State Registry Data Access Notifications for Estonian eID Holders

Bachelor's Thesis Defense

Arkadi Statsenko

University of Tartu
Computer Science Curriculum

August 2025

Supervisor: Daniel Würsch, MSc

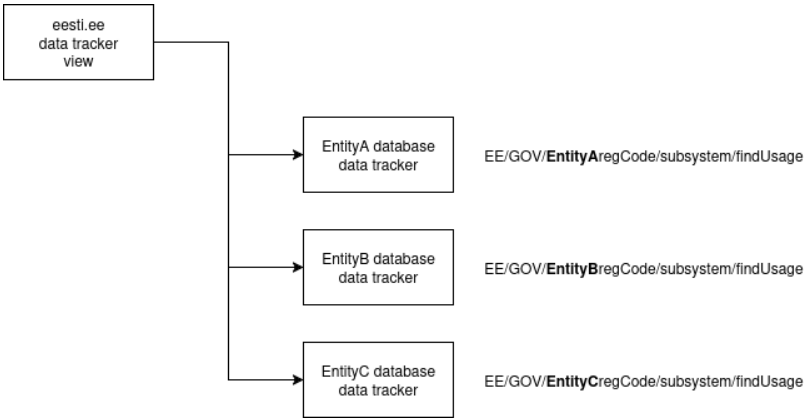
The Problem

- Estonia has numerous state databases containing personal data
  - Population Registry (*Rahvastikuregister*)
  - Health Portal (*Terviseportaal*)
  - Digital Registry (*Digiregistratuur*)
  - And many others...
- Data is accessed by various parties, including private entities.
- *Andmejälgija* (Data Tracker) exists where users can see data access logs.
- Current system requires manual checking on *eesti.ee*

Goal: Create real-time notifications for data access events

Current System: *Andmejälgija* (Data Tracker)

- Protocol created by RIA in 2017
- X-Road based distributed system
- Users access via *eesti.ee* web portal



X-Road vs Standalone Approach

X-Road Service

Advantages:

- Full API access to *Andmejälgija*
- Multiple potential notification channels
- Official integration path

Disadvantages:

- Legal entity required
- HSM hardware (~€9,000)
- Compliance obligations
- Permission (contract) needed from each data controller
- Another data controller introduced

Standalone Approach

Advantages:

- No legal entity requirements
- Open source development possible
- User maintains control

Disadvantages:

- Reverse engineering of *eesti.ee*
- Self-hosting required
- Session management complexity

Mobile App: Making Standalone Viable

How Mobile App Solves Standalone Limitations

- **Easy Setup:** One-click installation from GitHub releases
- **Built-in Notifications:** Native Android notification system
- Operates as standalone client - no reliance on third-parties.

Mobile app transforms standalone approach into a practical solution

Data Access Notifier - Architecture

- Authentication to *eesti.ee* happens through TARA, leveraging Android WebView.
- Resulting cookies are used to poll internal *eesti.ee* API
- A combination of AlarmManager and foreground services is used for consistent session extention and API polling.

Key Implementation Challenges

Session Management

- Keeping the session alive (JWT token lives 30 minutes) restriction

Background Processing

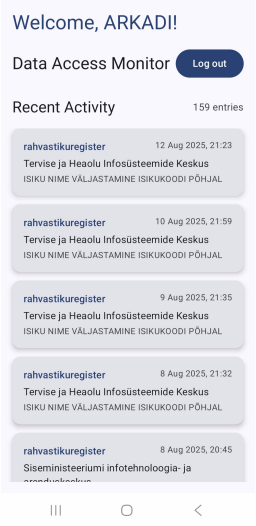
- WorkManager: Unreliable for this use case due to system-managed delays
- Foreground Services: dataSync limited to 6 hours/day on Android 15+
  - **Solution:** Hybrid AlarmManager + Foreground service approach

Data Handling

- Filter self-queries (including queries to *Andmejälgija* that also produce logs)
  - **Solution:** Filter 'receiver' by personal code.
- Deduplication
  - **Solution:** Proto Data Store + Kotlin Set data structure.

Implementation Results

- **Platform:** Android 8.1+ (96.4% coverage)
- **Language:** Kotlin
- **License:** MIT (Open Source)
- **Distribution:** GitHub Releases
- **Battery Impact:** Minimal
- **Tested Devices:**
  - Xiaomi Poco X3 Pro (CrDroid)
  - Xiaomi Redmi 7A (LineageOS)
  - Samsung Galaxy S25 (Stock)



Implementation Results

Key Observations During Testing

Delayed Log Entries

- Notifications received for events months in the past
  - May 2025 (and even February 2025) events appearing in August 2025
  - Suggests delays in logging infrastructure

Session Reliability

- AlarmManager + Foreground service approach highly reliable
  - Successful operation even during extended device inactivity
  - Maintains connectivity during network fluctuations

Current Limitations

Technical Limitations

- **12-hour session lifespan** - hard server-side limit
- Android-only implementation
- Dependence on reverse-engineered API

Coverage Limitations

- Limited to databases implementing *Andmejälgija*
  - Doesn't support E-File system

- Systematic issues

Systematic Issues

Poor Quality Descriptions

Bad Practice	Good Practice
PERSONAL DATA BY PERSONAL CODE	Prescription viewed by doctor; prescription number 1018472350
INDIVIDUAL EXTENDED INFO QUERY	Individual query for valid driver's licenses through state portal eesti.ee

Bad Practice	Good Practice
Doctor Viktor Pihlakas	INSTITUTION X
Jaan Kask 32405023456	FOUNDATION Y

Limited Coverage

- *Andmejälgija* protocol is not legally mandated
  - Even if database implements *Andmejälgija*, not everything is necessarily logged.

Conclusions

Objectives Achieved

- **Done:** Created functional mobile notification system
- **Done:** Surveyed state database *Andmejälgija* implementation
- **Done:** Identified critical gaps in data access transparency

Key Findings

- 12-hour GovSSO session limitation.
- Possible delays in logging

Future Work

- Mitigation of 12-hour session constraint
- iOS/cross-platform implementation
- Getting listed on application stores (like Google Play)

Thank You

Questions?

Data Access Notifier

GitHub: `https://github.com/ArkadSt/DataAccessNotifier`

Contact: arkadistatsenko@gmail.com

Questions So Far

- Why is Android 8.1 the minimum? Are there any libraries requiring Android 8.1 minimum?
- How long does it take to log in and view access logs in the app?
- Is it possible to forge JWT token to bypass eesti.ee API authentication checks?
- Which user's data is exactly accessed by an entity? Is it only personal identity code?
- What can users do after receiving a notification from the app?