UPPSALA UNIVERSITET

Användarkonton i AKKA vid Uppsala universitet

Version 3.6 utkast

1. Inledning

Detta dokument är en informativ beskrivning över hur Uppsala universitet hanterar användarkonton i universitetets gemensamma katalog- och behörighetstjänst AKKA. Beskrivningen omfattar kontots fulla livscykel, dvs. från att de skapas och aktiveras till att de avvecklas. I AKKA finns fem olika typer av användarkonton (eller uu-konto för de fyra första):

- konto för studerande,
- konto för anställda och övriga verksamma,
- konto för externa konsulter eller samarbetspartners,
- konto för funktioner samt
- konto för besökande gäster eller biblioteksbesökare.

Alla utom de två sista typerna av konton kan användas inom identitetsfederationen SWAMID för interna tjänster vid universitetet, tjänster som universitetet köper av externa leverantörer och gemensamma tjänster inom utbildningssektorn både i Sverige och utomlands.

2. Beskrivning av olika typer av användarkonton

2.1 Konto för studerande

Personer som studerar vid universitetet har rätt att få ett studentkonto vilket de använder för att genomföra sina studier vid universitetet. Dessa konton går att använda inom identitetsfederationen SWAMID.

För att kunna aktivera sitt studentkonto måste personen uppfylla något av kriterierna via kontroll mot studiedokumentationssystemet LADOK:

- antagen till kurs eller program innevarande eller nästa termin,
- registrerad på kurs föregående eller innevarande termin,
- fått registrerat resultat föregående eller innevarande termin,
- vara registrerad som utresande utbytesstudent innevarande termin eller
- ha registrerat studieuppehåll för förtroendevalt arbete vid studentkår eller nation som är definierad enligt 4 kap. 8-15 §§ i högskolelagen (SFS 1992:1434).

För att behålla studentkonto kommande terminer gäller samma kriterier för automatisk förlängning med undantaget att det inte räcker med att den studerande är antagen till aktuell termin. För de personer som uppfyller kriterierna under en hösttermin är kontot aktivt fram till den 15 september året efter, motsvarande för vårterminen är 15 februari året efter.

Kontot kan ha tillitsnivå 1, 2 eller 3 beroende på aktiveringsmetod. Ett konto kan höja tillitsnivån genom kontoaktiveringsprocessen.

2.2 Konto för anställda och övriga verksamma

Personer som är anställda eller övriga verksamma vid universitetet har rätt att få ett anställdakonto vilket de använder i sin verksamhet vid universitetet. Dessa konton går att använda inom identitetsfederationen SWAMID.

För att kunna aktivera sitt anställdakonto måste personen vara verksam som antingen anställd eller övrig verksam. Som anställd räknas alla som är registrerade som anställda i universitets personaladministrativa system Primula. Till övrig verksam räknas person som inte är registrerade som anställda i Primula men har en aktiv och tydlig verksamhet vid en institution[1] på universitetet. Prefekt[2] är ansvarig för övriga verksamma. Exempel på övrig verksam är forskare, forskarstuderande, läkare med undervisningsplikt, stipendiat, arvodist, gästlärare och aktiv emerita/emeritus. Studerande på grundnivå och avancerad nivå räknas inte till övriga verksamma.

Katalogadministratörer vid institutionerna administrerar på prefektens uppdrag vilka som är verksamma vid institutionen i AKKA. Vem som är anställd respektive övrig verksam sköts av AKKA tillsammans med Primula automatiskt. Så länge en person finns inlagd som verksam vid minst en institution är ett aktiverat anställdakonto fortfarande aktivt. När personen inte längre finns inlagd som verksam i AKKA avslutas användarkontot automatiskt.

Kontot kan ha tillitsnivå 1, 2 eller 3 beroende på aktiveringsmetod. Ett konto kan höja tillitsnivån genom kontoaktiveringsprocessen.

2.3 Konto för externa konsulter eller samarbetspartner

Personer som varken är studerande, anställda eller övriga verksamma och som inte kan använda en befintlig användare vid annat lärosäte för federativ inloggning till någon av universitetets IT-tjänster kan få ett särskilt konto för externa konsulter eller samarbetspartners, ett s.k. externkonto. Dessa konton går att använda inom identitetsfederationen SWAMID och har tillitsnivå 1.

Ett externkonto beställs av Servicedesk enligt särskilda rutiner. De som kan beställa externkonton är ansvarig för aktuell IT-tjänst eller för medarbetarportalen gruppägare.

[1] Med institution menas även annan organisatorisk enhet med egen resultatenhet.

[2] Med prefekt menas även motsvarande chef vid annan organisatorisk enhet med egen resultatenhet.

Externkonton har ett sista giltighetsdatum som kan flyttas framåt av Servicedesk efter överenskommelse med ansvarig för IT-tjänsten respektive gruppägaren i medarbetarportalen.

2.4 Konto för funktioner

Funktionskonton, eller konton som inte är bundna till enskild person, används för två saker, dels för e-postadresser som läses av flera personer, t.ex. alla studievägledare vid en institution, och dels för system-till-systemåtkomst, t.ex. ett system som behöver ha åtkomst till AKKAs inloggnings-skyddade LDAP-servrar. Dessa konton går *inte* att använda inom identitetsfederationen SWAMID. Funktionskonton kan finnas i följande tre varianter:

E-post med endast eftersändning: All inkommande e-post eftersänds till angivna e-postadresser och kontot går inte att använda för inloggning, en s.k. minilista.

E-post med brevlåda utan egen inloggning: All inkommande e-post levereras till användarkontots brevlåda som definierade anställda eller övriga verksamma får tillgång till via sin egen inloggning i Exchange.

Fullständigt funktionskonto med eller utan e-post. Om e-post i Exchange används kan även definierade anställda eller övriga verksamma få tillgång till användarkontots brevlåda via sin egen inloggning i Exchange. Funktionskonton för studentorganisationer är en specialvariant av dessa.

Funktionskonto beställs av Servicedesk av prefekt, IT-ansvarig eller kataloganvarig. För varje funktionskonto definieras en ansvarig person vid universitetet. Denna person är den som i förekommande fall kan genomföra aktivering och lösenordsåterställning.

Funktionskonton för studentorganisationer beställs ordförande för en godkänd studentorganisation, eller förste kurator för en studentnation.

Funktionskonton har ett sista giltighetsdatum som kan flyttas framåt av Servicedesk efter överenskommelse med ansvarig för funktionskontot.

2.5 Konto för besökande gäster eller biblioteksbesökare

Observera att konton för gäster och biblioteksbesökare inte hanteras på samma sätt som övriga kontotyper. Dessa konton går *inte* att använda inom identitetsfederationen SWAMID.

Varje anställd och övrig verksam kan genom självservicegränssnitt ge sina besökande ett konto som är giltigt i maximalt sju dagar. Den anställde eller övrigt verksamme kan maximalt ha fem aktiva gästkonton samtidigt.

Bibliotekspersonal kan via särskilt administrativt gränssnitt skapa obegränsat antal gästkonton per dag men dessa är giltiga endast den aktuella dagen eller i särskilda fall maximalt sex månader.

Servicedesk samt utpekade personer på universitet kan via särskilt administrativt gränssnitt skapa obegränsat antal gästkonton med en giltighetstid upp till sex månader för t.ex. konferens-deltagare.

Användningen av gästkonton är begränsad till lokalt trådlöst nätverk och inloggning i biblioteksdatorer.

3. Kontohantering

Alla kontotyper förutom konton för besökande gäster eller biblioteksbesökare använder nedanstående aktiviteter för kontohantering.

3.1 Aktivering av användarkonto

När en person vill aktivera sitt användarkonto vid universitetet surfar personen till en särskild webbtjänst för kontoaktivering och lösenordsåterställning[3].

Användaren betraktas som bekräftad användare (SWAMID tillitsnivå 2) när någon av följande aktiveringsmetoder används

- Användaren genomför en inloggning med en giltig Svensk E-legitimation med tillitsnivå 3 eller högre.
- Användaren genomför en inloggning med Freja eID för utländska medborgare med tillitsnivå 2 eller högre.
- Användaren aktiverar kontot genom en inloggning med eduID.se konto och denna inloggning har SWAMID tillitsnivå 2 eller högre
- Användaren anger en engångskod som användaren fått vid en reception efter att genomfört en fullständig identitetskontroll.
- Användaren anger en engångskod som användaren fått skickat till sin folkbokföringsadress.

3 https://uu.se/konto

I övriga fall betraktas kontot som obekräftad användare (tillitsnivå 1)

Det är även möjligt att aktivera konto med ett annat personligt användarkonto vid universitetet, dvs. ett anställdakonto om man är studerande och vice versa. Det aktiverade kontot betraktas då ha samma tillitsnivå som kontot som används för aktivering.

Nya anställda och övriga verksamma rekommenderas att hämta en engångskod mot uppvisande av legitimation samtidigt som de kvitterar ut sitt campus-/passerkort och eventuella nycklar. Ansvarig för ett funktionskonto kan även logga in med sitt personliga användarkonto vid universitetet för att aktivera funktionskontot.

När inloggningen är genomförd fyller personen i ett webbformulär där personen bland annat godkänner universitetets användarregler och anger sitt eget lösenord A. Studerande som aktiverar sitt konto anger även om de vill få sin e-post vid universitetet eftersänd till en annan e-postadress, som de själva anger, samt hur de vill synas i studentportalens deltagarlistor. Användarkontot aktiveras efter att personen fyllt i formuläret och tryckt på avsedd knapp för att skapa kontot.

Externa konton och funktionskonton är alltid att betrakta som obekräftade användare (tillitsnivå 1) med avseende på att engångskoden kan skickas med vanlig post till kontoinnehavaren respektive ansvarig för funktionskontot.

3.2 Utlämnande av engångskod

Anställda, övriga verksamma och studerande som inte kan aktivera sitt konto via eduID.se eller e-legitimation, går till en reception som hanterar engångskoder vid universitetet. Vid receptionen kan de mot uppvisande av i Sverige giltig legitimationshandling (pass, europeiskt nationellt identitetskort, svenskt körkort, skatteverkets identitetskort, SIS-märkt identitetskort samt körkort inom EU/EES som har ett foto samt ett sista giltighetsdatum) hämta en engångskod som sedan kan användas för att aktivera användarkontot eller genomföra lösenordåterställning. I samband med identitetskontrollen genomför handläggaren i receptionen en bedömning av handlingens äkthet och registrerar uppgifter från handlingen i AKKA. I AKKA finns ett inbyggt stöd vid kontrollen av identitetshandlingens äkthet. Personen får efter identitetskontrollen en engångskod kopplad till det användarkonto som ska behandlas utskriven på ett papper. Engångskoder som hämtas i reception är giltiga i fyra timmar. Som förregistrerad identifierare används personnummer när det finns. Saknas personnummer används istället identitetshandlingens idnummer i kombination med utfärdandeland eller kombinationen födelsedatum, förnamn, efternamn och identitetshandlingens utfärdandeland.

Anställda, övriga verksamma och studerande kan få engångskod skickad med traditionell post till sin folkbokföringsadress. Engångskoder som skickas via post är giltiga i fyra veckor.

Engångskoder för externkonton kan även skickas med traditionell post till av beställaren definierad postadress. En vidimerad elektronisk kopia på i Sverige giltig legitimationshandling måste bifogas beställningen av externkonto till Servicedesk för att engångskoden ska kunna skickas. Engångskoder som skickas via post är giltiga i fyra veckor. För externkonton används personnummer, förnamn och efternamn som förregistrerade identifierare. Om personnummer saknas används istället födelsedatum.

I särskilda fall kan studerande utan svenskt personnummer eller svensk folkbokföringsadress få engångskod skickad till registrerad adress i LADOK. Detta används när den studerande aldrig finns i universitetets lokaler, s.k. IT-distans, eller då distansstudier förutsätter studier på hemmaplan innan första sammankomsten. För att engångskoden ska skickas till den studerande krävs att den studerande skickar via e-post in följande handlingar: vidimerad kopia på pass eller motsvarande identitetshandling med foto, vidimerad kopia på en på personen utställd hushållsräkning samt då hushållsräkningen inte är skriven med det latinska alfabetet en vidimerad översättning till engelska. Innan engångskoden skickas av Servicedesk görs kontroll av id-handlingens personuppgifter mot LADOK, en rimlig bedömning att det är rätt person samt att namn och adressen mellan LADOK och hushållsräkningen tillräckligt väl överensstämmer. Engångskoder som skickas via post är giltiga i fyra veckor.

3.3 Återställning av lösenord A med hjälp av konto eller engångskod

Om en person glömt lösenord A till sitt användarkonto skapar användaren ett nytt genom att först logga in i tjänsten som används för att aktivera användarkonto med någon av metoderna i avsnitt 3.1. Efter inloggningen får personen möjlighet att genomföra lösenordsåterställningen.

3.4 Återaktivering av tidigare aktivt användarkonto

Har ett användarkonto varit avstängt i mindre än ett år aktiveras det automatiskt om kriterierna för att kontot ska vara aktivt uppfylls. Användarkonton som har varit avstängda längre än ett år aktiveras på samma sätt som om kontot aldrig varit aktivt.

3.5 Godkännande av uppdaterade användarregler

När universitetet uppdaterar ”Allmänna regler för användning av användarkonton och datornät” ska användaren godkänna dem innan de kan fortsätta använda IT-tjänster vid universitetet. Hanteringen av godkännande av användarregler, förutom för nya användare, genomförs via universitetets webbaserade identitetsutgivare Gemensam webbinloggning. Om användarreglerna har uppdaterats eller om påminnelse är aktuell kommer användaren tvingas att godkänna användarreglerna med hjälp av en tilläggstjänst i Gemensam webbinloggning innan inloggning i efterfrågad webbtjänst kan ske.

3.6 Aktivering, återställning och inaktivering av lösenord B

Lösenord B är ett lösenord som används till nätverksinloggning via eduroam. Ingen användare får något lösenord B när kontot aktiveras utan användaren skapar detta senare med hjälp av lösenord A i AKKAs självservicegränssnitt.

Glömmer kontoinnehavaren bort sitt lösenord B skapar personen ett nytt via självservicegränssnittet.

Har användaren inte längre behov av lösenord B tar personen bort lösenordet via självservicegränssnittet.

3.7 Återanvändning av användaridentiteter

För att minska risken för att en person av misstag ska få tillgång till en annan persons sparade data, till exempel personuppgifter, e-post och dokument, återanvänds aldrig aktiverade användaridentiteter för annan person än den person som tidigare innehaft användarkontot.

3.8 Personverifierad andra faktor

En användare kan få en personverifierad andra faktor kopplad till sitt konto. Detta görs genom att besöka en reception som hanterar detta och legitimera sig på samma sätt som för uthämtning av engångskod (se 3.2). Användaren får då en personverifierad andra faktor i form av en U2F-kompatibel Yubikey kopplad till sitt konto.

Vid utlämning av personverifierad andra faktor upplyses användaren om att inte dela faktorn med någon annan person.

Den personverifierade andra faktorn kan spärras av kontoadministratör eller av användaren själv.

Ny personverifierad andra faktor kan utlämnas efter spärrning och görs då på samma sätt som första gången.

3.9 Egenverifierad andra faktor

En användare kan själv koppla en egenverifierad andra faktor till sitt konto. Det görs i AKKA:s självservicegränssnitt. Byte av egenverifierad andra faktor kan göras i samma gränssnitt men endast om användaren autentiserat sig med den aktuella andra faktorn först.

Den egenverifierade andra faktorn implementeras med Time Based One Time Password, RFC 6238.

Den egenverifierade andra faktorn kan spärras av kontoadministratör eller av användaren själv. En spärrad faktor kan inte återanvändas.

Byte av egenverifierad faktor kräver att användaren autentiserar sig med multifaktor alternativt autentiserar sig enligt någon av de aktiveringsmetoder som gäller för Swamid AL2 enligt avsnitt 3.1.

När användare kopplar egenverifierad andra faktor till sitt konto upplyses hen om att inte dela faktorn med någon annan person.

4. Personliga certifikat genom Sunet Trusted Certificate Service

För att personer med e-postadress vid Uppsala universitet ska kunna beställa personliga certifikat av typen *GÉANT Personal Certificate* och *GÉANT IGTF-MICS Personal* måste de ha uppvisat i Sverige giltig legitimation för personal vid universitetet. Vidare måste denna kontroll ha registrerats i AKKA. Alla som hämtat engångskod mot uppvisande av legitimationshandling i en reception vid universitet har fått denna markering och kan därmed beställa dessa certifikat. De som inte har hämtat en engångskod kan få markeringen genom att gå till samma receptioner där engångskod lämnas ut för att genomföra en legitimationskontroll som registreras i AKKA. *GÉANT Personal Certificate* används främst för säker e-post, dvs. att e-posten signeras av avsändaren och ev. krypteras så att endast mottagarna kan läsa meddelandet. Certifikat av typen *GÉANT IGTF-MICS Personal* används för att logga in i vissa typer av vetenskapliga forskningssystem, till exempel GRID-baserade system.