



**Australian Government**  
**Medicare Australia**

# **PKI API Glossary**

## **PKI eSignature API**

Release Date: September 2008

Online Technical Support: 1300 550 115  
Email: [pki@medicareaustralia.gov.au](mailto:pki@medicareaustralia.gov.au)



Use of the Medicare Australia eSignature API Version V2.3.1 is subject to the terms of the  
Medicare Australia eSignature API Licence Agreement.

**Copyright © 2008- Medicare Australia - Canberra Australia**

This product uses software from the **OpenSSL** and **SQLite** toolkits.

**OpenSSL:**

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>) Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

This product includes cryptographic software written by Eric Young. ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))

**SQLite:**

This product includes software developed by Hwaci - Applied Software Research. (<http://www.sqlite.org/>)

This product was written by Dr. Richard Hipp ( [drh@hwaci.com](mailto:drh@hwaci.com) ) and is unrestricted open source.

## Version Log

Version	Description	Date	Author
0.1	Initial draft	August 2003	Neil Britliff
0.2	Draft update	15/02/2006	Kip Deveson
0.3	Final update	24/03/2006	Kip Deveson
1.0	First Release	17/05/2007	Kip Deveson
1.1		02/09/2008	Kevin Wong

## Table of Contents

<b>Introduction .....</b>	<b>1</b>
Purpose.....	1
Scope.....	1
Stakeholders .....	1
Target Audience.....	1
Pre-Requisites .....	1
<b>PKI API Glossary.....</b>	<b>2</b>

## Introduction

This manual is a Glossary for use with all of the Medicare Australia PKI eSignature API Reference Manuals.

## Purpose

The purpose of this document is to provide a glossary of terms and acronyms for use with the Medicare Australia PKI eSignature API reference documents.

## Scope

The scope of this document only covers the terms and acronyms used in the Medicare Australia PKI eSignature API reference documents.

## Stakeholders

The stakeholders in this document/product are:

- PKI Team, Solutions Branch, ITSD, Medicare Australia
- Medicare Australia Applications Developers
- Vendor Applications Developers

## Target Audience

The target audience of this document is:

- Medicare Australia Applications Developers
- Vendor Applications Developers

## Pre-Requisites

There are no pre-requisites for the reader to understand and be able to use this document.

## PKI API Glossary

Term	Description
<b>Bouncy Castle</b>	The Cryptographic Toolkit used by the webMethods PKI toolkit.
<b>CRL</b>	The Certificate Revocation List
<b>HL7</b>	The Health Level Seven message format, a standard for clinical data interchange.
<b>HOP3</b>	The messaging protocol used by HIC Online to communicate between client adaptor, server adaptor and HUB
<b>HTTP</b>	Hypertext Transfer Protocol. The communications protocol upon which the World Wide Web (WWW) is based. HTTP is implemented on top of the TCP/IP protocol, which provides a reliable connection-oriented transport
<b>HUB</b>	The central component in the HIC Online architecture, used as a coordinator for business processes.
<b>J2EE</b>	Java 2 Enterprise Edition development standard.
<b>JAXB</b>	The Java XML Binding Architecture – a standard for mapping between XML Schemas and Java objects
<b>JKS</b>	Java Key Store
<b>JNI</b>	Java Native Interface.
<b>Key</b>	A large number used by a cryptographic algorithm to encrypt or decrypt data. A person's public key, for example, allows other people to encrypt messages to that person. The encrypted messages must be decrypted with the corresponding private key.
<b>LDAP</b>	Lightweight Directory Access Protocol - A protocol for accessing directory services across multiple platforms. LDAP is a simplified version of Directory Access Protocol (DAP), used to access X.500 directories.
<b>Logic Pack</b>	A discrete software unit deployed within the client and server adaptors that encapsulates a set of related business processes. The logic pack contains data models, data formatting and parsing code and business rules.
<b>Nonrepudiation</b>	The inability, of the sender of a message, to deny having sent the message. A regular hand-written signature provides one form of nonrepudiation. A digital signature provides another.
<b>PAS</b>	Patient Administration System – software used in a hospital
<b>PKCS #</b>	RSA Data Security Inc. Public Key Cryptography Standards which range from PKCS #1 to PKCS #15.
<b>PKCS #11</b>	The public-key cryptography standard that governs security devices such as smartcards.
<b>PKCS #11 Module</b>	A program on your computer that manages cryptographic services (ie encryption and decryption) using the PKCS #11 standard. Also called cryptographic modules, cryptographic service providers, or security modules, PKCS #11 modules control either hardware or software devices.  A PKCS #11 module always controls one or more slots, which may be implemented as some form of physical reader (ie, for reading smart cards) or in software. Each slot for a PKCS #11 module can in turn contain a security device (also called a token), that is the hardware or software device, to provide cryptographic services and stores certificates and keys.
<b>PKCS-12</b>	Standard for cryptographic devices
<b>PKCS-7/CMS</b>	Cryptographic Message Syntax specification
<b>PKCS-8</b>	Standard for private key protection
<b>PKI</b>	Public Key Infrastructure. Public Key Infrastructure refers to the standards and services that facilitate the use of public-key cryptography and certificates in a networked environment.
<b>PSI</b>	Public Key Security Interface - The second version of the Client eSignature API
<b>Root CA</b>	The Certificate Authority (CA) with a self-signed certificate at the top of a certificate chain.
<b>S/MIME</b>	Secure Multipurpose Internet Mail Extension.
<b>Secure Sockets Layer (SSL)</b>	A protocol that allows mutual authentication between a client and a server for the purpose of establishing an authenticated and encrypted connection. SSL runs above TCP/IP and below HTTP, LDAP, IMAP, NNTP, and other high-level network protocols.
<b>Signing Key</b>	A private key used for signing only. A signing key and its equivalent public key, together with an encryption key and its equivalent public key, constitute dual key pairs.
<b>Slot</b>	A piece of hardware, or its equivalent in software, that is controlled by a PKCS #11 module and designed to contain a security device.

**Unclassified**  
**Medicare Australia**

<b>Smartcard</b>	A small device or 'token', typically about the size of a credit card, that contains a microprocessor and is capable of storing cryptographic information (such as keys and certificates) and performing cryptographic operations. Smart cards use the PKCS #11 standard. A smart card is one kind of security device.
<b>SMTP</b>	Simple Mail Transfer Protocol.
<b>Token</b>	A device used for secure storage of digital certificates (see Smartcard).
<b>Trust</b>	Confident reliance on a person or other entity. In the context of Public-Key Infrastructure (PKI), trust usually refers to the relationship between the user of a certificate and the Certificate Authority (CA) that issued the certificate.
<b>UN/EDIFACT</b>	United Nations/Electronic Data Interchange for Administration, Commerce and Transport message format standard.
<b>URI</b>	Uniform Resource Identifier.
<b>USB</b>	Universal Serial Bus.
<b>webMethods</b>	Server side business process integration software used by Medicare Australia