SWAMID

SWAMID

Policyöversyn 2020
Community Consensus Process 1

Presentation av förslag till ändringar av SWAMIDs federationspolicy och tillitsprofilerna SWAMID AL1 och SWAMID AL2 samt ny tillitsprofil SWAMID AL3

SUNET

Agenda

- Vad är en Community Consensus Process?
- Vad innehåller SWAMID Policy Framework?
- Varför en policyöversyn?
- Förändringar i SWAMIDs federationspolicy
- Generella förändringar i tillitsprofilerna
- Förändringar i tillitsprofil SWAMID AL1
- Förändringar i tillitsprofil SWAMID AL2
- Ny tillitsprofil SWAMID AL3
- Vad händer nu?

Community Consensus Process

- I korthet hur man förankrar förändringar i ett gemensamt överenskommet regelverk enligt en överenskommen metod
  - SWAMID har inte en formell gemensam överenskommen metod så SWAMID Operations har lånat från vår systerfederation inCommon.
- Metoden i korthet
  1. En definierad arbetsgrupp tar fram ett förändringsförslag, i detta fall SWAMID Operations
  2. SWAMID Operations skickar ut förslaget till förändring för påsyn
  3. Alla federationsmedlemmar samt tjänsteleverantörer har möjlighet att diskutera, kommentera och föreslå förbättringar av förslaget
  4. Arbetsgruppen bearbetar de förslag som kommer in och förbättrar förslaget
     a) Om förändringarna i förslaget är stora skickas ett nytt förslag ut igen, gå till punkt 2
     b) Om förändringarna är små eller ringa skickas förslaget till SWAMID Board of Trustees
  5. SWAMID Board of Trustees beslutar om förändringen

SWAMID Policy Framework

- SWAMIDs policy består av flera olika delar:
  - Federationspolicy (huvudpolicy)
  - Tillitsprofiler

  ← Community Consensus Process 1
  - Teknologiprofiler
  - Incidenthantering i SWAMID
- Teknologispecifika policydokument
  - Nyttjanderegler av SWAMIDs Metadata
  - Interfederation Metadata Registration Practice Statement

Varför en policyöversyn?

SWAMID

- I samband med att inloggningsprofilen SWAMID Person-Proofed Multi-Factor Profile skrevs såg SWAMID Operations att nuvarande policyramverk var både svårläst och föråldrat
- De olika policydelarna har skrivits under en period på 10 år och hade därför olika språk för samma sak
- Efter 10 år behöver även både teknik och processer ses över så att de följer det som är aktuellt men ändå inte vänder upp och ner på allt
- Behoven från tjänsterna av inloggningstillit förändras och blir tydligare både genom omvärldskrav och verksamhetskrav

SWAMID

Federationspolicyn

SUNET

Förändringar i SWAMIDs grundpolicy

- Generellt har läsbarheten blivit bättre genom mer eller mindre omfattande omformuleringar

Avsnitt 1.1

- Nytt avsnitt som definierar några viktiga termer som används ofta i hela policyn

Avsnitt 2

- Avsnittet är omformulerat för att göra avsnittet tydligare och enklare att läsa
- Sista stycket i avsnittet har utökats med exemplifiering

Förändringar i SWAMIDs grundpolicy

Avsnitt 4.1

- Sunet tagit över det formella ansvaret för att överenskommelser och avtal med nationella och internationella organisationer

Avsnitt 4.2

- SWAMID har fått det formella ansvaret för att genomföra det dagliga arbetet samt fortsätta utveckla och underhålla identitets-federationen
- Ansvaret för att utse medlemmar i SWAMID Operations flyttats till Sunet beroende på att Sunet är den som formellt tecknar avtal med medlemsorganisationer för inlånad personal

Förändringar i SWAMIDs grundpolicy

Avsnitt 4.3

- Avsnittet är både förenklat och förhoppningsvis tydligare
- För att bli medlem i SWAMID måste organisationen vara ansluten till Sunet om inte särskilda skäl föreligger som Sunet godkänner
- Tjänsteleverantörer förväntas inte vara medlemmar av Sunet om de inte också har en identitetsutfärdare registrerad i SWAMID
- Alla identitetsutfärdare i SWAMID måste vara godkänd för minst en tillitsprofil
  - Alla medlemmar uppfyller inte detta krav idag utan definierad övergångs-period behöver beslutas av SWAMID Board of Trustees

SWAMID

Tillitsprofilerna

SUNET

Generella förändringar i tillitsprofilerna

SWAMID

- Språk och uppbyggnad av de tre tillitsprofilerna är både moderniserat och harmoniserat utan att ändra avsikten i olika avsnitt
- Begreppsensning, t.ex. används nu enbart begreppet member organisation istället för både home organisation och member organisation
- Begreppen Credential issuing, Credential re-issuing, Credential renewal och Credential revocation är definierade i avsnitt 1.1

SWAMID

SWAMID AL1

Jämförelse mellan nuvarande och nya förslaget

SUNET

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 2

- Definerad som lägsta tillitsnivå för IdP:er inom SWAMID
  - Alla medlemsorganisationer måste vara godkända för minst SWAMID AL1
- A claim at this Identity Assurance Profile implies the following:
  - the subject is affiliated with the Member Organisation;
  - the subject is a natural person;
  - the subject is identified by a unique permanent user identifier; and
  - attributes/information released may be self-asserted.
- Lagt till jämförelser med andra motsvarande tillitsramverk

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 3.2

- Förtydligande om och när medlemsorganisationer behöver skicka in en uppdaterad Identity Management Practice Statement (IMPS) inkl. självdeklaration om att man uppfyller SWAMID AL1
- Vid förändrade rutiner som påverkar godkända tillitsprofiler måste en ny IMPS skickas in och godkännas före förändringen driftsätts

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 5.1.1

- Lösenord är inte längre den enda inloggningsmetoden
  - Stöd för passwordless och multifaktorinloggning
  - Andra faktor via SMS, återuppringning och push via inloggningsapp är ej tillåtet enligt tillitsprofilen
    - Tjänar sitt syfte som utökat personligt lösenordsskydd i andra tjänster
- Lösenordskraven är höjda till samma som för SWAMID AL2
  - Brytande förändring men alla lärosäten med SWAMID AL1 uppfyller detta idag
- zxcvbn är tillagt som möjlig metod för att räkna lösenordsentropi

Förändringar i tillitsprofil SWAMID AL1

SWAMID

Avsnitt 5.1.3

- Avsnittet har utökats med en "guidance" om att användarna ska uppmanas att inte använda lösenordet i andra tjänster på internet
  - En brytande förändring som alla godkända medlemsorganistioner inte uppfyller idag, därför "guidance" istället för krav
  - Att uppnå detta görs enklast via uppdatering av lösenords- och användarregler

Avsnitt 5.2.3

- En persons globala unika identifierare (i WebSSO SAML oftast eduPersonPrincipalName) får inte återanvändas för annan person

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 5.2.5

- EU-lagstiftningen kräver idag att om man använder nationellt eID i en tjänst måste man också tillhandahålla inloggning via eIDAS
- eIDAS Low är precis som svenskt eID LoA2 godkänt för att belägga att en användare är godkänd för SWAMID AL1
- Ny tydlig beskrivning om att koppla användare mot lokal användardatabas måste göras med förregistrerad identifierare
  - I "guidance" finns en lista med identifierare knutna till varje metod i avsnittet
- I "guidance" finns även en kraftig rekommendation om att inte tillåta SSO från aktiveringstjänst mot identitetsutgivare i punkt 1-3.

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 5.3.3

- Avsnittet är omskrivit för att mer tydligt visa att lösenords-återställning måste göras på ett sätt som tillräckligt väl knyter användarkontot till samma användare som tidigare, dvs. genom att använda samma förregistrerade identifierare som i avsnitt 5.2.5
- Att matcha med förregistrerad identifierare torde göra så att inte annan person får tillgång en annan persons information och följer av GDPR

Förändringar i tillitsprofil SWAMID AL1

SWAMID

Avsnitt 5.4.1

- Avsnittet är omskrivit för att mer tydligt visa att både användaren själv och medlemsorganisationen kan återkalla inloggningsuppgifter

Avsnitt 5.4.2

- Samma krav som i 5.3.3 om förregistrerade identifierare
- Nytt formellt krav på att medlemsorganisationen måste informera varför användare har fått sina inloggningsuppgifter återkallade

Avsnitt 5.4.3

- Krav omformulerat i ny punkt om att medlemsorganisationen ska vidta försiktighetsåtgärder för att incidenter inte återuppträder

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 5.5.2

- Kravet på upptid på 95% är omskrivet på så sätt att medlems-organisationen garanterar att identitetsutfärdarna har minst en upptid som gör att interna system går att logga in i
  - Exempel på interna system är Ladok, Nais och Primula hos SSC

Avsnitt 5.6.4

- Avsnittet är omskrivet och handlar nu endast om att SSO-sessioner får max vara giltiga i 12 timmar
  - Långsiktiga säkra inloggningsnycklar i webbläsarnas ”browser store” räknas inte in här utan tillhör passwordless och ska uppfylla avsnitt 5.1.1

Förändringar i tillitsprofil SWAMID AL1

Avsnitt 6

- Avsnittet har fått ny rubrik och innehåll
- Avsnittet beskriver nu hur AL1-nivån ska signaleras i de teknologiprofiler som kan signalera tillitsinformation
  - OBS! Just nu är det bara WebSSO via SAML som kan signalera tillitsinformation

SWAMID

SWAMID AL2

Jämförelse mellan nuvarande och nya förslaget

SUNET

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 2

- A claim at this Identity Assurance Profile implies the following:
  - the subject is affiliated with the Member Organisation;
  - the subject is an identified natural person;
  - the subject is identified by a unique permanent user identifier; and
  - the Member Organisation is responsible for the attributes/information released.
- Lagt till jämförelser med andra motsvarande tillitsramverk
- ”Guidance" om när SWAMID AL2 ska användas är bortplockad

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 3.2

- Förtydligande om och när medlemsorganisationer behöver skicka in en uppdaterad Identity Management Practice Statement (IMPS)
- Ny IMPS behöver skickas in och godkännas före en förändring som ger effekt för godkännande av tillitsprofiler skickas driftsätts, inte efter

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 5.1.1

- Exakt samma förändring som i SWAMID AL1

Avsnitt 5.1.3

- Exakt samma förändring som i SWAMID AL1

Avsnitt 5.1.4

- Exakt samma förändring som i SWAMID AL1

Avsnitt 5.2.3

- Exakt samma förändring som i SWAMID AL1

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 5.2.5

- EU-lagstiftningen kräver idag att om man använder nationellt eID i en tjänst måste man också tillhandahålla inloggning via eIDAS
- eIDAS Substantial är precis som svenskt eID LoA3 godkänt för att belägga att en användare är godkänd för SWAMID AL2
- Vid beläggande om att det är rätt användare med hjälp av identitets-handling ska polisens regelverk för utfärdande av pass användas
- Körkort från annat EU/EES-land är ej längre godkända beroende på för dålig kvalité

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 5.2.5 (forts)

- Ny tydlig beskrivning om att koppla användare mot lokal användardatabas måste göras med förregistrerad identifierare
  - I "guidance" finns en lista med identifierare knutna till varje metod i avsnittet
- I "guidance" finns även en mycket kraftig rekommendation om att inte tillåta SSO från aktiveringstjänst mot identitetsutgivare i punkt 1-3.

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 5.3.3

- Avsnittet är omskrivit för att mer tydligt visa att lösenords-återställning måste göras på ett sätt som tillräckligt väl knyter användarkontot till samma användare som tidigare, dvs. genom att använda samma förregistrerade identifierare som i avsnitt 5.2.5
- Att matcha med förregistrerad identifierare torde göra så att inte annan person får tillgång en annan persons information och följer av GDPR

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 5.4.1

- Exakt samma förändring som i SWAMID AL1

Avsnitt 5.4.2

- Avsnittet är omskrivit för att mer tydligt visa att lösenords-återställning måste göras på ett sätt som tillräckligt väl knyter användarkontot till samma användare som tidigare, dvs. samma förregistrerade identifierare som i avsnitt 5.2.5
- Nytt formellt krav på att medlemsorganisationen måste informera varför användare har fått sina inloggningsuppgifter återkallade

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 5.4.3

- Krav omformulerat i ny punkt om att medlemsorganisationen ska vidta försiktighetsåtgärder för att incidenter inte återuppträder

Avsnitt 5.4.3

- Exakt samma förändring som i SWAMID AL1

Avsnitt 5.5.2

- Exakt samma förändring som i SWAMID AL1

Avsnitt 5.6.4

- Exakt samma förändring som i SWAMID AL1

Förändringar i tillitsprofil SWAMID AL2

Avsnitt 6

- Avsnittet har fått ny rubrik och innehåll
- Avsnittet beskriver nu hur AL2-nivån ska signaleras i de teknologiprofiler som kan signalera tillitsinformation
  - OBS! Just nu är det bara WebSSO via SAML som kan signalera tillitsinformation
- Om en användare uppfyller kraven för SWAMID AL2 ska identitetsutfärdaren även signalera att användaren uppfyller kraven för SWAMID AL1

SWAMID

SWAMID AL3

Jämförelse mellan förslag för uppdaterad
SWAMID AL2 och nya SWAMID AL3

Ersätter Person-Proofed Multi-Factor with high identity assurance

SUNET

Ny tillitsprofil SWAMID AL3

Avsnitt 2

- A claim at this Identity Assurance Profile implies the following:
  - the subject is affiliated with the Member Organisation;
  - the subject is an identified and confirmed natural person;
  - the subject is identified by a unique permanent user identifier;
  - the Member Organisation is responsible for the attributes/information released; and
  - the authentication of the subject was a multi-factor authentication.
- Lagt till jämförelser med andra motsvarande tillitsramverk

SUNET

Ny tillitsprofil SWAMID AL3

Avsnitt 3.2

- Granskningen ökar genom att SWAMID Operations skriver en formell granskningsrapport inför godkännande av tillitsnivån
- SWAMID Operations genom ett eller flera möten med ansökande organisation
  - Mötet kan vara fysiskt eller över länk

Ny tillitsprofil SWAMID AL3

Avsnitt 5.1.1

- Multifaktorinloggning måste alltid användas
- Om lösenord används som fristående faktor tillsammans med någon annan faktor måste lösenordet uppfylla samma krav som i SWAMID AL2

Ny tillitsprofil SWAMID AL3

Avsnitt 5.2.5

- Person kan verifieras med annan identitetsutgivare inom SWAMID om både identitetsutfärdaren och personen är godkänd för SWAMID AL3
- Vid offline-verifiering av användare måste rekommenderat brev med personlig utlämning adresserat till folkbokföringsadressen användas
- Medlemsorganisationen måste ha definierade rutiner för hur identitetskontroll genomförs med beskrivning om hur kontroll av identitetshandling sker
- Alla som genomför identitetskontroll på tillitnivån måste följa rutinerna

Ny tillitsprofil SWAMID AL3

Avsnitt 5.3.3

- Endast definierade metoder i 5.2.5 får användas

Avsnitt 5.4.2

- Endast definierade metoder i 5.2.5 får användas

Avsnitt 6

- Om en användare uppfyller kraven för SWAMID AL3 ska identitetsutfärdaren även signalera att användaren uppfyller kraven för SWAMID AL2 och SWAMID AL1

Alltid multifaktorinloggning?

SWAMID

- En användare kan uppfylla kraven för SWAMID AL3 men ändå endast genomföra en inloggning med en faktor, t.ex. lösenord
- I det fallet får inte identitetsutfärdaren meddela tjänsten att användaren är SWAMID AL3, utan maximalt SWAMID AL2

SWAMID

Avslutning

SUNET

Vad händer nu?

SWAMID

- Community Consensus Process är öppen under perioden 7 april till och med 15 maj (saml-admins@swamid.se alt. operations@swamid.se)
- SWAMID Operations kommer därefter att gå igenom alla kommentarer och förändringsförslag för att inlemma förslaget eller avslå förslaget med en motivering varför
- Beroende på hur stora förändringarna är kommer ett nytt förslag på förändringar alternativt presenteras förslagen på förändringar som beslutsförslag för SWAMID Board of Trustees
- Beslut tas i Board of Trustees inkl. ev. övergångsperioder för införande.

Avslutande diskussion

- Ordet fritt…

SWAMID

SUNET

SWAMID