January 2021

SYSTEM AND PROCESS FOR SSL CERTIFICATE SHARING AND INSTALLATION USING QR CODES

HP INC

System and process for SSL certificate sharing and installation using QR codes

A system and a process are disclosed allowing users to quickly and securely install a network device's SSL (X509) certificate on their computing device (e.g. smartphone) using QR codes.

Many network-connected devices (such as routers, printers, IoT devices) provide a web interface to make their settings available for users to change. Users access the configuration interface via a web browser on their device (e.g. smartphone) by introducing the device IP address or hostname in the browser's address bar. The browser then connects to the device via HTTP or its secured version HTTPS.

When establishing an HTTPS connection, the browser, and the network device exchange SSL (X509) certificates. An HTTPS connection can be considered truly secure when the browser "trusts" the certificate presented by the network device. Every browser/operating system has a certificate store with all trusted certificates.

Typically, network devices use a self-signed certificate that is not trusted by the user's device. In such a case, the browser would warn the user about the insecure connection. The user can then decide to continue with the insecure connection at her own risk or cancel the operation. To be able to securely connect to the device, the user must add/install the network device's certificate into her device's certificate store.

As of today, there are no simple and secure processes to retrieve a network device certificate and install it on a user device. Current methods to achieve this are:

- Store the network device certificate on a storage device (e.g. USB), transfer it to the user device, and manually install it. This is a long process that requires both devices to support the same storage medium and for the user to be tech-savvy.
- Downloading the network device certificate via its web interface. This method is insecure as it requires to first connect insecurely to the device.

Possible solutions today either take too long or require deep technical knowledge or both. This leads to most users connecting insecurely to network devices and putting their home/office network at risk.

The use of QR codes has recently increased and most smartphones today can read and decode them. QR codes are used for sharing websites, contacts, and even WiFi network information. Having the ability to share SSL certificates using QR codes introduces a simple and secure way compared to methods available today.

Figure 1 illustrates an example computing device and elements of the computing device that support the methods described in this article.

Described below is a system and a process allowing users to quickly and securely install a network device's SSL certificate on their computing device using QR codes.

1. The network device generates a self-signed certificate in PEM format (base64 encoded)
2. The network device encodes the certificate and generates a QR code
3. The network device displays the QR code to the user:

   a. By showing the QR code on the device's display (control panel)
   b. In the absence of a display, by printing the QR code (if the network device has printing capabilities).
4. The user scans the generated QR code with the camera of her computing device
5. The user's computing device decodes the certificate from the scanned QR code
6. The user's computing device add/installs the certificate in its certificate store
7. The user securely accesses the network device's web interface

Figure 2 provides an example application of the described system and process. In this example, the user's computing device is a smartphone. The network device is a printer.

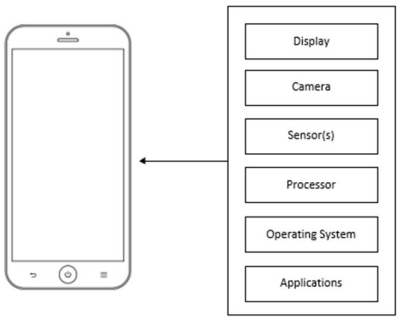

Figure 1

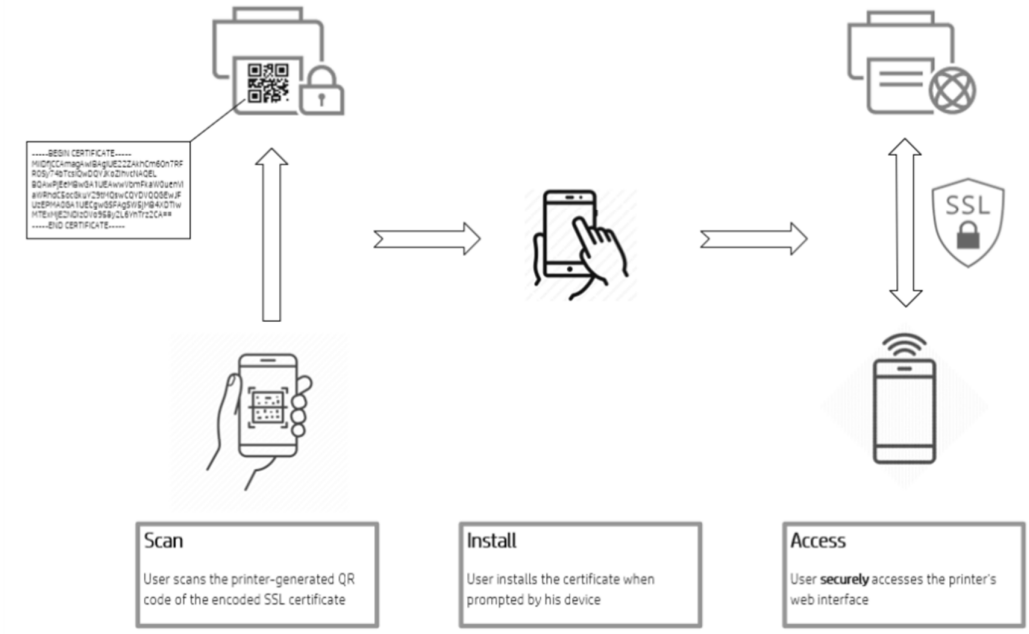

Figure 2

Disclosed by Nidam Zubidat and Alejandro Gomez Bover, HP Inc.