



## PKI and X509v3 Authentication Schemes

Document Control	
Document	PLR02_WP-x509_SH01_12-12.doc
Date Created	10/25/2002 12:25 PM
Version	1.00
Author	Simon Harris
Approved by	David Merry

**Table of Contents**

PKI and X509v3 Authentication Schemes..... 1  
    Document..... 1  
    Introduction ..... 3  
Theory of operation..... 3  
Source identity ..... 4  
Message Authenticity..... 4  
Communications network services ..... 4  
Benefits ..... 4  
Disadvantages ..... 5  
    Caveats and Disclaimers ..... 6  
        Technical ..... 6  
        General..... 6

**Commercial – In Confidence;**

**This document is released to individuals or organisations on a confidential basis.**

**It may not be passed to third parties without the written permission of the management of Polar Computer Communications Ltd.**

**The contents of the document may not be discussed in any way, with third parties without the written permission of the management of Polar Computer Communications Ltd.**

**© 2003 - This document is copyright Polar Computer Communications Ltd.**

**All Rights Reserved.**

**All trademarks are acknowledged.**

**This document may not be reproduced in part without the written permission of Polar Computer Communications Ltd.**

## ***Introduction***

The X509v3 standard introduces a method of implementing a scheme to carry out;

- Data Encryption
- Digital Signing
- Message Validation

In essence the schema is a digital version of Identification, Non-Repudiation and Authenticity, such as recognising someone's face, signature, voice or fingerprint.

In the digital world there is no room for ambiguity such as a forged signature, as there could be transactions worth millions and millions of pounds at stake.

In simple terms when setting up a session for secure data transmission, the devices will encrypt their session keys and send them, using the public key of the remote device. In this way the strong encryption key management process is used to protect the session key distribution.

## **Theory of operation**

The concept of a PKI (Public Key Infrastructure) is diametrically opposed to the concept of a Pre Shared Key (or Secret). With a Pre Shared Key, there is a requirement to keep the Key completely secret or else the Scheme collapses.

In the PKI scheme the whole process is based upon the free distribution of a public key and the explicit trust of a Certification Authority (CA) to perform the validation that whoever is sending or using the key is a verified entity.

It is easiest to consider the difference between Pre Shared Keys and Public Key Infrastructure to understand how they operate.

With a Pre Shared Key, the key is distributed to all parties that need to communicate securely. They know and understand the type of encryption (algorithm) and key.

In this case it is very easy for the key to be compromised as it is being passed from one party to another or installed across a public network (e.g. by Telnet). Anyone monitoring the session could be decrypting the data using the same key.

In some cases the key can even be read by logging onto the device that is using the key (e.g. VPN device). This is of particular concern should a device be lost in transit, hacked into or stolen.

With PKI, a pair of keys is produced, one private, which is not distributed to anyone and one public, which can be freely distributed to anyone. The public key can be used to **encrypt** data, whereas the private key is required to **decrypt** data.

In short, having the public key is of no benefit when it comes to decrypting the data.

## Source identity

So far, the fact that a PKI is less vulnerable to loss of control of the critical key through key distribution is clear, however, a hacker could use the public key of the central site device to impersonate the remote site.

In this instance, the process of authentication is used to ensure that the person or device that is sending the session initiation request is actually an authorised member of the trusted group.

A digital signature provides this function. By creating a signature using the private key, anyone with the corresponding public key can decrypt the signature. This is based on the concept that only the owner of the private key can perform the act of creating a signature that is verified by using the public key.

## Message Authenticity

It is important to ensure that a message is really the message that was sent and that it has not undergone substitution or modification in transit.

It is possible to include a summary of the message information in the signature. By doing so, a summary can be created by the receiver and both summaries can be compared.

## Communications network services

In the context of a network security solution, a x509v3 certification process can ensure validated identity of the remote site in the following way (simplified);

A message is sent from the remote site to the central site giving the central site an encrypted session key and a digital signature.

The session key is encrypted using the central site's public key. The central site is the only entity able to decrypt the message using the central site private key.

Once the message is decrypted the digital signature is tested against the public key. The public key is obtained from the trusted CA, therefore the public key belongs to the trusted remote site.

The central site can now be assured that the remote site is a trusted party and has a session key to initiate an IPSec session and open an encrypted tunnel to the remote site.

## Benefits

The clear benefits of a Certification Authority are that;

- The key used to decrypt data is only known to the receiving device/person therefore there is no risk of the key being intercepted or lost in transit.
- The ability to completely and unequivocally prove the identity of the sender.
- A message, that in this case is the exchange of session keys, has not been tampered with.
- The implementation of a CA that links to a global trusted CA entity (Baltimore, Entrust etc.) allows data to be encrypted in order to be emailed between users within the organisation and to other organisations that trust the same CA as your organisation.

## Disadvantages

The main disadvantages of a Certificate Authority scheme are;

- Cumbersome to set up.
- Requires strong technical understanding to maintain.
- Can be a costly process to link to TTP (Trusted Third Parties) to exchange inter-company keys.

## ***Caveats and Disclaimers***

### ***Technical***

This information is provided in good faith, as-is for informational purposes only and is accurate to the best of our belief.

Polar Computer Communications accept no responsibility or liability whatever for any inaccuracies in this text.

Polar Computer Communications accept no responsibility or liability whatever for any consequential losses as a result of using (or not using) the information contained in this document.

It is the responsibility of the reader to satisfy themselves as to the accuracy of this information prior to acting upon it.

### ***General***

Please note: This information and all services and products are provided in accordance with our Standard Terms and Conditions of business which can be found at;  
<http://www.polar-cc.co.uk/text/stc.html>