QR ID™ is a replacement for OTP (One Time Password) schemes

- No user-ID to remember, it's all in the *certificate*. Yes, it is based on PKI
- 128+ versus 40-bit entropy, no need for "login throttling" or account lockout
- No counter/time-stamp per user state-holding needed in the server, a root certificate + OCSP/CRL suffice
- No guesswork regarding token to use, credential filtering does it automatically and displays an associated logotype as well
- No fuzzy inputting of ever-changing digits, a static PIN will do
- Designed for mobile phones and *on-line provisioning*

PrimeKey

QR ID™ from a user's perspective - Login

① Web Service

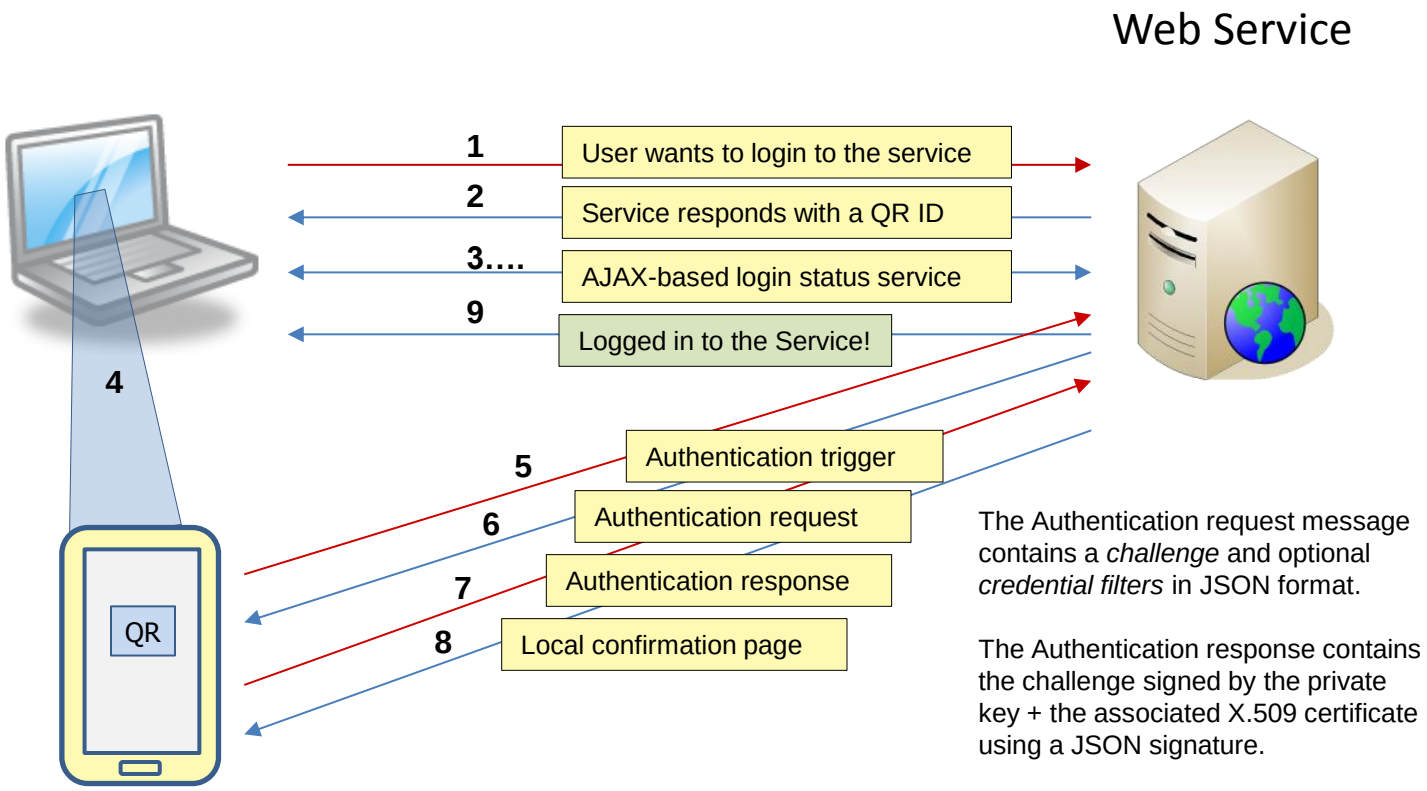
The user wants to login to a service from a PC or similar. The service responds with a QR ID display and asks the user to open the QR ID app.

② Automatic step ③

The user opens the QR ID app and points to the web page. When the QR ID is recognized the app automatically invokes the authentication app.

The user is presented with a login app and responds with a PIN to activate the credential. After that the user should be able to use the service from the PC (not shown here).

QR ID™ - How does it actually work?



The Authentication request message contains a *challenge* and optional *credential filters* in JSON format.

The Authentication response contains the challenge signed by the private key + the associated X.509 certificate using a JSON signature.

The QR code contains an URL with a random session ID used in #5 as well as an application indicator since QR ID can be used to start other local applications like enrollment.