

## How to Revoke an IGC Digital Certificate

An IGC 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 Agent.

### **If you are the Subscriber you may revoke your certificate in one of the following ways:**

- Complete a Self-Revocation by logging into the Certificate Management Center (CMC) <https://secure.identrust.com/tscmcapp> and using the account number and password to log in.  
Select the “Revoke” option from the drop-down menu.
- Send a digitally signed email with the private key of the certificate to be revoked. The digitally signed message may be submitted to the IdenTrust Support team, [Support@IdenTrust.com](mailto:Support@IdenTrust.com)  
Provide the reason for revocation such as ‘key compromised’, ‘suspected fraudulent use’, or ‘no longer with the organization’.
- Submit over the phone by calling the IdenTrust Support Team at (888) 339-8904 and request the account be revoked.

### **If you are an Authorized Representative of the Subscribing Organization (Affiliated accounts):**

- Send a Digitally Signed Revocation request RA, by establishing a Client-Authenticated SSL/TLS Encrypted Session, using the Signing Key Pair associated with the Certificate being Revoked, or
- Contact the RA’s LRA or TA on the phone to place the request stating the reason for Revocation.

The Subscriber or Sponsor are required to indicate the Subject of the Certificate to be Revoked, the reason for the Revocation request, and the LRA or TA, when the request is submitted via email or phone, will document the reason for the request and archive this documentation.

Reason codes are included in the CRLs Issued by IdenTrust, including the reason code of Revocation because of Key compromise

### IGC Mobile Authentication Accounts:

A Mobile Authentication Certificate 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.

The digitally signed message may be submitted to the IdenTrust Support team, [Support@IdenTrust.com](mailto:Support@IdenTrust.com) providing the 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.

Upon positive verification of the digital signature, an IdenTrust Support Agent will revoke the Subscriber's IdenTrust IGC Mobile Authentication digital certificate used to create the signature.

For the revocation process for certificate types not listed or for detailed information, please refer to the Section 4.9 of the current CPS: <https://www.identrust.com/support/documents/igc>