

|  |
| --- |
| Client incident management systemApplication program interfaceCertificationHow to guideVersion 1.1 August 2017 |

|  |
| --- |
| Client incident management systemApplication program interfaceCertificationHow to guideVersion 1.1 August 2017 |
|  |

|  |
| --- |
|  |
| To receive this publication in an accessible format email CIMS CIMS@dhhs.vic.gov.auAuthorised and published by the Victorian Government, 1 Treasury Place, Melbourne.© State of Victoria, Department of Health and Human Services June 2017.Available on the [funding agency channel](https://www.dhs.vic.gov.au/funded-agency-channel/about-service-agreements/incident-reporting) at https://www.dhs.vic.gov.au/funded-agency-channel/about-service-agreements/incident-reporting |
|  |

Contents

[How to get and properly setup a SSL certificate for client authentication? 5](#_Toc484683877)

[Step 1 5](#_Toc484683878)

[Step 2 5](#_Toc484683879)

[Step 3 6](#_Toc484683880)

[Step 4 6](#_Toc484683881)

[Error 403 – Mutual SSL is failing 7](#_Toc484683882)

[How to download the swagger definition file 8](#_Toc484683883)

[Organisation name and API user details 8](#_Toc484683884)

[Example JSON for API interface Incident POST/PUT (Create/Update) 9](#_Toc484683885)

[Frequently Asked Questions (FAQ) 12](#_Toc484683886)

[What is a client certificate authentication? 12](#_Toc484683887)

[What is a digital certificate? 12](#_Toc484683888)

[What is a public key certificate? 12](#_Toc484683889)

[What is meant by SSL handshake? 12](#_Toc484683890)

[What is an authentication certificate? 12](#_Toc484683891)

[How does an SSL work? 12](#_Toc484683892)

[What is mutual authentication? 12](#_Toc484683893)

[What is the certificate authority? 12](#_Toc484683894)

[How do public and private keys work? 12](#_Toc484683895)

# How to get and properly setup a SSL certificate for client authentication?

## Step 1

For production environments, the organisation will need to buy a certificate from a trusted Certificate Authority. The certificate must be issued to the organisations domain.

* Wild card certificates are accepted.
	+ Multiple domain certificates will not be accepted.

For test environments, the organisation will need to generate a new self-signed certificate:

* Either with “<All>” intended purposes;
	+ Or “Client Authentication” intended purpose.

## Step 2

Install the certificate.

Once the certificate is generated, please install it **with the private keys** under the personal store of “Certificates – Current User” and “Certificates – Local Machine”.

Figure Certificate installed with intended purpose of client authentication



Please note the icon of the installed certificate has a small key drawn on the top-left corner . This indicates that the certificate has been installed with the private keys.

Figure Enhanced key usage details for a certificate with client authentication purposes



## Step 3

Activate the certificate.

Please forward the certificate’s .CER file to the Department of Health and Human Services (department) so that DHHS can load it into our systems. Please ensure that it is the .CER file that is forwarded, as this file contains only the public key of certificate. Do not share the certificate’s private key with any parties.

## Step 4

Update the organisations site to use HTTPS.

The CIMS API interface will authenticate external applications through Mutual SSL authentication mechanism. The DHHS servers will present a certificate issued to CN = \*.cims.vic.gov.au. It is the organisations responsibility to validate the department’s certificate to ensure that it is connecting to the department’s servers.

The interface will allow external systems to submit completed incidents to CIMS for review. Any further communication regarding the submitted incident will be managed through email notifications workflows.

The link to ‘swagger’ for CIMS API Non-production environment is:

* + [Swagger user interface](https://api-cims-dev-staging.azurewebsites.net/swagger/docs/v1) <https://api-cims-dev-staging.azurewebsites.net/swagger>

# Error 403 – Mutual SSL is failing

“Error 403 – This web app is stopped”, means that Mutual SSL is failing.

Has the certificate been imported with the private keys or public keys only? If only the .CER file was imported, than only the public keys have been imported, which will then fail connection when establishing SSL with mutual authentication.

Certificates will be imported together with their private keys usually through .PFX files.

To test the connection to CIMS with your browser (such as Google Chrome), import the PFX file under the “Personal” certificates store. Certificates imported with their private keys will contain an icon with a small key on the top left.

Figure Certificate imported with the private key



The imported certificate needs to have an Intended Purpose of “<All>” or “Client authentication”. To verify if the certificate can be used for client authentication purposes:

1. Open the **Microsoft Management Console**
2. Click on menu option **File 🡪 Add/Remove Snap-in…**. A new window will open.
3. On the **Add/Remove Snap-ins** window, select **Certificates** on the list on the left and click the “**Add >**” button. A new window will open.
4. On the **Certificates snap-in** window, select the account where the certificate is installed. If testing the Swagger UI link, select the **My user account** option. Once an option has been selected, click the **Finish** button to return to the previous window
5. Click the **OK** button to return to the previous window
6. Back in the Microsoft Management Console’s main window, the list on the left will contain a ”**Certificates – Current User**” item. Go to the “**Certificates – Current User 🡪 Personal 🡪 Certificates**” folder.
7. The list on the right will show the certificates installed in the personal store. The value of the “**Intended Purposes**” must list “<All>” or “Client Authentication”.

Figure Certificates installed with the private key and client authentication intended purpose.



# How to download the swagger definition file

The swagger definition file for the CIMS API can be downloaded through the following URL:

* + [Swagger definition](https://api-cims-dev-staging.azurewebsites.net/swagger/docs/v1) <https://api-cims-dev-staging.azurewebsites.net/swagger/docs/v1>

Prior to testing the CIMS API interface it is advised that the JSON payloads are verified using a [JSON validator](https://jsonformatter.curiousconcept.com/) such as https://jsonformatter.curiousconcept.com/.

When submitting incidents through the CIMS API, please use the “Organisation name” provided by the department.

To submit a new incident, use the POST incident endpoint.

Once an incident has been submitted successfully, the response to the request on the POST Incident Endpoint will return a new “incidentId”, which will be in the format of a GUID (XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX).

The “PUT” http verb (which we’ll call PUT Incident endpoint) should only be used when updating an incident that has been previously submitted with the “POST” http verb (which is called the POST Incident endpoint).

If subsequent updates to this same incident are required, use the PUT Incident endpoint with the new incident data. The “incidentId” that was returned through the response of the POST Incident endpoint must be specified in the URL.

Possible errors:

* The JSON is not valid, i.e. format errors etc. This can be verified by using a JSON validator.
* The version number of the reference data in the JSON is incorrect.
	+ On a PUT request the GUID in the URL is incorrect.

# Organisation name and CIMS API user details

The organisation name that is linked to the certificate is very important. This should be the name of the service provider and should match the organisation name in the CIMS system.

This name must be the name provided in the incident report details:

* + "organisationName": "External Organisation name"

A designated email address must be provided for each organisation that is submitting incidents via the CIMS API so that emails can be received by the external service providers from the department.

# Incident statuses

The organisation name that is linked to the certificate is very important. This should be the name of the service provider and should match the organisation name in the CIMS system.

This name must be the name provided in the incident report details:

* "organisationName": "External Organisation name"

A designated email address must be provided for each organisation that is submitting incidents via the CIMS API so that emails can be received by the external service providers from the department.

# Example JSON for CIMS API interface Incident POST/PUT (Create/Update)

The “externalIncidentId” must be the unique incident id from the vendor’s system.

The “reportedDate” is used as the 24 hour trigger for Major incidents.

The “referenceVersion” number must equal a valid reference data version number.

The payloads for POST and PUT Incident are the same. However, on [PUT requests](https://api-cims-dev-staging.azurewebsites.net/api/Incidents/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX), the ‘incidentId’ is required as part of the url i.e. https://api-cims-dev-staging.azurewebsites.net/api/Incidents/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

{

 "externalIncidentId": "1",

 "reportedDate": "2017-03-10T08:00:00.000Z",

 "referenceVersion": 1,

 "incidentData": {

 "organisationName": "External Organisation name",

 "organisationAddressStreetNumberAndName": "50 Lonsdale",

 "organisationAddressSuburb": "Melbourne",

 "organisationAddressState": "VIC",

 "organisationAddressPostCode": "3141",

 "dhhsArea": "Goulburn",

 "program": "Disability",

 "serviceType": "Targeted services",

 "incidentDate": "10/03/2017",

 "incidentDateAccuracy": "As I was told",

 "incidentTime": "11:30",

 "incidentTimeAccuracy": "As I was told",

 "incidentDisclosedDate": "10/03/2017",

 "incidentDisclosedTime": "00:30",

 "incidentLocation": "Incident location is Laverton",

 "incidentDescription": "This is the description for the incident",

 "briefSummaryOfIncident": "This is the brief summary of the incident",

 "reportedToPolice": "Yes",

 "policeInvestigationInitiated": "Yes",

 "staffStoodDown": "Not applicable",

 "officerGivenName": "Officer Given Name Co",

 "officerSurname": "Officer Sur Name Co",

 "officerRole": "Officer Role",

 "dateCompleted": "11/03/2017",

 "officerPhoneNumber": "123456677",

 "officerAccessRestricted": "No",

 "officerEmail": "officer@gmail.com",

 "officerComment": "These are the comments from the reporting officer",

 "majorDelegateSurname": "minor Rajannna",

 "majorDelegateGivenName": "major Rajannn",

 "majorDelegateRole": "Major Delegate Role",

 "majorAuthorisationDate": "10/03/2017",

 "majorDelegatePhone": "1234545454",

 "majorDelegateEmail": "majorDelegate@email.com",

 "clients": [

 {

 "impactType": "Non-Major",

 "sourceSystem": "CRIS number",

 "sourceSystemId": "11111",

 "surname": "surName",

 "givenName": "givenName",

 "sex": "Not Stated/Inadequately Described",

 "indigenousStatus": "Torres Strait Islander but not Aboriginal",

 "birthDate": "21/01/2000",

 "addressStreetNumberAndName": "50 Lonsdale Street",

 "addressSuburb": "Melbourne",

 "addressState": "VIC",

 "addressPostCode": "3141",

 "lastServiceDate": "05/09/2016",

 "primaryIncidentType": "Emotional/psychological abuse",

 "primaryAllegedPerpetratorVictim": "Staff to Client",

 "primaryRoleInIncident": "Victim",

 "immediateSafetyNeedsMet": "No",

 "medicalAttentionProvided": "No",

 "debriefingOrCounselling": "No",

 "referralToSupportServices": "No",

 "supportPlanChanged": "No",

 "carerNotified": "No"

 }

 ],

 "others": [

 {

 "surname": "Water1",

 "givenName": "Earth1",

 "relationToClient": "Paid Staff",

 "incidentRole": "Alleged perpetrator",

 "birthDate": "19/12/1979"

 }

 ]

 }

}

# Frequently Asked Questions (FAQ)

## What is a client certificate authentication?

In cryptography, a client certificate is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester’s identity.

## What is a digital certificate?

Digital Certificates are a means by which consumers and businesses can utilise the security applications of Public Key Infrastructure (PKI). PKI comprises of the technology to enable secure e-commerce and Internet based communication.

## What is a public key certificate?

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove the ownership of a public key.

## What is meant by SSL handshake?

SSL handshake is the negotiation that happens between a client and server to start a SSL session.

## What is an authentication certificate?

With user certificates, the certificate is issued by a certification authority, who guarantees the link between a physical identity and a cryptographic public key. The verifier may be a distinct entity, and can verify such a link and use it to authenticate the user, without getting the ability to impersonate the user.

## How does an SSL work?

The browser/client requests that the web server identities itself. The web server sends the browser/client a copy of its SSL certificate. The browser/client checks to see whether or not it trusts the SSL certificate. The web server sends back a digitally signed acknowledgement to start an SSL encrypted session.

## What is mutual authentication?

Mutual Authentication is a security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection.

## What is the certificate authority?

A certificate authority (CA) is a trusted entity that issues electronic documents that verify a digital entity’s identity on the Internet. The electronic documents, which are called digital certificates, are an essential part of secure communication and play an important part in the public key infrastructure (PKI).

## How do public and private keys work?

An unpredictable (typically large and random) number is used to begin generation of an acceptable pair of keys suitable for use by an asymmetric key algorithm. In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt.