Code Signing Certs

Activating Code-Signing Certificates for Departments

To activate code-signing certificates at the Departmental level, you will need to enable departments, domains, and admins.

To enable a department for code-signing certificates, do the following:

1. Go to Settings --> Organizations
2. Select the Edit button on the right hand side under the controls column
3. In the pop up window select the Code Signing tab
4. Click Enable

To enable a domain for code-signing certificates, do the following:

1. Go to Settings --> Organizations
2. Select the chosen department's Domains button on the right hand side under the controls column
3. In the pop up window select the Delegate button under the controls column
4. Enable Code Signing for either your organization or your department

To enable a department administrator for code-signing certificates, do the following:

1. Go to Admin Management
2. Select the Edit button on the right hand side under the controls column
3. Under Role enable the department admin for Code Signing
4. Click Ok

Use of Code Signing Certificates

This information is based on section 3.2.3 of the Code Signing CPS. [PDF]

Code Signing Certificates are a standard part of the InCommon Certificate Service and are automatically available to Registration Authority Officers (RAOs) at all subscribing organizations. RAOs can determine whether or not to make Code Signing Certificates available at the department level.

Code Signing Certificates may be issued to individuals or to specifically identified departments. An organization may also elect to have a single code signing certificate or a group of certificates that identify the organization at large. It is the responsibility of subscriber organizations to authenticate and identify individual entities for which it issues Code Signing Certificates.

Subscriber organizations will issue certificates to its end users and/or specifically identified departmental organizations using a process that is at least as strong as its existing practice for managing accounts for central services such as electronic mail, calendaring, and access to central file storage.

For complete administrative details, see the Certification Practices Statement (CPS) for Code Signing Certificates [PDF]. We have also created a DIFF file that shows the changes [PDF] between the baseline SSL Certificate CPS and the Code Signing CPS.

Note: All code signing certificates, their issuance and use, are governed by the CPS. Subscribers are required to comply with its provisions.

Policy Issues

Issuance of Code Signing Certificates must comply with the corresponding Certification Practices Statement (CPS). Of particular note:

3.2.3.1 Special Rule for Code Signing Certificates: Code Signing Certificates are used by software on relying party's computers to verify that software downloaded and intended to run on their computer in fact originates from the source named in the certificate. However most software verification systems ONLY DISPLAY THE COMMON NAME FIELD of the code signing certificate used. It is therefore the responsibility of the organization Subscriber to ensure that this field properly identifies the organization entity responsible for signing the software. This field SHOULD NOT be filled in so as to confuse the relaying party as to the origin of the software or otherwise represent itself in a fraudulent manner.

4.2.1 Performing Identification and Authentication Functions: The Comodo website or API server validates that the “Country”, “ “Domain Name” and “Organization” fields of submitted CSRs are correct as determined at subscription time. It is the responsibility of the Subscriber institution to ensure that other relative distinguished name components are accurate for a given client certificate. In particular the institution must ensure that the Common Name (CN) relative distinguished name is properly provided. See 3.2.3.1.

Risk Perspective

An SSL certificate permits end users to establish a secure connection to a particular webserver located on your campus. By contrast, a Code Signing Certificate permits its holder to create software and distribute that software through any method to any personal computer in the world and it will run without significant warning. If the creator of the software signs malware, it will be traceable to the university.