Contribution ID: **298** Type: **not specified**

New web services and portal for UK CA

Wednesday, 21 May 2014 16:00 (20 minutes)

The UK CA is testing a new Web portal that creates Certificate Signing Requests (CSRs) and .p12 files using a client-side Javascript crypto library that is compatible across all modern Web browsers. Certificates can be requested, renewed and downloaded without ever sending the private key or password over the wire to the CA. In addition, since the Javascript library is served by the portal, this approach greatly simplifies dealing with certificates as users no longer need to install any special client-side crypto software.

The following sequence of events is executed when requesting and/or renewing a certificate: a) the user provides the requested certificate attributes so that a new public/private key pair and CSR can be locally generated using Javascript, b) the private key file is encrypted with the user's password and is saved locally in a plain text file, c) the public CSR is POSTED to the CA for subsequent approval (via SSL), d) after approval and signing, the user is emailed their certificate serial number, e) user accesses a second interface to download their certificate from the CA, e) the user provides their local private key file and password f) a local .p12 file created using Javascript.

Primary author: MEREDITH, david (STFC)

Presenter: MEREDITH, david (STFC)

Session Classification: Authentication & Authorisation