External Certificate Authority Service Description

Introduction

External Certificate Authority (ECA) is a program sponsored by the U.S. Department of Defense Public Key Infrastructure (DoD PKI) in response to *Department of Defense Instruction 8500*. This directive stipulates, among other things, that all Department of Defense (DoD) information systems must employ risk management to secure access to information deemed "Sensitive But Unclassified Information". Under this program, external contractors must have a PKI-based digital certificate issued by an authorized vendor to securely communicate with DoD or authenticate to a DoD information system.

Symantec™ ECA Service has received DoD accreditation as an authorized vendor of ECA digital certificates. In order to achieve this accreditation, Symantec maintains an ECA Certification Practice Statement (CPS) defining policies and procedures to manage the ECA digital certificate lifecycle (*e.g.*, issuance, revocation, etc.) that are sufficient to meet the requirements specified in the ECA Certificate Policy (CP). Symantec is audited on an annual basis by a globally known, independent auditor to ensure compliance with the ECA CP and CPS. The ECA digital certificates are issued from an intermediate certificate authority (CA) that chains to the root CA created for the ECA program. As a result, the ECA digital certificates are interoperable with the DoD PKI.

Capabilities

Symantec ECA Service provides the following key capabilities:

- *Certificate Pair*
  Issue a certificate pair that includes an authentication/signing certificate and an encryption certificate. A subscriber can use the authentication/signing certificate to log-in to a DoD information system and/or create a digital signature within an application (*e.g.*, Microsoft Outlook, Adobe Acrobat, etc.). Also, a subscriber can use the encryption certificate to encrypt a transaction or a file to securely communicate with the DoD.
- *Key Escrow*
  Offer remote hosting of the key management service for the private key of the encryption certificate. If access to the private key has been lost (*e.g.*, computer crash, etc.), a subscriber can request the recovery of the escrowed copy of that private key. In addition, an organization's legal officer, security officer, or human resources representative may also request a recovery. Also, a law enforcement official with a court-authorized order may request a recovery.
- *Authentication Service*
  Provide three methods to verify the identity of a subscriber prior to issuing the certificate pair: public notary, trusted agent, and DoD employee. The public notary method requires a subscriber to appear before a public notary or U.S. consular officer, if outside the United States, and present two forms of identification and proof of citizenship (*e.g.*, driver's license, passport, etc.). The trusted agent method allows an individual within an organization to be designated a trusted agent. This trusted agent is then authorized to perform the equivalent functions as a public notary and maintain records of subscriber's applications. The DoD employee method enables an authorized DoD employee to perform equivalent functions as a trusted agent for foreign nationals residing outside of the United States that need to do business with the DoD.

Symantec ECA Service will be provided to you upon execution of ***Symantec ECA Services Agreement***.

Additional Options

Additional options are available at additional charges:

- *PKI Tokens*
  - PKI-enabled USB hardware tokens are available for purchase.
  - Credentials are stored on tokens, and managed through "*Symantec PKI Client*" software provided to you.
  - Symantec will provide standard technical support for tokens and the software to your Trusted Agents.