Printing Infrastructure Discovery through Adaptive QR Codes

Valer BOCAN, PhD[1], Simona CIURAR[2]
[1]Aleea Ionel Perlea nr.10, Ap. 25, 300672 Timişoara, România
[2]Aleea Ionel Perlea nr.11, Ap.15, 300672 Timişoara, România
[1]valer@bocan.ro, [2]simona_ciurar@yahoo.com

Keywords: printer, infrastructure, discovery, authentication, audit, QR code, adaptive

Abstract— This paper describes a protocol for discovering, authenticating and printing to a previously unknown printing device, using a smartphone or tablet with an on-board camera. Printers equipped with a graphic display can be accessed by mobile devices, without prior knowledge of the network setup and credentials.

Introduction

By using QR-code [1] displays on printers in public areas, any client with a mobile device can have access to the printing service. This process is very simple for the client, who just scans the QR code with the camera of the mobile device, sends the document to the printer after establishing a connection and uses an online payment system to pay for the service and get the document in paper form. The protocol accommodates various scenarios, such as:

- anonymous printing in public areas
- agreement-bound printing in public areas
- guest printing in corporate environments
- audited printing in corporate environments

Key elements of the system are:

A. The printer

In the context of our model, the printer is any device capable of printing, augmented with an external display, perhaps other than the built-in one. The main purpose of the display is to show the QR code that allows a mobile client to register itself to the printing infrastructure and to show other information such as help or advertising text.

B. The print server

The print server is the central component that manages, authenticates and authorizes access to printers. It receives registration and print requests from clients, manages the printer fleet, etc.

C. The mobile client

A mobile client is a smartphone or a tablet with wireless capabilities, endowed with an on-board camera which is able to store and retrieve documents from its internal storage.

System Functionality

A. Assumptions

In the context of this document the following assumptions have been made:

1) The print server has a pair of asymmetric keys:
   a) The public key (SRV_{PuK}) is known in advance by the client (embedded into the software client) and it is used to encrypt the messages from the client.
   b) The private key (SRV_{PrK}) is known only by the server and is used to decrypt the messages from the client.
2) The client also has a pair of asymmetric keys:

a) The public key (CL_{PuK}) is known in advance by the server and is used to encrypt the messages to the client.
b) The private key (CL_{PrK}) is known only by the client and is used to decrypt the messages from the server.

B. Access Token Structure

The backbone of the entire printing infrastructure discovery process is the access token generated by the print server and transmitted to the printer to be displayed as a QR code. The QR code is in turn read and decoded by the mobile client.

The token is essentially a collection of members, some of which relate to the security of the token itself, ensuring encryption, version compatibility and resilience to replay attacks and some other being the actual payload of the token.

$$Token = [V \mid T_s \mid N \mid WN_{SSID} | WN_{PASS} | EXP_{DATE} \ | SERVER_{IP}]_{CL_{PuK}} \qquad (1)$$

Security-related Members

- V – Version of the token specification. Having the version embedded in the token ensures forward compatibility with future evolutions of the project.
- T_s – Date and time of the moment when the token was created.
- N – A nonce, i.e. a large arbitrary number (typically 64-bit) used only once. It ensures that the token cannot be reused or be replayed by the mobile client. The entropy of such large numbers is big enough such that collisions are rare.
- CL_{PuK} – The public key of the client used to encrypt the contents of the token (such that only the client can decrypt it using the private key CL_{PrK}.

Payload Members

- WN_{SSID} – Name of the wireless network to which the mobile client should connect in order to be able to access the printing infrastructure.
- WN_{PASS} – Password of the wireless network.
- EXP_{DATE} – Nonce expiration date. No jobs can be submitted after this moment using this nonce.
- $SERVER_{IP}$ – IP address of the print server. The mobile client uses this information to learn the address of the server to which it will direct all future requests.

C. Printer Initialization

Each time a new printer comes online in the printing infrastructure or when a mobile client has registered with the printer and that in turn needs a new QR code to display (it is said that the client has “consumed” the QR code), the following steps are taken (Fig. 1):

1. The print server generates a new access token, encodes the resulting data into a QR code image and sends the information to the printer for displaying it on the designated panel.
2. The access token is refreshed at regular intervals (typically 5 minutes) even if no mobile clients have registered to the printer meanwhile (i.e. the QR code hasn’t been consumed yet). This ensures that no stale QR codes remain valid on client devices for prolonged periods of times and forces the user to print while in physically vicinity of the printer.
3. The printer displays the QR code on its screen along with human-readable information for the mobile user.

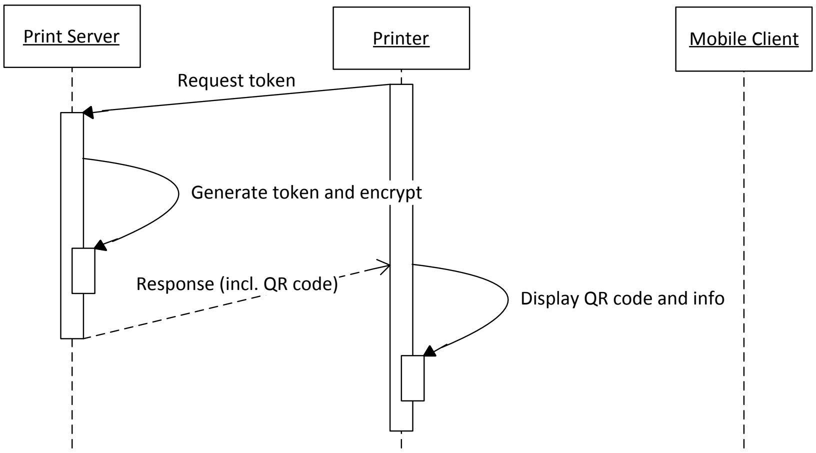

Fig. 1 Sequence diagram of the new printer initialization

D. Mobile Client Registration

Before a mobile client is able to submit documents for printing, it must register itself to the printing infrastructure (Fig. 2). This typically means connecting to a (secured) wireless network and sending an authentication token to the print server.

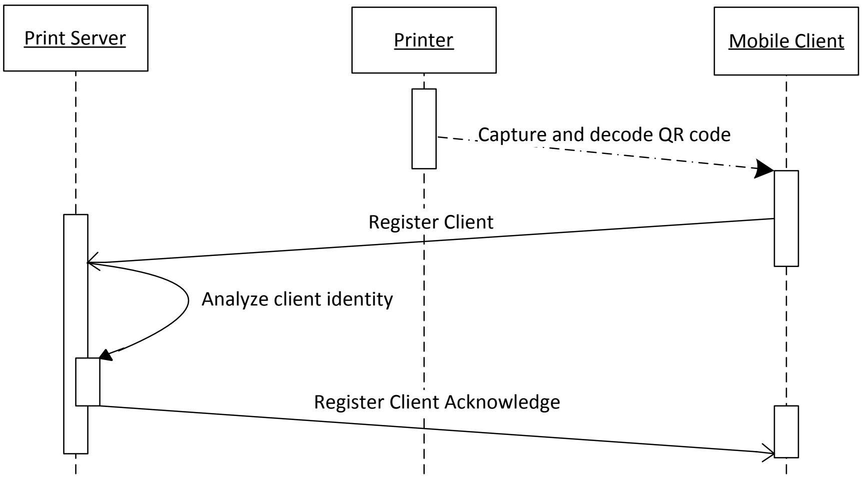

Fig. 2 Sequence diagram of mobile client registration

The scenario for registering the mobile client with the printing infrastructure is as follows:

1. The user aims the mobile device camera towards the QR code displayed prominently on the printer to which it intends to print and the client reads the QR code.
2. The client decrypts the payload of the token using its own private key CL_{PrK}.
3. The client verifies that the version V of the token is supported, the time stamp T_s is recent (typically less than 5 minutes), and then uses WN_{SSID} and WN_{PASS} to connect to the wireless network. The mobile client stores $SERVER_{IP}$ and N.
4. The client builds a Register Client message with the structure below and sends it to the print server designated by IP address contained by $SERVER_{IP}$:

$$Register\ Client = [M_{ID} \mid N]_{SRV_{PuK}} \tag{2}$$

- M_{ID} – Mobile identity information / whatever unique piece of information the client can provide, typically stored in hardware.
- N – The nonce (read from the QR code payload).
- The message is encrypted with the public key of the server SRV_{PuK} in order to avoid eavesdropping.

5. The print server decrypts the message with its private key $SRV_{PrK.}$ It analyzes the nonce N and ensures that it is a valid one (comparing it with the nonce list it maintains) then associates the mobile client identity M_{ID} with the printer for which the nonce was originally generated. In case of a replayed message (i.e. the M_{ID} / N combination has been seen before), the print server simply ignores the request.
6. The print server replies back to the client with a Register Client Acknowledge message:

$$Register\ Client\ Acknowledge =\ [M_{ID} \mid N \mid SK]_{CL_{PuK}}) \qquad (3)$$

- M_{ID} – Mobile identity information (must match what the client has sent previously).
- N – The nonce (must match what the client has sent previously).
- SK – A random session key that will serve as a key for encryption of print data upon submission.
- The message is encrypted with the clients public key CL_{PuK} such that it is only accessible to the client itself.

7. From this point on, the mobile client is registered with the print server. Print request originating from the mobile client can be charged against its account.

E. Document Submission from the Mobile Client

After successful authentication with the print server, the mobile client is able to submit documents to print on printers to which it has already registered for. The steps for printing from the mobile client are as follows (Fig. 3):

1. The client builds up a Print Request as follows:

$$Print\ Request = M_{ID} \mid [N \mid DATA_{META} \mid DATA_{PRINT}]_{SK}) \qquad (4)$$

- M_{ID} – Mobile identity information / whatever unique piece of information the client can provide, typically stored in hardware.
- N – The nonce (read from the QR code payload upon registration).
- $DATA_{META}$ – Print settings information such as color mode, number of copies, priority, resolution, etc.
- $DATA_{PRINT}$ – Actual payload of the message consisting of documents to be printed. The nonce N and the data are encrypted with the session key SK of the client.
- The mobile identity M_{ID} is intentionally left out of the encryption process in order to avoid the possibility of denial of service (DoS) attacks on the print server.

2. The print server checks M_{ID} and N and decides whether the client is authorized to print at the designated printer. It then sends the print data to the printer, optionally updating accounting information.

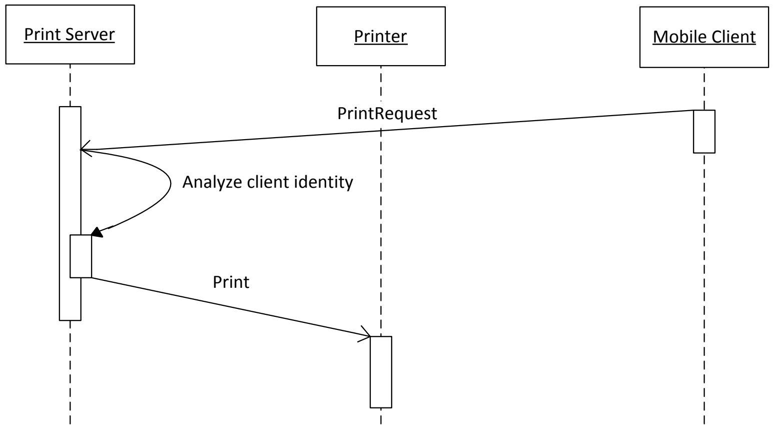

Fig. 3 Sequence diagram of document submission process

Conclusion

We presented a protocol for discovery, authentication and printing of documents using a mobile device. The protocol assumes no prior knowledge of the network infrastructure. Using the information contained in the QR code displayed in the vicinity of the printer, the client is able to discover the wireless network SSID, password and the IP address of the print server. The unique identity of the mobile device is then used by the print server to authorize and audit the printing process.

Acknowledgements

The present work has been done by the authors while being employed by Océ Software Romania SRL, a Canon company. The authors wish to express their gratitude for the support received during the research.

References

[1] ISO 18004:2006. QR Code bar code symbology specification. ISO, Geneva, Switzerland.