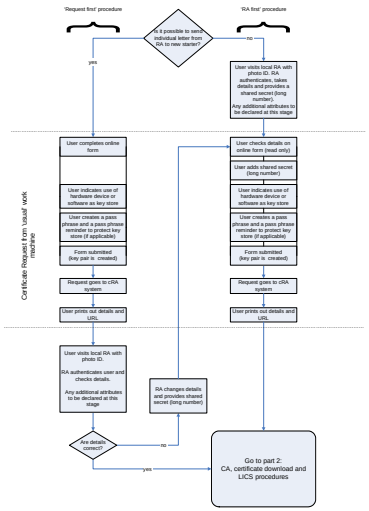
Can personal digital certificates work in the real world?

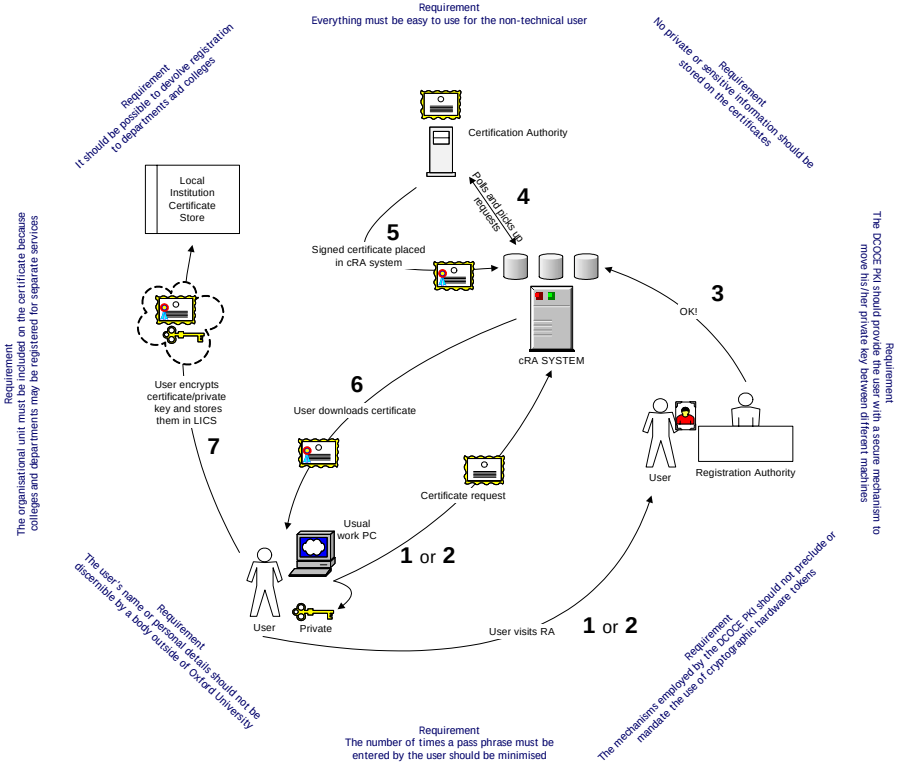
Oxford University's Digital Certificate Operation in a Complex Environment (DCOCE) project attempts to answer this question.

Summer 2004 - What has the project done so far?

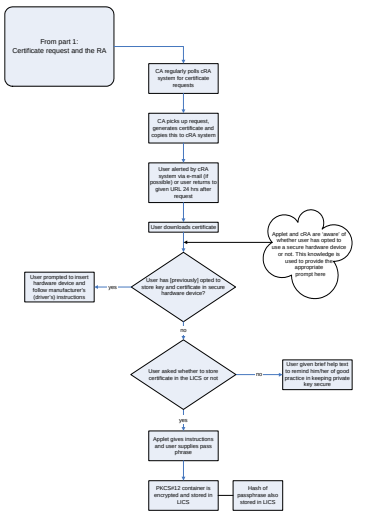
- Looked at existing PKI projects
- Consulted stakeholders on issues of difficulty and general requirements
- Evaluated 'hopes and fears' of stakeholders
- Formulated requirements (some reproduced here)
- Consulted Athens and Zetoc (MIMAS)
- Proposed an architecture
- Raised the profile of digital certificates and the DCOCE project at Oxford
- Developed certificate issuing, storage and management structures and interfaces
- Begun to recruit users

Applying for the first certificate - part 1: Certificate request and the RA





Applying for the first certificate - part 2: CA, certificate download and LICS procedures



Project findings so far

- Requirements vary between end users (and their representatives) and more technical (informed) users
- Expectations of very high security must be managed
- Browser vendors could do far more to ease usability issues
- Two different models of registration (see graphic) must be provided for
- It is possible to store certificates and private keys centrally so that no-one except their rightful owners can access them
- It is possible to work with commercial CA vendors
- Signing and encryption certificates should be handled separately from authentication certificates
- When cryptographic hardware tokens become cheaper and the drivers more widespread, many of the difficult usability issues will disappear
- Personal digital certificates for authentication *have* a future, but more work from browser and operating system manufacturers is needed as well as successful national (CA) initiatives

The next steps...

Initial feedback from test users - Technical debugging - Make on-line apps certificate ready - Feedback from RAs - Athens - Zetoc - Feedback from users - Analysis - Report writing - Recommendations

Your private key

Please keep in a safe place

Your digital certificate

DCOCE is a two year project funded by the Joint Information Systems Committee, based at Oxford University Computing Services, Oxford University Library Services and the Oxford e-Science Centre. External partners include Manchester Information and Associated Services and Athens at EduServ.