

Entrust Managed Services PKI

Standard Versus Branded Certificate Service

Choose the hosted PKI solution that fits your needs. Whether you need a standard certificate service or our customer-branded option, Entrust offers a set of flexible, industry-proven certificate services designed to meet your organization's requirements.

STANDARD CERTIFICATE SERVICE	CUSTOMER-BRANDED CERTIFICATE SERVICE
<p>A reliable, secure and cost-effective service that includes:</p> <ul style="list-style-type: none"> • Quick and easy certificate issuance to partners, suppliers, customers and distributors, making it easy to conduct business securely • No client software required — enrollment and administration done via intuitive Web interface • Administration utility offers several enrollment options, from self-service to automatic enrollment • Administrative accounts at no additional cost • Auditor-witnessed CA key generation and storage of CA key in HSM to protect against the creation of fraudulent certificates • Annual ISO 21188 audit by a professional auditing firm • High-end servers offer robust performance enabling you to scale as your business grows • Rigorous SLA backed by enterprise-class monitoring, high-availability and disaster recovery mechanisms • High-end security for end-to-end data protection: bomb-proof facilities, encryption, stringent access controls, firewalls, antivirus software and more • Established Certificate Policy and CPS, shortening time-to-market • Certificates can be used to secure multiple applications • Encryption keys are archived in case of loss • Certificate Revocation Lists (CRLs) published every six hours • 24x7x365 phone support • Easy upgrade to Branded Certificate Service <p>See reverse side for additional options around OCSP, client-side software, smartcards and tokens, as well as publication of certificates to directories.</p>	<p>Get all the features of the Standard Certificate Service, plus:</p> <ul style="list-style-type: none"> • Establish your own private community of trust • Brand certificates with your organization's name; users see your organization as the "Issuer" of a certificate rather than Entrust (<i>more on page 2</i>) • Customize your Certificate Policy and CPS to meet organizational requirements, allowing you to specify things like: <ul style="list-style-type: none"> – Custom vetting process for subscribers – Custom certificate content – The CA key length and user certificate lifetimes – Certificate Revocation List lifetimes • Brand the enrollment and administrative Web interfaces with your organization's name and/or logo • Write certificates to Active Directory or any LDAP directory at your site • Take advantage of these options: <ul style="list-style-type: none"> – Integration with in-house authentication mechanisms – CA hierarchies – CRLs published hourly – Online Certificate Status Protocol (OCSP) – Roaming services

Client-Side Software

Deploy Entrust's thin client on the desktop for automatic certificate updates without any user intervention, thus reducing the total cost of ownership of your PKI. Entrust's client simplifies deployment of Microsoft Encrypting File System (EFS), adds file encryption and includes a built-in OCSP client. Use our toolkits to integrate cryptographic functionality into custom applications.

Smartcards & Tokens

For an additional level of security, Entrust can store certificates on a variety of smartcards and tokens that interoperate seamlessly with your Entrust hosted PKI.

Revocation Options

Entrust offers revocation over OCSP and premium revocation*, which increases the CRL refresh rate from every six hours to hourly. Frequent CRL updates ensure revoked users are locked out of your systems in a timely manner.

Roaming Services*

Have users access their certificates from any computer. Certificates are stored on a centralized server residing at your site or ours.

Integration with In-House Authentication Mechanisms*

Leverage information you already have about your users and use it to create custom certificate issuance processes. For example, have users enter a known password from an existing authentication database or verify payroll system data to begin a certificate approval workflow.

CA Hierarchies*

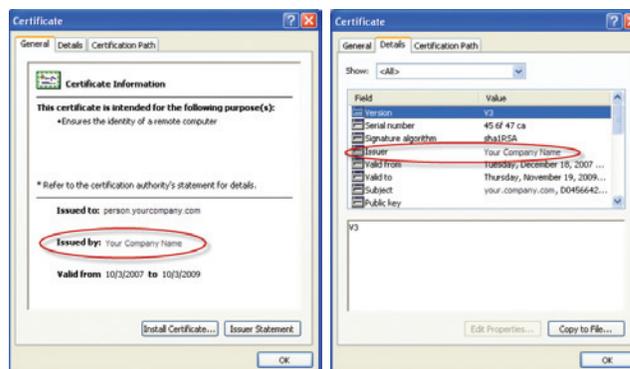
Add your own root CA with underlying issuing CAs. A CA hierarchy keeps trust centralized at the root, while allowing underlying organizational units to manage and control their own intermediate CA.

Directory Support

Use a directory hosted by Entrust or write certificates to Active Directory or any LDAP directory at your site

Name Value

With Entrust's Customer-Branded Certificate Service, certificates include your organization's name in the "Issued By" and "Issuer" fields, letting relying parties know the certificate is issued with the approval of your organization.



* Only available with Entrust's Customer-Branded Certificate Service.

About Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

