

InCommon®



InCommon Certificate Manager

Code Signing on Demand
Cloud Version

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

1 Introduction

- Code Signing on Demand (CSoD) 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, WAR, JAVA JAR and Android application files.
- InCommon CM is also capable of hash signing, whereby developers upload a hash of their files for signing instead of the files themselves. The developer then needs to embed the hash with their files.

Code signing on demand is available in two deployment options:

- In-House Hosted Mode
 - Developers upload software to a local portal. The code signing process is handled by a locally installed controller. The controller will generate CSoD 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. HSM integration is mandatory if you use the controller in cluster mode. All CSoD agents should be configured to connect to a single HSM.
- Cloud Mode
 - The signing service is hosted on InCommon's highly secure cloud servers. The service generates CSoD enabled code signing certificates for developers to sign files. The certificates and their private keys are generated and stored in encrypted format in InCommon's data-center for the lifetime of the certificate, tightly protected by InCommon'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 CSoD service in **Cloud Mode**.

Note: CSoD is not enabled by default. Please contact your account manager if you require the service.

Process in brief

- A new 'Code Signing on Demand' tab will appear in the InCommon CM title bar after the service is enabled.
- Admins need to assign a person as a 'Developer' in InCommon CM. Admins will request and approve the CSoD certificates on behalf of the developer. The developer will submit files for signing and subsequently collect the signed files.
- After enrolling for a code signing certificate, the CSoD service generates the certificate request and submits the request to InCommon CM.
- The service tracks the order and collects the certificate once issued.

- The developer can then upload files to the cloud portal for signing. After admin approval, the service will sign the code file and notify the developer to collect the signed file.

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

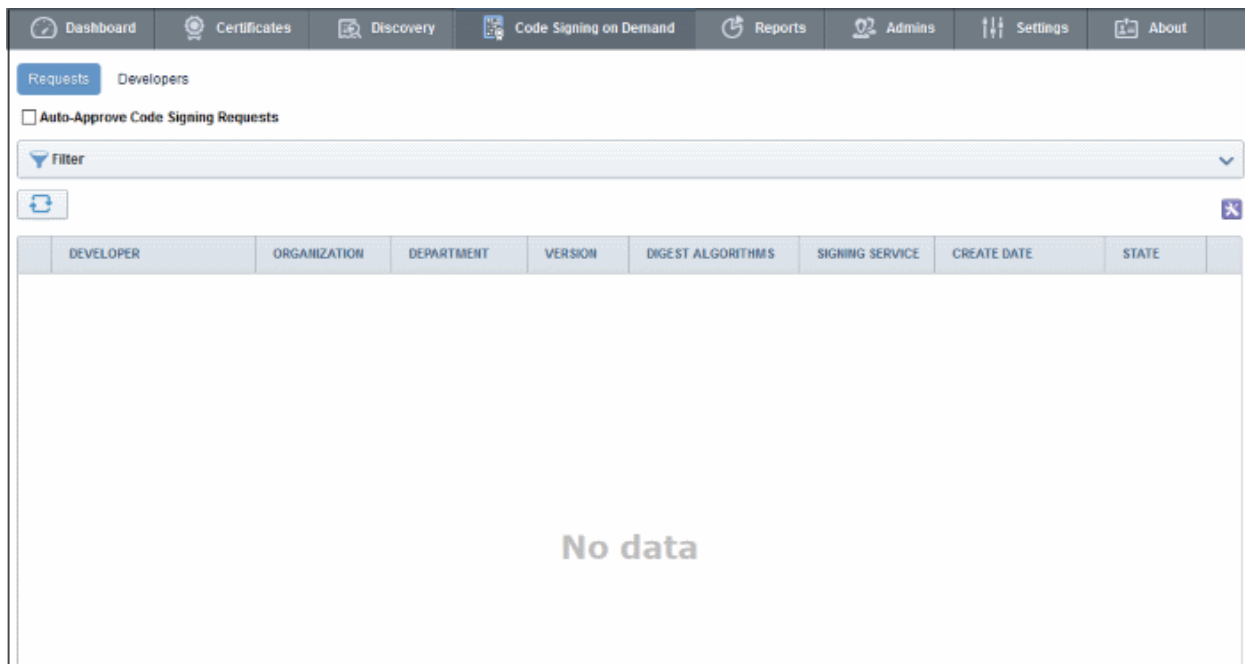
- [The 'Code Signing on Demand' Interface](#)
- [Add Developers](#)
- [Obtain a Code Signing Certificate For CSoD](#)
- [How to sign code using CSoD](#)
- [Configure the CSoD service](#)

1.1 The 'Code Signing on Demand' Interface

The 'Code Signing on Demand' area lets you manage 'Developers' and signing requests.

The interface is divided into two main sections:

- The 'Requests' tab - View and approve/decline code signing requests from developers
- The 'Developers' tab - Add and manage 'Developer' accounts in InCommon CM.



Visibility of the CSoD area is restricted to:

- MRAO administrators - Can configure the controller, add developers and manage code signing requests for any organization or department.
- RAO Code Signing administrators - Can add developers and manage code signing requests for organizations/departments that have been delegated to them.
- DRAO Code Signing administrators - Can add developers and manage code signing requests for departments that have been delegated to them.

1.2 Add Developers

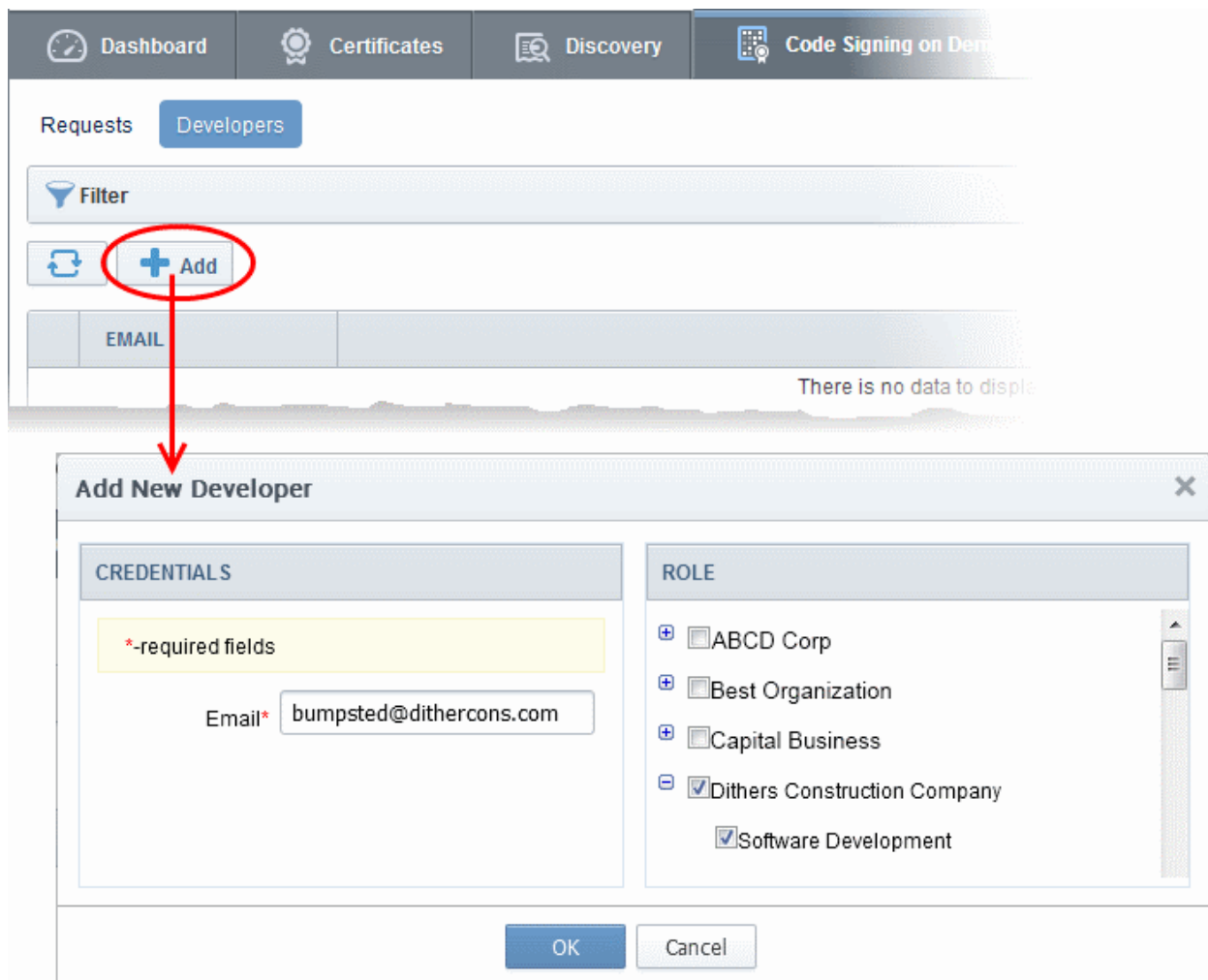
A 'Developer' is a role in InCommon CM with permission to:

- Login to the CSoD service
- Upload files or hashes for code-signing
- Download the signed file or signed hash

You can create a developer as a new user, or add developer privileges to an existing InCommon CM user. An MRAO or RAO administrator will need to approve the developer's actual signing requests, unless you enable auto-approve in the [CSoD configuration](#) screen.

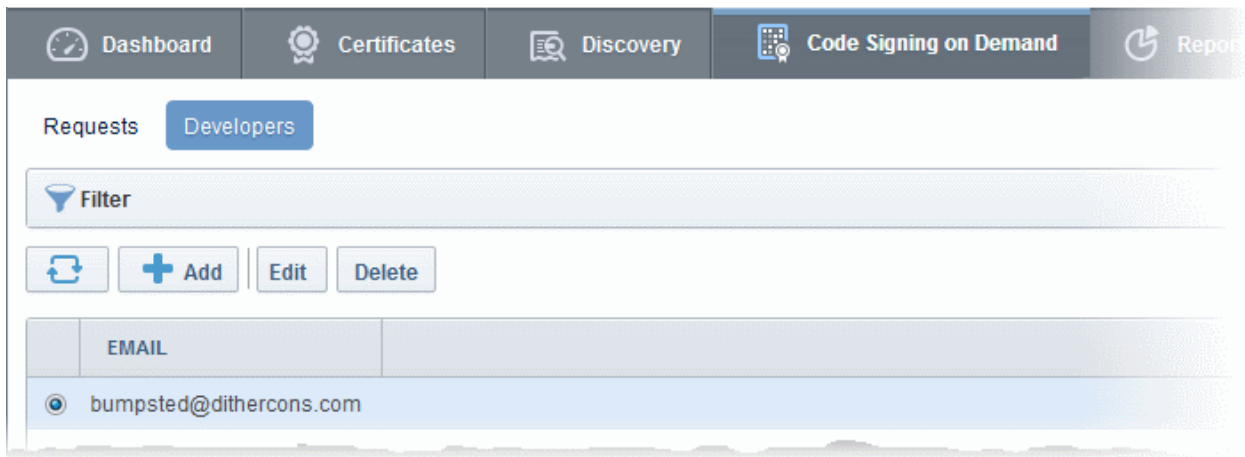
To add a developer

- Open the 'Developers' interface by clicking 'Code Signing on Demand' > 'Developers'
- Click the 'Add' button. This will open 'Add New Developer' dialog.

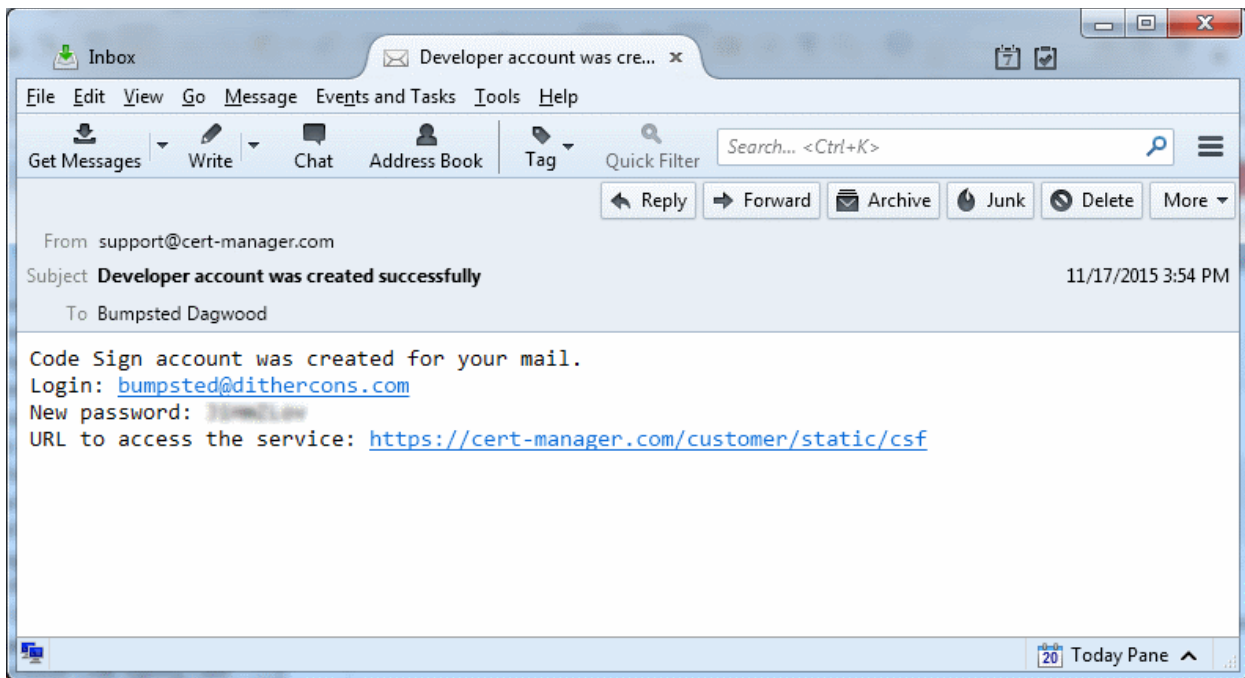


- Type the email address of the developer in the email field.
- Use the right-hand pane to select the Organization(s) / Department(s) to which the developer should belong.
- Click 'OK' to confirm your selection.

The developer will be added to the list. You can edit the user to change their Organization/Department, reset their password or to remove the developer.



A notification email will be sent to the developer with the credentials to access the CSoD service. An example is shown below:

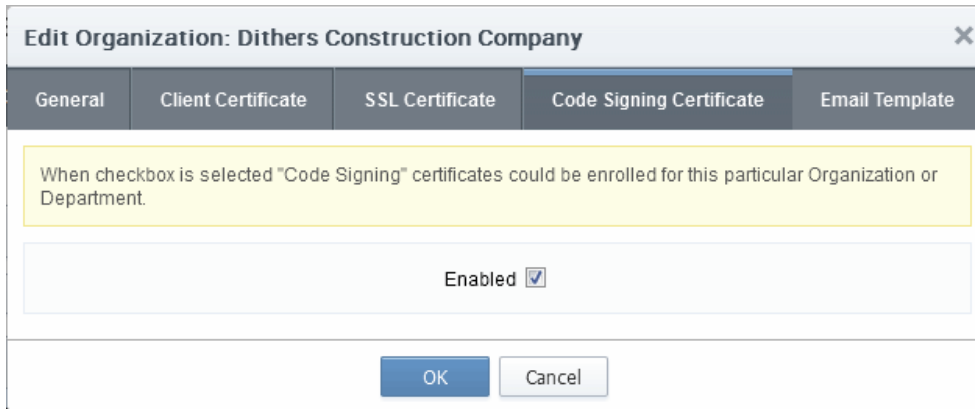


1.3 Obtain a code-signing certificate for CSoD

Prerequisites:

- You have created a 'Developer' role as explained in the preceding section.
- The domain from which the certificate is to be issued has been enabled for code signing certificates, and that the domain has been activated by your InCommon 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 InCommon. All certificate requests made on validated domains or sub-domains are issued automatically. Certificate requests for new domains will first have to undergo validation.
- The domain has been delegated to an organization or department.
- An 'RAO Code-Signing' or 'DRAO Code-Signing' admin has been delegated control of the organization/ dept.

- The admin has enabled code signing certificates for the organization in the 'Code Signing tab' of the organization's settings (see screen-shot below). 'Edit' an organization to access these settings.



Edit Organization: Dithers Construction Company [X]

General | Client Certificate | SSL Certificate | **Code Signing Certificate** | Email Template

When checkbox is selected "Code Signing" certificates could be enrolled for this particular Organization or Department.

Enabled

OK Cancel

- Optional. You can choose to generate and store keys on a HSM appliance.

Procedure Overview:

- The administrator confirms completion of the [prerequisite steps](#).
- 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 CSoD service generates and stores the key pair on the secure cloud server and submits the CSR to InCommon CA. Once the certificate is issued, the service automatically downloads the certificate and stores it on the cloud server. If the HSM service is used, the key pair is generated and stored on the HSM. The service will collect the certificate after it is issued and will store it on the HSM.

To add a code signing certificate for the developer

- Click 'Certificates' > 'Code Signing Certificates' to open the 'Code Signing Certificates' interface
- Click the 'Add' button to open the 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.

Dashboard Certificates Discovery Code Signing on Demand

SSL Certificates Client Certificates Code Signing Certificates

Filter

Refresh Add Export Import from CSV

NAME	EMAIL	ORDER NUMBER	STATE	ORC
Alfred	diridharana@comeda.com	1599128	Issued	Dithe Car

Add New Code Signing Certificate

*-required fields

Organization: Dithers Construction Company

Department: None

Domain: dithercons.com

Email Address*: bumpsted@dithercons.com

Term: 1 year

Full Name*: Bumpsted Dagwood

Contact email:

Code Signing on Demand: *i*

Signature Algorithm: RSA

Key Size: 2048

Subscriber Agreement

EULA

I agree.* *Scroll to bottom of the agreement to activate check box.*

The following table explains the fields on the form:

Field	Description
Organization	Select the Organization to which the developer belongs.
Department	Select the Department to which the developer belongs.
Domain	Select the domain to which you want to issue the certificate. This will be a domain that is assigned to the organization/department
Term	Select the term of the certificate.
Email Address	Enter the email address of the developer.
Full Name	Full name of the applicant.
Contact Email	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 support@company.com, sales@company.com etc.
Code Signing on Demand	Enable to allow the certificate to be used by the CSoD service.
Signature Algorithm	Choose the signature algorithm to be used by the certificate.
Keysize	Choose the key-size (in bits) by the certificate. Recommended = 2048 bit or higher.
Subscriber Agreement	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.

- Click 'OK' to submit the request.

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



NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION	DEPARTMENT	EXPIRES	CODE SIGNING ON-THE-FLY
Bumpsted Dagwood	bumpsted@dithercons.com		Init	Dithers Construction Company			<input checked="" type="checkbox"/>

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



Dashboard Certificates Discovery Code Signing on Demand Reports Admins Settings About

SSL Certificates Client Certificates Code Signing Certificates

Filter is applied

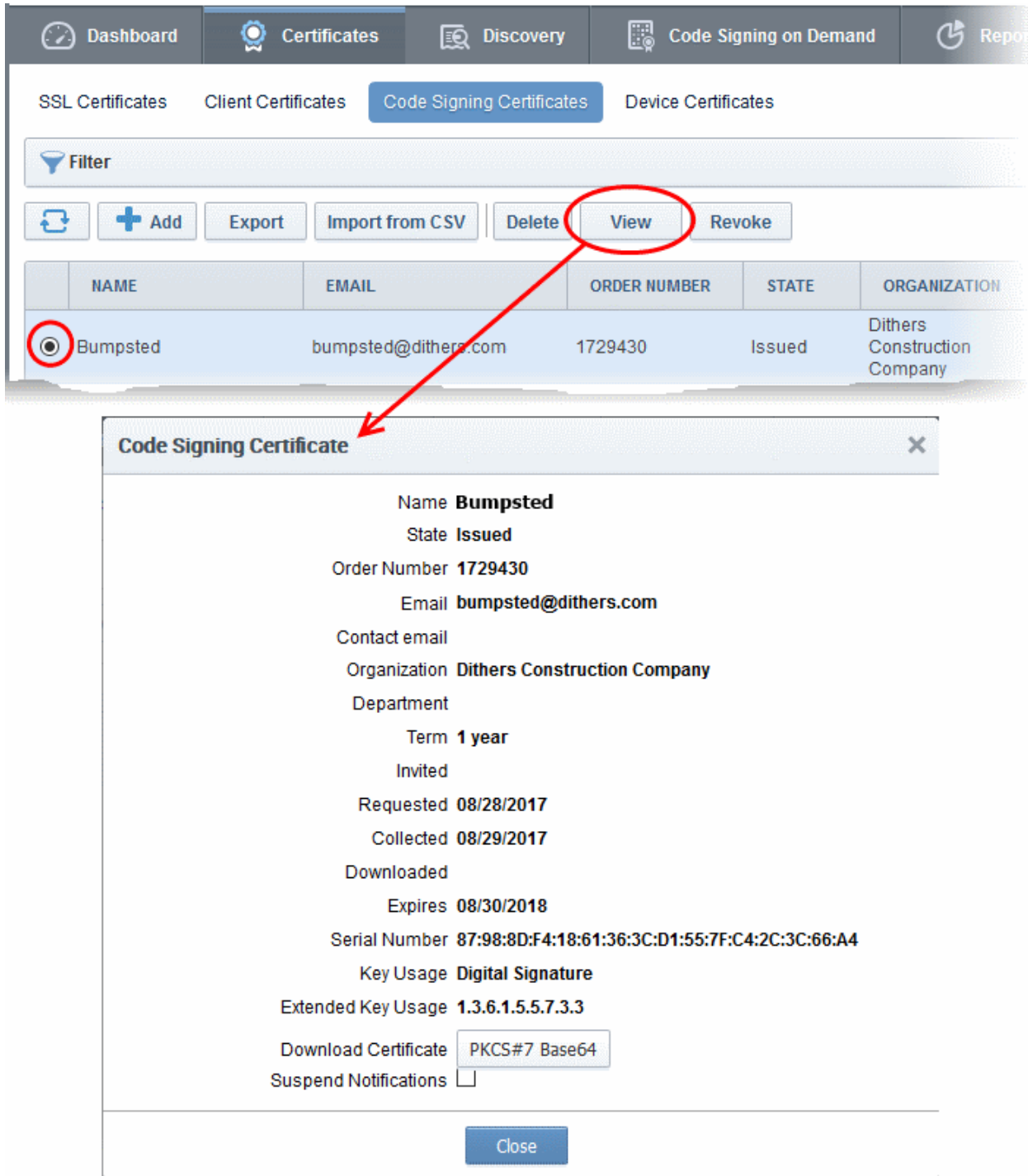
Refresh Add Export Import from CSV Delete View Revoke

	NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION	DEPARTMENT	EXPIRES	CODE SIGNING ON-THE-FLY
<input checked="" type="radio"/>	Bumpsted Dagwood	bumpsted@dithercons.com	1503301	Issued	Dithers Construction Company		11/20/2016	<input checked="" type="checkbox"/>

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 [CSoD interface](#).

Viewing and Downloading the certificate

- Select the certificate and click 'View' to see certificate details:



The screenshot shows the 'Certificates' section of the InCommon Certificate Manager. The 'Code Signing Certificates' tab is active. A table lists certificates, with the first one, 'Bumpsted', selected. A red circle highlights the 'View' button in the toolbar, and another red circle highlights the 'Bumpsted' entry in the table. A red arrow points from the 'View' button to a modal window titled 'Code Signing Certificate'.

	NAME	EMAIL	ORDER NUMBER	STATE	ORGANIZATION
<input checked="" type="radio"/>	Bumpsted	bumpsted@dithers.com	1729430	Issued	Dithers Construction Company

Code Signing Certificate ✕

Name **Bumpsted**
 State **Issued**
 Order Number **1729430**
 Email **bumpsted@dithers.com**
 Contact email
 Organization **Dithers Construction Company**
 Department
 Term **1 year**
 Invited
 Requested **08/28/2017**
 Collected **08/29/2017**
 Downloaded
 Expires **08/30/2018**
 Serial Number **87:98:8D:F4:18:61:36:3C:D1:55:7F:C4:2C:3C:66:A4**
 Key Usage **Digital Signature**
 Extended Key Usage **1.3.6.1.5.5.7.3.3**
 Download Certificate
 Suspend Notifications

- Click the 'Download' button to download the certificate in PKCS#7 format

1.4 How to sign code using CSoD

Once you have [created a developer](#) and [obtained at least one CSoD enabled code-signing certificate](#), your developer is ready to upload files or hashes for signing.

- Code Signing – Developers can upload EXE .DLL .CAB .MSI .OCX .SY, JAVA JAR, WAR and Android application files.

- Hash Signing – Developers can upload a text file containing the SHA or MD5 hash value of their software which will be signed with their code signing certificate. Developers can embed the signed hash and certificate with their binary. This is useful if:
 - The source files are large and the developer wishes to avoid longer upload times
 - Company policy allows code signing of binaries to be performed only within a local system

See [Obtain a code-signing certificate for CsoD](#) if you need help with getting a code-signing certificate.

Note: The 'Hash Signing' feature is only available if enabled for your account. Please contact your InCommon account manager if you wish to add this service.

Overview of steps:

- [Step 1 - Upload the files to be Signed](#) - The developer logs-in to the CSoD service portal, enters the details of the file(s) to be signed, selects the signing service and uploads their code or hash. This will create a request which can be viewed in the 'Code Signing on Demand' > 'Requests' interface.
- [Step 2 - Approve the Code Signing Request](#) (optional) - An administrator views the request, checks the files to be signed and approves the request from the 'Code Signing on Demand' > 'Requests' interface. Note - this step can be skipped if 'Auto-Approve Code Signing Requests' is enabled in the CSoD interface.
- [Step 3 - Download Code-Signed files](#) - After the signing process is complete, 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.

Step 1 - Upload the files to be Signed

- Once a developer has been added, they will be able to login to InCommon CM using the link in their confirmation email.
- By default, the format of this URL is <https://cert-manager.com/customer/InCommon/csod>.

Create Code Signing request

Email: *

Password: *

AUTHORIZE

- Developers can then upload files using the following form:

Create Code Signing request

Email: * bumpsted@dithers.com

Password: * ●●●●●●●●

Organization: * Dithers Construction Company

Department: * None

Digest Algorithms: *

- MD5
- SHA1
- SHA256
- SHA384
- SHA512

Version: *

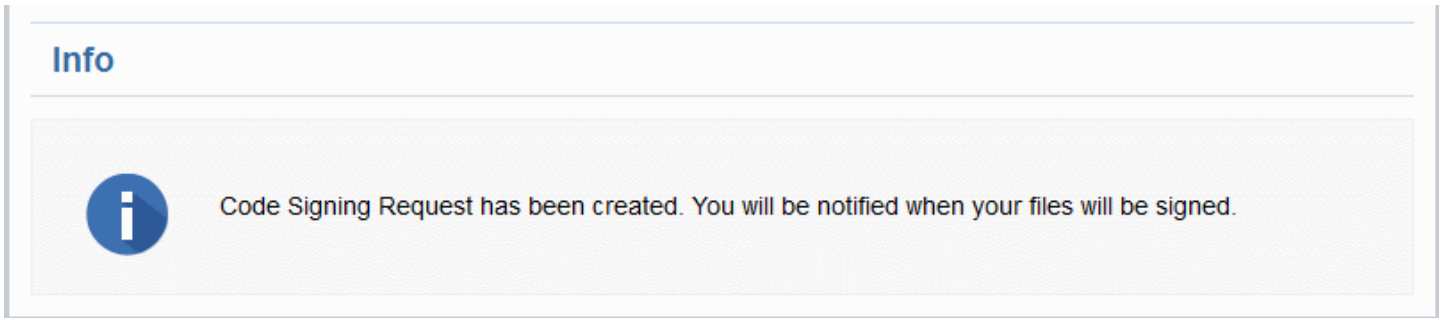
Signing Service: * Microsoft Authenticode

No files selected.

- **Organization** - 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.
 - **Digest Algorithm** - Select the algorithm you wish to use to create the file hash-code (aka 'digest'). The hash-code is used by client software to verify the integrity of your signed code. Recommended = SHA256 and upwards.
 - **Version** - Developer should type the version number of the software they wish to sign.
 - **Signing Service** - Select the appropriate signing service for the type of file you want to sign:
 - i. **Files** - Choose 'Microsoft Authenticode', 'Java' or 'Android' as the signing service.
 - ii. **Hash values** - Choose 'Hash Signing' as the signing service. You need to generate a hash-code of your file with the SHA or MD5 algorithm (to generate a .sha or .md5 file). Alternatively, create a .txt file containing the hash value.
- Note:** 'Hash Signing' is only available if the service is enabled for your account. Contact your account manager if you want to enable 'Hash Signing'.
- **Browse...** - Choose the files or hashes you want to upload for signing. Multiple files can be uploaded.

- The developer should complete the form and click the 'Create' button to submit the signing request to the CSoD service.

A confirmation dialog will be displayed:



- The code signing request can be seen in 'Code Signing on Demand' > 'Requests'.
- By default, the request needs to be approved by the appropriate MRAO, RAO or DRAO administrator before the signing will take place.
- If 'Auto-Approval' of Code Signing Requests is enabled, the service will sign the code immediately. See ['Configure the CSoD service'](#) to enable this feature.

Step 2 - Approve the Code Signing Request

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

- Click the 'Code Signing on Demand' tab and choose the 'Requests' sub tab
- A list of requests will be displayed:



	DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
<input checked="" type="radio"/>	bumpsted@dithers.com	Dithers Construction Company		1.1	[MD5]	Java	08/31/2017 16:25:46	Created
<input type="radio"/>	bumpsted@dithers.com	Dithers Construction Company		1.0	[MD5]	Hash Signing	08/30/2017 17:13:46	Signed

- Click 'Details' to view the specifics of the request:

Request Details

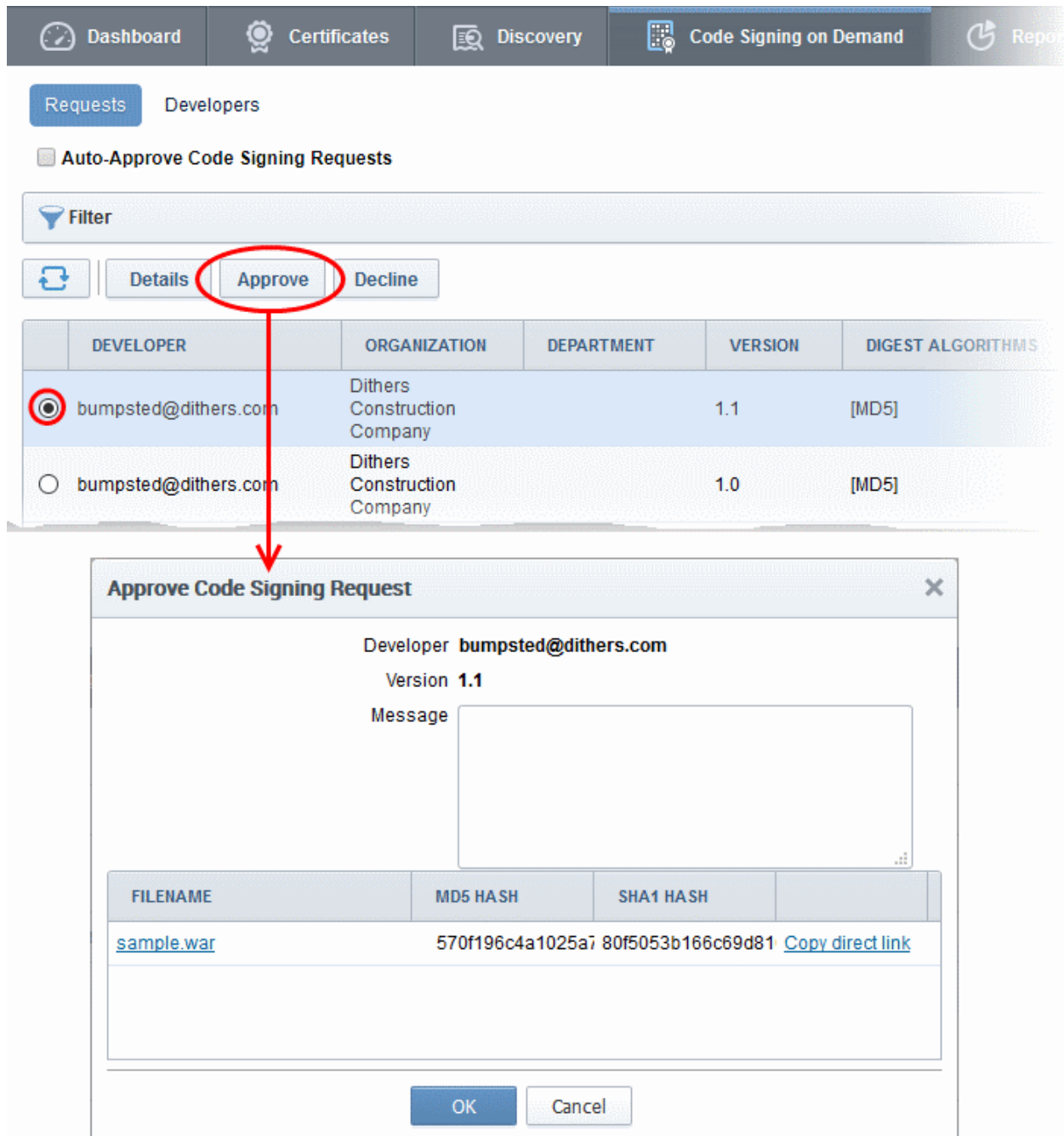
Developer **bumpsted@dithers.com**
Version **1.1**
Signing Service **Java**
Organization **Dithers Construction Company**
Department

FILENAME	MD5 HASH	SHA1 HASH	
sample.war	570f196c4a1025a7	80f5053b166c69d81697t	Copy direct link

[Close](#)

The details dialog shows the developer's name, file details, and the MD5 and SHA1 hash values of the files.

- Click the file name to download the file for examination
- Select the request and click 'Approve' to allow the signing process to go ahead



The screenshot shows the 'Code Signing on Demand' section of the Certificate Manager. The 'Approve' button is circled in red, and a red arrow points from it to a modal dialog titled 'Approve Code Signing Request'.

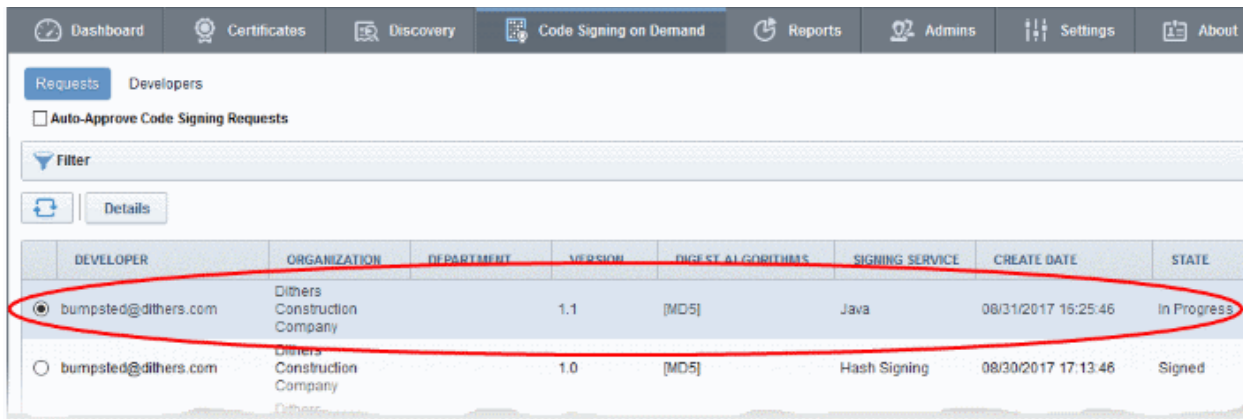
The modal dialog displays the following information:

- Developer: **bumpsted@dithers.com**
- Version: **1.1**
- Message:

FILENAME	MD5 HASH	SHA1 HASH	
sample.war	570f196c4a1025a7	80f5053b166c69d81	Copy direct link

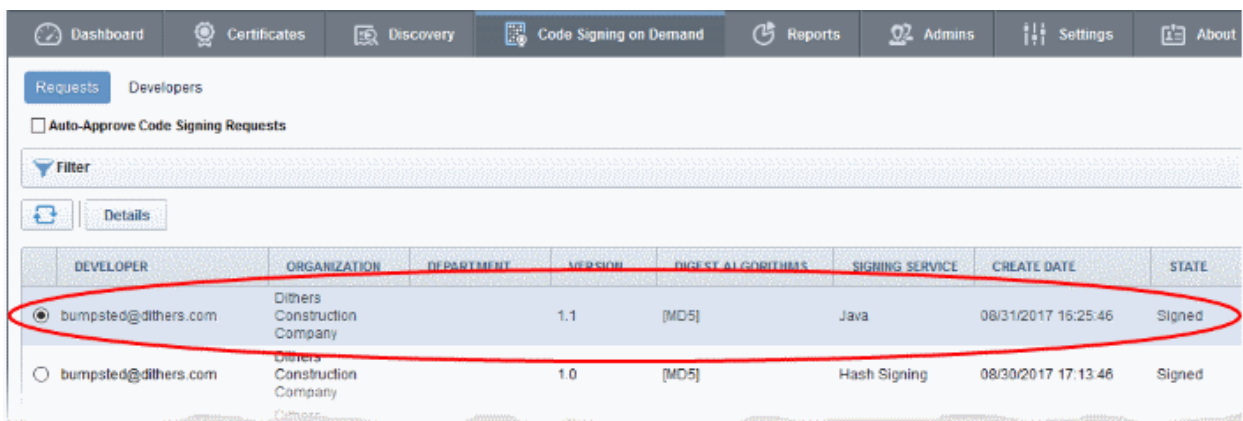
Buttons: **OK** (blue), **Cancel** (grey)

- Enter an approval message in the 'Message' field and click 'OK'
- The request will be approved and its state will change to 'In Progress':



DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
<input checked="" type="radio"/> bumpsted@dlthers.com	Dlthers Construction Company		1.1	[MD5]	Java	08/31/2017 16:25:46	In Progress
<input type="radio"/> bumpsted@dlthers.com	Dlthers Construction Company		1.0	[MD5]	Hash Signing	08/30/2017 17:13:46	Signed

- The request state will change to 'Signed' once the signing process is complete.
- 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 three days after signing.
- If required, you can resend the email by clicking 'Resend Signed Notification'

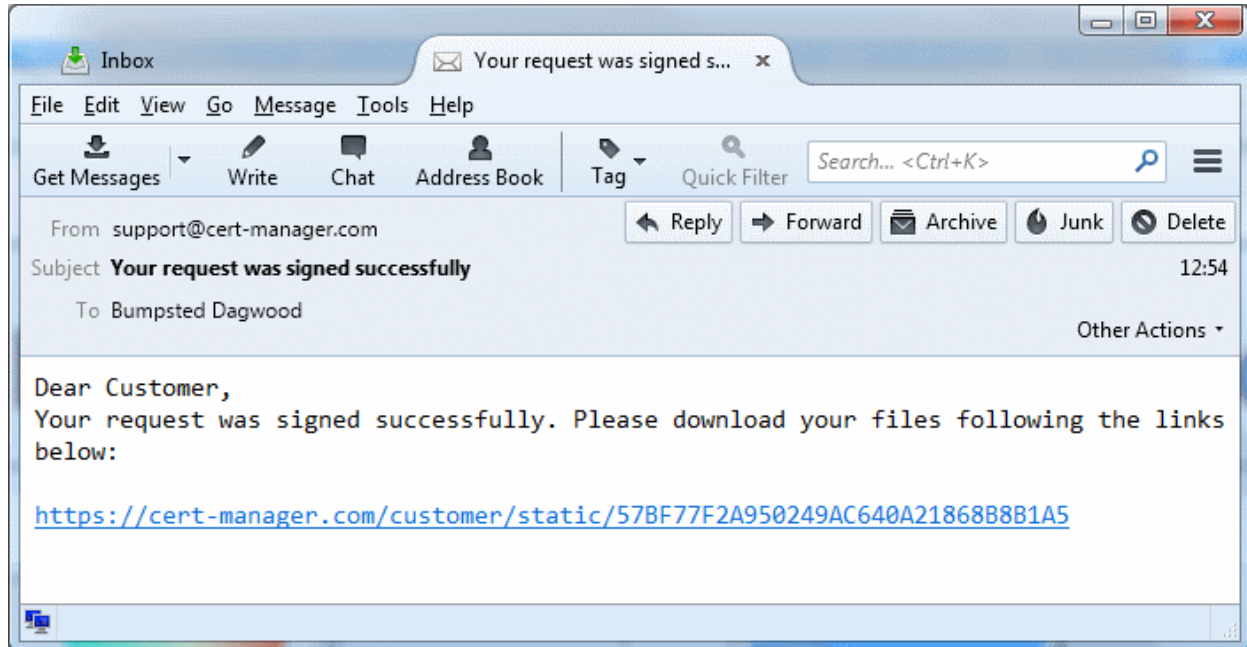


DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	DIGEST ALGORITHMS	SIGNING SERVICE	CREATE DATE	STATE
<input checked="" type="radio"/> bumpsted@dlthers.com	Dlthers Construction Company		1.1	[MD5]	Java	08/31/2017 16:25:46	Signed
<input type="radio"/> bumpsted@dlthers.com	Dlthers Construction Company		1.0	[MD5]	Hash Signing	08/30/2017 17:13:46	Signed

Note. As mentioned earlier, administrators have the option to forgo the approval process by enabling 'Auto-Approve Code Signing Requests' in the 'Code Signing on Demand' interface.

Step 3 - Download Code-Signed files

After completing the signing process, the developer will receive an email with links to download each signed file. An example is shown below.

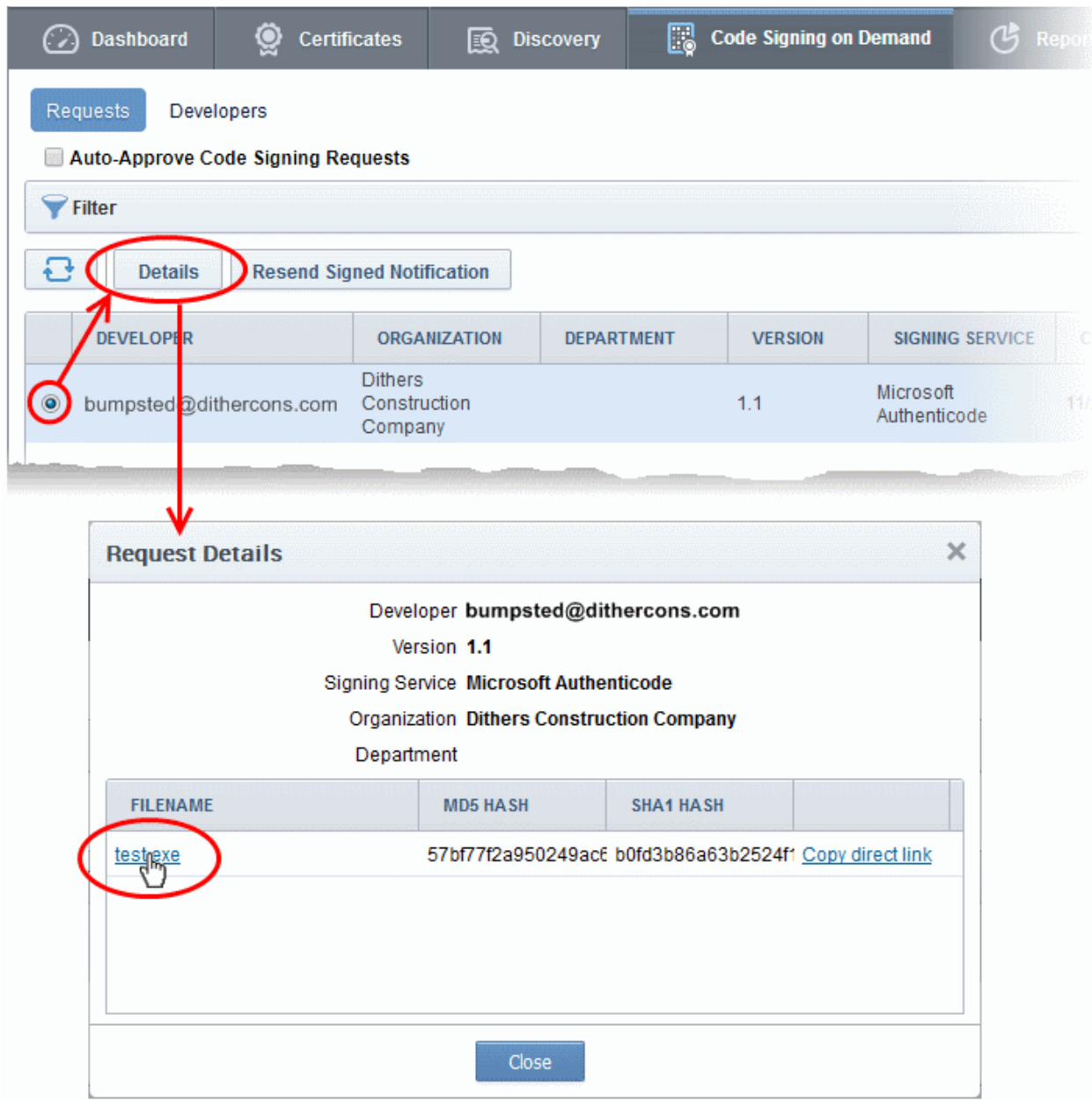


If a hash was uploaded, the developer can download the signed hash and embed it into the binary to create a digitally signed file.

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



The screenshot shows the 'Code Signing on Demand' section of the InCommon Certificate Manager. A table lists a request for developer `bumpsted@dithercons.com` from 'Dithers Construction Company' with version 1.1, signed by Microsoft Authenticode. A 'Details' button is circled in red, with an arrow pointing to a 'Request Details' dialog box. In this dialog, the file name 'test.exe' is also circled in red, with a mouse cursor hovering over it.

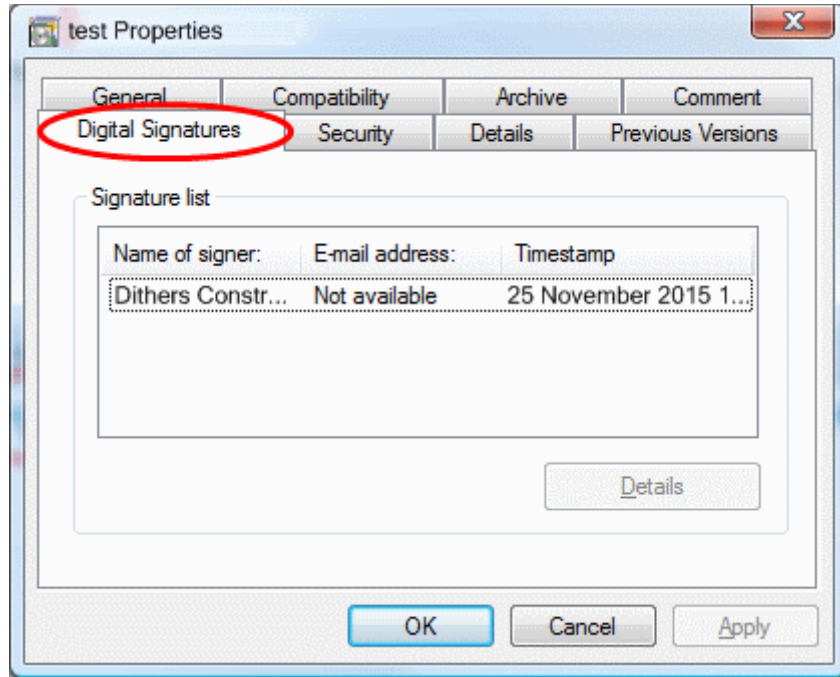
DEVELOPER	ORGANIZATION	DEPARTMENT	VERSION	SIGNING SERVICE
bumpsted@dithercons.com	Dithers Construction Company		1.1	Microsoft Authenticode

FILENAME	MD5 HASH	SHA1 HASH	
test.exe	57bf77f2a950249ac6	b0fd3b86a63b2524f1	Copy direct link

- 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 CSoD service

- By default, code signing requests from developers must be approved by an MRAO, RAO or DRAO administrator. Requests can be viewed, managed and approved in the 'Code Signing on Demand' > 'Requests' interface.

To configure the CSoD service

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



- Auto-Approve Code Signing Requests - Enable this setting if you want signing to commence without administrator approval. The service will start the signing process immediately after files are uploaded by the developer. See [How to sign code using CSoD](#) for more details.