

Root Hosting

Public Key Infrastructure (PKI) technologies and software are widely understood and available, leading some organisations to operate their own certification authority (CA) operations. However, when the PKI hierarchy carries significant liability, organisations may seek the assistance of a proven provider like QuoVadis to enhance the trust of their Root.

The security of the Root is paramount, since it is used to sign all certificates issued by the underlying PKI. If the integrity of the Root were ever to legitimately be called into question, all certificates and protections provided by the PKI would also be suspect. In a live commercial environment that could have dire consequences.

Some of the threats to Roots include unauthorised use, modification, copying, theft, or loss/destruction (intentional or otherwise) of the Root private key.

As a commercial PKI provider, with over a decade of experience and subject to audits and accreditations for this specialist area, QuoVadis has the facilities and expertise to properly generate Root keys and maintain the Root through its operational life.

QuoVadis advises our Root customers on the appropriate Certification Policy/Certification Practise Statement (CP/CPS) that will govern the use of the PKI, including the Root and its subordinates.

We also design and fully document a formal CA Root Key generation ceremony to help assure the non-refutability of the integrity of the Root keys and, in particular, the private signing keys. Additional policies document the ongoing control and use of the Root.

As an independent trusted third party, QuoVadis offers the assurance that the Root was generated in a trusted manner, and that the PKI was founded on a reliable basis.

Going forward, by placing the Root with QuoVadis, the customer and its users gain security that the Root may only be operated in the prescribed manner, and may not be neglected nor compromised through operational shortcuts.

QuoVadis and its partners have extensive experience in the selection of appropriate PKI software and hardware security modules (HSM) as well as their configuration. This includes custom CA software that runs entirely within HSM frameworks for specific Root applications.

QuoVadis Deliverables

QuoVadis has extensive experience in Root activities in compliance with PKI standards such as WebTrust and ETSI.

Documentation

- CP/CPS
- Root Key generation ceremony

Key Generation

- Physically secure environment
- Trusted personnel
- Multiple person control
- Appropriate PKI software configuration, algorithm, and key size
- Trusted devices (HSM) meeting FIPS 140-2 level 3 or EAL 4, appropriately implemented

Key Storage, Backup, and Recovery

- Controls for access and use
- Maintain equivalent control for backups as for primary
- Orchestration and documentation of subordinate signing events

