BILAGA 2

Säkerhetsföreskrifter för Användarorganisationer anslutna till Skolfederation

Version 2.3

Skolfederation strävar mot att definiera och inom ramen för Federationen erbjuda den eller de tillitsnivåer (grader av skydd) i identifieringen som efterfrågas bland de förlitande Tjänsteleverantörerna. Denna efterfrågan drivs av dessa aktörers behov av att hantera de egna riskerna inom E-tjänsten, där även regulatoriska och rättsliga krav som kan komma att bli tillämpliga.

Denna bilaga syftar till att definiera den grundskyddsnivå som samtliga Användarorganisationer i tillämpliga delar förväntas arbeta mot, och som samtidigt är praktisk och tillämplig från kostnads- och användbarhets-synpunkt. I ett längre perspektiv är det möjligt att den inom Skolfederation definierade grundskyddsnivån harmoniseras med andra federationers skyddsnivåer och internationellt vedertagna principer.

En säkerhetsmodell för federerad elektronisk identifiering

I definitionen av grundskyddsnivån utgår Skolfederation ifrån en allmänt vedertagen modell för elektronisk identifiering som delas in i tre olika faser:

- Fastställande av sökandens identitet och registrering,
- Utfärdande och tillhandahållande av elektronisk ID-handling, samt
- Verifiering av elektronisk ID-handling och utställande av identitetsintyg.

I var och en av dessa faser krävs särskilda åtgärder för att upprätthålla en definierad skyddsnivå i hanteringen av elektroniska identiteter. Skyddsåtgärderna är i dessa delar endast tillämpliga för de Användarorganisationer som utfärdar elektroniska ID-handlingar som används inom Federationen. Gemensamt för samtliga faser och för sådana Användarorganisationer som tillhandahåller behörighetsstyrande Attribut är säkerhetskrav som rör:

- Organisatoriska och operationella aspekter,
- Fysisk, administrativ och personorienterad säkerhet, samt

• Teknisk säkerhet.

Det är viktigt att det finns utrymme för de olika aktörerna att lösa grundskyddsnivån i Regelverket på ett effektivt sätt som passar den egna verksamheten. Det bör vara möjligt för den enskilda aktören att utforma sina egna kontroller som säkerställer skyddet. Det bör också vara möjligt att utelämna de delar av grundskyddsnivån som inte är tillämpliga i den egna verksamheten. Därför formuleras i Regelverket den övergripande och långsiktiga grundskyddsnivån som en målsättning för att uppnå den angivna skyddsnivån för de av Användarorganisationen tillhandahållna tjänsterna.

Föreskrifter för säkerhet och tillit

Informationssäkerhet

Informationssäkerhetsarbetet inom Användarorganisationens verksamhet ska ledas, styras, utvärderas och utvecklas med stöd av ett ledningssystem. Till grund för ett sådant arbete kan ledningssystem-standarden ISO/IEC 27001 användas. Avgränsningen för ledningssystemet ska innefatta alla delar i Användarorganisationens verksamhet som berör dennes medverkan i Skolfederation. Grundläggande är att informationssäkerhetsarbetet kontinuerligt utvärderas och anpassas till identifierade risker och aktuella verksamhets- och omvärldskrav. Arbetet innefattar organisations- och resursfrågor, samt tekniska och administrativa säkerhetsåtgärder som berör Användarorganisationens medverkan i Skolfederationen. Specifikt bör Användarorganisationen tillse att informationssäkerhetsarbetet innefattar att:

1. samtliga säkerhetskritiska administrativa och tekniska processer har dokumenteras och att roller, ansvar och befogenheter finns tydligt definierade,

2. säkerställa att denne vid var tid har tillräckliga personella resurser till förfogande för att uppfylla sina åtaganden,

3. ha en process för riskhantering som på ett ändamålsenligt sätt regelbundet analyserar hot och sårbarheter i verksamheten, och som genom införande av säkerhetsåtgärder balanserar riskerna till acceptabla nivåer,

4. ha en process för incidenthantering som systematiskt säkerställer kvaliteten i tjänsten, former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder kan vidtas för att lindra eller förhindra skada vid inträffade incidenter.

Användarorganisationen ska också tillse att de delar av den tekniska driftmiljön som är av betydelse för säkerheten i Skolfederation skyddas fysiskt mot skada som följd av t.ex. miljörelaterade händelser, otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till

behörig personal, att informationsbärande lagringsmedia och pappersdokument förvaras och utmönstras på ett säkert sätt, samt att tillträde till dessa skyddade utrymmen kontinuerligt övervakas.

Användarorganisationen ska säkerställa spårbarheten vid all logisk och fysisk åtkomst till känsliga IT-system. Åtkomst ska kunna härledas på individnivå, och identifieringen av individen ska ske på ett betryggande och säkert sätt. För alla åtgärder som rör hanteringen av Elektroniska identiteter och Attribut ska finnas revisionsspår att följa. Elektronisk kommunikation som direkt eller indirekt berör känsliga uppgifter ska skyddas mot manipulation och insyn via starka kryptografiska metoder.

Internkontroll

Efterlevnaden av de krav som ställs på Användarorganisationen genom Regelverket ska över en treårsperiod vara föremål för internrevision, utförd av oberoende intern kontrollfunktion, såvida inte organisationens storlek eller annan försvarbar orsak motiverar att revision sker på annat sätt. Dokumentation som stöder efterlevnaden av kraven enligt detta Regelverk ska bevaras så länge som det krävs för att säkerställa möjlighet till uppföljning. Material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.

Identifiering och registrering

Användare inom Skolfederation ska identifieras på likvärdigt sätt som vid inskrivning vid den aktuella skolenheten. Om en Användare redan har identifierats vid ett inskrivningsförfarande, och dennes identitet därigenom gjorts känd, får denna relation ligga till grund för identifieringen.

Om det råder ett anställnings- eller uppdragsgivarförhållande mellan Användaren och Användarorganisationen, ska denna relation ligga till grund för identifieringen istället för enligt ovan.

Användarorganisationen ska, beaktat reglerna för persondataskydd, föra register över anslutna Användare. Registreringen bör innefatta personnummer eller samordningsnummer, samt de uppgifter som i övrigt är nödvändiga för att Användarorganisationen ska kunna tillhandahålla den elektroniska ID-handlingen och utfärda Identitetsintyg.

Användarorganisationen ska kontrollera att de personuppgifter som registrerats är korrekta och fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register. Det är Användarorganisationens ansvar att säkerställa att de Attribut som tillförs en Elektronisk identitet är korrekta, fullständiga och aktuella. Användarorganisationen ska också skyndsamt avregistrera Användare och spärra den elektroniska ID-handlingen när relationen med den anslutna Användaren upphör.

Utfärdande av elektronisk identitetshandling

I utfärdandefasen kopplas en elektronisk ID-handling till den tidigare fastställda identiteten. Utformningen av den elektroniska ID-handlingen kan variera beroende på vilka säkerhetskrav som i övrigt är tillämpliga, men gemensamt för samtliga idag förekommande metoder för elektronisk identifiering är att ett stycke konfidentiell information binds till användaren på ett tillräckligt säkert sätt. Detta kan vara ett lösenord eller en uppsättning koder, en kryptografisk nyckel eller en personlig säkerhetsmodul.

Den elektroniska ID-handlingen ska utformas och framställas på ett sätt som gör det osannolikt att någon utomstående kan gissa eller räkna ut den konfidentiella information som ligger till grund för den elektroniska identifieringen, ens på maskinell väg.

Användarorganisationen ska också tillhandahålla en tjänst där användaren kan spärra sin elektroniska ID-handling (spärrtjänst). Tjänsten ska ha god tillgänglighet och Användarorganisationen ska behandla anmälan om spärr skyndsamt. Den Användarorganisation som tillhandahåller elektroniska ID-handlingar inom Skolfederation ska spärra sådana elektroniska ID-handlingar om denne uppmärksammas på eller att det annars kan misstänkas att dessa används eller kan komma att användas i bedrägliga syften.

Utgivning av identitetsintyg

Användarorganisation som tillhandahåller tjänst för utgivning av Identitetsintyg till förlitande E-tjänster, ska följa de tekniska specifikationer som Federationsoperatören från tid till annan föreskriver. Utlämnande av Identitetsintyg ska föregås av en tillförlitlig kontroll av den angivna Elektroniska identiteten och den elektroniska ID-handlingens giltighet.

Lämnade Identitetsintyg ska vara giltiga endast så länge som det krävs för att användaren ska få tillgång till den efterfrågade E-tjänsten, samt skyddas så att informationen endast är läsbar för den avsedda mottagaren och att den som tar emot intyget kan kontrollera att mottagna Identitetsintyg är äkta.

Användarorganisationen ska, beaktat de elektroniska ID-handlingarnas utformning, säkerställa att tekniska säkerhetskontroller införts vid verifiering av användarens elektroniska ID-handling och utfärdande av Identitetsintyg, så att det är osannolikt att utomstående genom avlyssning, återuppspelning eller manipulation av kommunikation, eller genom att gissa koder eller lösenord, kan utge sig för att vara en annan användare än de verkligen är.