/Default.aspx.
3) Standard CN SE – these are Standard-class End-user certificates issued to individuals for Authentication, Signing and Encryption purposes. They can be used for S/MIME (signing and encrypting eMails) as well as authenticating users for specific projects (e.g. 2-factor authentication to specific web portals/applications).

Certificate issuing process for all End User certificates

- The issuing process for all End User certificates is initiated by an Agent Administrator of the organisation (Sub-LRA). This needs to be done **each time** an End User needs to obtain a new End-User certificate for themselves as part of their organisation. Before initiating the End User invitation, the Agent Administrator contacts the End User via telephone to obtain a **shared** secret question and answer or a unique **shared** passphrase (which is case sensitive) that the End User chooses. This will be needed by the End User to download the certificate later. Examples of shared secret questions are:
    - What is the manufacturer and model of the first car you owned?
    - What are the last four digits of your staff number?
- The Agent Administrator logs into Trust/Link and clicks on Invite End Users
- The Agent Administrator selects the Individual Invitation Form (unless doing a CSV file bulk upload for multiple certificates for multiple End-User certificates)
- The form is broken down into three parts. The first part includes the details that go into the certificate itself – this will be the End Users details (e.g. Name, eMail). The second part is the Registrant Information – this collects more details about the Registrant – most of this information may be duplicated form the first part.

- The third part is the Registrant Authentication and includes the shared secret question and answer or passphrase supplied by the End User. For "ID Type Audited" field, select "Client KYC[3] Record" for "Standard CN SE" certificates. For Grid End User certificates you will need to select one of the other methods of verifying identity listed in the drop down list (after complying with the grid end user identity verification steps referred to above).
- The End User is then eMailed an invitation for the certificate. They click on a link in the eMail and it takes them to a secure web page where they input their eMail address and answer to their shared secret question or previously supplied passphrase.
- They are then prompted to create a password for the certificate and confirm the details for the certificate content.
- They then submit this form and the certificate will be issued. They receive a second eMail with another link where they are routed to a secure webpage. They input the password they created in the step above, and they are then able to download the certificate. It is important this step is done from the same browser and computer the End User will use to access the certificate. It is recommended that the certificate be backed-up so it may be exported to a different computer and a different browser, if required.

[3] KYC means Know Your Customer. It just means the Registrants are employees or contractors of the organisation (Sub-LRA) which is inviting and authorising them to obtain an End User certificate.