IdenTrust
part of HID Global

How to Revoke a DoD ECA Digital Certificate

A DoD ECA digital certificate must be revoked when, among other reasons, it has been compromised, lost or someone in the organization has left or been terminated.

In order to request revocation, you need to be the Subscriber, an Authorized Employee within the organization or the Trusted Correspondent.

If you are a Subscriber, please follow the Subscriber Revocation Procedure below:

A Subscriber's revocation request must be communicated electronically to IdenTrust by sending a digitally signed email with the private key of the certificate to be revoked. As an additional insurance measure, the request must also be submitted over the phone by calling the IdenTrust helpdesk at **+1 (888) 882-1104 (U.S.)** or **+1 (801) 384-3474 (International)**.

The digitally signed message may be submitted to the IdenTrust helpdesk (ecaservices@identrust.com) or to the organization's authorized Trusted Correspondent. In either case, the Subscriber must provide a reason for revocation. If the revocation is being requested for reason of key compromise or suspected fraudulent use of the private key, then the revocation request must so indicate.

- If the email is addressed directly to IdenTrust, upon positive verification of the digital signature, an IdenTrust Registration Agent will revoke the Subscriber's IdenTrust DoD ECA digital certificate used to create the signature.
- If the email is addressed to the Trusted Correspondent, she/he will:
  - Verify the Subscriber's signature;
  - Ensure a revocation reason is provided;
  - Collect and zero out any information on the smart card or USB token;
  - Create a record; and
  - Submit the request to the IdenTrust helpdesk via email and a telephone call.

  The Trusted Correspondent will:
  - Provide the Subscriber's information;
  - A revocation reason;
  - Attach the original signed request; and
  - Digitally sign the message with his/her IdenTrust DoD ECA digital certificate.

Medium Hardware certificates require an in-person identity verification by an IdenTrust employee or by a Trusted Correspondent. Requests for these certificates must indicate if the smart card or USB token was returned and zeroed out by including its' serial number.

An IdenTrust Registration Agent will verify the Trusted Correspondent's digital signature, confirm completeness of the information and ensure that the Trusted Correspondent is authorized by the Subscribing Organization. Upon positive confirmation, the IdenTrust Registration Agent will revoke the Subscriber's certificate.

If the Subscriber cannot digitally sign a revocation request (i.e., a locked or lost token), the individual must contact its' authorized Trusted Correspondent in person and provide proof of identity equivalent to the proof provided during initial registration. If the request is for a Subscriber Certificate, after confirming the Subscriber's identity, the Trusted Correspondent will submit a digitally signed revocation request to the IdenTrust helpdesk as outlined above.

If you are an Authorized Representative of the Subscribing Organization, please follow the Subscribing Organization Revocation Procedure below:

An organization must request revocation through its' authorized Trusted Correspondents. The Trusted Correspondent is responsible for authenticating requests other than those received from the Subscriber. The Trusted Correspondent will confirm the identity of the requestor in-person or by using a message from the requestor digitally signed with an IdenTrust DoD ECA digital certificate.

In exceptional cases, when the organization does not have immediate access to a Trusted Correspondent (i.e., the Trusted Correspondent is being terminated), an organization's representative (i.e., personnel office representative) can request revocation directly via a signed email and a call to the IdenTrust helpdesk, or by mailing the IdenTrust Registration Desk on company letterhead containing a notarized signature. The communication should include the information about the Subscriber's certificate to be revoked. If the revocation is being requested for reason of key compromise or suspected fraudulent use of the private key, or if the smart card or USB token could not be collected and zeroed out, then the revocation request must indicate key compromise.

2017-12-22-identrust-revoke-dod-digi-cert-en