

ENTRUST

Remote Signing Service

Administrator Quick START GUIDE

April 4, 2022

Entrust and the hexagon design are trademarks, registered trademarks and/or service marks of Entrust Corporation in Canada and the United States and in other countries. All Entrust product names and logos are trademarks, registered trademarks and/or service marks of Entrust Corporation. All other company and product names and logos are trademarks, registered trademarks and/or service marks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2022, Entrust. All rights reserved

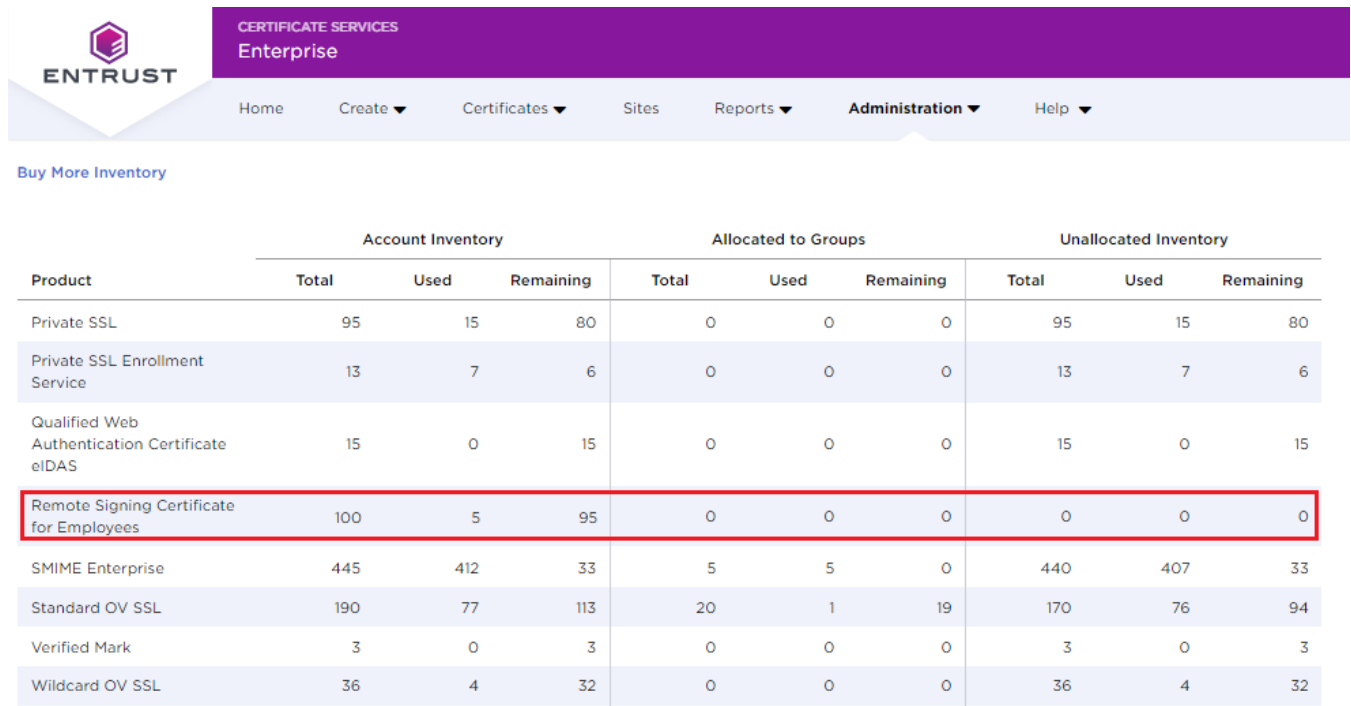
Contents

- 1 Checking the inventory.....4**
- 2 Service setup and management.....5**
 - 2.1 Signer user/employee setup 5
 - 2.2 Managing Signer users..... 7
 - 2.3 Managing Remote Signing Certificates..... 8
 - 2.4 Signer user enrollment..... 10
- 3 Integrating with signing applications12**
 - 3.1 Entrust Remote Signing Service RESTful API..... 12
 - 3.2 Entrust Desktop Virtual Card 13

1 Checking the inventory

Before starting to create the Signer users, it is recommended to check that the inventory is sufficient for the number of users that are needed.

- 1 Log in to the ECS Portal as a Super Admin or Requester user.
- 2 Navigate to **Administration > Inventory > View Total Inventory**.
- 3 Look for the row that starts with *Remote Signing Certificate for Employees* and check that the *Remaining* value is sufficient.



ENTRUST CERTIFICATE SERVICES Enterprise

Home Create ▼ Certificates ▼ Sites Reports ▼ Administration ▼ Help ▼

[Buy More Inventory](#)

Product	Account Inventory			Allocated to Groups			Unallocated Inventory		
	Total	Used	Remaining	Total	Used	Remaining	Total	Used	Remaining
Private SSL	95	15	80	0	0	0	95	15	80
Private SSL Enrollment Service	13	7	6	0	0	0	13	7	6
Qualified Web Authentication Certificate eIDAS	15	0	15	0	0	0	15	0	15
Remote Signing Certificate for Employees	100	5	95	0	0	0	0	0	0
SMIME Enterprise	445	412	33	5	5	0	440	407	33
Standard OV SSL	190	77	113	20	1	19	170	76	94
Verified Mark	3	0	3	0	0	0	3	0	3
Wildcard OV SSL	36	4	32	0	0	0	36	4	32

2 Service setup and management

The general steps for setting up the Remote Signing Service for your employees are:

- 1 In your Entrust Certificate Services Enterprise account, create a Signer user for each employee who will need to sign documents.
- 2 The employee receives an email prompting them to complete Personal Identity Validation.
- 3 When the Personal Validation has been completed, the employee receives another email, confirming success of their Personal Validation and providing a link and credentials for the RSS Portal.
- 4 The employee logs into the RSS Portal, sets up second-factor authentication, and grants consent to create their personal signing certificate.
- 5 The employee's Remote Signing certificate is created.

The employee can now sign documents. There are three ways to sign documents:

- 1 The employee chooses to sign using the Entrust Desktop Virtual Card.
 - The Desktop Virtual Card is a plug-in that allows Windows applications to use remote keys located in the Entrust Remote Signing Service for authentication and signing.
 - To Use: Activate the Entrust Virtual Card with credentials, then use a second factor authenticator to sign in from Adobe Acrobat or other Windows desktop application.
- 2 The employee chooses to sign through a Signing Partner (e.g. Adobe, Sysmosoft).
 - The employee logs in to the Signing Partner web page or application and uploads the document to be signed. When prompted to select the Digital ID provider and selecting Entrust, they will be prompted for their Remote Signing Service credentials, both first and second factors.
- 3 The employee signs using a custom signing app, developed using the CSC Remote Signing API.
 - CSC is "Cloud Signature Consortium." This body develops and maintains architectures, protocol, and API specifications for remote signature applications.
 - Entrust has developed a RESTful API based on CSC specification for use in developing custom signing applications.

2.1 Signer user/employee setup

An ECS Enterprise Super Admin or Requester user logs into the ECS Portal, and adds the employee as a Signer user.

- 1 Log in to the ECS Portal as a Super Admin or Requester user.
- 2 Navigate to **Administration > User Management**, and click **Add User**.

- 3 Select **Signer**, and click **Next**.
- 4 Complete the Signer details, and select the checkbox labelled **Allow this user to register for the Remote Signing Service**.
Note: The domain in the user's email address must be a verified domain.
- 5 Click **Submit**.

Fill in the user's name and email address. The domain in the email address must already be verified.

The new Signer user appears in the Users grid with status **Pending**.

Actions	Name ↓	Phone	User ...	Email Address	Group	Status	R
<input checked="" type="checkbox"/>	Sally Hatfield	6135555555		sally.hatfield@ Company.com		Pending	Si
<input type="checkbox"/>	name surname	6135555555		name@testcertificates.com		Pending	Si
<input type="checkbox"/>	Frank Smith			fsmith@testcertificates.com		Active	Si
<input type="checkbox"/>	Bob Lee			bob.lee@entrust.com		Active	Si

Page 1 of 1 250 items per page 1 - 10 of 10 items

The new Signer User (Sally Hatfield) receives an email containing instructions for completing Personal Validation and for obtaining the Entrust Identity application.

2.2 Managing Signer users

An ECS Enterprise Super Admin can deactivate a Signer user, if necessary; you might want to do this if the employee associated to the Signer user leaves the company or changes job responsibilities and no longer needs to sign documents.

There are two ways to deactivate a Signer user from the User grid, using the Actions menu or using the Deactivate toggle.

NOTE: When a Signer user is deactivated, their certificate is revoked and returned to inventory and can be used for another user.

- 1 Log in to the ECS Portal as a Super Admin.
- 2 Navigate to **Administration > User Management > Signer Users**.
- 3 On the row for the Signer User to deactivate:
 - Select the checkbox, and click **Actions > Deactivate**.
 - Click the toggle in the **Actions** column.
- 4 A confirmation dialog box appears. Click **OK**.

When the Signer User is deactivated, their credentials are no longer valid.

It is recommended that you also make sure that the Remote Signing certificate associated with the Signer user is revoked.

The screenshot shows the Entrust Certificate Services Enterprise interface. At the top, there's a navigation bar with 'Buy', 'Messages', 'Support', 'Chat', and 'Account'. Below that, a secondary navigation bar includes 'Home', 'Create', 'Certificates', 'Sites', 'Reports', 'Administration', and 'Help'. A search bar is located on the right. On the left, there's a sidebar with user categories: 'Add User', 'Super Admin Users', 'Sub Admin Users', 'Requester Users', 'Signer Users', and 'All Users'. The main content area displays a table of users with columns for Name, Phone, User ID, Email Address, Group, Status, and Role. The 'Actions' dropdown menu is highlighted with a red circle, showing 'Open' and 'Deactivate' options. The table lists three users: Bob Lee, Frank Smith, and TechFirst TechLast, all with 'Active' status and 'Signer' role. At the bottom, there's a pagination bar showing 'Page 1 of 1' and '250 items per page'.

2.3 Managing Remote Signing Certificates

There are three management actions that can be performed on Remote Signing Certificates.

2.3.1.1 Revoking a Remote Signing certificate – Super Admin only

If an employee leaves the company or a certificate becomes compromised, the ECS Super Admin can revoke the certificate from the ECS Portal.

NOTE: Revoked certificates are returned to inventory and can be used for another user.

- 1 Log in to the ECS Portal as a Super Admin.
- 2 Navigate to **Administration > Certificates > Managed Certificates**.
- 3 On the row for the Remote Signing Certificate to revoke, select the checkbox, and click **Actions > Revoke**.
- 4 A Revoke dialog box appears. Select a reason for revoking the certificate, and click **Confirm**.

ENTRUST CERTIFICATE SERVICES Enterprise

Home Create Certificates Sites Reports Administration Help

Buy Messages Support Chat Account

Logout

ECS Certificates Foreign Certificates Pending Approvals Pending User Pickup Active Remote Signing Pending Requester Confirmation PKI Certificates

Actions Revoke

Search: Provide at least 3

Tracking ID	Certificate Type	Common Name	Serial Number (Hex)	Pickup Status	SAN List	Cert Friendly Name	Organization (O)	Organizational Unit (OU)	Subject DN	Issue Date	Ex
<input checked="" type="checkbox"/> 494269	Remote Signing Certific...	Enric Granda	14837E55CEC34FB4E72A...	Active		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 18, 2021	Fe
<input type="checkbox"/> 494161	Remote Signing Certific...	Enric Granda	3D207E3CF567A19AA23...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494160	Remote Signing Certific...	Enric Granda	3B8FD157D328EDFF038E...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494159	Remote Signing Certific...	Enric Granda	57D9532E524AADE7273...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494158	Remote Signing Certific...	Enric Granda	22AE0B5C88DD2F4AA0...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494157	Remote Signing Certific...	Enric Granda	605DBA45C8DCBEE7BC...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494156	Remote Signing Certific...	Enric Granda	2A1FE4C0936C7A35981...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494155	Remote Signing Certific...	Enric Granda	2AD76CAB52ED9AFBA53...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494154	Remote Signing Certific...	Enric Granda	6FA664CE6859EB7DC65...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494153	Remote Signing Certific...	Enric Granda	5A4F818230412C3979F8...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 16, 2021	Fe
<input type="checkbox"/> 494143	Remote Signing Certific...	Enric Granda	216CBA7C63EFD1C7785...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 15, 2021	Fe
<input type="checkbox"/> 494139	Remote Signing Certific...	Enric Granda	5DFB3B66C5F7E9F42E...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 15, 2021	Fe
<input type="checkbox"/> 494132	Remote Signing Certific...	Enric Granda	155F02C59A127A76809D...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 15, 2021	Fe
<input type="checkbox"/> 494131	Remote Signing Certific...	Enric Granda	4CB6776C9F68FD58F5...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 15, 2021	Fe
<input type="checkbox"/> 494112	Remote Signing Certific...	Enric Granda	124D0B7AC42365B5C507...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 12, 2021	Fe
<input type="checkbox"/> 494111	Remote Signing Certific...	Enric Granda	6F28392310E79CB21334F...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 12, 2021	Fe
<input type="checkbox"/> 494110	Remote Signing Certific...	Enric Granda	7A9CFB957255BD264C8...	Renewed		entrust.com (Enric Grand...	DMortimer Company		email=enric.gran...	Feb 12, 2021	Fe

Page 1 of 10 25 items per page 1 - 25 of 240 items

© 2021 Entrust Corporation. All rights reserved. Legal Privacy Statement

2.3.1.2 Renewing a Remote Signing certificate – Signer User only

In the RSS Portal, the Signer User can see the status of their certificate at any time by clicking **Manage Certificate**. The certificate will be in one of three states:

- Active
- Expiring Soon
- Expired

The Signer User can renew their certificate by clicking **Renew Certificate**.

ENTRUST CERTIFICATE SERVICES Remote Signing Service

Home **Manage Certificate** View Activity Logout

Remote Signing Certificate Details

These are the details that make up your Signing Certificate. If any of these details change, please contact the Certificate Administrator in your company.

Status: **Expiring soon**

Owner Name: John Doe

Email: John.Doe@gigabyte.com

Organization: Gigabyte

Issue Date: Oct 13 2020, 03:30 PM

Expiry Date: Oct 14 2021, 12:00 AM

Your certificate will expire soon. Click **Renew Certificate** before the expiry date to create a new certificate, and avoid an interruption in your ability to sign documents.

Renew Certificate

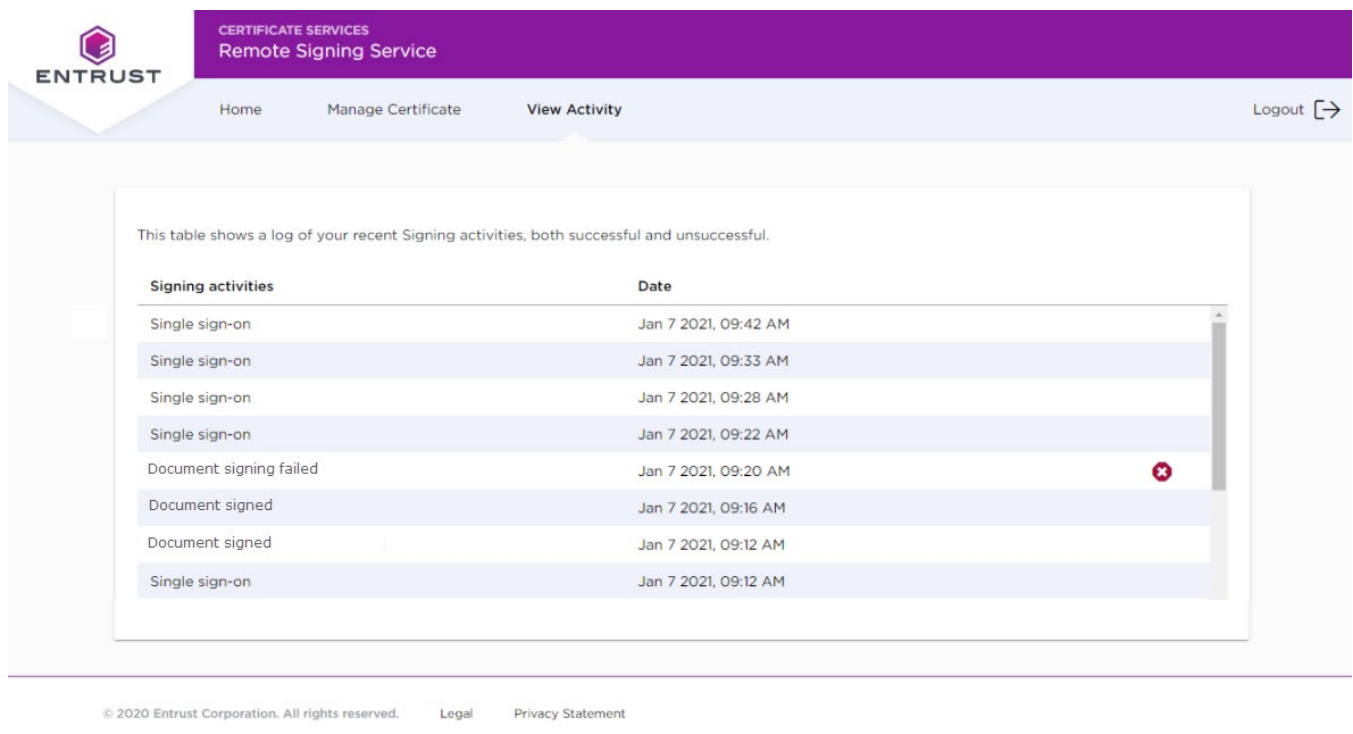
2.3.1.3 Viewing Signings log – Signer User only

In the RSS Portal, the View Activity menu allows the Signer User to see the log activity. The following events are shown on this log:

- Creation of the Signer User RSS account
- Creation of the Remote Signing certificate
- Sign-on to the Signer User Portal
- Successful document signings
- Revocation of the Remote Signing certificate

And also the failure cases:

- Failure of account creation
- Failure of certificate creation
- Failure of document signing



The screenshot shows the Entrust Remote Signing Service (RSS) portal. The header includes the Entrust logo and the text 'CERTIFICATE SERVICES Remote Signing Service'. The navigation menu has 'Home', 'Manage Certificate', 'View Activity', and 'Logout'. The main content area displays a log of signing activities. The log is a table with two columns: 'Signing activities' and 'Date'. The activities are as follows:

Signing activities	Date
Single sign-on	Jan 7 2021, 09:42 AM
Single sign-on	Jan 7 2021, 09:33 AM
Single sign-on	Jan 7 2021, 09:28 AM
Single sign-on	Jan 7 2021, 09:22 AM
Document signing failed	Jan 7 2021, 09:20 AM
Document signed	Jan 7 2021, 09:16 AM
Document signed	Jan 7 2021, 09:12 AM
Single sign-on	Jan 7 2021, 09:12 AM

The failed signing entry is marked with a red asterisk icon. Below the table, there is a footer with the text: '© 2020 Entrust Corporation. All rights reserved. Legal Privacy Statement'.

2.4 Signer user enrollment

The new Signer User receives an email containing instructions for completing Personal Validation and for obtaining the Entrust Identity application.

To enroll, the new Signer User must:

1. Follow the link to the Personal Validation form. Fill in the form, accept the license agreement and click **Submit**. Make a note of the password set here.

2. Open the email that follows to see instructions for completing Personal Validation, and complete the validation.
3. Download and install Entrust Identity for Mobile or Entrust Identity for Desktop.
4. Log into the Entrust Identity desktop or mobile app, and create an Identity. Give the new Identity a unique name.
5. Log into the RSS Portal using the email address and password from step 1, then enter the code generated using the Entrust Identity desktop or just tap on the push notification received in the Entrust Identity app.
6. Click **Create Remote Signing Certificate**, and Authorize creation of the certificate.

When these steps are complete, the Signer User is ready to sign documents.

The screenshot shows the Entrust Remote Signing Service web interface. At the top left is the Entrust logo. The top navigation bar is purple and contains the text 'CERTIFICATE SERVICES' and 'Remote Signing Service'. On the top right, there is a 'Logout' link with an arrow icon. The main content area has a light blue header that reads 'Create your Remote Signing Certificate'. Below this header, the text states: 'To prepare to sign documents using the supported signing providers, you need to create your Remote Signing Certificate. This is a two-step process:'. This is followed by a numbered list: '1. Click the **Create Remote Signing Certificate** button below.' and '2. On the Consent screen that appears, grant your consent to create the certificate.' Below the list, it says 'And that's it! You will then be ready to begin signing documents. You can find a list of supported signing providers at <https://www.entrust.com/go/remote-signing>.' At the bottom center of the content area, there is a blue button with the text 'Create Remote Signing Certificate', which is circled in red.

3 Integrating with signing applications

As described above, the Entrust Remote Signing Service is deployed in the cloud. It relies on the CSC (Cloud Signature Consortium) Remote Signing Protocol for communication between your applications and the Entrust service.

The service can also be used from user desktop applications through the Entrust Desktop Virtual Card plug-in that allows applications to connect transparently to the Entrust Remote Signing Service for signing.

3.1 Entrust Remote Signing Service RESTful API

The RESTful API is based on the CSC specification v0.1.7.9 for remote electronic signatures. This API is used to integrate cloud signing applications with the Remote Signing Service so that Remote Signing certificates can be used to perform document signing.

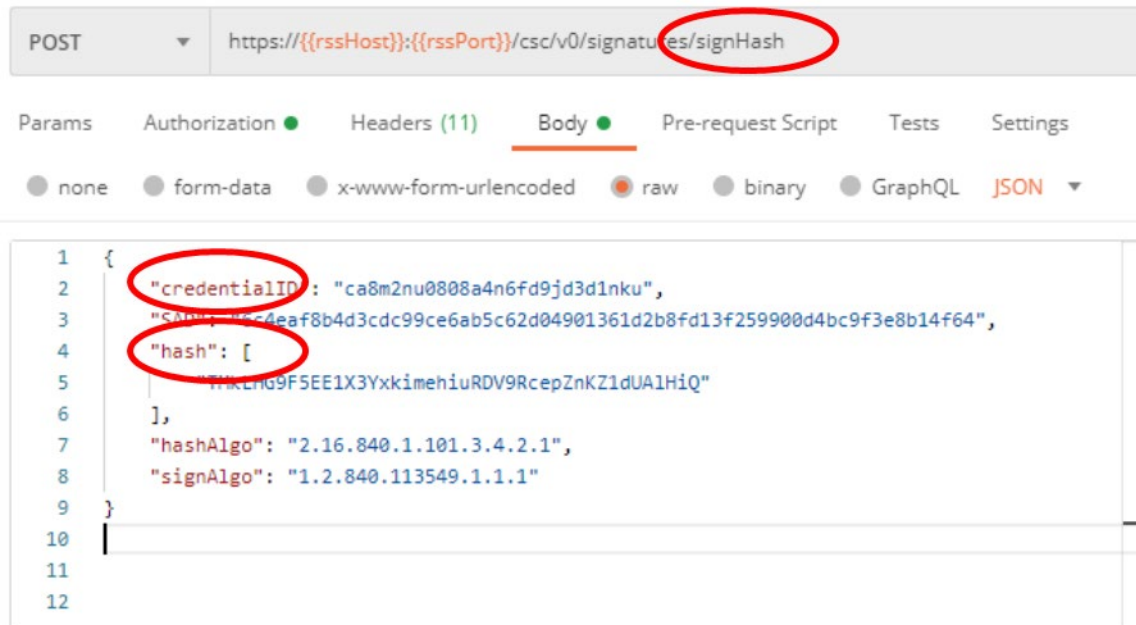
- Signing applications authenticate to the API using the CSC-standard *clientID* and *clientSecret*, supplied by Entrust when signing providers register.
- The Signer user Remote Signing certificate is retrieved from the Entrust RSS and the document is prepared for signing.
- The signing application creates the hash of the Signer user's document and sends it to the RSS.
- The signed hash (the signature) is "attached" to the document being signed. One document can be signed in each transaction.

The Entrust Remote Signing Service includes timestamping and OCSP validation services; these services are used through the standard IETF protocols.

The following CSC API operations are supported:

Operations	Description
info oauth2/authorize oauth2/token	These operations do not require an access token.
credentials/list credentials/info	These operations require 1 access token: "service".
signhash	These operations require 2 access tokens: "service" and "credential".

A signHash operation example follows.



The CSC API Reference Guide and the demo tutorial examples prepared to run with the Postman tool and instructions are available from the ECS Portal: **Help > API Documentation**.

3.1.1 Timestamp and OCSP server

When adding timestamps to signatures, the signature date is accurate and backed by a trusted entity. Timestamps also allow creating Long Term Validation (LTV) signatures when combined with the certificate revocation status provided by the OCSP server.

The Timestamp and OCSP URL services are available in the Remote Signing certificates issued by Entrust.

3.2 Entrust Desktop Virtual Card

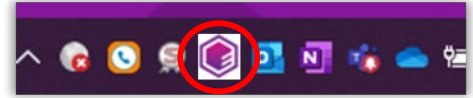
The Desktop Virtual Card is a plug-in that enables digital signatures using remote keys located in the Entrust Remote Signing Service. Depending on the type of certificate, it also can be used for web authentication with digital certificate.

From a user's perspective, it acts like a virtual smartcard because they can remotely utilize PKI keys and certificates in the Service from their desktop applications and office software.

3.2.1 Desktop Virtual Card setup

Users can download the Virtual Card from the RSS Portal and install the plug-in in one or more computers.

The virtual card tray icon shows the connection status (logged in/logged out) and the certificate information.



3.2.2 Signing with the virtual card

The Signer user experience is the same as when using USB tokens. The user will provide their second factor authenticator to activate the Entrust Remote Signing key and create the signature with their desktop application.

