Systembeskrivelse: SkrittLotto

Fra Aktivitet til Trekning

Versjon 2.0 · Basert på App v1.6.2 / Web v5.9.10
Sist oppdatert: 10. januar 2026

skrittlotto.no · thomas@skrittlotto.no

Innhold

1. Introduksjon

Dette dokumentet beskriver den tekniske logikken, sikkerhetsarkitekturen og dataflyten i SkrittLotto-piloten.

Systemet er bygget etter prinsippet om **«Privacy by Design»**, der brukernes personvern ivaretas samtidig som integriteten til en loddtrekning sikres.

Hva er SkrittLotto?

SkrittLotto er et digitalt folkehelsetiltak som belønner daglig fysisk aktivitet med lodd til ukentlige premier. Konseptet er enkelt:

- **Gå 5 000 skritt** = få **ett lodd** til ukens trekning
- **Maksimalt 7 lodd per uke** (ett per dag)
- **Ingen pengeinnsats** – innsatsen er kun fysisk aktivitet

2. Installasjon og Unik Identitet

Når appen installeres, genererer systemet automatisk to unike identifikatorer som lagres i telefonens lukkede lagringsområde (DataStore):

Identifikator	Format	Beskrivelse
Spiller-ID (Offentlig)	`SL-XXXXXXXX`	En unik kode med 8 heksadesimale tegn som fungerer som brukerens anonyme lottokupong-nummer. Brukes ved annonsering av vinnere.
Sikkerhetskode (Privat)	UUID (36 tegn)	En hemmelig nøkkel som fungerer som brukerens «vinnerbevis». Lagres kun lokalt på enheten.

Gjenoppretting (Pilot-modus)

Appen har en funksjon for å gjenopprette profil via sikkerhetskoden. I denne pilotversjonen er gjenopprettingen **simulert i frontend**:

- Systemet validerer at koden er nøyaktig 36 tegn
- Gir en visuell bekreftelse til brukeren
- Overskriver **ikke** faktiske lokale data for å beskytte test-data

---

3. Aktivitet og Loddgenerering

Appen henter skrittdata fra **Health Connect** eller telefonens innebygde skritteller.

Parameter	Verdi
Dagsmål	5 000 skritt
Konvertering	5 000 skritt = 1 lodd
Maks per dag	1 lodd
Maks per uke	7 lodd
Lokal lagring	365 dager før automatisk sletting

Loddopptjening

```
Dag 1: 6 200 skritt → 1 lodd ✓
Dag 2: 3 100 skritt → 0 lodd ✗
Dag 3: 8 500 skritt → 1 lodd ✓
...
Uke totalt: 5 lodd
```

---

4. Innsendingslogikk og Smart-sjekk

Deltakelse i trekningen krever aktiv «levering» av lodd via en ukesrapport. Handlingen styres av **SubmissionStatus**:

Mekanisme	Beskrivelse
6-timers cooldown	Brukeren kan som hovedregel oppdatere sin innsending hver 6. time.

Mekanisme	Beskrivelse
Dynamisk Reset	Cooldown-perioden nullstilles umiddelbart i det øyeblikket brukeren opptjener et helt nytt lodd.
Smart-sjekk (UP_TO_DATE)	Systemet blokkerer innsending dersom det ikke har skjedd endringer siden forrige vellykkede levering.
Tidsfrist	Innsending er stengt fra søndag kl. 18:00 til mandag kl. 08:00.

5. Sikkerhet og Personvern

5.1 Autentisering

Android-appen bruker **Firebase Anonymous Authentication** for enkel brukeridentifikasjon:

- Ingen e-post eller passord kreves
- Systemet genererer automatisk en unik `firebaseUserId`
- Denne ID-en brukes for å knytte innsendinger til riktig bruker

> **Merknad:** Nettsiden bruker e-post-basert innlogging (Magic Link) for kontrollert pilotering. Kun inviterte brukere får tilgang til administrative funksjoner.

5.2 Master Switch (Kommune)

Brukeren har granulær kontroll over deling, men systemet har innebygde personvern-låser:

- Deling av kommune er teknisk låst til `"Privat"` dersom den globale bryteren for statistikk-deling er slått **AV**
- Brukeren kan når som helst endre sine personverninnstillinger

5.3 SHA-256 Signatur

Appen sender **aldri** sikkerhetskoden i klartekst:

1. Sikkerhetskoden hashes lokalt med SHA-256
2. Kun hashen (`securitySignature`) sendes til backend
3. Ved verifisering sammenlignes hasher – aldri råkoder

5.4 Kvittering

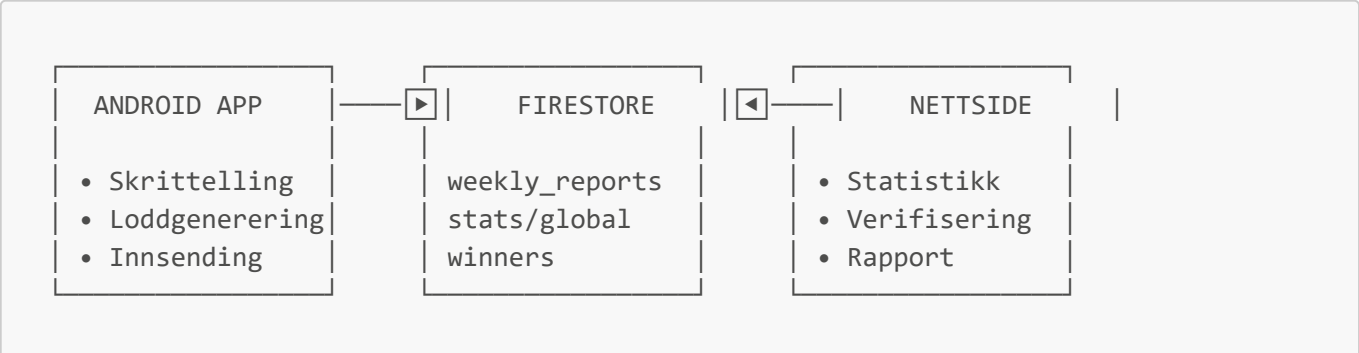
Hver innsending får et unikt kvitteringsnummer (`receiptId`) for sporbarhet, f.eks. `#L-101744`.

---

6. Backend og Dataflyt

6.1 Firebase Firestore

Systemet bruker **Firebase Firestore** som backend-database. All kommunikasjon mellom app og backend går via Firestore.



6.2 Datastruktur: `weekly_reports`

Ved innsending genereres en **WeeklyReport** med følgende felter:

Felt	Type	Beskrivelse
`playerId`	String	Spiller-ID (f.eks. `SL-444F308F`)
`firebaseUserId`	String	Anonym Firebase-bruker-ID
`receiptId`	String	Kvitteringsnummer (f.eks. `#L-101744`)
`securitySignature`	String	SHA-256 hash av sikkerhetskoden
`userName`	String	Valgfritt brukernavn
`municipality`	String	Kommune eller `"Privat"`
`totalTickets`	Long	Antall lodd (0-7)
`dailySteps`	Map<String, Long>	Daglige skritt (f.eks. `{"2026-01-06": 5200}`)
`timestamp`	Long	Unix timestamp (millisekunder)
`weekNumber`	Long	ISO ukenummer
`year`	Long	År

6.3 Global Statistikk-aggregering

Appen oppdaterer automatisk `stats/global`-dokumentet i Firestore:

Felt	Type	Beskrivelse
`totalTickets`	Long	Totalt antall lodd fra alle brukere
`totalSteps`	Long	Totalt antall skritt fra alle brukere

Beskyttelse mot dobbelt-telling:

- Oppdatering skjer **kun ved første innsending** for hver uke
- Re-innsendinger (oppdateringer) påvirker ikke global statistikk
- Bruker `FieldValue.increment()` for atomisk, thread-safe oppdatering

> **Pilot-merknad:** I pilotfasen kan autentiserte brukere oppdatere statistikk. Ved skalering flyttes denne logikken til sikret backend-funksjon (Cloud Functions).

6.4 Firestore Security Rules

Dataene beskyttes av Firestore Security Rules:

```
rules_version = '2';
service cloud.firestore {
  match /databases/{database}/documents {

    // weekly_reports: Kun eier kan skrive/endre/slette
    match /weekly_reports/{reportId} {
```

```
      allow read: if request.auth != null;
      allow create: if request.auth != null
                    && request.resource.data.firebaseUserId == request.auth.uid;
      allow update: if request.auth != null
                    && resource.data.firebaseUserId == request.auth.uid
                    && request.resource.data.firebaseUserId == request.auth.uid;
      allow delete: if request.auth != null
                    && resource.data.firebaseUserId == request.auth.uid;
    }

    // winners: Kun lesing (admin setter via Console)
    match /winners/{document} {
      allow read: if request.auth != null;
      allow write: if false;
    }

    // stats: Offentlig lesing, autentiserte kan skrive
    match /stats/{document} {
      allow read: if true;
      allow write: if request.auth != null;
    }
  }
}
```

Nøkkelpunkter:

- `firebaseUserId` valideres ved både opprettelse og oppdatering
- Brukere kan kun lese/skrive sine egne rapporter
- Vinner-data er skrivebeskyttet (kun admin via Firebase Console)

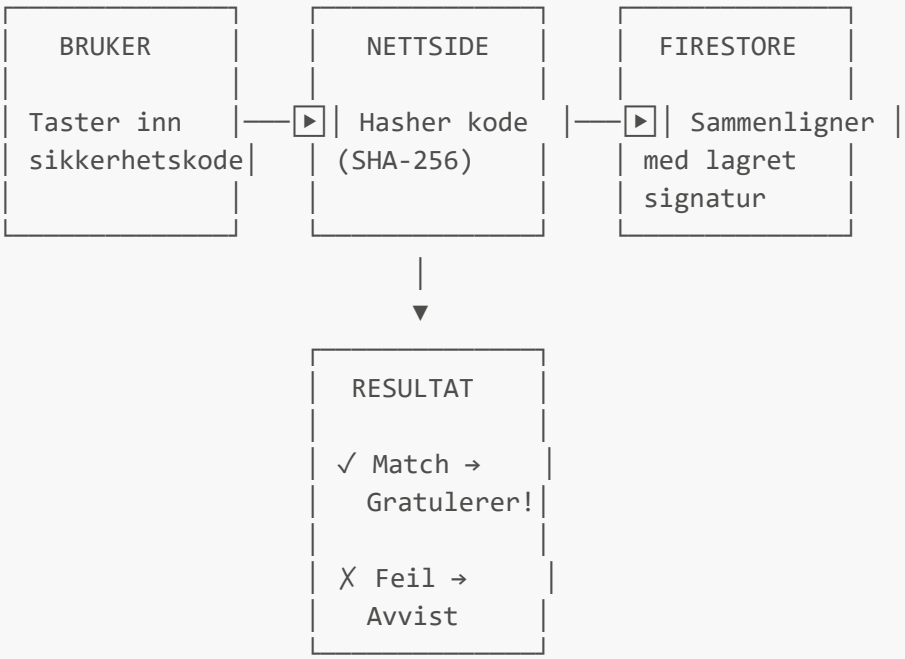
7. Trekning og Verifisering

7.1 Trekningsprosess

1. Admin velger tilfeldig `receiptId` fra `weekly_reports`
2. Vinner-lodd annonseres på nettsiden med Spiller-ID

7.2 Verifiseringsflyt

Når en vinner annonseres, kreves gevinsten ved å vise frem sikkerhetskoden:



7.3 Sikkerhetslag

Lag	Beskrivelse
ID-match	Verifiserer at Spiller-ID stemmer med annonsert vinner
Beviskontroll	Systemet hasher inntastet sikkerhetskode og sjekker mot lagret signatur
Enhetsverifisering	Telefonen fungerer som fysisk nøkkel – sikkerhetskoden finnes kun lokalt

---

skrittlotto.no · thomas@skrittlotto.no