

UNI•Login

Adgangskontrol

UNI•Login
Adgangskontrol

© UNI•C februar 2012

Indhold

| | | |
|-----|---|---|
| 1 | Adgangskontrol med UNI•Login | 4 |
| 1.1 | Hvordan virker det? | 4 |
| 1.2 | Hvordan identificerer applikationen sig overfor serveren? | 5 |
| 1.3 | Hvordan ser billetten ud? | 6 |
| 1.4 | Hvordan logger man ud af UNI•Login? | 6 |
| 1.5 | Single Login og gruppe-login | 7 |
| 1.6 | Hvordan integreres UNI•Login grafisk? | 7 |

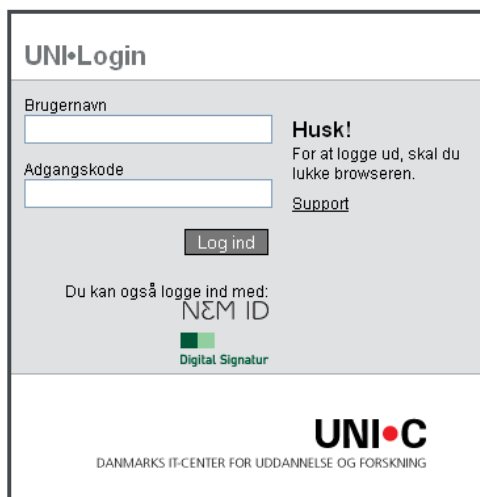
1 Adgangskontrol med UNI•Login

UNI•Login er en tjeneste til adgangsstyring og brugeradministration for udbydere af net-baserede applikationer i uddannelsessektoren. Dette dokument beskriver den tekniske grænseflade, som applikationerne skal integreres med, i relation til adgangsstyring med UNI•Login.

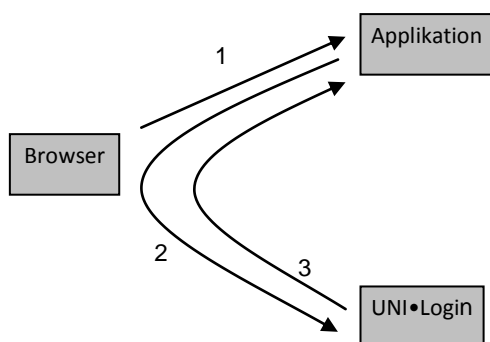
1.1 Hvordan virker det?

Når en applikation ønsker at logge en bruger ind via UNI•Login, sker det ved, at applikationen viderestiller brugerens browser til en UNI•Login-server.

Brugeren vil her blive præsenteret for en standard login-formular, hvor brugernavn og adgangskode indtastes:



Hvis brugeren godkendes, viderestiller UNI•Login brugerens browser tilbage til applikationen sammen med en billet, der beviser, at brugeren er godkendt. Billetten skal valideres af applikationen, som derefter overtager ansvaret for brugerens session. Princippet er illustreret nedenfor:



- 1) Brugeren kontakter applikationen
- 2) Applikationen viderestiller til UNI•Login
- 3) UNI•Login viderestiller tilbage med en billet

UNI•Login understøtter Single Sign On. Hvis brugeren i løbet af sin browser-session allerede tidligere er logget ind i UNI•Login, vil vedkommende ikke igen blive afkrævet brugernavn og adgangskode. Brugeren vil automatisk blive godkendt af UNI•Login-serveren og blive viderestillet tilbage til applikationen med en billet. Denne funktionalitet gør det muligt at give brugeren en oplevelse af, at de forskellige UNI•Login applikationer er integrerede. Det er muligt at undgå denne funktionalitet ved at benytte Single Login i stedet for Single Sign On. I så fald vil brugeren altid blive afkrævet et password ved adgang til tjenesten.

1.2 Hvordan identificerer applikationen sig overfor serveren?

Applikationen identificerer sig overfor UNI•Login-serveren ved at sende parameteren "id" med i viderestillingen, f.eks. kunne applikationen viderestille til:

<https://sso.emu.dk/unilogin/login.cgi?id=test>

Hver applikation har et unikt "id" med en tilhørende unik fælles hemmelighed, som er aftalt på forhånd mellem producenten og UNI•C.

Ofte er retur-URL ligeledes aftalt offline. Visse applikationer har imidlertid brug for, at UNI•Login dynamisk kan viderestille brugeren tilbage til forskellige sider i applikationen. Dette kan afstedkommes ved at applikationen medsender parametrene "path" og "auth" i den originale viderestilling.

| Parameter | Beskrivelse |
|-----------------|--|
| id | Hver applikation har et unikt "id" |
| secret | Unik fælles hemmelighed, som er aftalt på forhånd mellem producenten og UNI•C |
| returURL | Er normalt aftalt på forhånd, men kan medsendes dynamisk i "path" |
| path | Indeholder returURL. Beregnes som <code>URI_ESCAPE(BASE64(returURL))</code> |
| auth | Et fingeraftryk, der autentificerer "path" Beregnes som <code>MD5(returURL+secret)</code> |

Eksempel på viderestilling med dynamisk retururl:

<https://sso.emu.dk/unilogin/login.cgi?id=test&path=aHR0cDovL3d3dy5lbXUuZGsvYXBwbA%3D%3D&auth=59169cb39fab40cb0ad6ade6a6eb491e>

I eksemplet er "retur-URL" <http://www.emu.dk/appl> og secret er "abc123". Beregningerne bliver således:

```
path = URI_ESCAPE(BASE64("http://www.emu.dk/appl")) =  
URI_ESCAPE("aHR0cDovL3d3dy5lbXUuZGsvYXBwbA==")=  
"aHR0cDovL3d3dy5lbXUuZGsvYXBwbA%3D%3D"
```

```
auth = MD5("http://www.emu.dk/applabc123") =  
"59169cb39fab40cb0ad6ade6a6eb491e"
```

1.3 Hvordan ser billetten ud?

Billetten er indkodet i URL'en, der viderestilles tilbage til. Den kunne f.eks. se således ud:

```
http://www.emu.dk/appl?user=testuser&timestamp=20030505125952&  
auth=5e55280df202c8820a7092746b991088
```

Der indgår altid følgende tre parametre i viderestillingen:

| Parameter | Beskrivelse |
|------------------|---|
| user | Brugernavnet på den godkendte bruger. I eksemplet er brugernavnet "testuser". |
| timestamp | Tidsstempel på formatet YYYYMMDDhhmmss, som angiver tidspunktet for billetens udstedelse i UTC (GMT). |
| auth | Et fingeraftryk, der autentificerer "user" og "timestamp". Fingeraftrykket er angivet hexadecimalt og beregnes som MD5(timestamp+secret+user), hvor "secret" er en forud aftalt hemmelighed mellem applikationen og UNI•Login-serveren. |

Når applikationen modtager billetten bestående af disse parametre, skal applikationen verificere, at fingeraftrykket er korrekt og at billetten ikke har været benyttet før. Korrektheden af fingeraftrykket verificeres ved, at applikationen genberegner MD5(timestamp+secret+user). Værdien skal være den samme som modtaget i "auth"-parameteren. I ovenstående eksempel er der benyttet en fælles hemmelig med værdien "abc123". Fingeraftrykket beregnes derfor til:

```
auth = MD5("20030505125952abc123testuser") = 5e55280df202c8820a7092746b991088
```

At billetten ikke har været benyttet før, kan verificeres ved at gemme brugte billetter. Alternativt kan man acceptere billetter, der er udstedt inden for et kortere tidsvindue, f.eks. 60 sekunder. Vinduet må ikke være kortere end den tid, det tager at viderestille brugerens browser. Bruger man tiden til at afgøre billetens validitet, er det vigtigt, at applikationens ur går rigtigt. UNI•Login er tidsmæssigt synkroniseret mod centrale NTP-servere på Internettet.

Hvis "auth" kan valideres og billetten ikke er genbrugt, er "user" autentificeret og applikationen kan nu oprette en session med brugeren, f.eks. ved at udstede en session cookie.

1.4 Hvordan logger man ud af UNI•Login?

UNI•Login understøtter Single Sign On, og dermed er det ikke tilstrækkeligt at en applikation ved logout blot nedlægger sin egen session med brugeren. Hvis brugeren kontakter applikationen igen, vil vedkommende blot komme direkte ind igen uden at skulle forny sit login, da UNI•Login stadig vil udstede en billet på baggrund af det tidligere login.

Det er derfor nødvendigt at logout-processen foruden at nedlægge applikationens egen session med brugeren også omstiller til UNI•Login, således at brugerens UNI•Login session også kan nedlægges.

URL'en der skal henvises til ved logout er:

<https://sso.emu.dk/logout>

Bemærk, at UNI•Login ikke automatisk logger brugeren ud af øvrige applikationer, som brugeren måtte være logget ind i direkte eller indirekte i løbet af sin session. Den eneste sikre måde at komme ud af alting på er at lukke browseren. Det er derfor en generel anbefaling ved brugen af UNI•Login Single Sign On at opfordre brugeren til at lukke browseren efter brug. Ved logout fra UNI•Login vises derfor følgende advarsel:



1.5 Single Login og gruppelogin

Hvis applikationen ønsker fuld kontrol over login-processen, kan Single Login anvendes i stedet for Single Sign On. Konsekvensen er, at brugeren altid vil blive afkrævet et password ved adgang til tjenesten, hvilket kan ødelægge oplevelsen af integrationen af tjenester i f.eks. en elevportal.

Single Login kan f.eks. anvendes til at implementere gruppelogin ved at lade deltagerne logge ind enkeltvis med Single Login, mens deres identiteter sammenknyttes i applikationen.

For at anvende Single Login skal man benytte serveradressen sli.emu.dk frem for sso.emu.dk. På alle andre områder er dokumentationen den samme.

1.6 Hvordan integreres UNI•Login grafisk?

Det anbefales, at linket til login eller login-knappen består af en tekst skrevet med fonten Arial fed tekst. Teksten findes i to udgaver: en kort og en lang, som kan vælges alt efter behov.

Fontstørrelsen skal være 10px/1em.

Farven på font vælges, så der sikres tilstrækkelig kontrast til baggrunden.

Her er knappen vist på henholdsvis en lys og en mørk baggrund:

UNI•Login

Log på med UNI•Login

UNI•Login

Log på med UNI•Login

Linket til logud eller logudknappen består af en tekst skrevet med fonten Arial fed tekst.

Fontstørrelsen skal være 10px/1em.

Farven på font vælges, så der sikres tilstrækkelig kontrast til baggrunden.

Her er knappen vist på henholdsvis en lys og en mørk baggrund:

Log ud af UNI•Login

Log ud af UNI•Login