

# Becoming an ECA Vendor

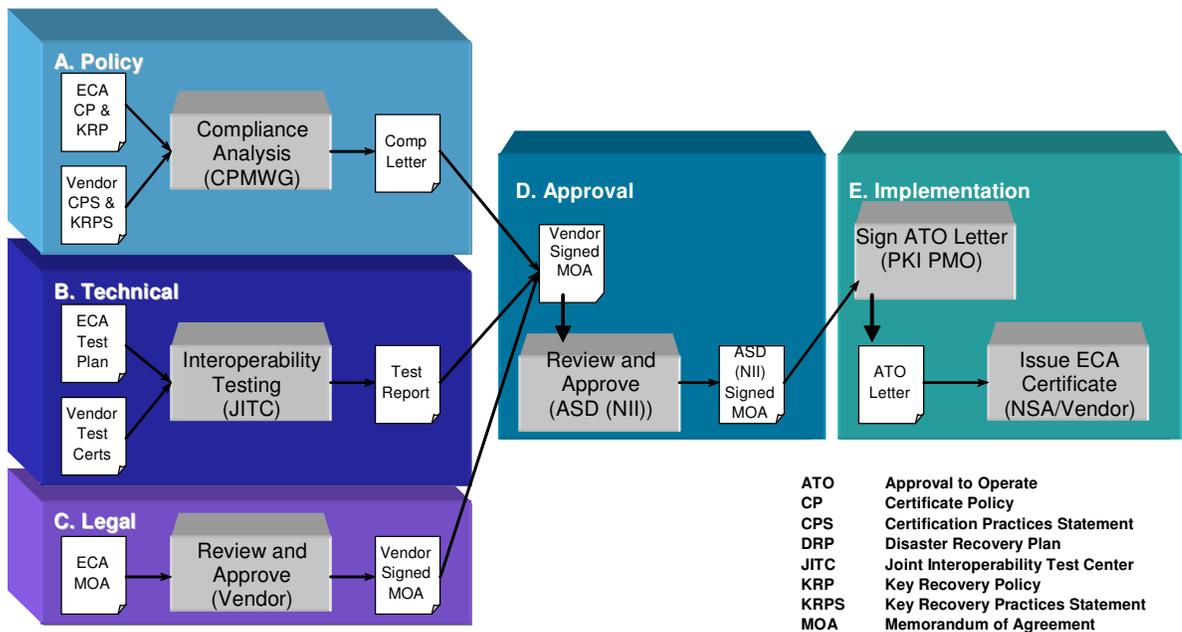
---

The Department of Defense (DoD) has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities. The ECA program is designed to provide a mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems.

DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" requires DoD Public Key Enabled applications that have users who are not eligible to get certificates from the DoD PKI to accept certificates from DoD-approved external PKIs, including the ECA PKI.

The ECA PKI is a hierarchical PKI with a single Root CA trust anchor and a single layer of Subordinate CAs. The ECA Root CA is hosted by National Security Agency (NSA) and the Subordinate CAs are owned and operated by commercial vendors who have been approved by the DoD as meeting all ECA technical, policy, and security requirements. Currently, there are two approved ECA vendors participating in the program; Operational Research Consultants (ORC) and VeriSign. The IECA vendor, Digital Signature Trust (DST) is in process to become an ECA.

The following figure illustrates the five steps required to become an ECA. Details for each step are provided in the following pages.



## **A. Policy Compliance**

1. Review the ECA Certificate Policy (CP) and Key Recovery Policy (KRP) to determine the requirements for operating as an ECA. The current version of the CP and KRP can be downloaded from <http://iase.disa.mil/pki/eca/documents.html>.
2. Develop a Certification Practice Statement (CPS) that aligns with the ECA CP and Key Recovery Practice Statement (KRPS) that aligns with the ECA KRP.
3. CPS compliance review:
  - Submit CPS to the PMO.
  - A compliance analysis will be conducted on the CPS against the ECA CP and an analysis report showing where the CPS does not comply with the CP.
  - Vendor will update the CPS in response to compliance related comments and resubmit to the PMO.
  - The compliance analysis of the CPS is complete when the vendor and the PMO have resolved all issues except those that the vendor wishes to be reviewed by the full CPMWG.
4. CPS CPMWG review:
  - The CPS and the compliance analysis report will be submitted to the CPMWG for review.
  - The vendor and the CPMWG will meet to discuss any comments.
  - Vendor will update the CPS in response to comments and resubmit the CPS to the CPMWG.
  - The CPMWG review of the CPS is complete when the CPMWG votes to approve the CPS as fully compliant with the ECA CP.
  - Upon approval of the CPS the CPMWG will provide a letter of approval.
5. KRPS compliance review:
  - Submit KRPS to the PMO.
  - A compliance analysis will be conducted on the KRPS against the ECA KRP and an analysis report showing where the KRPS does not comply with the KRP.
  - Vendor will update the KRPS in response to the compliance analysis report related comments and resubmit to the PMO.
  - The compliance analysis of the KRPS is complete when the vendor and the PMO have resolved all compliance related issues except those that the vendor wishes to be reviewed by the full CPMWG.
6. KRPS CPMWG review:
  - The KRPS and the compliance analysis report will be submitted to the CPMWG for review.
  - The vendor and the CPMWG will meet to discuss any comments.
  - Vendor will update the KRPS in response to comments and resubmit the KRPS to the CPMWG.
  - The CPMWG review of the KRPS is complete when the CPMWG votes to approve the KRPS as fully compliant with the ECA KRP.
  - Upon approval of the KRPS the CPMWG will provide a letter of approval.

## **B. Technical Compliance**

1. Determine which types of certificates will be supported. Certificate types and profiles are listed in Appendix A of the ECA CP.

2. Review the DoD PKI ECA Master Test Plan, available from [http://jitic.fhu.disa.mil/pki/eca\\_testing.html](http://jitic.fhu.disa.mil/pki/eca_testing.html) .
3. Contact JITC at [pke@fhu.disa.mil](mailto:pke@fhu.disa.mil) to arrange for testing of their ECA test certificates and the payment of fees.
4. Create test certificates in accordance with ECA CP profiles. Test certificates must fully comply with ECA CP profiles, but may be issued by a test CA that the vendor is already operating.
5. Submit the test certificates to JITC.
6. JITC will conduct the test. Technical compliance testing is complete when JITC generates a test report certifying that test certificates meet all requirements in the test plan.

### ***C. Legal***

1. Review the ECA MOA template, which is available from the PMO upon request.
2. Coordinate with the DoD legal counsel to approve any requested changes from the text in the MOA template.
3. Sign and submit three (3) paper copies of the approved MOA to the PMO, along with the name and contact information of the individual who will be presenting the request for the ECA Subordinate CA Certificate.

### ***D. Approval***

1. After the successful completion of steps A<sup>1</sup>, B, and C, the PMO will submit signed copies of the MOA, along with the CPS Approval letter to ASD(NII) for signature. ASD(NII) signature on the MOA indicates that the vendor is approved to become an ECA.

### ***E. Implementation***

1. Upon receipt of a signed MOA from ASD (NII), the PKI PMO generates an Approval To Operate (ATO) letter indicating the vendor is an approved ECA, identifying the name and contact information of the individual who will be presenting the request (from Step C), and identifying the Subordinate CA certificate profile (from Appendix A of the CPS).
2. The PKI PMO submits the ATO to the ECA Root CA facility.
3. The ECA Root CA facility contacts the vendor to arrange a mutually convenient date for a site visit.
4. The ECA vendor brings a diskette that contains the certificate request from their Subordinate CA to ECA Root CA facility.
5. The ECA Root CA issues the Subordinate CA certificate.
6. The ECA Root CA facility personnel copy the newly issued Subordinate CA certificate and the Root CA certificate onto the diskette and return it to the vendor.
7. The ECA Root CA facility adds the vendor to their mailing list for ECA Root CA CRLs.
8. Subordinate CA CRLs are pulled from vendor repositories. To assist in this process, the vendor is requested to coordinate with the PMO in providing information on how to access CRLs from the vendor's repository.
9. The vendor installs the new Subordinate CA certificate on their CA.
10. The vendor ensures that the ECA Subordinate certificate and all CRLs are available to the Global Directory Service.

---

<sup>1</sup> Step A.6 is not required to be completed prior to MOA signature. However, this step must be completed by the vendor once CPMWG comments are provided on the KRPS.