UPPSALA
UNIVERSITET

Enheten för informations-tekniskt stöd (IT-stöd)
Pål Axelsson

Postadress:
Box 887
751 08 Uppsala

Gatuadress:
Lägerhyddsvägen 2, hus 3
752 37 Uppsala

Telefon:
018 - 471 7918

Telefax:
018 - 471 7876

Hemsida:
www.its.uu.se

Epost:
Pal.Axelsson@its.uu.se

IT Support Department
Pål Axelsson

Postal address:
Box 887
SE-751 08 Uppsala
SWEDEN

Visiting address:
Lägerhyddsvägen 2, building 3
SE-752 37 Uppsala
SWEDEN

Telephone:
+46 18 - 471 7918

Telefax:
+46 18 - 471 7876

Web site:
www.its.uu.se

E-mail:
Pal.Axelsson@its.uu.se

2005-09-16

Vad är CWAA och vad kan vi använda det till?

Under hösten 2003 började medlemmarna i CodeX diskutera behovet av att studenter och anställda vid ett universitet/högskola skulle kunna ansluta till datornätet vid ett annat universitet/högskola. Med avseende på att universiteten och högskolorna normalt sett inte vill låta användare ansluta datorer till nätet utan särskilt tillstånd eller nätpåloggning behövdes en modell för att sköta autentisering mellan olika universitet och högskolor. Ungefär samtidigt funderade Uppsala universitet på hur vi skulle göra så att när man loggar in i studentportalen så är man automatiskt även inloggad i bl.a. PingPong, filarea och webbmail – så kallad ”Web Initial Sign-on” (WebISO).

På ett CodeX-möte strax före jul 2003 arbetade en arbetsgrupp med medlemmar från olika universitet och högskolor med att finna en lösning på hur nätpåloggning vid ett annat universitet eller högskola tekniskt skulle utformas. Den första modellen vi tittade på var om användaren skulle ange användaridentitet, lösenord och hemmaorganisation på webbsidan för nätpåloggningstjänsten. Den idén ansågs olämplig därför att användaren alltid bör logga in via en för användaren känd inloggningssida i sin hemmaorganisation – t.ex. inloggninssidan för den av hemmaorganisationen valda applikationen för WebISO.

Arbetsgruppen fortsatte med att titta om vi kunde använda oss av befintlig WebISO – men det visade sig olämpligt beroende på att de två universitet som då hade tagit WebISO i bruk hade valt två helt olika lösningar – CAS och PubCookie. Nästa steg var att se om vi kunde hitta någon redan existerande lösning. Vi fann några – t.ex. Shibboleth från Internet2, Moria från UNINETT, PAPI från RedIRIS och A-Select från SURFnet – men de var antingen för komplicerade eller krävde en centraliserad tjänst på t.ex. nationell nivå.

En idé växte fram om att bygga ett decentraliserat system som skulle vara enkelt att integrera med befintliga system på ett för användare, webbtjänster och autentiseringstjänster säkert sätt via s.k. webbläsaromdirigering. Systemet som fick namnet ”Common Web Authentication Architecture” (CWAA) skulle inte heller vara begränsat till nätpåloggning utan även fungera bra vid autentisering av andra typer av webbtjänster.

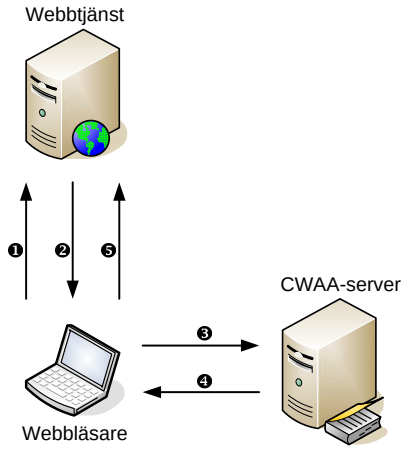
CWAA använder ”Cryptographic Message Syntax” (CMS; IETF RFC 3369) och ”PKI for Universities and University Colleges in Sweden” (SwUPKI) för att säkerhetsmässigt säkerställa att det är en godkänd applikation som använder CWAA samt att ingen kan ändra vem användaren som loggat på är. Detta innebär att med hjälp av en standardiserad öppen krypteringsmetod – som

UPPSALA UNIVERSITET

använder befintlig certifikatstruktur – säkerställs att endast godkända webb-tjänster kan använda CWAA samt att ingen kan förfalska vem som loggat på.

Förutom att CWAA tillhandahåller vem som loggat på via ”Universal Principal Name” (UPN; användarid@domän) – t.ex. abcd1234@user.uu.se – kan även andra uppgifter presenteras för webbtjänsten såsom namn, e-postadress och personnummer. Vilka andra uppgifter som görs tillgängliga för webbtjänsten definieras per webbtjänst i CWAA-servern. Detta gör att CWAA är lämpligt att använda för webbapplikationer från externa leverantörer – eller där webbapplikationen finns hos en extern tjänsteleverantör – där mer information än användaridentitet behövs – t.ex. i Tur&Retur där personnummer används.

Schematiskt fungerar inloggning med CWAA enligt följande:



1. Användaren ansluter till en webbtjänst skyddad med CWAA.
2. Webbtjänsten meddelar användarens webbläsare att webbtjänsten skyddas med CWAA med hjälp av en webbläsaromdirigering.
3. Användarens webbläsare ansluter automatiskt till CWAA-servern.
4. Efter att användaren har loggat in i CWAA meddelar CWAA-servern användarens webbläsare att den ska ansluta till webbtjänsten igen med hjälp av en ny webbläsaromdirigering. Användaridentitet – och eventuellt andra persondata – är krypterade i omdirigeringsanropet.
5. Användarens webbläsare ansluter automatiskt till webbtjänsten och användaren är nu inloggad i webbtjänsten.

I dagsläget använder Stockholms universitet och de andra högskolorna i stockholmsområdet CWAA för studenternas nätpåloggning i studentpalatset. NyA kommer att använda CWAA för att studerande ska kunna söka kurser och program med hjälp av sitt befintliga studentkonto – på något universitet eller högskola.

Uppsala universitet har sedan CWAA skapades börjat använda CAS som WebISO samt installerat CWAA så att CWAA använder CAS för inloggningen – och därmed är integrerad med universitetets centrala behörighetssystem AKKA. Detta betyder att om våra användare vill använda en webbapplikation som använder CWAA och de redan tidigare loggat in i en tjänst som använder CAS – t.ex. studentportalen – blir de automatiskt inloggade. Detta innebär även att CWAA använder samma kända inloggningssida som övriga tjänster.