An alternative driver's license presentation method

This writeup is in response to feedback I received at IIW in Day 1 / Session 2 / Room L when I presented the demonstration described in A driver's license credential usable for website registration and traffic stops. In a traffic stop, the QR code that the officer presents to the driver includes a challenge and must therefore be dynamic. Philip Quinlan pointed out that a dynamic QR code would be displayed on a small screen, and the driver would have to come close to it to scan it, which would be unsafe for the officer. This alternative presentation method uses a challenge for proof of possession, but the challenge is not in the QR code. The QR code can be a large preprinted image that can be scanned by the driver from a safe distance.

Francisco Corella, 10/26/2025

The patrol car has a bunch of large preprinted one-time-use QR codes for use in traffic stops (Traffic Stop QR codes, or TSQR codes).

Each TSQR code encodes a URL that targets the credential request endpoint of the digital driver's license issuer and has a query string with parameters:

- A callback endpoint of a server that supports the fleet of patrol cars (the fleet server).
- A patrol car Id.
- A TSQR Id

The TSQR Id is a small number that is also printed next to the QR code so that it can be read by the police officer.

The patrol car asks a speeding vehicle to stop.

When the vehicle stops, the patrol car stops behind it, then the officer walks up to the vehicle and asks the driver to scan a large TSQR code from a safe distance. The officer puts aside the TSQR code that it uses, for later reference.

The driver scans the TSQR code with a mobile phone.

That causes the default browser in the mobile phone to do a *page transition to the URL in the TSQR code*, causing a GET request to be sent to the URL.

[[A *page transition to a URL* is what happens when you enter the URL into the address bar of the browser and hit enter.]]

The GET request is intercepted by the service worker that was registered by the credential issuer when the credential was issued.

The service worker creates a page that contains the TSQR Id, the patrol car Id, and the callback endpoint (as values of JavaScript variables).

The page asks the driver for consent to present the driver's license credential to the relying party, using a user-friendly designation of the relying party such as "the Mountain View Police Department" obtained by looking up the domain name of the callback endpoint in a registry.

After obtaining consent, JavaScript code in the page causes a *page transition to the callback endpoint with parameters*:

- the patrol car Id, and
- the TSQR Id.

[[An endpoint is a URL without a query string. A *page transition to an endpoint with parameters* is a page transition to the URL obtained by appending a query string with the parameters to the endpoint.]]

This causes a GET request to be sent to the fleet server. Upon receiving the GET request, the fleet server creates a session record with:

- a session Id,
- a challenge,
- the patrol car Id, and
- the TSQR Id.

Then the fleet server does *POST redirection* to the credential request endpoint, *with parameters*:

- the session Id, and
- the challenge.

[[Doing a *POST redirection with parameters* means downloading a code-only page where JavaScript code constructs a form with the parameters in hidden fields and submits the form, thus sending a POST request.]]

The POST request is intercepted by the service worker. It is a second interception by the service worker, but this is not a problem because the request is a POST request this time instead of a GET request.

The service worker creates a code-only page with JavaScript code that retrieves the private key and the full disclosure certificate from localStorage, computes a signature on the challenge and the callback endpoint, and performs a page transition to the callback endpoint with parameters:

- the session Id,
- the signature, and
- the full disclosure certificate.

Then the fleet server:

- uses the session Id to access the session record,
- verifies the signature, and
- validates the full disclosure certificate.

Upon successful verification and validation, the fleet server:

1. Notifies the driver that the driver's license credential has been successfully presented, by performing a page transition to a credential-presented page, and
2. Sends a message to the patrol car identified by the patrol car Id, containing the TSQR Id.

The message is displayed by equipment in the patrol car, and the officer verifies that the TSQR Id in the message is the Id of the TSQR code that the officer put aside after it was scanned by the driver.