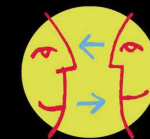




Presentation Trust.Wider®

Protecting your identity
Protecting your freedom
in a connected world



KEYNECTIS



Available as *SAAS or Licence*

- Digital Identity Protection

- PKI
- CMS
- KMS
- e-Passport / e-ID

- Security of documents and transactions

- On-line subscription BtoC
- E-Billing
- Document workflow (PDF)
- E-Commerce (SSL)
- Signature and encryption of e-mails
- Time Stamping



- Protection of infrastructures

- VPN IPSEC
- Terminal Certification (EAC, SCEP)
- Secure Extranets (SSL)



Objectives of Keynectis' *TrustWider* solution

- Why *TrustWider* ?
 - Allow internal PKI to be recognized also by external organizations
 - Enable automatic recognition by large spread IT solutions (Microsoft, Mozilla/Thunderbird, Safari,...)
 - Propose neutral third party services necessary for interoperability (publication, validation)
- The solution targets :
 - Organizations that want to open their PKI to external partners
 - Software companies that want to include Bridge CA functions (OEM)
 - Trust Services Providers (TSP) that want to include this offer in their portfolio of value added services



KEYNECTIS' Public CAs

- Class 3 Primary CA 2019 Qualified Certificates
- Class 2 Primary CA 2019 User & Server Certificates
for SSL, S/MIME
- Class 1 Primary CA 2020 User Personal Certificates
- Class 3P Primary CA 2019 Validation Authority
- Class 3TS Primary CA 2019 TimeStamping Authority



Available Services by *TrustWider*[®]

- Usages :
 - Secure inter company eMail Communication
 - Private SSL
 - Validation Authority
 - Easy Certificate Deployment





Services proposed by *TrustWider*

- Standard Services :
 - Seamless Recognition within browsers and e-mail clients
 - IE (IE 5 and upwards) / Outlook / Outlook Express
 - Mozilla / Firefox / Thunderbird
 - Safari
 - Opera
 - Publication of the Root CA CP
 - Publication of the ARL
 - Annual Audit of the associated CA and delivery of the TrustWider certificate (based on ETSI 101 456)
- Enhanced Services:
 - LDAP Publication LDAP
 - OCSP Validation Authority



Conditions of *TrustWider* eligibility for a CA

- The CA shall have a depth (Basic Constraints) of 0 : direct certificate emission
- The PC of the CA shall force at least a 2 channel authentication mechanism
- The CA private key shall be operated on a HSM FIPS 140 level 3 or Common Criteria EAL4+ under control of at least 2 distinct roles.
- The CA private key shall have back-up
- The CA validity period and the certificate validity period shall be the end date of the KEYNECTIS Root.
- The CA shall be submitted to an anual *TrustWider audit*



TrustWider: Key Advantages for you

- *Add true value to your PKI services*
- *Guarantee the recognition **of your organization's certificates***
- *Measure and drive **the quality and security of your PKI according to a public reference***
- *Benefit of the security level and the expertise of Europe's N°1 Trust Services Provider : KEYNECTIS*

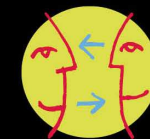




Thank you for your attention.

**11-13 rue René Jacques - 92131 Issy-les-Moulineaux Cedex France
+33 (0)1 55 64 22 00 - www.keynectis.com**

Protecting your **identity**
Protecting your **freedom**
in a connected world



KEYNECTIS