Digitally signed by National E-Health Transition Authority Ltd
Date: 2013.02.25 15:45:52 +11'00'

ACK RELEASE DATE	29/10/2012	ID	1.0.0	CONTACT	Philip Wilford
CATEGORY	**Vendors & Integration**				
AFFECTS	**<All Sites>**				
TOPIC	**Trusted Certificates**				
DETAIL	**Question:** When receiving a CDA Package, how can we ensure that the content is from a trusted source?				

Answer

CDA packaged content received from services including PCEHR and Secure Message Delivery can assert the approver/sender of the document. This is achieved by the inclusion of a digital signature that signs the content and asserts an identity.

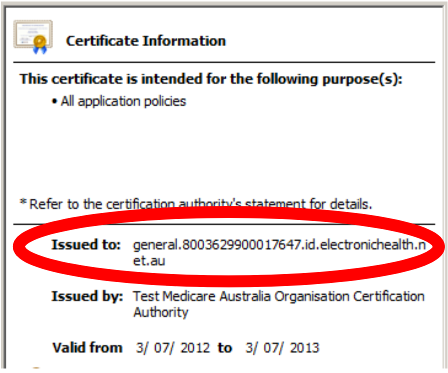
The digital signature itself will include a public key infrastructure (PKI) certificate issued by a Certificate Authority (CA) and if it is necessary to validate the signature then an appropriate process needs to be is applied to ensure the identity of the source of content received can be trusted.

The digital signature (eSignature) can be found in CDA Package manifest as a fixed filename *CDA_SIGN.xml.* It signs the payload *CDA_ROOT.xml* and contains a signing certificate in the PKI X509 v3 format. These can be found in the *X509Certificate* (*http://www.w3.org/2000/09/xmldsig#*) element in the Signed Container structure as defined by *E-Health XML Secured Payload Profiles* [Standards Australia ATS 5821—2010]. Certificates can be checked in the following ways to ensure they are valid and can be trusted.

Example CDA_SIGN.XML

```
<signedPayload xmlns="http://ns.electronichealth.net.au/xsp/xsd/SignedPayload/2010">
  <signatures>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <Reference URI="#dca2eab1-f1fe-47e9-8148-32118f15c570">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <DigestValue>v3S1Qap+gvFvIimucRaiok5j1A8=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>...Signature Value...</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509Certificate>...PEM Format Certificate...</X509Certificate>
        </X509Data>.
      </KeyInfo>
    </Signature>
  </signatures>
  <signedPayloadData id="dca2eab1-f1fe-47e9-8148-32118f15c570">
    <q1:eSignature xmlns:q1="http://ns.electronichealth.net.au/cdaPackage/xsd/eSignature/2012">
      <Manifest xmlns="http://www.w3.org/2000/09/xmldsig#">
        <Reference URI="CDA_ROOT.XML">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <DigestValue>O5h7+qbsKhNk/nCqATqknyjQyoc=</DigestValue>
        </Reference>
      </Manifest>
      <q1:signingTime>2012-04-24T04:00:40.0134816Z</q1:signingTime>
      <q1:approver>
        <q1:personId>http://ns.electronichealth.net.au/id/hi/hpii/1.0/800361xxxxxxxxxx</q1:personId>
        <q1:personName>
          <q1:nameTitle>Dr.</q1:nameTitle>
          <q1:givenName>Andrew</q1:givenName>
          <q1:familyName>JOHNS</q1:familyName>
          <q1:nameSuffix>Jr</q1:nameSuffix>
        </q1:personName>
      </q1:approver>
    </q1:eSignature>
  </signedPayloadData>
</signedPayload>
```

1) *Check the issued to identity matches the asserted approver/sender of the content.*



Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

* Refer to the certification authority's statement for details.

Issued to: general.8003629900017647.id.electronichealth.net.au

Issued by: Test Medicare Australia Organisation Certification Authority

Valid from 3/ 07/ 2012 to 3/ 07/ 2013

Within the certificate itself check the identity by looking at the 'Issued to' details and ensure the identity there is consistent to that provided in the details of the CDA Package [The certificate can be found in PEM format highlighted in yellow in the example above].

For PCEHR, the identity SHOULD match up with the author organisation of the uploadDocument B2B operation which can be found in the metadata logical field called author:authorInstitution or in the CDA document xpath:

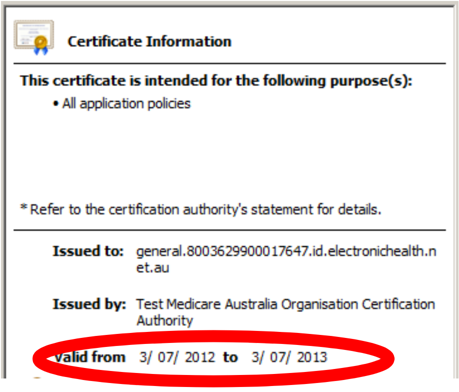
/cda:ClinicalDocument/cda:author/cda:assignedAuthor/cda:assignedPerson/ext:asEmployment/ext:employerOrganization/cda:asOrganizationPartOf/cda:wholeOrganization/ext:asEntityIdentifier/ext:id

For SMD, the identity SHOULD match up to the senderOrganisation field in the metadata of the deliver SMD operation.

The match can also be made more complicated in that the organisational identifiers may be networked organisations of the certificate (which could be higher up in the organisation chart).

For this reason, a warning MAY be given to the user if there is a mismatch.

2) *Check the document creation date-time is within the period of validity of the certificate.*



Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

* Refer to the certification authority's statement for details.

Issued to: general.8003629900017647.id.electronichealth.net.au

Issued by: Test Medicare Australia Organisation Certification Authority

Valid from 3/ 07/ 2012 to 3/ 07/ 2013

Check the CDA document within the CDA package was created within the valid period for the certificate.

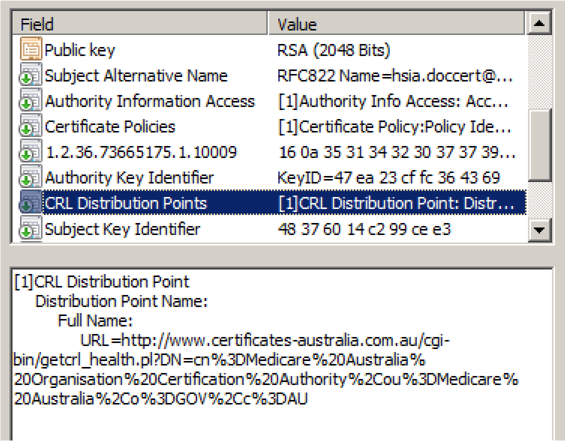
This has to be taken into consideration, as a stored CDA package will eventually contain an out of date certificate.

3) *Check that the Certificate Authority had not revoked the certificate at time of use*

When it comes to checking if a certificate has been revoked by a CA, each certificate contains a related policy with the details of where to find the Certificate Revocation List (CRL) and the On-line

Certificate Status Protocol (OCSP). Either method can be used to gain the current status of the certificate. Software tools exist to easily verify certificate trust chain and revocation lists such as with .NET (System.Security.Cryptography.X509Certificates) and Java – Bouncy Castle (java.security.spec.x509EncodedKeySpec).

Check the CDA document within the CDA package was created and signed by a certificate that wasn't revoked at that time. If it has been revoked, check the revocation date and make sure the CDA Package was created before that date.

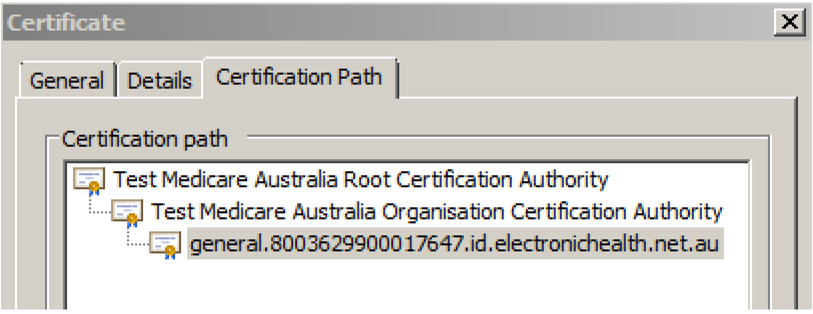


Field	Value
Public key	RSA (2048 Bits)
Subject Alternative Name	RFC822 Name=hsia.doccert@...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
1.2.36.73665175.1.10009	16 0a 35 31 34 32 30 37 37 39...
Authority Key Identifier	KeyID=47 ea 23 cf fc 36 43 69
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Subject Key Identifier	48 37 60 14 c2 99 ce e3

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://www.certificates-australia.com.au/cgi-
bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%
20Organisation%20Certification%20Authority%2Cou%3DMedicare%
20Australia%2Co%3DGOV%2Cc%3DAU
```

4) *Check the Certificate Authority that issued the certificate can be trusted.*

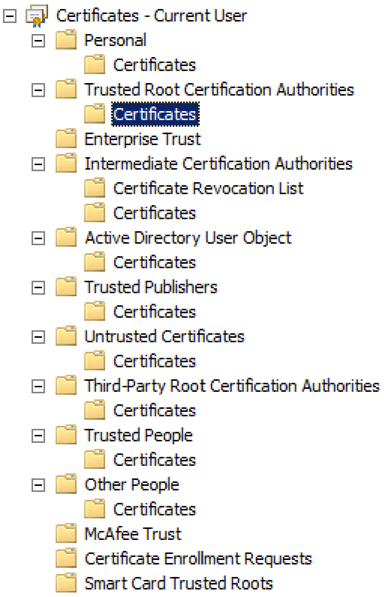
To check the Certificate Authority, each certificate has a Certification Path which shows the certificate chain (or hierarchy) of where it came from. For example:



```
Test Medicare Australia Root Certification Authority
    Test Medicare Australia Organisation Certification Authority
        general.8003629900017647.id.electronichealth.net.au
```

Generally there are two levels of CA; a Root Certificate, and an Intermediary Certificate. The Root certificate usually has a long expiry period (20 years), whilst the Intermediary Certificate has a shorter life span (10 years) which allows a CA to create multiple Intermediaries with different Policy settings, grouping private keys under these Intermediaries.

For a certificate to be trusted for use generally the 'Trusted Root Certification' and 'Intermediate Certification' Authorities that issued the certificate will be registered in a certificate trust store. This allows configuration of the operating environment to



```
Certificates - Current User
    Personal
        Certificates
    Trusted Root Certification Authorities
        Certificates
    Enterprise Trust
    Intermediate Certification Authorities
        Certificate Revocation List
        Certificates
    Active Directory User Object
        Certificates
    Trusted Publishers
        Certificates
    Untrusted Certificates
        Certificates
    Third-Party Root Certification Authorities
        Certificates
    Trusted People
        Certificates
    Other People
        Certificates
    McAfee Trust
    Certificate Enrollment Requests
    Smart Card Trusted Roots
```

trust certificates for an identified list of certificate issuing Certificate Authorities. For example this may be a Windows Current User Certificate Store (in the *Trusted Root Certification Authorities* and *Intermediate Certification Authorities* folders) or a Java Trust Store.

Trusted Certificate Authorities

There are a number of well-known Certificate Authorities that are in use today within e-health. The National Authentication Service for Health (NASH) was set up to be the one single source of CA within e-Health. There have been a number of delays in the project, and as such, interim solutions have been put in place.

Medicare Australia currently has a PKI solution in place for Claims and Payments, as well as for the HI Service, and with the delay of NASH, has also supplied an interim solution for the PCEHR.

For vendor software, it is suggested that the following Root and Intermediate CA certificates are included in your installations. These include both Test and Production versions:

Medicare Australia (production)	Medicare Australia Root CA.cer Medicare Australia Organisation CA.cer (2006-2016) Medicare Australia Organisation CA.cer (2012-2022) Sourced from: http://www.certificates-australia.com.au/general/cert_search_health.shtml
Medicare Australia (testing)	Test Medicare Australia Root CA.cer Test Medicare Australia Organisation CA.cer (2006-2016) Test Medicare Australia Organisation CA.cer (2012-2022)

These would be in addition to the well-known CAs such as Verisign, Thawte, Entrust, Geotrust to name but a few.

All certificates can be downloaded from this location: http://www.nehta.gov.au/vendors

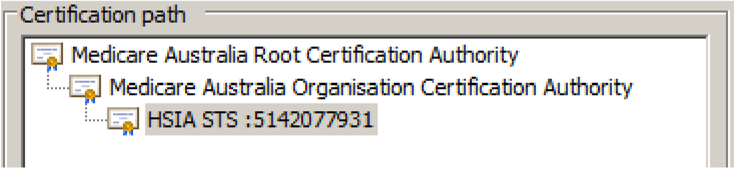
Further certificate details below:

Medicare Australia Root Certificates

Subject	Medicare Australia Root Certification Authority
Thumbprint	8b e8 08 c2 25 44 18 b1 85 57 84 b6 e1 93 4b f9 ed 66 25 7c
Valid from	Monday, 10 Jul 2006 3:53:18 PM
Valid to	Friday, 10 Jul 2026 3:50:41 PM

Subject	Medicare Australia Organisation Certification Authority
Thumbprint	a1 c0 9b 11 5e 99 88 3e d3 62 2e 46 4e 01 ba 3c 16 56 f8 be
Valid from	Monday, 10 Jul 2006 4:53:41 PM
Valid to	Sunday, 10 Jul 2016 4:50:52 PM

Subject	Medicare Australia Organisation Certification Authority
Thumbprint	86 5c ae 52 61 53 ec a9 3a 87 6e 2f 09 07 cb a3 5c 9a 9b 19
Valid from	Tuesday, 13 Mar 2012 10:24:05 AM
Valid to	Sunday, 13 Mar 2022 10:23:51 AM



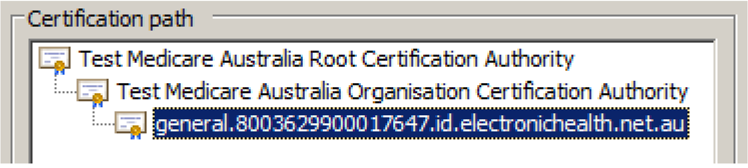
- Medicare Australia Root Certification Authority
  - Medicare Australia Organisation Certification Authority
    - HSIA STS :5142077931

Test Medicare Australia Root Certificates

Subject	Test Medicare Australia Root Certification Authority
Thumbprint	2b 3b 5c 37 a1 6b f8 06 fc ee d1 f5 6f 2b a1 ca e0 ec f0 91
Valid from	Monday, 14 Aug 2006 3:25:38 PM
Valid to	Friday, 14 Aug 2026 3:25:07 PM

Subject	Test Medicare Australia Organisation Certification Authority
Thumbprint	2d 89 cd bc 41 b9 e2 f1 14 3d 93 72 19 eb 95 a0 28 d8 52 16
Valid from	Monday, 14 Aug 2006 3:43:28 PM
Valid to	Sunday, 14 Aug 2016 3:43:08 PM

Subject	Test Medicare Australia Organisation Certification Authority
Thumbprint	0b 30 51 be 82 52 45 af 0b 04 73 69 da d9 9e 34 ca aa 40 a4
Valid from	Monday, 5 Mar 2012 10:54:26 AM
Valid to	Saturday, 5 Mar 2022 10:54:10 AM



- Test Medicare Australia Root Certification Authority
  - Test Medicare Australia Organisation Certification Authority
    - general.8003629900017647.id.electronichealth.net.au