Teknisk beskrivning av datahantering i PRIIS

Last updated by | Daniel Nordström | 26 feb. 2026 at 14:04 CET

Teknisk beskrivning av datahantering i PRIIS

Målgrupp: Dataskyddsombud, Göteborgs kommun
Datum: 2026-02-26
Källor: Kodbas (backend och frontend), README-filer, Azure DevOps Wiki (PRIIS.wiki), samt interna verksamhets- och förvaltningsunderlag för gallring.

1. Syfte och avgränsning

Detta dokument beskriver på en övergripande teknisk nivå hur data hanteras i PRIIS, vilka skyddsåtgärder som finns i systemet och vilka delar som behöver kompletteras med ytterligare drift- eller verksamhetsunderlag.

Dokumentet fokuserar på:

- Inloggning, tvåfaktor och skydd mot bruteforce
- Behörighetsstyrning och accesshantering
- Separation mellan förvaltningar och kommuner
- Loggning och spårbarhet
- Vilka data som behandlas i olika steg
- Inblandade system
- Gallringstider (nuläge och beslutsunderlag)

2. Systemöversikt

PRIIS består i huvudsak av:

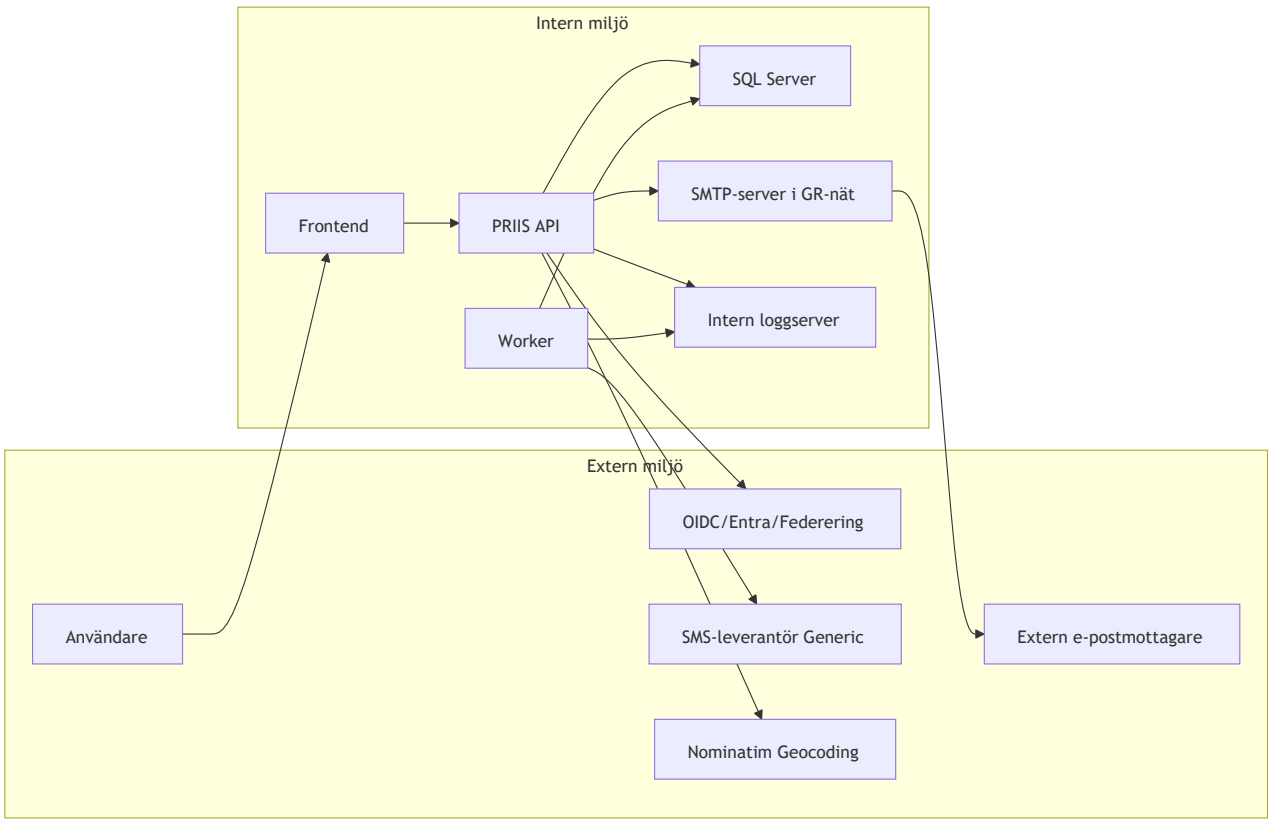
- Webbgränssnitt för användare (frontend)
- Tjänstelager för systemfunktioner (API)
- Databas
- Bakgrundsprocesser
- Externa integrationer för identitet, e-post, SMS och geokodning Trafiken kan

delas upp enligt följande:

- **Intern trafik:** Webbgränssnitt ↔ API, API ↔ databas, bakgrundsprocesser ↔ databas, API ↔ intern SMTP-server i GR:s nät, API/bakgrundsprocesser ↔ intern loggserver.
- **Extern trafik:** API/bakgrundsprocesser ↔ externa tjänster (OIDC/Entra/federering, SMSleverantör, Nominatim) samt utgående e-postleverans från intern SMTP vidare till externa mottagare.

Observera att API och Worker inte har direkt trafik mellan varandra; samordning sker via databasen.

Kommunikation till PRIIS sker via HTTPS.
Databasen är placerad i internt nät och är inte exponerad för direkt extern åtkomst.
Fördjupad drift- och åtkomstinformation med dataskyddsrelevans redovisas i avsnitt 9 i detta dokument.



3. Inloggning och skyddsåtgärder

Inloggning i PRIIS är uppbyggd som flera skyddande lager i följd: identitetskontroll, eventuell tvåfaktor/flerfaktor, behörighetskontroll och aktiv kontext (roll + entitet). Syftet är att minska risken för obehörig åtkomst även om en enskild kontroll kringgås.

3.1 Inloggning

Systemet stödjer två huvudvägar för autentisering:

- **Lokal inloggning** med e-post/lösenord mot PRIIS identitetshantering.
- **Federerad inloggning** via OIDC, där autentisering sker hos extern identitetsleverantör.

Vid federerad inloggning hanterar PRIIS inte användarens lösenord. PRIIS tar i stället emot identitetsattribut från identitetsleverantören och använder dessa för kontoidentifiering, behörighetsmappning och åtkomstbeslut.

3.2 Tvåfaktorautentisering

PRIIS har stöd för tvåfaktor i det lokala inloggningsflödet. När användarnamn/lösenord är korrekt men kontot kräver ytterligare verifiering sätts sessionen i ett särskilt verifieringsläge där inloggning inte slutförs förrän faktor två är godkänd.

För **icke-federerade användare** erbjuder PRIIS följande 2FA/MFA-metoder i nuläget:

- Engångskod via e-post
- Engångskod via SMS
- Authenticator-app (TOTP-baserad engångskod) Passkey-baserad verifiering
- i relevant flöde

Tvåfaktorkoder hanteras via separata endpoint-flöden för utskick och verifiering.

3.3 MFA-krav (kravbild och nuläge)

För dataskyddsändamål gäller följande kravbild per autentiseringsväg:

- **Lokal inloggning i PRIIS:** systemet stödjer och verkställer tvåfaktor när kontots konfiguration kräver det.
- **Federerad inloggning:** PRIIS kräver att extern identitetsleverantör tillämpar 2FA/MFA som del av inloggningspolicyn.

Detta innebär i praktiken att federerade inloggningar ska vara skyddade med flerfaktorsautentisering i den externa identitetsmiljön (exempelvis Entra/OIDC-policy). PRIIS förlitar sig på att denna policy är aktiverad och korrekt tillämpad hos respektive federation.

Det innebär att den samlade MFA-nivån beror både på PRIIS-konfiguration för lokala konton och respektive federationsparts identitets- och villkorspolicy.

3.4 Skydd mot bruteforce och missbruk

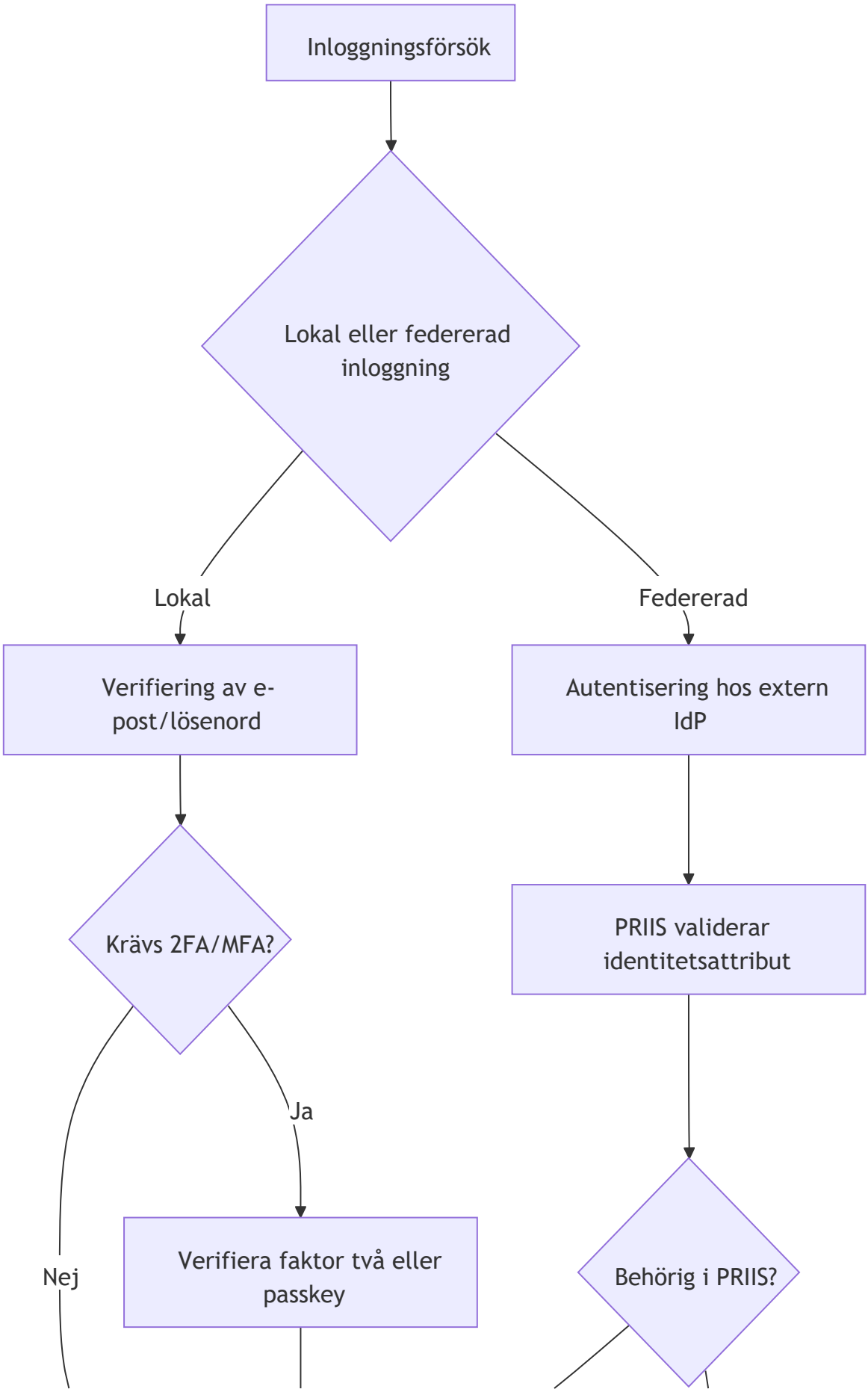
Kontolåsning vid upprepade misslyckade inloggningsförsök är aktiverad och konfigurerad i miljöinställningar.

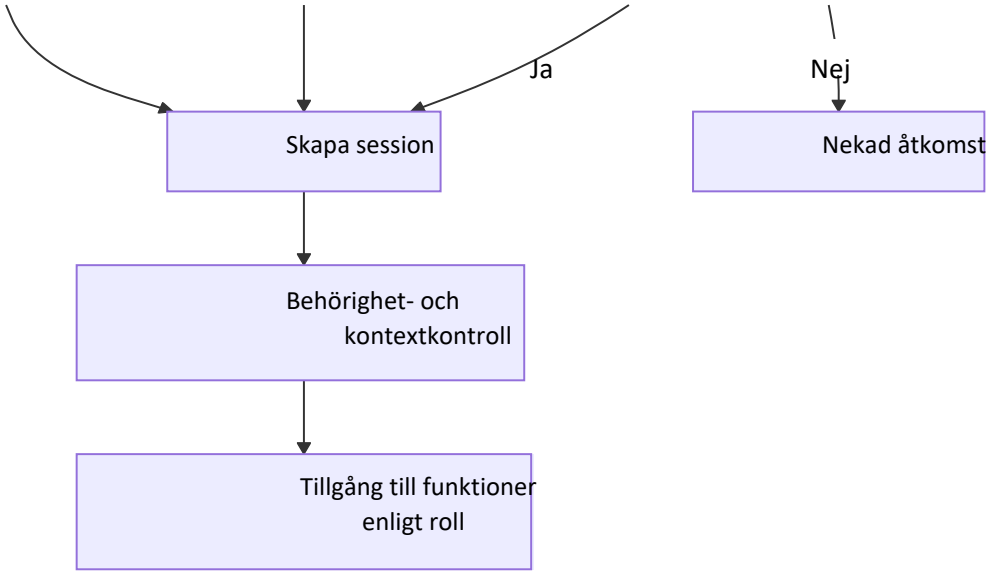
Verifierat nuläge:

- Lockout påslagen
- Maximalt 5 misslyckade försök innan låsning Låstid 5
- minuter

Därutöver används anropsbegränsning på utvalda tjänsteanrop för att minska effekten av upprepade, snabba eller automatiserade anropsmönster.

3.5 Inloggningsflöde i korthet





3.6 Bedömning för dataskydd

Sammantaget innebär detta att inloggningsskyddet är flerskiktat och att obehörig åtkomst motverkas genom kombinationen av:

- Flera autentiseringsvägar med tydlig separering
- Tvåfaktor/flerfaktor i lokala flöden
- Krav på 2FA/MFA hos extern identitetsleverantör i federerade flöden
- Kontolåsning och anropsbegränsning
- Efterföljande behörighet - och kontextkontroll innan åtkomst ges

4. Behörighetsstyrning och hantering av access

Behörighet i PRIIS är roll- och regelstyrd:

- En användare kan ha en eller flera roller.
- Roller är kopplade till organisatorisk kontext (exempelvis förvaltning/entitet).
- Åtkomst till funktioner styrs av systemåtgärder och policykontroller i tjänstelagret (API).

Behörighetsmodellen är uppbyggd för att ge hög spårbarhet och tydlig ansvarsfördelning. Det gör att åtkomst inte enbart styrs av vem användaren är, utan även av vilket uppdrag användaren utför i aktuell arbetssituation.

Access bedöms i två dimensioner:

1. **Vad** användaren får göra (systemåtgärd/behörighetsregel)
2. **I vilken kontext** användaren agerar (vald rolltyp och entitet)

Begäran utan giltig behörighet eller kontext nekas.

4.1 Administrativ accessprocess

Tekniskt stöd för roller och behörigheter finns i systemet. Processdelar såsom beställning, attest, periodisk översyn och avaktivering behöver fortsatt beskrivas och förankras i verksamhetens styrande rutiner, och markeras därför som kompletteringspunkt.

4.2 Praktisk hantering av access l

praktiken innebär modellen att:

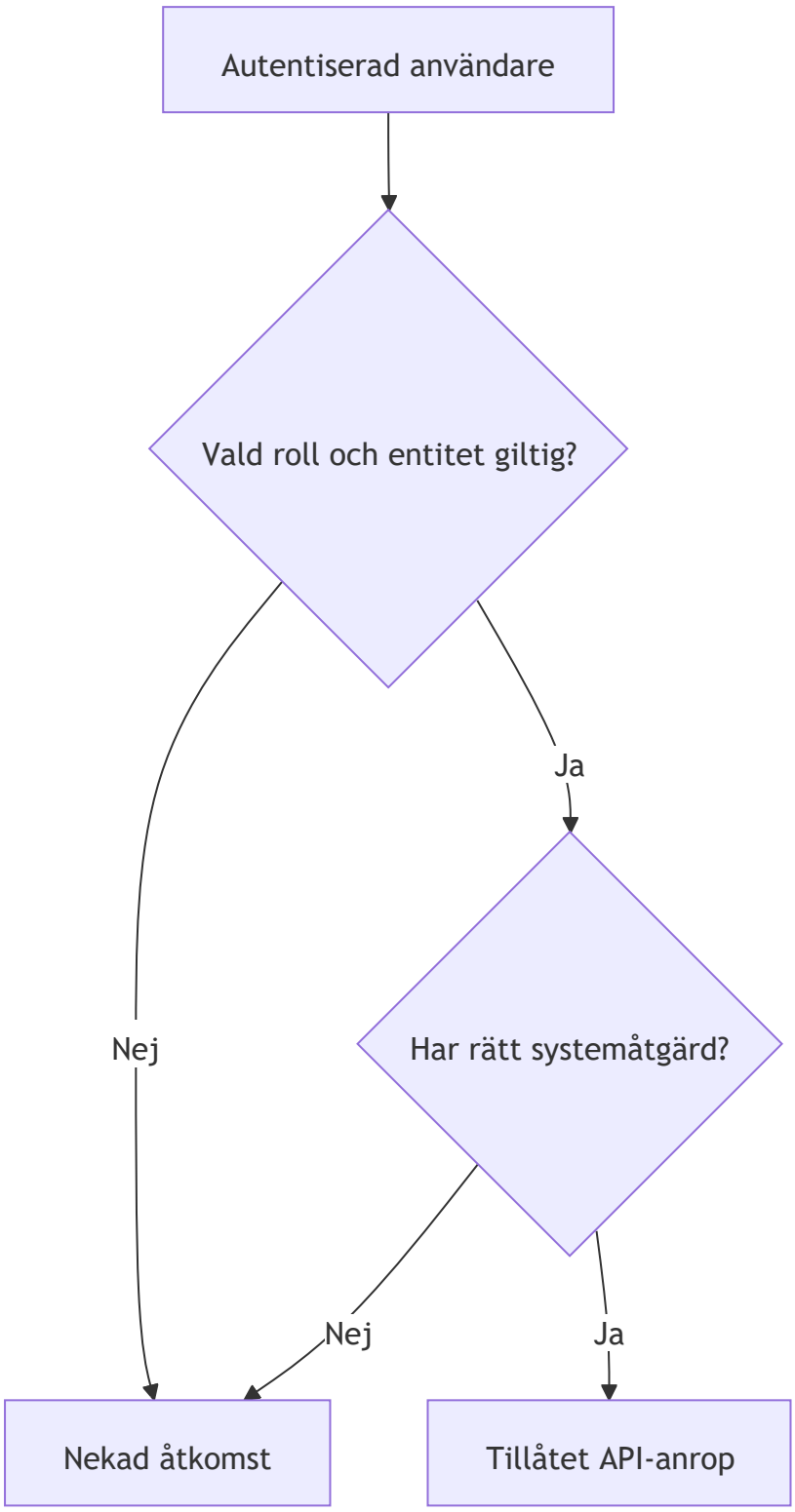
- användare kan växla mellan behöriga arbetskontexter beroende på uppdrag, åtkomst till
- funktioner prövas per API-anrop mot aktuella åtkomstregler, samma användare kan ha
- olika tillgång till data beroende på vald roll och entitet.

Detta minskar risken för otillåten horisontell åtkomst mellan förvaltningar eller verksamheter, eftersom åtkomst inte är generell utan kontextberoende.

4.3 Dataskyddsnytta

Ur dataskyddsperspektiv stödjer modellen följande principer:

- **Behovsstyrd åtkomst:** åtkomst ges utifrån roll och arbetsuppgift.
- **Minimerad exponering:** användare ser i första hand data inom vald kontext.
- **Kontrollerbarhet:** beslut om åtkomst kan följas upp via loggning och behörighetsregler.



5. Separation mellan förvaltningar och kommuner

5.1 Övergripande separationsmodell

Separation mellan förvaltningar och kommuner i PRIIS bygger i huvudsak på **logisk separering** i applikations- och behörighetslagret, inte på separata databaser per organisation.

5.2 Databasarkitektur och konsekvens

PRIIS använder en gemensam databas för berörda organisationer. Detta innebär: data för flera

- förvaltningar/kommuner lagras i samma databasmiljö, separering uppnås genom
- åtkomstregler, kontextval och behörighetskontroller, det finns inte en fysisk
- databasseparation per förvaltning/kommun i nuläget.

Ur dataskyddsperspektiv medför detta att korrekt och konsekvent tillämpning av behörighetsstyrning är en central skyddsåtgärd.

5.3 Tekniska kontrollpunkter för logisk separation (verifierad)

Följande kontrollpunkter används för att upprätthålla separation i den gemensamma databasen:

- **Roll- och åtgärdsstyrning:** åtkomst till funktioner och data prövas mot systemåtgärder och rollbaserade regler.
- **Arbetskontext per anrop:** vald rolltyp och entitet (t.ex. förvaltning/verksamhet) används som aktiv kontext.
- **Validering av kontext:** ogiltig eller otillåten kontext nekas.
- **Predikatstyrd dataåtkomst:** rollregler avgränsar vilka objekt användaren kan läsa och hantera.
- **Ytterligare skydd för skyddade uppgifter:** särskilda filter tillämpas för data med högre skyddsnivå.

Denna modell begränsar horisontell åtkomst mellan organisationer när reglerna tillämpas korrekt.

5.4 Tokenbaserade flöden och separation

I vissa externa flöden används engångslänkar (token) i stället för inloggad session. Även här finns separerande mekanismer genom att token är kopplad till specifik mottagare och specifikt ärende-/avtalssammanhang samt har giltighets- och konsumtionskontroller.

6. Loggning och spårbarhet

PRIIS har två centrala spårbarhetsnivåer:

1. **Ändringsspår för data**
   Uppdateringar av data spåras med metadata för skapad/ändrad av. Datamodellen innehåller dessutom stöd för historik på tabellnivå.

2. **Applikations- och API-loggning**
   API-anrop loggas med kontext, inklusive användaridentitet där tillgängligt.

Känd retention i nuläget:

- Loggar för applikations- och API-händelser sparas i cirka sex månader.
- Dessa loggar lagras på intern loggserver.

6.1 Vad loggning används till

Loggning och spårbarhet används för att:

- kunna utreda vem som gjort en förändring och när den utfördes, följa
- upp åtkomst och användning av API:er, stödja incidentutredning och
- intern kontroll, ge underlag för revision och verksamhetsuppföljning.

6.2 Spårbarhet vid datauppdateringar

Vid uppdatering av dataobjekt sparas metadata som möjliggör historisk uppföljning. Detta omfattar både förändringshändelser i applikationslagret och historikstöd i datalager där tillämpligt.

6.3 Spårbarhet vid tjänsteanrop (API)

Loggning av tjänsteanrop (API) innehåller anropskontext och användarrelaterad information där sådan finns tillgänglig i sessionen. Detta gör det möjligt att följa händelsekedjor från inloggning, till anrop, till förändring i data.

För tokenbaserade flöden (exempelvis svar på matchningsförfrågan via länk) skiljer sig spårbarhetsbilden från ordinarie inloggade flöden:

- anrop kan ske anonymt med token som autentiseringsbärare, användaridentitet i logg är därför
- inte alltid tillgänglig via ordinarie inloggningskontext, spårbarheten är i hög grad beroende av hur
- tokenkopplad data kan följas i datalagret.

6.3.1 Nuläge för engångslänkar (MatchingInquiryToken) Nulägesanalysen visar att

token används för att:

- läsa matchningsförfrågan, läsa kommentarer, lämna svar och
- konsumera token (engångsanvändning).
- Det finns datamodellstöd för spårbarhet i form av kopplingar till urval, kontrakt, mottagare, giltighetstid och konsumtionstid. Samtidigt är applikationsloggningen i detta flöde inte fullt ut utbyggd för detaljerad händelsespårning per tokenhändelse.

6.3.2 Identifierad förbättringspunkt

Följande punkt är identifierad som möjlig förbättring vid behov:

- mer detaljerad och konsekvent loggning för tokenflödet (valideringsutfall, konsumtion och avvisade försök),
- tydlig strategi för att kunna korrelera tokenhändelser i logg utan att exponera känsliga tokenvärden,
- tydligare uppföljning av skillnaden mellan anonym tokenåtkomst och inloggad användaråtkomst.

Detta är i nuläget dokumenterat som ett förbättringsområde och inte en genomförd förändring i kod.

6.4 Dataskyddsnytta

Kombinationen av ändringsspår och API-loggning ger ett viktigt skydd mot obemärkt felaktig hantering, eftersom avvikelser kan identifieras, analyseras och följas upp över tid.

6.5 Dataklassning av applikations- och API-loggar (övergripande)

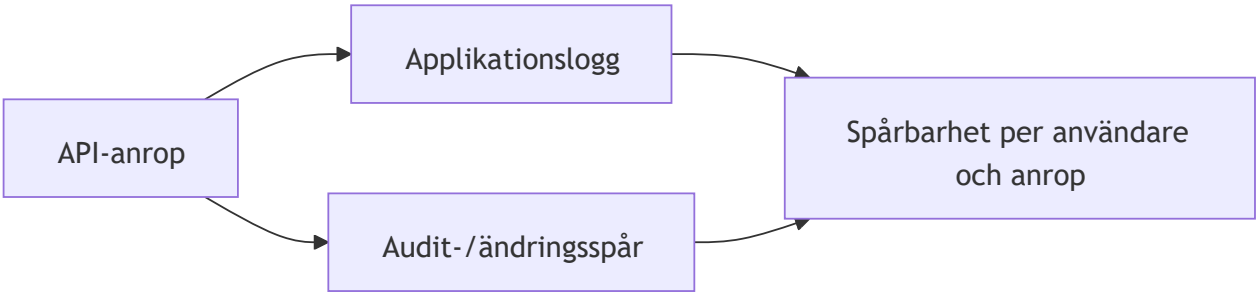
Baserat på nuvarande loggupplägg bör applikations- och API-loggar behandlas som information som kan innehålla personuppgifter och åtkomstrelaterade metadata.

Övergripande klassning i detta dokument:

- **Identifierande uppgifter:** kan förekomma, exempelvis användaridentifierare i anropskontext.
  Teknisk spårbarhetsdata: förekommer, exempelvis endpoint, tidpunkt och fel-/händelsenivå.
- **Anropsrelaterade parametrar:** kan förekomma i loggkontext och behöver hanteras med försiktighet.

Detta innebär att loggar på intern loggserver bör hanteras med samma dataskyddsperspektiv som annan spårbarhetsinformation: behovsstyrd åtkomst, tydlig ansvarsfördelning, och uppföljning av vilka som har åtkomst till loggdata.

Åtkomst till intern logginfrastruktur sker behovsstyrt och skyddas med VPN samt MFA.



7. Vilket data behandlas i vilket steg

Nedan beskrivs databehandling på övergripande nivå.

Steg 1: Inloggning och identitet

- Identitetsuppgifter från lokal/federerad inloggning
- Nödvändiga attribut för kontoidentifiering och behörighetsmappning

Steg 2: Behörighet och kontextval

- Rollinformation
- Entitetskoppling (kommun/förvaltning/verksamhetskontext)

Steg 3: Operativ handläggning i systemet

- Ärende- och verksamhetsdata
- Avtals- och leverantörsrelaterad information
- Händelsedata kopplat till uppdateringar och statusförändringar

Steg 4: Kommunikation

- E-post för notifieringar och vissa säkerhetsflöden
- SMS för vissa notifierings- och säkerhetsflöden

Steg 5: Uppföljning och spårbarhet

- API-loggar
- Ändringsloggar/auditdata

8. Externa parter och datautbyte

Avsnitt 2 beskriver den interna systemarkitekturen. Detta avsnitt fokuserar endast på externa parter och vilket datautbyte som sker på övergripande nivå.

Följande externa parter och tjänster ingår:

- **OIDC/Entra och federerade identitetsleverantörer:** används för identitetskontroll vid federerad inloggning.
- **Extern e-postdistribution via intern SMTP-kedja:** används för utskick av meddelanden, notifieringar och säkerhetsrelaterad kommunikation.
- **Generic (SMS-leverantör):** används för SMS-utskick, inklusive vissa säkerhetsflöden.
- **Nominatim/OpenStreetMap:** används för geokodning av adressdata.

Datautbytet med externa parter omfattar främst:

- identitets- och inloggningsrelaterade uppgifter, kontakt- och
- distributionsuppgifter för meddelanden, adressrelaterade
- uppgifter för geografisk positionering.

9. Servermiljö

Nuvarande tekniska underlag visar containeriserad drift och CI/CD-baserad leverans.

På övergripande nivå gäller följande:

- Servermiljön är uppdelad mellan test- och produktionsnära miljöer.
- Åtkomst till interna driftresurser (inklusive loggning och containerdrift) skyddas med VPN och MFA.
  Patchning sker enligt fastställd månatlig rutin med fördröjning mellan test och produktion.
- Säkerhetskopiering sker i flera nivåer (virtuella maskiner, filer och databaser).
  Övervakning och larmhantering är etablerad för resurser och tjänster.
- Nätverkssegmentering används för att begränsa åtkomst och minska spridningsrisk.
-

- **9.1 Patchning (processnivå)**
- Driftmiljön patchas i separata grupper för test respektive produktion.
- Testmiljö patchas först, följt av produktionsmiljö efter verifieringsperiod.
- Upplägget används för att minska driftrisk vid säkerhets- och systemuppdateringar.

9.2 Säkerhetskopiering och återställbarhet (processnivå)

- Backupstrategin omfattar flera nivåer: VM-baserad backup, filbackup och databasbackup.
  Dataskyddet omfattar både lokala och separata lagringsmål (off-site) för återställningsförmåga.
- Databaser säkerhetskopieras med stöd för transaktionssäker återställning (point-intime).
  Upplägget är utformat för att stödja verksamhetens mål för återställningstid (RTO) och acceptabel
- dataförlust (RPO).

- **9.3 Övervakning och larm (processnivå)**
- Övervakning omfattar både resursnivå (exempelvis CPU, minne och disk) och tjänstenivå.
  Larmnivåer används för att prioritera och hantera incidenter.
- Larm som skickas som aktiv notifiering ska ha dokumenterad åtgärd och ansvarig hantering.
-

9.4 Nätverk och åtkomstskydd

- Nätverkssegmentering används för att isolera system och begränsa åtkomst till känsliga resurser.
  Databasen är placerad i internt nät och är inte direkt exponerad externt.
- Kommunikation till PRIIS sker via HTTPS, och intern åtkomst till driftresurser kräver VPN + MFA.
-

10. Gallringstider

10.1 Verifierat i teknik (nuläge)

Det finns stöd i systemet för radering och livscykelhantering av dataobjekt, men fullständig och enhetlig automatisk gallring för samtliga datakategorier är inte slutligt implementerad som produktionsverifierad helhet.

10.2 Beslutsunderlag för gallring (preliminärt)

Följande tider används som preliminärt beslutsunderlag i arbetet med gallring och arkivering:

- Matchningsärenden med status avslutat/avbrutet: gallring tre år efter senaste uppdatering
  Leverantörer, verksamheter, avtal och avtalsmallar med avslutad status: gallring tidigast tre år efter
- senaste uppdatering
  Ändringslogg: årlig rapportering för bevarande, gallring från PRIIS tidigast efter tre år Användare:
- gallring tidigast efter tre års inaktivitet, under förutsättning att kopplingar inte kvarstår
-

Dessa punkter ska betraktas som verksamhets- och förvaltningsunderlag tills implementation, förvaltning och drift har bekräftat full tillämpning i produktion.

11. Sammanfattning av skyddsåtgärder

- • Tvåfaktor/flerfaktor i lokala inloggningsflöden när kontokonfiguration kräver detta Federerad inloggning via extern identitetsleverantör med krav på 2FA/MFA i identitetsleverantörens policy
- Kontolåsning vid upprepade misslyckade inloggningar
- Anropsbegränsning för att minska missbruk av känsliga anrop
- Policy- och rollbaserad behörighetsstyrning
- Kontextstyrd access per rolltyp och entitet
- Loggning av API-anrop med användarkontext
- Spårbarhet av datauppdateringar via ändringsmetadata och historik