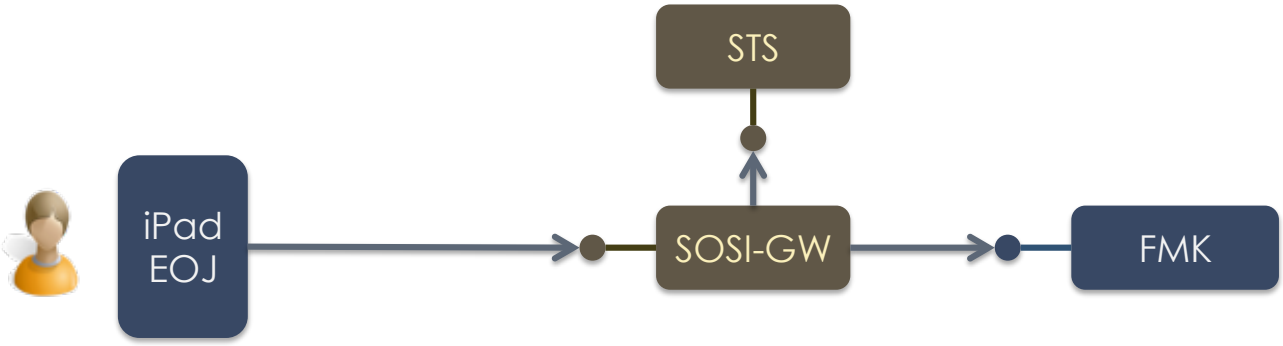
Dato: 28.08.2012
Christian Gasser / Lakeside
Tlf. 2843 3872
mail: chg@lakeside.dk

SOSI digital signatur POC

Nærværende dokument beskriver i korte træk SOSI digital signatur proof-of-concept'en som viser hvordan den digital signatur kan anvendes på en iOS enhed til at få udstedt et SOSI idkort der er adgangsgivende til FMK.

I drifts-setup har en mobil enhed ikke direkte adgang til en Security Token Server (STS) som udsteder SOSI idkort, men vil tilgå STS'en via en SOSI-Gateway (og formentlig også gennem en fagsystem server). Det er derfor ikke nødvendigt at kunne foretage XML transformationer og beregning af XML digest som indgår i XML signering af et idkort-request til STS'en på den mobile enhed. I stedet er det kun nødvendig at kunne foretage et SHA-1 hash og signering et hash'et.



Kildekoden

Indgangspunktet for projektet er SOSIViewController'en som fungerer som main-controller; for hver af de andre klasser der indgår i projektet er der en kort beskrivelse sat i toppen af klassefilen.

Der er to test-certifikater indlejret i projektet som pkcs12 filer – et OCES1 og et OCES2. Password til certifikaterne samt CVR nummer og de til certifikaterne tilknyttede CPR numre er hard-kodet.

GUI'en er minimal og består af en enkel knap der udløser udstedelsen af et idkort:

1. På enheden dannes et usigneret idkort
2. Der sendes et requestForDigest med det usignerede idkort til SOSI-GW
3. SOSI-GW foretager XML transformationer og beregner digest som sendes retur sammen med en URL til en applet (som ikke anvendes her)
4. På enheden ekstraheres digesten som bliver SHA-1 hashet og digital signeret
5. Den signerede digest sendes retur til SOSI-GW sammen med certifikatet (den offentlige del)
6. SOSI-GW kommunikerer med STS for at få udstedt idkortet.

7. Enheden modtager svar fra SOSI-GW – enten 'ok' eller en fejlbesked
8. Enheden kalder 'logout' i SOSI-GW for at vende tilbage til udgangspunktet (ingen idkort i SOSI-GW)

Afvikling af POC'en

For at kunne afvikle POC'en kræves en kørende SOSI-Gateway – endpointet for denne rettes i SOSIViewController#goDo (default er http://localhost:8080/sosigw/service/sosigw).

Import af nøglefil fra Desktop

I projektet er file-sharing via iTunes enabled ved at 'UIFileSharingEnabled' property'en er sat i Info.plist – desuden er der en stump udkommenteret kode under SOSIViewController#handleDigestResponse som illustrer hvordan man fra en applikation kan tilgå filer som brugeren har overført til applikationen gennem iTunes.

Overførsel af nøglefiler gøres via iTunes under Apps->File Sharing, se nedenstående screenshot.

Disclaimer

I og med projektet er udformet som proof-of-concept er det på ingen måde tale om produktions-moden kode.