Teknisk spesifikasjon for SASene (v1.0)

Grensesnitt for innrapportering av individdata for grunnskolen

Denne spesifikasjonen beskriver hvilke individopplysninger skoleeier skal sende til Utdanningsdirektoratet (Udir) gjennom API-et for grunnskolen. Innsendingen omfatter opplysninger om elevens identifikasjon, skoletilhørighet, skoleperiode, trinn og klasse, fravær og eventuell plass i skolefritidsordningen (SFO), inkludert avtalt oppholdstid og foreldrebetaling.

Les mer på Udirs informasjonsside om innrapportering av individdata.

Generell informasjon

- Data overføres som JSON via API. Feltnavnene i dokumentet tilsvarer feltnavnene i API-et.
- Kolonnen "Påkrevd" angir om feltet er obligatorisk. J betyr obligatorisk, N betyr valgfritt, og J* betyr obligatorisk når vilkåret i kommentarfeltet er oppfylt.
- Teknisk API-dokumentasjon for QA-miljøet: Swagger Individdata
- SasDataDto beskriver hele innsendingen. Feltet individualData inneholder en liste med elevopplysninger, der hver element i listen følger strukturen IndividualDataDto.

Data som sendes til Udir ved innrapportering av individdata for grunnskolen

For hvert skoleår skal innsendingen omfatte **alle elever som har vært aktive ved en skole i løpet av skoleåret**, også elever som har sluttet eller byttet skole før rapporteringstidspunktet.

Innsendingen skal omfatte kun **primære skoleforhold / hoved skole.**

SasDataDto

SasDataDto beskriver hele innsendingen fra skoleeier til Udir.

#	Feltnavn	Datatype	Obl.	Kommentar
1	submitterName	string	Ja	Navn på skoleeier som rapporterer dataene.
2	submitterEmails	array<string>	Ja	E-postadresse(r) som skal motta resultatet av innsendingen.
3	individualData	array<IndividualDataDto>	Ja	Liste over elevoppføringer. Hver oppføring følger IndividualDataDto. En elev kan forekomme flere ganger dersom periodene ikke overlapper.

IndividualDataDto

IndividualDataDto beskriver én elevoppføring med opplysninger om skolegang, fravær og SFO.

#	Feltnavn	Datatype	Obl.	Kommentar
1	externalId	string	Ja	Elevens unike identifikator i skoleadministrativt system (SAS). Identifikatoren skal ikke være elevens fødselsnummer eller D-nummer og skal heller ikke inneholde navn[1]. Det bør være en intern referanse som kan brukes av skoleeiere for å slå opp eleven i SAS og håndtere feil i innrapportert data.
2	personNin	string	J	Elevens fødselsnummer eller D-nummer.
3	grade	integer	J	Elevens trinn, for eksempel 1, 5 eller 10.

4	class	string	J	Navn eller kode på klassen eleven tilhører, for eksempel 10A eller 1C. Verdien forkortes til de første fire tegnene ved mottak.[2]
5	startDate	date-time	J	Dato eleven startet ved skolen. Eksempel av 'date-time' format er *'2026-07-21T17:32:28Z'*
6	endDate	date-time / null	N	Dato eleven sluttet ved skolen. Skal være null dersom eleven fortsatt er elev.
7	organisationNumber	string	J	Organisasjonsnummeret til skolen eleven går eller gikk på.
8	totalAbsenceDays	integer	J	Totalt antall hele fraværsdager i inneværende skoleår.
9	totalAbsenceMinutes	integer	J	Totalt antall fraværminutter i inneværende skoleår.
10	hasSfo	boolean	J	Angir om eleven har plass i SFO.
11	agreedStayDurationSfo	integer	N	Antall timer eleven etter avtalen har plass i SFO i en ordinær uke. Oppgi avtalt oppholdstid, ikke faktisk tilstedeværelse eller SFO-ordningens åpningstid.[3]
12	hasReducedPaymentSfo	boolean	J*	Angir om eleven omfattes av inntektsbasert redusert foreldrebetaling. Feltet er obligatorisk og kan ikke være tomt når hasSfo er true.
13	amountPaidSfo	decimal	J*	Faktisk beløp som foresatte betaler per måned for elevens SFO-plass etter eventuelle moderasjoner. Feltet er obligatorisk og kan ikke være tomt når hasSfo er true. Verdien 0 skal brukes dersom foresatte ikke betaler for plassen. For skoleåret 2026-2027 er dette feltet valgfritt.

1. Dette begrenser unødvendig spredning av fødselsnummer og følger prinsippet om dataminimering i personvernforordningen artikkel 5 nr. 1 bokstav c. Etter personopplysningsloven § 12 kan fødselsnummer bare brukes når det er saklig behov for sikker identifisering og bruken er nødvendig. Siden feltet personNin allerede ivaretar sikker personidentifikasjon i innsendingen, skal fødselsnummer ikke gjenbrukes som externalId.
2. Begrensningen reduserer risikoen for at fritekstfeltet overfører personnavn eller andre unødvendige personopplysninger, ettersom enkelte skoler bruker navn på elever eller lærere i klassenavn. Systemleverandører bør legge til rette for korte, nøytrale klassekoder, og skoleeiere bør unngå personnavn i klassenavn.
3. Dersom kommunen organiserer plassen over en lengre periode, for eksempel fire uker, skal timetallet omregnes til gjennomsnitt per uke.

Svar fra Udir

ImportResponseDto

#	Feltnavn	Datatype	Obl.	Kommentar
1	referenceId	string	J	Referanse-ID som returneres for mottatt innsendingen.

ProblemDetails

ProblemDetails beskriver strukturen på feilsvar fra API-et.

#	Feltnavn	Datatype	Obl.	Kommentar
1	type	string / null	N	Type feil.
2	title	string / null	N	Kort beskrivelse av feilen.
3	status	integer / null	N	HTTP-statuskode.
4	detail	string / null	N	Detaljert beskrivelse av feilen.
5	instance	string / null	N	Referanse til den aktuelle forekomsten av feilen.

Tilgang til individata API via Maskinporten – guide for API-konsumenter

Denne guiden er for kommuner og systemleverandører som skal kalle Udirs API maskin-til-maskin. Systemleverandøren kaller API-et på vegne av kommunen. Maskinporten sjekker at kommunen har delegert tilgangen til leverandøren. API-et støtter ikke Altinn systembruker. Tilgang gis kun gjennom **API-delegering i Altinn**: kommunen delegerer tilgang til API-et til leverandørens organisasjonsnummer.

Rollene

Rolle	Ansvar
Udir (API-tilbyder)	Eier scopet udir:individdata/skole.write og gir kommunen tilgang til det
Kommunen (konsument)	Delegerer tilgangen videre til systemleverandøren i Altinn
Systemleverandøren	Har klienten i Maskinporten, henter token og kaller API-et

---

Del 1 – Forutsetninger (kommunen)

Steg 1: Kommunen må ha tilgang til scopet

Udir må ha gitt kommunens organisasjonsnummer tilgang til scopet udir:individdata/skole.write i Maskinporten. Uten dette kan ikke kommunen delegere noe videre. Ta kontakt med Udir hvis kommunen ikke har fått tilgang.

Steg 2: Kommunen delegerer ressursen til systemleverandøren i Altinn

En person i kommunen med riktig rettighet i Altinn delegerer API-ressursen til leverandørens organisasjonsnummer (API-delegering). Delegeringen gjøres én gang per kommune og leverandør. Når leverandøren ber om token, sjekker Maskinporten denne delegeringen mot Altinn.

Del 2 – Sett opp klient i Maskinporten (systemleverandøren)

Steg 3: Opprett en klient

Opprett en ny klient i Maskinporten (via Samarbeidsportalen eller selvbetjenings-API-et) med disse innstillingene:

Innstilling	Verdi
Scope	udir:inviddata/skole.write
Applikasjonstype	web
Autentiseringsmetode	private_key_jwt (aktivert)
Tillatt grant type	urn:ietf:params:oauth:grant-type:jwt-bearer

Noter **client_id** som klienten får. Den brukes som iss senere.

Steg 4: Lag et RSA-nøkkelpar

Generer et RSA-nøkkelpar (minst 2048 bit). Nøkkelparet består av:

- **Privat nøkkel**: brukes til å signere forespørsler. Den forlater aldri systemet deres og må lagres sikkert, for eksempel i et nøkkelhvelv.
- **Offentlig nøkkel**: lastes opp til Maskinporten.

Ved signering bruker dere én av algoritmene RS256, RS384 eller RS512, som Maskinporten støtter.

Steg 5: Last opp offentlig nøkkel og noter kid

Last opp den offentlige nøkkelen på klienten. Samtidig genereres en **kid** (key ID). Noter den. Den skal med i hver forespørsel, slik at Maskinporten vet hvilken nøkkel signaturen skal sjekkes mot.

> **Om virksomhetssertifikat:** Det går fortsatt an å bruke virksomhetssertifikat i stedet for egen nøkkel. Da sendes sertifikatkjeden i header-feltet x5c i stedet for kid. Dette er på vei bort, så vi anbefaler egen nøkkel med kid.

Del 3 – Hent token og kall API-et

For å få et access token lager dere en kort, signert melding (en *JWT grant*). Den sendes til Maskinporten, som svarer med et token. Grant-en består av tre deler: **header**, **payload** og **signatur**.

Steg 6: Lag header

Headeren sier hvordan meldingen er signert og med hvilken nøkkel.

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "<kid fra steg 5>"
}
```

Felt	Betydning
alg	Signeringsalgoritmen. Må stemme med hashen dere signerer med (RS256 betyr SHA-256)
typ	Typen melding: alltid JWT
kid	Nøkkel-ID-en fra steg 5

Steg 7: Lag payload

Payloaden sier hvem dere er, hva dere ber om og på vegne av hvem.

```
{
  "aud": "https://test.maskinporten.no/",
  "iss": "<client_id fra steg 3>",
  "scope": "udir:individdata/skole.write",
  "iat": 1760360000,
  "exp": 1760360120,
  "jti": "3f1c9a2e-7b4d-4e8a-9c1f-2d6b8e0a5f71",
  "consumer_org": "<kommunens organisasjonsnummer>"
}
```

Felt	Påkrevd	Betydning
aud	Ja	Hvem meldingen er til, altså Maskinporten. Test: https://test.maskinporten.no/. Produksjon: https://maskinporten.no/. Den avsluttende skråstreken må være med
iss	Ja	Klientens client_id
scope	Ja	Tilgangen dere ber om: udir:individdata/skole.write

iat	Ja	Når meldingen ble laget, i sekunder siden 1.1.1970 (UTC). Maskinporten avviser grants der iat avviker mer enn 10 sekunder fra deres klokke, så serverklokka må være synkronisert
exp	Ja	Når meldingen utløper. Maks 180 sekunder etter iat, og 120 sekunder anbefales
jti	Anbefalt	En unik ID (GUID) per melding. En grant kan ikke gjenbrukes
consumer_org	Ja, når leverandør kaller på vegne av kommune	Organisasjonsnummeret til **kommunen dataene gjelder**. Udirs API bruker denne verdien (via token) til å avgjøre hvilken kommune innsendingen tilhører. Se viktig merknad under.

Ikke legg inn andre felter enn disse. Ukjente claims gir 400 Bad request med «Invalid assertion».

Viktig: Riktig kommune i consumer_org

Udirs API bruker kommunen som står i tokenet til å bestemme hvilken kommune en innsending gjelder. Kommunen i tokenet kommer fra consumer_org. Maskinporten sjekker bare at kommunen har delegert tilgang til dere. Maskinporten sjekker **ikke** at dataene dere sender faktisk tilhører den kommunen.

Dette betyr at hvis dere er leverandør for flere kommuner, og setter en annen kommunes organisasjonsnummer i consumer_org enn kommunen dataene gjelder:

- **overskrives den andre kommunens innsending** med feil data, og
- **kommunen dere egentlig sendte for får ingen innsending.**

Feilen gir ingen feilmelding, verken fra Maskinporten eller fra API-et, fordi dere har gyldig delegering fra begge kommunene.

Dere må derfor sørge for at:

- consumer_org alltid hentes fra den samme kommunen som dataene i innsendingen tilhører
- tokens aldri gjenbrukes på tvers av kommuner. Hvis dere mellomlagrer tokens, må nøkkelen være kommunens organisasjonsnummer
- logikken som kobler kommune og token er testet med flere kommuner

Steg 8: Signer meldingen med den private nøkkelen

1. Gjør headeren om til JSON-tekst, kod den som UTF-8 og deretter som **Base64URL**. Base64URL er Base64 uten = på slutten, med - i stedet for + og _ i stedet for /.
2. Gjør det samme med payloaden.
3. Sett de to sammen med punktum: <header>.<payload>. Dette er teksten som signeres.
4. Signer UTF-8-bytene i denne teksten med den private nøkkelen. Bruk RSA med PKCS#1 v1.5-padding og hashen som hører til alg. For RS256 er det SHA-256.
5. Base64URL-kod signaturen.
6. Sett alt sammen: <header>.<payload>.<signatur>

Resultatet er én lang tekststreng med to punktum, for eksempel:

eyJhbGciOiJSUzI1NiIs... . eyJhdWQiOiJodHRwczov... . kR8x0vQ2mN...

Maskinporten bruker den offentlige nøkkelen (funnet via kid) til å sjekke at signaturen stemmer. Det beviser at meldingen kommer fra dere og ikke er endret underveis.

> **Tips:** Bruk et etablert JWT-bibliotek for språket deres i stedet for å bygge signeringen selv. Det gjør steg 1–6 for dere.

Steg 9: Send grant-en til Maskinporten

Send en **POST** til Maskinportens token-endepunkt:

Miljø	Token-endepunkt
Test	https://test.maskinporten.no/token
Produksjon	https://maskinporten.no/token

Endepunktet kan også slås opp automatisk via /.well-known/oauth-authorization-server på samme adresse.

Forespørselen sendes som skjemadata (Content-Type: application/x-www-form-urlencoded) med to felter:

Felt	Verdi
grant_type	urn:ietf:params:oauth:grant-type:jwt-bearer
assertion	Den signerte strengen fra steg 8

Ved suksess svarer Maskinporten med (eksempel):

```
{
  "access_token": "eyJraWQiOiJ...",
  "token_type": "Bearer",
  "expires_in": 120,
  "scope": "udir:individdata/skole.write"
}
```

Inne i access tokenet står det både hvem som kaller (leverandøren) og hvem det gjelder (kommunen):

```
{
  "scope": "udir:individdata/skole.write",
  "consumer": { "authority": "iso6523-actorid-upis", "ID": "0192:<kommunens orgnr>" },
  "supplier": { "authority": "iso6523-actorid-upis", "ID": "0192:<leverandørens orgnr>" }
}
```

Steg 10: Kall API-et

Send tokenet i `Authorization`-headeren på hvert kall:

```
Authorization: Bearer <access_token>
```

Gjenbruk tokenet til det nærmer seg `expires_in`. Hent deretter et nytt med en **ny** grant: nytt `iat`, nytt `exp` og ny `jti`. Hver kommune skal ha sitt eget token. Et token hentet for én kommune må aldri brukes til å sende inn data for en annen kommune (se merknaden i steg 7).

API-dokumentasjon (Swagger)

Udirs API er dokumentert i Swagger. Der finner dere endepunkt, påkrevde felter, datatyper og eksempler på forespørsler og svar.

Miljø	Swagger-URL
Test	https://qa-individdata.udir.no/api/sas/swagger
Produksjon	https://individdata.udir.no/api/sas/swagger

Bruk Swagger som fasit for hvordan innsendingen skal se ut. Kall mot API-et krever et gyldig Maskinporten-token som beskrevet i steg 6–10.

Feilmeldinger fra API-et

HTTP-kode	Melding	Årsak	Hva dere bør sjekke
401 Unauthorized	(ingen melding)	Token mangler, er ugyldig eller har utløpt	At `Authorization: Bearer <token>` er med, at tokenet er hentet fra riktig miljø (test/prod) og ikke har utløpt. Hent nytt token og prøv igjen
403 Forbidden	(ingen melding)	Tokenet er gyldig, men gir ikke rett til å sende inn. Enten mangler scopet, eller kommunen i tokenet godtas ikke	At tokenet inneholder scopet `udir:individdata/skole.write`, og at `consumer_org` er satt til riktig kommune. Sjekk også at kommunen har tilgang til scopet og har delegert til dere (steg 1–2)
403 Forbidden	`Missing organization – "The authenticated caller has no organization number."`	Kallet er autentisert, men API-et fant ikke noe organisasjonsnummer i tokenet	At `consumer_org` er satt i grant-en, og at access tokenet inneholder `consumer` med organisasjonsnummer. Kontakt Udir hvis feilen vedvarer

> **Tips:** Et access token kan dekodes (for eksempel i et JWT-verktøy) for å se hvilket `scope` og hvilken `consumer` det faktisk inneholder. Det er ofte den raskeste måten å finne årsaken til en 403.

Vi anbefaler følgende feilmelding til brukeren for 401 + 403 feil.

> **Ditt skoleadministrativt system mangler tilganger.**
>
> Ta kontakt med systemforvalter i din virksomhet og sjekk at det er gitt riktige tilganger til ditt skoleadministrativt system.
>
> Hvis problemet vedvarer ta kontakt med leverandøren av ditt skoleadministrativt system og sjekk at systemet har riktig tilganoppsett.
>
> Hvis problemet ikke blir løst, ta kontakt med Utdanningsdirektoratet.

Feilsøking

Symptom	Sannsynlig årsak
invalid_grant / «Invalid assertion»	Feil aud (husk skråstrek), exp mer enn 180 sekunder etter iat, klokka går feil, gjenbrukt jti, eller ekstra felter i payloaden
Signaturen avvises	Feil kid, feil nøkkel, eller alg stemmer ikke med hashen som er brukt
Ingen tilgang til scopet	Kommunen har ikke fått tilgang fra Udir (steg 1), delegeringen i Altinn mangler (steg 2), eller consumer_org har feil orgnr
Fungerer i test, ikke i prod	Ulik aud, ulikt endepunkt eller ulik client_id/kid mellom miljøene
En kommunes innsending er overskrevet, eller en kommune mangler innsending	Feil organisasjonsnummer i consumer_org, eller et token for én kommune er brukt til en annen kommunes data

---

Sources:

- JWT grant – Digdir Docs
- https://docs.digdir.no/docs/Maskinporten/maskinporten_guide_apikonsument.html
- https://samarbeid.digdir.no/
- https://docs.digdir.no/docs/idporten/oidc/oidc_api_admin_maskinporten