QuoVadis Group

EUGridPMA Update

September 2014

Overview

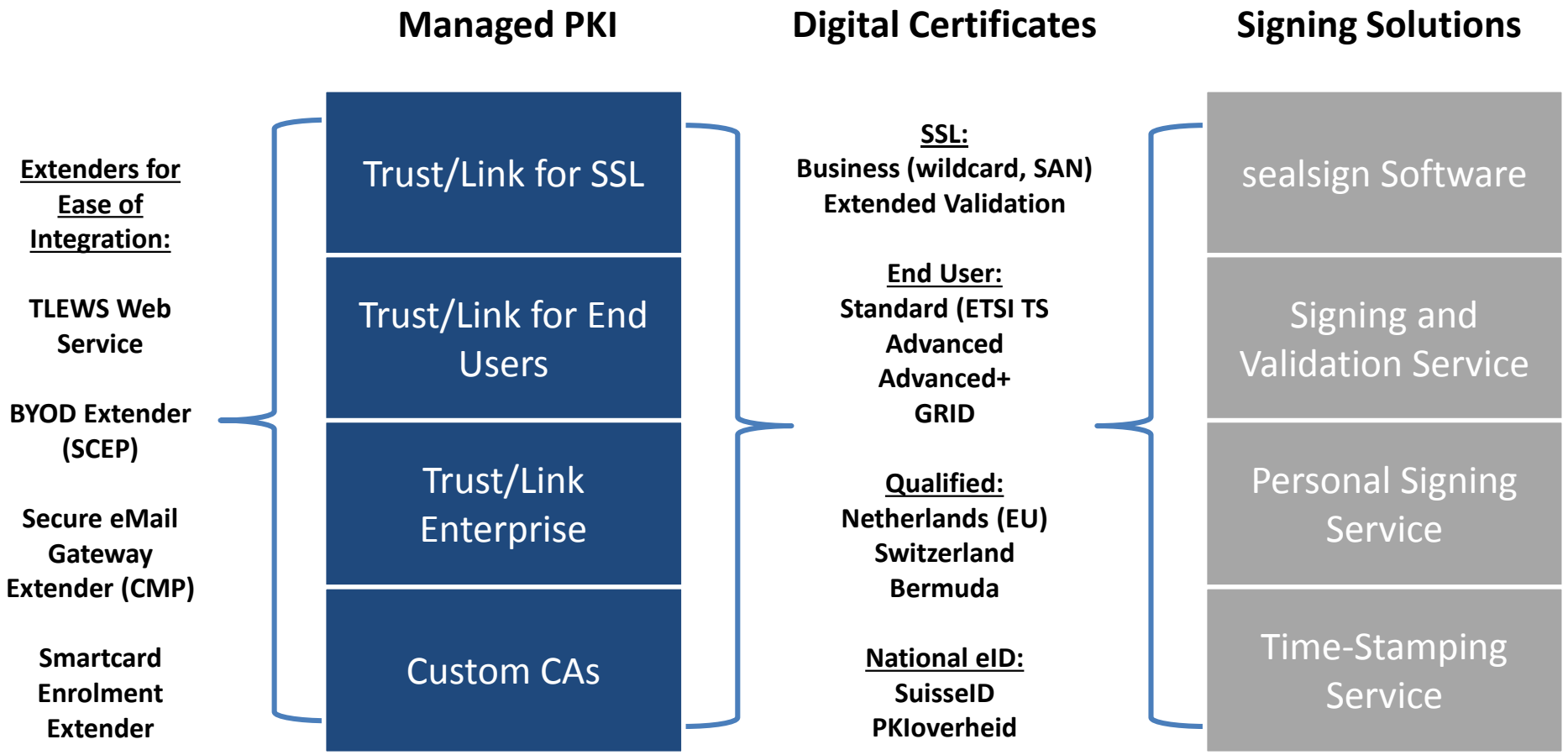
- Founded in 1999 in Bermuda, with particular focus providing PKI managed services to multinational organisations
  - More than 3,500 customers
  - Operations in Bermuda, Switzerland, Holland, Belgium, and UK
  - Provide CA services to several NRENs (Managed SSL, Grid)

- Leadership in major segments of CA business
  - 11th largest SSL CA and 6th largest EV SSL CA according to Netcraft (out of 80+ trusted CAs)
  - Leading Qualified CA in Europe; multiple jurisdictions
  - Significant expertise in digital signature solutions

- Roots are trusted in all major software including mobile devices
  - Including distribution of next-generation SHA256 roots

- More international audits and certifications than any other CA

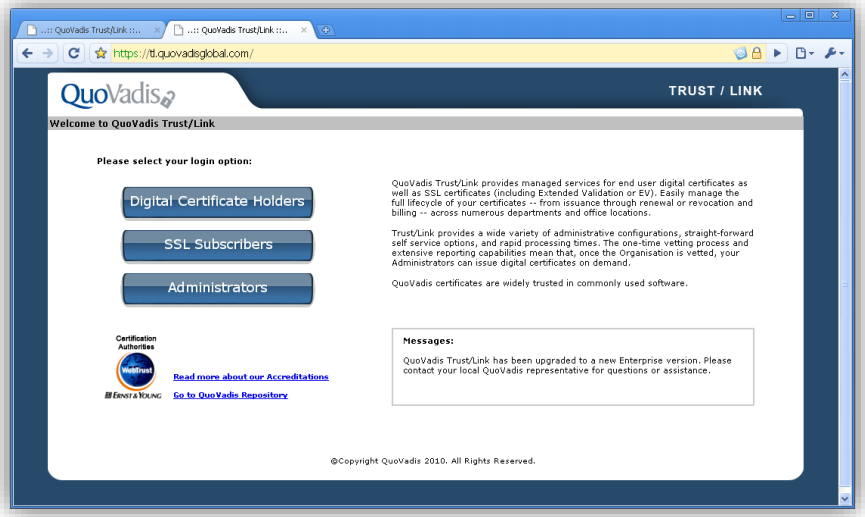
QuoVadis Offering



Managed PKI

Managed PKI service to easily manage the full lifecycle of digital certificates, from issuance through renewal or revocation, across numerous departments and locations.

- Easy-to-use Web console for rapid rollout
- Dependable costs, no client investment in CA infrastructure or operations
- Lifecycle management of all certificate types (SSL or End User)
- Real time issuance of certificates
- Easily scalable to large numbers of users
- Highly customizable by groups within account
  - Delegated administration, with granular roles and flexible workflows
  - Tailored signup forms and notification emails
  - Certificate templates
  - Reports and audit
- Optional API for integration with enterprise systems



Trust/Link

Signing Solutions

- sealsign software
  - In-house deployment allowing addition of digital signatures and validation to existing systems, such as e-invoicing and e-archiving
- Signing and Validation Service
  - “Signing as a service” allowing customers to rapidly deploy mass signing on existing systems, with signing platform and certificates securely hosted by QuoVadis
- Personal Signing Service
  - “Signing as a service” allowing individual users of enterprise applications and online transaction websites to digitally sign PDF documents from any web-enabled device
- Trusted Time-Stamping Service
  - Adds independent verification of when a transaction occurred
- Adobe and Microsoft
  - Automatically trusted signatures in Adobe Acrobat and Microsoft Office

EUGridPMA

- QuoVadis has been involved with the EUGridPMA since 2009.
  - QuoVadis are accredited by the EUGridPMA according to the “Classic X.509 CAs with secured infrastructure” Authentication profile.
  - The “QuoVadis Root Certification Authority” Certificate is included in the IGTF Distribution of Authority Root Certificates.

- QuoVadis seeks to become an independent/direct EUGridPMA member (previously we were “proxied” under SWITCH).
  - QuoVadis will perform a self-audit in accordance with "Guidelines for auditing Grid CAs version 1.0" (GFD-I.169) and the relevant Authentication Profiles. The results of this audit will be presented at a future EUGridPMA meeting.

- QuoVadis seeks to be accredited under the "Profile for Member Integrated X.509 Credential Services with Secured Infrastructure“ (MICS).

Summary of our Audits and Accreditations

- The accreditations maintained by QuoVadis include:
  - WebTrust for Certification Authorities
  - WebTrust for Extended Validation
  - WebTrust for Baseline Requirements
  - Swiss Qualified Certification Services Provider
    - SuisseID and Qualified Time-stamping Authority
  - Netherlands Qualified Certification Services Provider
    - PKIoverheid and eHerkenning
    - ISO/IEC 27001
  - Belgium Qualified TSP
  - Bermuda Authorised Certification Services Provider

SWISS QUALIFIED CERTIFICATION SERVICE PROVIDER

Certification Authorities WebTrust Ernst & Young

Certification Authorities WebTrust Extended Validation Ernst & Young

Certification Authorities WebTrust BR - SSL

BSI ETS 010

TRUST AUTHORISED BERMUDA CERTIFICATION SERVICE PROVIDER

WebTrust for Certification Authorities

- WebTrust for CAs is the dominant commercial standard to assess CAs
- Managed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).
- The annual WebTrust audit of QuoVadis is performed by Ernst & Young.
- To obtain and retain the WebTrust seal, the CA must meet all the WebTrust for CAs Principles and Criteria.
- The following areas are included in the scope of every WebTrust engagement
  1. CA Business Practices Disclosure
  2. Service Integrity
     - Key Life Cycle Management Controls
     - Certificate Life Cycle Management Controls
  3. CA Environmental Controls

Certification Authorities

WebTrust

Ernst & Young

WebTrust for EV/ Baseline Requirements

- WebTrust for Extended Validation (EV) is used to assess a CA's controls against the CA/B Forum "Guidelines for the Issuance and Management of EV Certificates". Created to provide basis for differentiating certificates which have stronger authentication standards. Only suitably accredited CAs may issue EV SSL certificates.

- WebTrust for Baseline Requirements (BR) is used to assess a CA's controls against the CA/B Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates". A successful WebTrust for BR audit is required by the Browsers, such as Mozilla.

- The annual WebTrust for EV/ BR audits of QuoVadis are performed by Ernst & Young.

- The EV Guidelines/ BR require quarterly Internal Audit testing of at least 3% of SSL certificates issued.

Swiss
Qualified Certification Services Provider

- ZertES is the Swiss digital signature law. Lays out requirements for electronic signature to achieve same legal status as hand written signature.
- ZertES accreditation is granted by the Swiss Accreditation Service (SAS) and the Swiss Federal Office of Communications (BAKOM) based on an audit by KPMG
- The following areas are included in the scope of the QuoVadis audit:
  - The Certification Service Provider (CSP) requirements of ZertES, the accompanying VZertES regulatory provisions and also the more detailed Technical and Administrative Regulations
  - Requirements for Time Stamping Authorities (TSA) based on ETSI TS 102.023 and ETSI TS 101.861
  - Requirements for Qualified Electronic Signatures according to ETSI TS 101.456, ETSI TS 101.862 and SR943.032.1

SWISS QUALIFIED CERTIFICATION SERVICE PROVIDER

Netherlands
Qualified Certification Services Provider

- PKIoverheid: the PKI designed for trustworthy electronic communication within and with the Dutch government. QuoVadis have PKIoverheid Issuing CAs under Dutch Government Root.
- QuoVadis is certified by BSI against the following requirements:
  - ETSI TS 101 456 (Qualified Certificates) and ETSI TS 102 042 (for PKIoverheid SSL/EV);
  - Dutch Digital Signature Law (Dutch Besluit Elektronische handtekeningen);
  - The following PKIoverheid Program of Requirements:
    - Part 3a (Personal certificates, Organisational)
    - Part 3b (Services/SSL) - based on Baseline Requirements
    - Part 3c (Citizen)
    - Part 3e (EV SSL) – this is based on the EV Guidelines but has additional requirements
- QuoVadis are supervised by the Netherlands Authority for Consumers and Markets (ACM). QuoVadis are also 'audited' by Logius and ACM.
- QuoVadis is "supervised" as a CSP in Belgium by FOD Economie on the basis of the Dutch accreditation.

Questions

Barry Kilborn: b.kilborn@quovadisglobal.com

Stephen Davidson: s.davidson@quovadisglobal.com