1 Introduction

Code Signing on Demand (CSD) offers customers a faster, more intuitive and highly secure way to digitally sign their software. The service is available in both hosted and cloud versions and is capable of signing EXE, DLL, .CAB, .MSI, .OCX, .SY, JAVA JAR and Android application files. The service is available in two modes:

- **In-House Hosted Mode** – Requires a controller installed on your network. The controller will generate CSD enabled code-signing certificates for developers to sign files. The certificates and their private keys are stored in encrypted form in a local database created by the controller.

  HSM integration. You can also configure the controller to generate and store the code-signing certificate on a local Hardware Security Module (HSM). Keys will be generated in PKCS # 11 format and saved in non-extractable format on the HSM device.

- **Cloud Service Mode** – The signing service is hosted on Comodo's highly secure cloud servers. The service generates CSD enabled code signing certificates for developers to sign files. The certificates and their private keys are generated and stored in encrypted format in Comodo's data-center for the lifetime of the certificate, tightly protected by Comodo's military grade security infrastructure.

  HSM integration. Please contact your account manager if you want to setup HSM integration while using cloud service mode.

This document describes how to setup and use the CSD service in **Cloud Mode**.

The Code Signing on Demand (CSD) feature is not enabled by default. If you require the CSD service, please contact your account manager. Once enabled, the 'Code-Signing on Demand' tab will appear in the title bar.

CCM allows you to add developers and enroll CSD enabled code signing certificates for them. After enrolling for a code signing certificate for a developer, the service generates the certificate request for the developer, submits the request to CCM, tracks the order and collects the certificate once issued. Developers can then upload files to the cloud portal for signing. Upon approval by the administrator, the service will sign the code and notify the developer to download the signed files.

Please see the following links for help to set up the service:

- The 'Code Signing on Demand' Interface
- Add Developers
- Obtain a Code Signing Certificate For CSD
- How to sign code using CSD
- Configure the CSD service

1.1 The 'Code Signing on Demand' Interface

The 'Code Signing on Demand' area allows you to configure the service, add and manage 'Developers', and manage developer signing requests.

The 'Code Signing on Demand' area is divided into three main administrative areas, namely:

- The 'Configuration' tab - Allows you to configure the service for auto-approval
- The 'Requests' tab - Allows you to view and approve/decline code signing requests from developers
- The 'Developers' tab - Allows you to add and manage 'Developer' accounts in CCM
Visibility of the 'Code Signing on Demand' area is restricted to:

- MRAO administrators - can configure the service and add developers and manage code signing requests for any Organization or Department.
- RAO Code Signing administrators - can add developers and manage code signing requests only for Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Code Signing administrators - can add developers and manage code signing requests only for Departments that have been delegated to them.

1.2 Add Developers

A 'Developer' is a role in CCM with permission to:

- Login to the CSD service
- Upload files for code-signing
- Download code-signed files

You can create a developer as a new user, or add developer privileges to an existing CCM user. An MRAO or RAO administrator will need to approve the developer's actual signing requests, unless you enable auto-approve in the CSD configuration screen.

To add a developer

- Open the 'Developers' interface by clicking 'Code Signing on Demand' > 'Developers'
- Click the 'Add' button. This will open 'Add New Developer' dialog.
• Type the email address of the developer in the email field.
• Select the Organization(s) / Department(s) to which the developer should belong on the right
• Click ‘OK’ to confirm your selection.

The developer will be added to the list. You can edit the user to change their Organization/Department, reset their password or remove the developer.
A notification email will be sent to the developer with the credentials to access the CSD service. An example is shown below:

1.3 Obtain a code-signing certificate for CSD

Prerequisites:

- You have created a 'Developer' role as explained in the preceding section.
- The domain for which the code signing certificate is to be issued has been enabled for Code Signing certificates and that the domain has been activated by your Comodo account manager. For example, if you wish to issue code signing certs to end-user@mycompany.com, then mycompany.com must have been validated by Comodo. All certificate requests made on validated domains or sub-domains are issued automatically. Certificate requests for new domains will first have to undergo validation by Comodo.
- The domain from which the code signing certificates are to be issued has been delegated to the Organization or Department.
- The RAO Code Signing or DRAO Code Signing administrator has been delegated control of this Organization or Department.
- The MRAO or delegated RAO administrator has enabled Code Signing Certificates for the
Organization/Department by selecting the 'Enabled' check-box in the 'Code Signing tab' of the 'Add New/Edit' Organizations dialog box (see screen-shot below)

- Optional. You have chosen to generate and store keys on a HSM appliance.

Procedure Overview:

1. The administrator confirms the completion of the prerequisite steps.
2. The administrator adds a new code-signing certificate for the Developer from the 'Certificates' > 'Code Signing Certificates' interface, with 'Code Signing on Demand' enabled for the certificate. The CSD service generates and stores the key pair on the cloud server and submits the CSR to Comodo CA. Once the certificate is issued, the service automatically downloads the certificate and stores it in the cloud server. If the HSM service is used, the key pair is generated and stored on the HSM. On issuance of the certificate, the service collects the certificate and stores it on the HSM.

To enroll a code signing certificate for the developer

- Open the 'Code Signing Certificates' interface by clicking 'Certificates' > 'Code Signing Certificates'
- Click the 'Add' button to open the code-signing certificate application form.
- Complete all required fields on the form, making sure:
  - The correct developers email address is used.
  - The correct Organization and Department are specified for the developer.
  - The 'Code Signing on Demand' box is checked.
The following table explains the fields on the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Select the Organization to which the developer belongs.</td>
</tr>
<tr>
<td>Department</td>
<td>Select the Department to which the developer belongs.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the domain pertaining to the Organization/Department</td>
</tr>
<tr>
<td>Term</td>
<td>Select the term of the certificate.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address of the developer.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Organization</td>
<td>Select the Organization to which the developer belongs.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Full name of the applicant.</td>
</tr>
<tr>
<td>Contact Email</td>
<td>Enter the contact email address of the applicant that should be included in the certificate. The contact email address may be the customer facing email address like <a href="mailto:support@company.com">support@company.com</a>, <a href="mailto:sales@company.com">sales@company.com</a> etc.</td>
</tr>
<tr>
<td><strong>Code Signing on Demand</strong></td>
<td>Enable this check-box to allow the certificate to be used by the CSD service.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Choose the signature algorithm to be used by the certificate.</td>
</tr>
<tr>
<td>Keysize</td>
<td>Choose the key-size (in bits) by the certificate.</td>
</tr>
<tr>
<td>Subscriber Agreement</td>
<td>Displays the End-User License Agreement (EULA) for the certificate. Read through the EULA and accept to it by selecting the 'I agree' checkbox for the application to proceed.</td>
</tr>
</tbody>
</table>

- Click 'OK' to submit the request.

The certificate will be added with the state 'init' indicating that the certificate enrollment has been initiated.

Once issued, the state of the certificate will change to 'Issued':

The certificate can now be used to sign code submitted by your developer. Each signing action will, however, need to be approved by an administrator UNLESS you enable 'Auto-approve code signing requests' in CSD Configuration.

### 1.4 How to sign code using CSD

Once you have created a developer and obtained at least one CSD enabled code-signing certificate, your developer is ready to upload files for signing.

Overview of steps:
Comodo Certificate Manager - Code Signing on Demand

- **Step 1 - Upload the files to be Signed** - The developer logs-in to the CSD service portal, enters the details of the file(s) to be signed, selects the signing service and uploads the files. This will create a request which can be viewed in the 'Code Signing on Demand' > 'Requests' interface. See **Step 1 - Upload the files to be Signed** for more details.

- **Step 2 - Approve the Code Signing Request** (optional) - The Administrator views the request, checks the files to be signed and approves the request from the 'Code Signing on Demand' > 'Requests' interface. See **Step 2 - Approve the Code Signing Requests** for more details. Note - this step can be skipped if 'Auto-Approve Code Signing Requests' is enabled in 'Configuration'.

- **Step 3 - Download Code-Signed files** - Once approved and digitally signed, the status of the request will change to 'Signed'. A notification mail is sent to the developer with a URL to download the signed files. See **Step 3 - Download Code Signed Files** for more details.

**Step 1 - Upload the files to be Signed**

Once a developer has been added to CCM they will be able to login to CCM using the link in their confirmation email. By default, the format of this URL is: https://cert-manager.com/customer/[REAL CUSTOMER URI]/csd.

- After logging in they can upload files using the following form:

![Comodo Certificate Manager](image)

- **Organization** - Displays the organization(s) to which the developer belongs. The organization selected here will be shown in the certificate as the publisher of the software.

- **Department** - Allows the developer to choose a department if departmental information is also required in the certificate.

- **Version** - Developer should type the version number of the software they wish to sign

- **Signing Service** - Select the signing service. Choices are 'Microsoft Authenticode', 'Java' and 'Android'.

- **Browse...** - Developer should choose the files they wish to upload and sign.

One all fields are complete and the file has been selected, click the 'Create' button to submit the signing request to the CSD service. A confirmation dialog will be displayed:
A code signing request will be created in the 'Code Signing on Demand' > 'Requests' interface. By default, the request needs to be approved by the appropriate MRAO, RAO or DRAO administrator before the code-signing action will take place. If 'Auto-Approval' of Code Signing Requests is enabled, the service starts the signing process immediately. See 'Configure the CSD service' to enable this feature.

**Step 2 - Approve the Code Signing Request**

After the files have been uploaded the developer, a code signing request will appear in the 'Code Signing on Demand' > 'Requests' area. Under the default settings, an administrator needs to review and approve the request before the service will actually sign the files.

**To view and approve/decline the code signing requests**

- Click 'Code Signing on Demand' tab and choose the 'Requests' sub tab.

A list of requests will be displayed.

- To view the details of a request and check the files, choose the request and click 'Details'.
The 'Request Details' dialog displays the developer's name and the file details along with the MD5 and SHA1 hash values of the files.

- To download the file for examination, click the file name.
- To approve the code signing request, select the request and click 'Approve':
• Enter an approval message and click ‘OK’.

The request will be approved and its state will change to ‘In Progress’:

Once the code-signing process has completed, the request state will change to ‘Signed’ and a notification mail will be sent to the developer to download the signed file.

The Developer must download the signed files within three days of the notification. The files will be removed from the database after three days after signing. If required, administrators can resend this notification by clicking the ‘Resend Signed Notification’ button:
Note. As mentioned earlier, administrators have the option to forgo the approval process by enabling 'Auto-Approve Code Signing Requests' in the 'Configuration' interface.

Step 3 - Download Code-Signed files

On successful completion of the signing process, the developer will receive a notification email with links to download each signed file. An example is shown below.

Note: The Developer must download the signed files within three days of the notification. The files will be removed from the database after three days from the date of signing.

Administrators can also download signed files from the 'Details' dialog of the request.

- Choose the request from the 'Code Signing on Demand' > 'Requests' interface and click 'Details'
Click the file name in the 'Request Details' dialog to download the signed file.

To check whether the file is signed

- Right click on the file and choose 'Properties'
- Choose the 'Digital Certificates' tab
The details of the signer will be displayed.

1.5 Configure the CSD service

By default, code signing requests from developers must be approved by an administrator before the actual signing will take place. Administrators can view, manage and approve requests from the 'Code Signing on Demand' > 'Requests' interface.

To configure the CSD service

- Click the 'Code Signing on Demand' tab then 'Configuration'

- Auto-Approve Code Signing Requests - If you want signing to commence without administrator approval, enable the 'Auto-Approve Code Signing Requests' check-box. The service will start the signing processes immediately after files are uploaded by the developer. Refer to the section How to sign code using CSD for more details.
About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,
United Kingdom.
Tel : +44 (0) 161 874 7070
Fax : +44 (0) 161 877 1767
Email: EnterpriseSolutions@Comodo.com

For additional information on Comodo - visit http://www.comodo.com.