LANCOM™ Techpaper
Certificate Management for Public Spots

Introduction

Security is a vital issue when operating a Public Spot. The focus here is on the encryption of user login data and not the general traffic over the wireless LAN. This is relevant to assure the system operator and the users that the access credentials cannot be misused. This techpaper describes how certificates are used to provide adequate security.

HTTPS

To assure that the login data is secure, a combination of HTTP and SSL (Secure Sockets Layer) known as HTTPS is used to encrypt the data transmitted between client and server. In this case the device that provides the Public Spot service is considered to be the server, and the client is the device using this service.

HTTPS relies on certificates according to the X.509 standard as specified by the International Telecommunication Union (ITU). A certificate consists of two components; a public key and a signature that is created with the use of a private key. The private key always remains in the possession of the server and is not transmitted.

Public and "self-signed" certificates

There are basically three different ways to create a certificate: A "self-signed" certificate, for which the server signs its public key itself; a public certificate as signed by a trusted certificate authority (CA); and the third option whereby the public key is signed by a private CA.

The task of a trusted CA is to ensure that any party applying for a certificate for a particular domain actually is the owner of that domain. The aim is to prevent the misuse of public certificates. If a root certification authority (root CA) is classified by a web browser as trustworthy, all certificates that were signed by that root CA are also considered to be trusted. It follows that a web browser will treat the login page of a Public Spot as trustworthy if it can provide an appropriate certificate as signed by a public root CA. The security warnings (Fig.1) triggered when no trusted certificate is found do not occur.

However, certificates of this type are subject to a fee and they only remains valid for a limited period, which is why they are generally used only when the Public Spot is operated for commercial purposes.

The browser security warnings triggered by "self-signed" certificates are unavoidable, because the browser initially does not consider the web server to be trustworthy. However, self-signed certificates also have their advantages. First of all, they are generated on demand by the server and do not have to be requested and, secondly, a self-signed certificate is free of charge because no external services are involved.

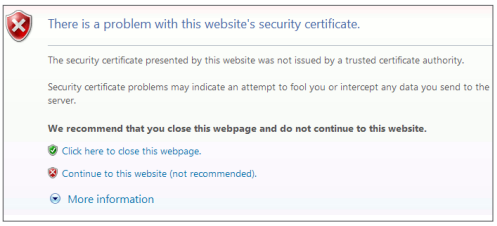

Fig. 1 Security warning from Internet Explorer

LANCOM Systems

LANCOM™ Techpaper
Certificate Management for Public Spots

Logging on

When an attempt is made to connect to a web server, the certificate is transferred to the client, which then checks whether the certificate is trustworthy. Copies of the certificates from the root CA, containing their public key and signed with their private key, are stored by the web browsers. If the signature is classified as being authentic, the client generates a random session key that is encrypted using the web server's public key. This key is sent to the web server, which uses its private key to decrypt the data.

Now both parties, server and client, have the session key. This is used to set up an SSL tunnel with 128-bit encryption between the web server and the client, and this tunnel can be used to transfer data between the two parties. In this way the login data is encrypted and cannot be misused by third parties.

The process of logging on is illustrated in fig. 2.

Additional security

A worthwhile consideration when operating a Public Spot is to utilize a firewall and block certain ports and protocols to prevent misuse.

User experience

A very important aspect for operating a Public Spot is the user experience it offers. For this reason, operators should make use of public certificates to avoid security warnings from the browser which cause users to be suspicious and reticent.

Purchasing certificates

Certificates that have been signed by a trusted root CA can be purchased from the relevant companies. Examples of companies that offer an this service include Deutsche Telekom (Telesec) and Verisign. The cost for standard certificates amounts approximately to a low double-figure sum in Euros per month.

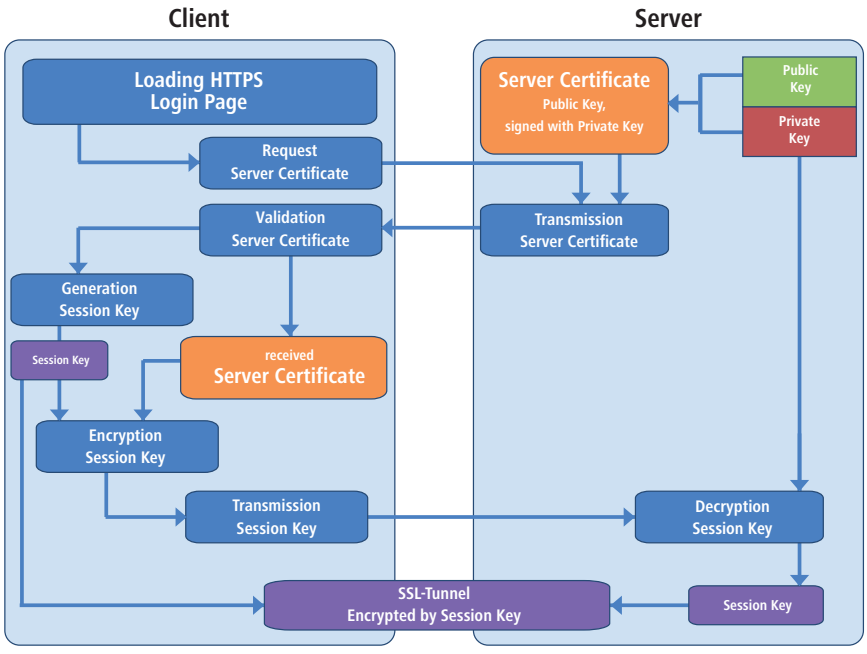

Fig. 2 Diagram of the HTTPS login procedure

LANCOM Systems

LANCOM™ Techpaper
Certificate Management for Public Spots

Implementation

Once the certificate is available, it must be stored in the device. With LANCOM devices, this can be done very conveniently with the aid of LANconfig or WEBconfig (fig. 3). Additionally, the name that refers to the certificate must be entered into the *Device hostname* field (fig. 4) with the help of WEBconfig or at the command line. Please ensure that the name is resolved for the corresponding IP address of the device.

Summary

When operating a Public Spot for commercial purposes, we strongly recommend that you use a trusted certificate. This offers better security and it avoids the suspicion and reticence that users feel when faced with security warnings from their web browsers. These certificates are economical and easy to obtain and they are quickly and easily integrated into LANCOM Public Spot solutions.

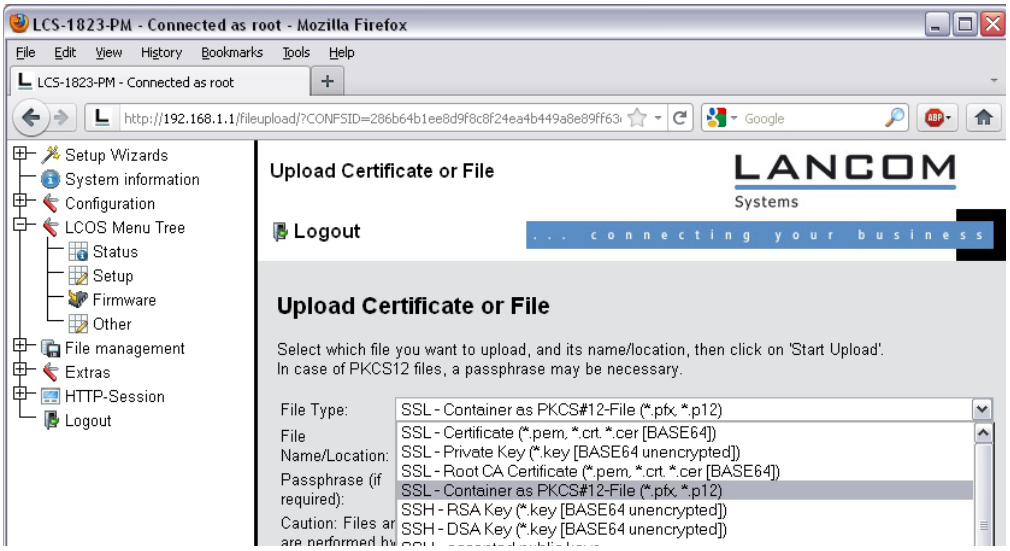

Fig. 3 Uploading a certificate with WEBconfig

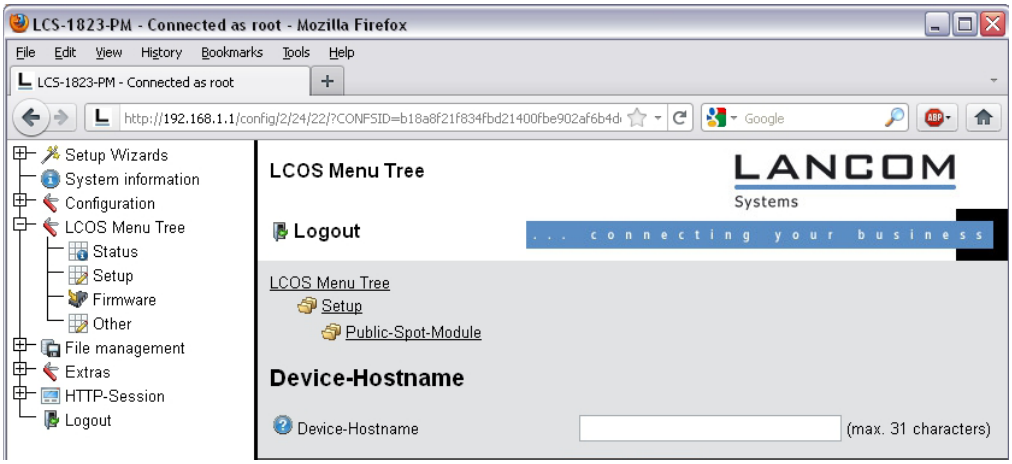

Fig. 4 Entering the device name in WEBconfig