TAIGA

USER FLOWS

User Flows

ORGANIZATION	defence
VERSION	1
DATE	April 14, 2026

Table of Contents

User Flows Overview

This document contains 7 user flows covering key user journeys.

- **Install and Configure Hälytin** — Finnish Resident: Download the Hälytin app, complete onboarding, grant required permissions, and be ready to receive air-threat alerts in under 2 minutes
- **Receive and Respond to Air-Threat Alert** — Finnish Resident: Receive a real-time air-threat alert, understand the threat and guidance, and take protective action
- **Verify and Dispatch Alert (Standard Workflow)** — Hätäkeskuslaitos Operator (Duty Officer): Verify an incoming FDF threat on the operator console, obtain four-eyes confirmation from a second operator, and dispatch the alert to all channels within 30 seconds
- **Abort or Correct Alert** — Hätäkeskuslaitos Operator (Duty Officer): Stop a dispatched alert or send a correction alert if new FDF data changes the threat classification or affected area
- **Ingest and Verify FDF Threat** — System (FDF Integration - Automated): Receive a signed threat object from FDF air surveillance, verify its cryptographic origin and data validity, and surface it to the Hätäkeskuslaitos operator console for human confirmation
- **Review Post-Incident Timeline** — Sisäministeriö Preparedness Official: Access a complete, signed audit trail of an incident from FDF detection through all-clear notification to verify system integrity, operator performance, and channel delivery
- **Receive Hälytin Installation Prompt** — Finnish Resident: Discover Hälytin through the 112 Suomi app cross-promotion banner and install it as part of the national awareness campaign

Abort or Correct Alert

Actor: Hätäkeskuslaitos Operator (Duty Officer)
Goal: Stop a dispatched alert or send a correction alert if new FDF data changes the threat classification or affected area


Alert has been dispatched to all channels
Operator sees 'Stop Alert' and 'Send Update' buttons on console
Reason to stop or correct?
New FDF data changes threat classification
New FDF data changes affected area
False alarm discovered
Operator clicks 'Send Update'
Operator clicks 'Stop Alert'
Console shows new threat data from FDF
Console shows confirmation: 'Are you sure? This will send all-clear to all channels'
Proposed update alert text in FI/SV/EN
Operator confirms?
Operator reviews: changed affected area or threat classification
No
Yes
Dialog closes; alert remains active
Update looks valid?
Operator enters reason for abort (e.g., 'False positive', 'Duplicate track')
No
Yes
Stop-alert signal sent to all channels simultaneously
App users see 'All clear - alert has been cancelled' notification
SMS users receive: 'Hälytin: Alert cancelled - no threat'
Broadcast relay sends all-clear to Yle
Website banner shows: 'Alert cancelled - all clear'
Operator clicks 'Reject Update'
Update severity?
Incident remains in current state; update is logged as rejected
Expansion of area
Contraction of area
Operator console shows: 'Alert stopped - all-clear sent'
Four-eyes confirmation required for update
Operator clicks 'Request Confirmation' for second operator
Single-operator confirmation required
Second operator reviews and confirms update
Operator clicks 'Confirm Update'
Update signal sent to all channels simultaneously
App users see 'Alert updated - new affected area' notification
SMS users receive: 'Hälytin: Alert updated - new area affected'
Website banner updated with new affected area
Operator console shows: 'Alert updated - delivery confirmed'

DIAGRAM

Steps

Abort Path:

1. Alert has been dispatched to all channels and is currently active
2. Operator receives new information indicating the alert was false (e.g., FDF track was a false positive, duplicate, or test track sent in error)
3. Operator clicks the 'Stop Alert' button on the console
4. Console displays a confirmation dialog: 'Are you sure? This will send all-clear to all channels and notify all users that the alert has been cancelled'
5. If the operator clicks 'No', the dialog closes and the alert remains active
6. If the operator clicks 'Yes', they are prompted to enter a reason for the abort (e.g., 'False positive', 'Duplicate track', 'Test track sent in error')
7. Operator enters the reason and clicks 'Confirm'
8. The stop-alert signal is sent to all channels simultaneously
9. App users receive a notification: 'All clear - alert has been cancelled'
10. SMS users receive: 'Hälytin: Alert cancelled - no threat'
11. Broadcast relay sends an all-clear signal to Yle
12. Website banner is updated to show: 'Alert cancelled - all clear'
13. Operator console displays: 'Alert stopped - all-clear sent' with timestamp and reason
14. The incident is closed and logged as 'Aborted' with the operator's reason

Correct/Update Path:

1. Alert is active; FDF provides new threat data that changes the affected area or threat classification
2. Operator receives the update notification on the console
3. Console displays the new threat data, the updated affected area polygon, and the updated alert text in FI/SV/EN
4. Operator reviews the proposed update to ensure it is valid and reflects the FDF data correctly
5. If the update is invalid or incorrect, the operator clicks 'Reject Update'; the incident remains in its current state and the rejection is logged
6. If the update is valid, the operator determines whether the change requires four-eyes confirmation:
    - If the affected area is expanding (new areas now at risk), four-eyes confirmation is required
    - If the affected area is contracting (previously affected areas now safe), single-operator confirmation is sufficient
7. For expansions, the operator clicks 'Request Confirmation' to notify a second operator
8. For contractions, the operator clicks 'Confirm Update' directly
9. Second operator (if required) reviews the updated threat data and affected area, then clicks 'Confirm Update'
10. Update signal is sent to all channels simultaneously
11. App users receive a notification: 'Alert updated - new affected area' with the updated map
12. SMS users receive: 'Hälytin: Alert updated - new area affected' with brief description

13. Website banner is updated with the new affected area polygon
14. Operator console displays: 'Alert updated - delivery confirmed' with timestamp and change summary
15. The incident remains open with the updated state; users continue to monitor the threat map

Key Decisions

- **Abort requires explicit confirmation to prevent accidental all-clear** — A single click cannot cancel an alert; the operator must confirm twice
- **Reason for abort is mandatory** — Every abort is logged with the operator's stated reason for post-incident review and accountability
- **Area expansion requires four-eyes confirmation; contraction does not** — Expanding the alert area increases the population affected and requires additional oversight; contracting the area is lower-risk
- **Updates are sent through all channels simultaneously** — Users in the newly affected area receive the update as quickly as users in the originally affected area
- **Stop-alert is irreversible** — Once sent, the all-clear cannot be unsent; if the threat re-emerges, a new alert must be dispatched (and will be, because FDF will send a new threat object)

Accessibility Notes

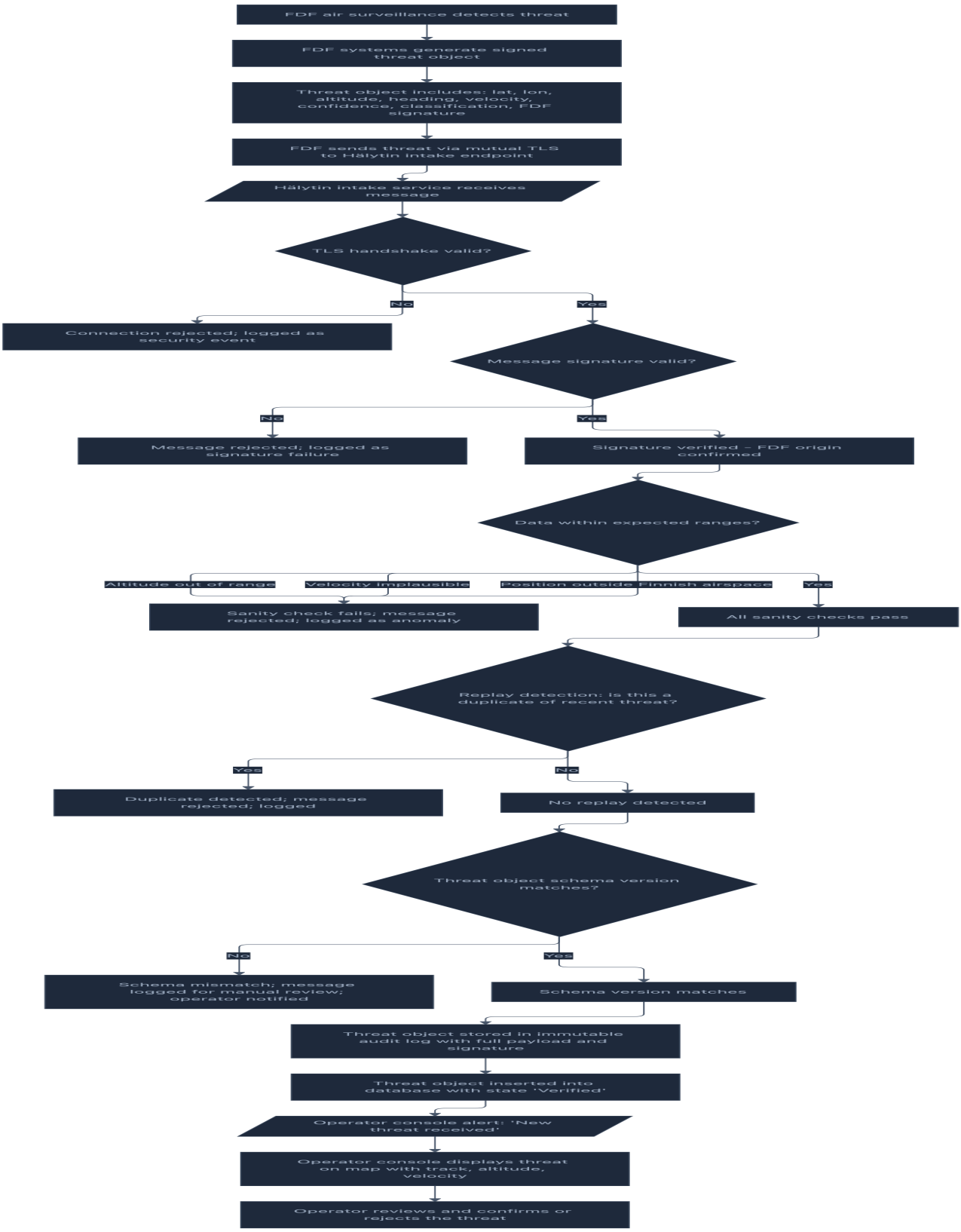
- 'Stop Alert' and 'Send Update' buttons are always visible and in consistent position on the console; no hidden menus or secondary clicks
- Confirmation dialogs use large text (18pt+) with high contrast and clear yes/no buttons
- Reason-entry field uses a dropdown with pre-populated reasons ('False positive', 'Duplicate track', 'Test track sent in error', 'Area corrected', 'Threat reclassified') to reduce operator typing
- Keyboard shortcuts available: S for 'Stop Alert', U for 'Send Update'
- Console provides audio feedback (distinct tone) when an update is received from FDF to alert the operator to new data

Error Recovery

- If the stop-alert signal fails to deliver to one or more channels (e.g., SMS gateway timeout), the console shows the failure and the operator can click 'Retry Stop' to re-send to failed channels
- If the operator clicks 'Stop Alert' but the dialog times out before confirmation, the alert remains active and the operator must re-initiate the stop
- If a second operator does not confirm an update within 60 seconds, the console shows a timeout warning and the first operator can click 'Escalate to Supervisor'
- If new FDF data arrives while an update is pending confirmation, the console queues the new update and notifies the operator; the first update must complete before the second is processed
- If the operator console loses connectivity while an abort or update is in progress, the action is logged but not sent; once connectivity is restored, the operator must re-initiate the action

Ingest and Verify FDF Threat

Actor: System (FDF Integration - Automated)
Goal: Receive a signed threat object from FDF air surveillance, verify its cryptographic origin and data validity, and surface it to the Hätäkeskuslaitos operator console for human confirmation



Steps

1. FDF air surveillance systems detect an inbound air threat (drone, missile, hostile aircraft, or unclassified track)
2. FDF threat-assessment systems generate a structured threat object containing: latitude, longitude, altitude, heading, velocity, confidence score, threat classification, FDF originator signature, and ingest timestamp
3. FDF systems establish a mutual TLS connection to Hälytin's dedicated intake endpoint (hosted in a DMZ, isolated from public internet)
4. FDF sends the threat object as a signed message over the authenticated TLS channel
5. Hälytin intake service receives the message and validates the TLS handshake
6. If the TLS handshake is invalid (certificate mismatch, untrusted CA, or connection from unauthorized IP), the connection is rejected and logged as a security event
7. If the TLS handshake is valid, the service verifies the message-level cryptographic signature using FDF's public key
8. If the signature is invalid or missing, the message is rejected and logged as a signature failure; no further processing occurs
9. If the signature is valid, the FDF origin is confirmed
10. The service performs sanity checks on the threat data:
    - Altitude is within plausible range for aircraft (0 to 15,000 meters)
    - Velocity is within plausible range for aircraft (0 to 2,500 km/h)
    - Position (lat/lon) is within or near Finnish airspace
    - Confidence score is between 0 and 1
11. If any sanity check fails, the message is rejected and logged as an anomaly; the operator is notified that a malformed threat was received
12. If all sanity checks pass, the service checks for replay attacks by comparing the threat object to recent threats received from FDF (within the last 5 minutes)
13. If an identical or near-identical threat is found (same position, altitude, velocity within 1% tolerance), it is treated as a duplicate and rejected; the duplicate is logged
14. If no replay is detected, the service checks whether the threat object schema version matches the current expected version
15. If the schema version does not match (e.g., FDF has updated the schema and Hälytin has not), the threat is logged for manual review and the operator is notified; no automatic processing occurs until the schema is updated
16. If the schema version matches, the threat object is stored in an immutable, cryptographically-chained audit log with the full payload, signature, and verification timestamp
17. The threat object is inserted into the database with state 'Verified' and is ready for operator review
18. The operator console receives an alert (audible tone + visual notification): 'New threat received'
19. The threat is displayed on the operator console map with the track (past and projected), altitude, velocity, and FDF classification

20. The operator reviews the threat and confirms or rejects it based on their assessment

Key Decisions

- **Signature verification is mandatory and non-negotiable** — Every threat must have a valid FDF signature; no exceptions, no workarounds
- **Sanity checks are strict to prevent operator confusion** — Out-of-range data is rejected immediately; the operator is never presented with implausible threats
- **Replay detection prevents duplicate alerts** — If FDF sends the same threat twice (due to a system error or retry), only one alert is dispatched
- **Schema versioning allows FDF and Hälytin to evolve independently** — If FDF changes the threat object format, Hälytin can be updated to handle the new format without disrupting the alert pipeline
- **Audit logging is immutable and append-only** — Every threat, verification result, and rejection is logged with timestamp and reason; no logs can be modified or deleted

Accessibility Notes

- Operator console displays verification status in plain language: 'Verified - FDF signature confirmed', 'Rejected - signature invalid', 'Rejected - data out of range', 'Pending - schema mismatch, manual review required'
- Verification results are displayed in high-contrast colors: green for verified, red for rejected, yellow for pending
- Operator console provides audio feedback (distinct tone) when a new verified threat arrives
- All technical details (signature algorithm, sanity check ranges, replay detection window) are documented in the operator manual but not displayed on the console; the operator sees only the result ('Verified' or reason for rejection)

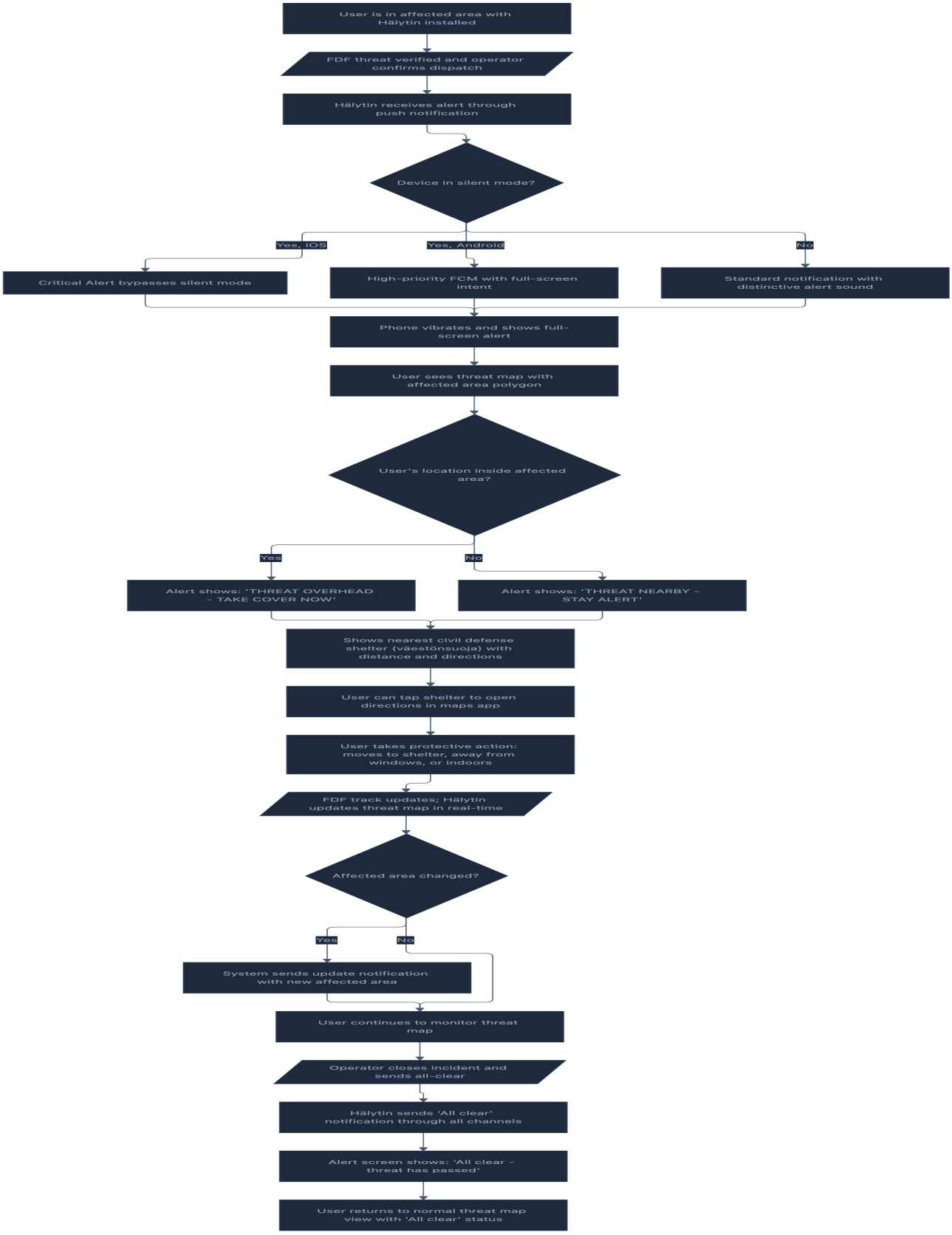
Error Recovery

- If the TLS connection is dropped mid-message, FDF automatically retries; Hälytin queues the message and processes it once the connection is re-established
- If signature verification fails due to an expired FDF signing key, the operator is notified and can request an updated key from FDF; threats are held pending until the key is updated
- If a sanity check fails (e.g., FDF sends a threat at 20,000 meters altitude due to a sensor error), the threat is logged and the operator is notified; the operator can choose to manually override the sanity check if they believe the data is valid (this action is logged with the operator's reason)
- If replay detection incorrectly identifies a new threat as a duplicate (due to a timing edge case), the operator can click 'Override Replay Detection' to process the threat anyway; this action is logged
- If the schema version does not match, the operator can click 'Process Anyway' to attempt to parse the threat with the current schema; if parsing succeeds, the threat is processed; if parsing fails, the threat is rejected and the operator is notified that the schema needs to be updated

Receive and Respond to Air-Threat Alert

Actor: Finnish Resident

Goal: Receive a real-time air-threat alert, understand the threat and guidance, and take protective action



DIAGRAM

Steps

1. User is in a geographic area with active Hälytin installation and receives an incoming air-threat alert
2. FDF has detected and classified the threat; Hätäkeskuslaitos operator has verified and confirmed dispatch
3. Hälytin's fan-out service receives the confirmed alert and pushes it through all active channels simultaneously
4. On iOS with notifications enabled, the alert is sent as a Critical Alert, which bypasses silent mode and plays the distinctive Hälytin alert sound
5. On Android with notifications enabled, the alert is sent through the high-priority FCM channel with full-screen intent
6. User's phone vibrates and displays the full-screen alert with the threat classification (drone, missile, hostile aircraft, or unknown) and the affected area highlighted on a map
7. If the user's location (from coarse location data or GPS if granted) is inside the affected area, the alert shows 'THREAT OVERHEAD - TAKE COVER NOW' in large, high-contrast text
8. If the user's location is outside but nearby, the alert shows 'THREAT NEARBY - STAY ALERT'
9. The alert screen displays the nearest civil defense shelter (väestönsuoja) with the distance, directions, and a button to open directions in the user's default maps application
10. User taps the shelter button or manually navigates to cover; the app remains on screen showing the live threat track
11. As FDF updates the threat track, Hälytin automatically updates the threat map on the user's screen in real-time without requiring the user to refresh
12. If the FDF track moves and the affected area changes materially, Hälytin sends an update notification with the new affected area
13. User continues to monitor the threat map until the operator closes the incident
14. Hätäkeskuslaitos operator closes the incident after the threat has passed; the system sends an 'All clear' notification through all channels
15. User's Hälytin screen transitions to 'All clear - threat has passed' and returns to the normal threat map view with 'All clear' status
16. User can close the app or continue to monitor; the system is ready for the next alert

Key Decisions

- **Alert reaches user regardless of app state** — The alert fires even if the app is closed, backgrounded, or the device is in silent mode; this is guaranteed by Critical Alerts (iOS) and high-priority FCM (Android)
- **Geographic precision determines alert text** — Users inside the affected area see 'TAKE COVER NOW'; users nearby see 'STAY ALERT'; this prevents alert fatigue from nationwide broadcasts
- **Shelter information is pre-loaded and never requires network** — Even if the cellular network is degraded, the user can see the nearest shelter without connectivity
- **Real-time threat map updates without user interaction** — The FDF track is pushed to the app as it evolves; the user does not need to refresh or re-open the app
-

All-clear notification is as prominent as the alert — Users know when the threat has passed through the same channels they received the alert

Accessibility Notes

- Alert text uses large, high-contrast fonts (at least 24pt) with sans-serif typeface for readability
- Vibration pattern is distinctive and recognizable; users with hearing impairments receive vibration + visual alert
- Threat map uses color-coding (red for affected area, yellow for nearby) with text labels; not color-dependent alone
- Shelter information includes both distance and walking time estimate for users with mobility considerations
- Screen reader announces threat level, affected area, and nearest shelter in plain language
- Vibration-only mode (selected during onboarding) suppresses sound entirely while maintaining vibration and visual alert

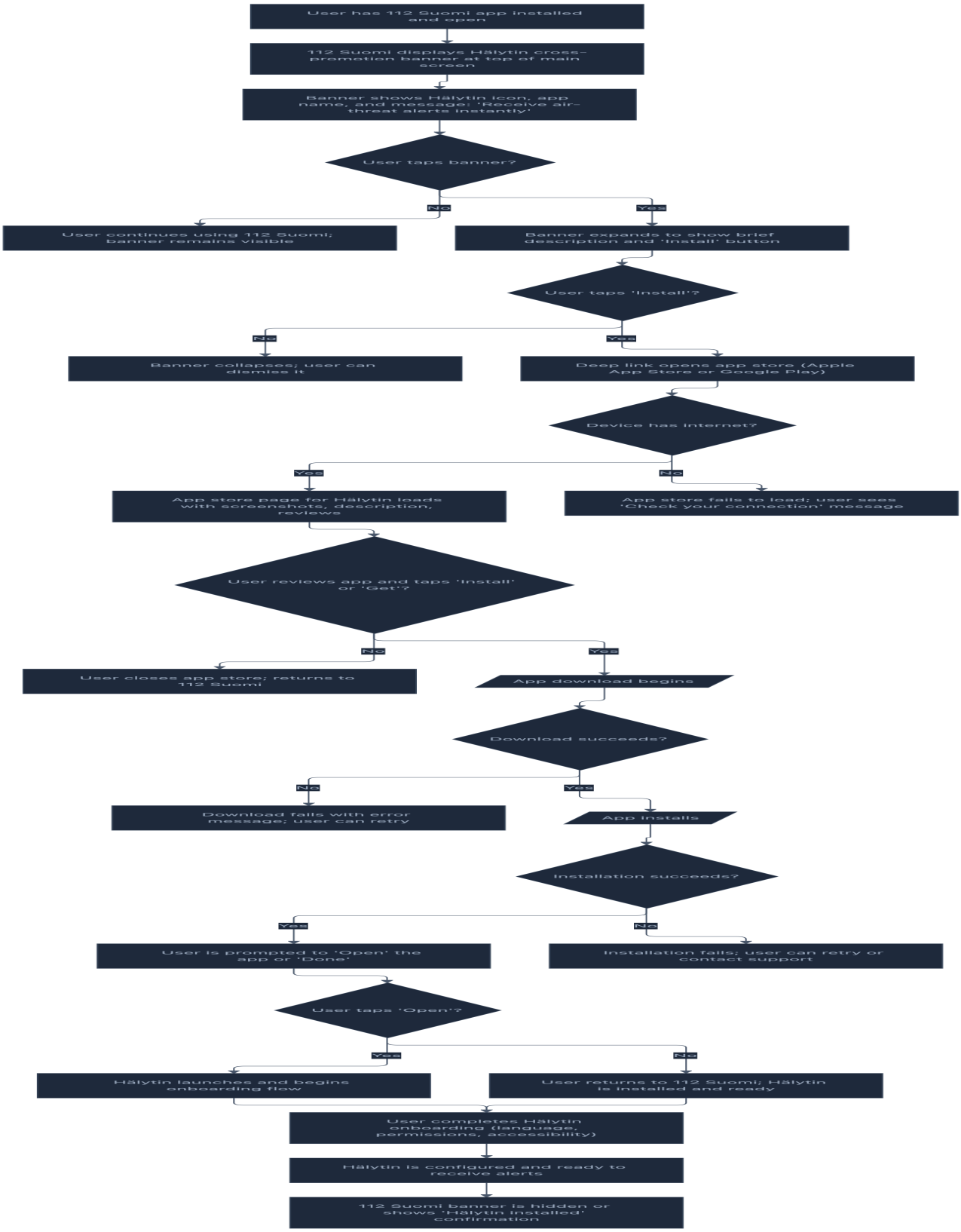
Error Recovery

- If the push notification fails to deliver (network outage, FCM service degradation), the alert is queued and re-delivered when connectivity is restored; the app also checks for missed alerts on next launch
- If the threat map fails to load (network error), the app shows cached map data from the last successful update; the user still sees the affected area polygon and shelter information
- If the user's location cannot be determined (GPS disabled, no cell tower data), the app defaults to coarse location from municipality data and shows 'THREAT IN YOUR AREA' without precise distance
- If the user dismisses the alert by accident, the alert remains on screen for 30 seconds minimum before allowing dismissal; after dismissal, the alert is still accessible from a 'Recent Alerts' history
- If the device runs out of battery during an alert, the user receives SMS (if SMS channel is active) as a fallback; SMS is also sent to ensure redundancy

Receive Hälytin Installation Prompt

Actor: Finnish Resident

Goal: Discover Hälytin through the 112 Suomi app cross-promotion banner and install it as part of the national awareness campaign



Steps

1. User has the 112 Suomi app installed on their phone and opens it to check emergency information or settings
2. 112 Suomi main screen displays a cross-promotion banner at the top showing the Hälytin icon, app name, and a brief message: 'Receive air-threat alerts instantly'
3. Banner is non-intrusive (not a full-screen takeover) but visually prominent (high contrast, recognizable Hälytin icon)
4. User can see the banner and has the option to tap it or ignore it
5. If the user does not tap the banner, they continue using 112 Suomi; the banner remains visible on subsequent app launches
6. If the user taps the banner, it expands to show a brief description of Hälytin and an 'Install' button
7. Description text (FI/SV/EN): 'Hälytin is a dedicated app that sends real-time air-threat alerts to your phone. Receive instant notifications about threats overhead and know where to take cover. Install now to protect yourself and your family.'
8. If the user taps 'Install', a deep link is triggered that opens the app store (Apple App Store on iOS, Google Play on Android) directly to the Hälytin app page
9. If the user closes the expanded banner or taps 'Not Now', the banner collapses and the user can dismiss it (banner will not show again for 7 days)
10. If the device does not have internet connectivity, the app store fails to load and the user sees an error message: 'Check your connection and try again'
11. If the device has internet, the app store page for Hälytin loads with app screenshots, a detailed description, user reviews, ratings, and the 'Install' (iOS) or 'Get' (Android) button
12. User can review the app information and decide whether to install
13. If the user taps 'Install' or 'Get', the app download begins (progress indicator shown)
14. If the download fails (network error, insufficient storage), the user sees an error message and can retry
15. If the download succeeds, the app is installed in the background
16. If the installation fails (corrupted download, incompatible device), the user sees an error message and can retry or contact support
17. Once installation succeeds, the user is prompted to 'Open' the app or 'Done'
18. If the user taps 'Open', Hälytin launches immediately and begins the onboarding flow (language selection, permissions, accessibility)
19. If the user taps 'Done', they return to 112 Suomi; Hälytin is installed and ready, and the user can launch it later from their home screen
20. User completes Hälytin onboarding (selecting language, granting location and notification permissions, selecting accessibility options)
21. Hälytin is now configured and ready to receive air-threat alerts
22. The 112 Suomi banner is hidden or updated to show 'Hälytin installed' confirmation
23. User can return to 112 Suomi or close Hälytin; both apps are now on the device

Key Decisions

- **Cross-promotion banner is non-intrusive but persistent** — It does not block the user from using 112 Suomi, but it remains visible on subsequent launches to drive awareness
- **Deep link goes directly to app store, not to a landing page** — This minimizes friction; the user goes from 112 Suomi to the app store in one tap
- **Banner can be dismissed for 7 days** — This prevents banner fatigue while giving the user multiple opportunities to install
- **Installation is optional** — The user is never forced to install Hälytin; they can continue using 112 Suomi without it
- **Post-installation confirmation** — Once Hälytin is installed, the banner is hidden or shows a confirmation, reinforcing that the installation was successful

Accessibility Notes

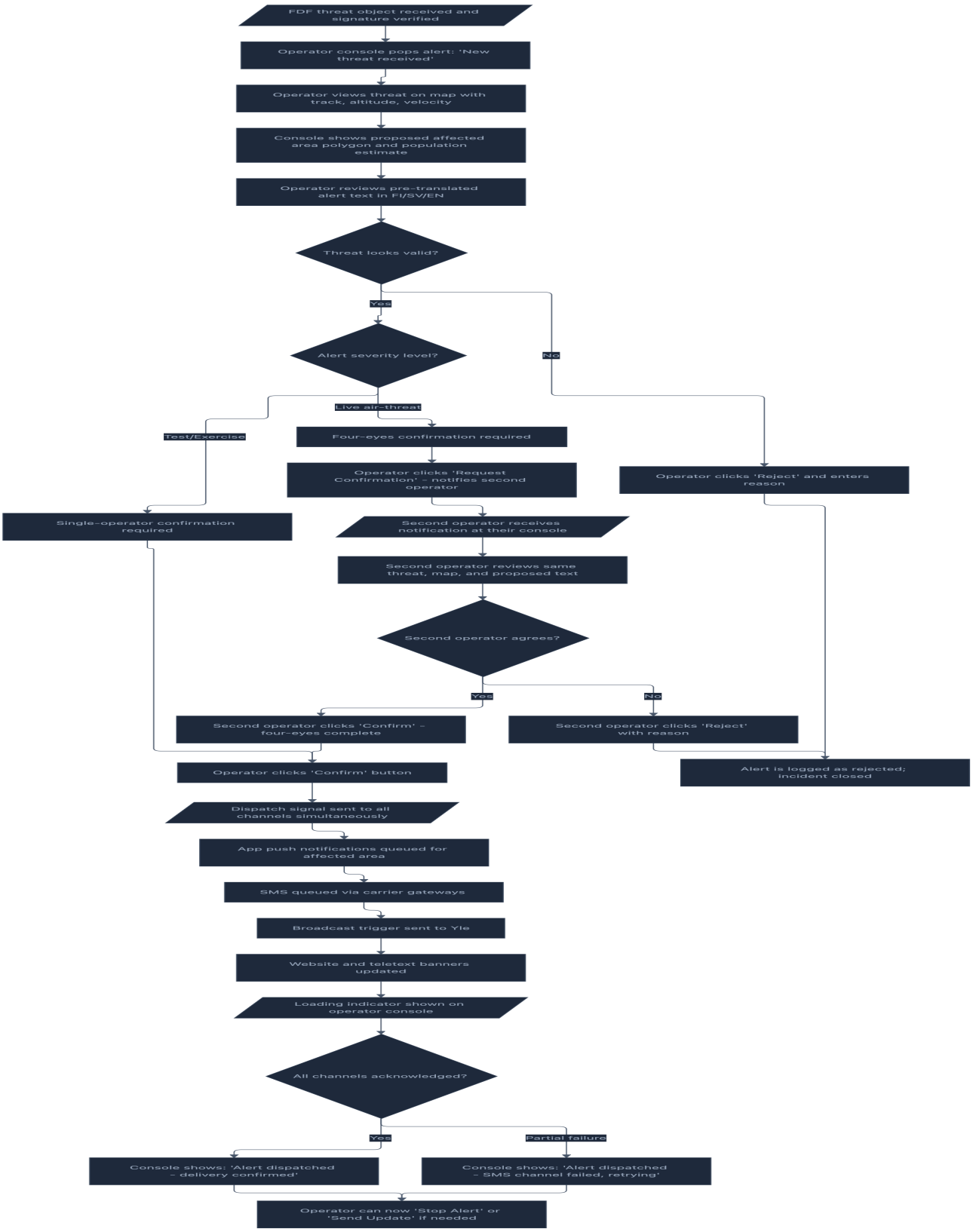
- Banner uses high-contrast colors (Hälytin's distinctive visual identity) so it is visible to users with low vision
- Banner text is at least 14pt and uses sans-serif typeface for readability
- 'Install' button is 48x48 points minimum and uses a distinct color (green) for accessibility
- Screen reader announces the banner and its purpose: 'Hälytin cross-promotion banner: Receive air-threat alerts instantly. Double-tap to install.'
- App store link opens in the user's default app store app (not a web browser), ensuring the user stays in the native app experience
- Error messages use plain language and include a 'Retry' button or link to contact support

Error Recovery

- If the deep link fails (app store app not installed, link malformed), the user is shown an error message and a manual link to search for Hälytin in the app store
- If the download fails due to network error, the user can tap 'Retry' to resume the download
- If the installation fails due to insufficient storage, the user is shown a message: 'Not enough storage. Free up space and try again.'
- If the app store page fails to load, the user is shown a retry button and can try again
- If the user accidentally closes the app store during installation, the download is paused; the user can resume by opening the app store again
- If the user's app store account has issues (payment method declined, account suspended), the user is shown an appropriate error message and directed to contact Apple or Google support

Verify and Dispatch Alert (Standard Workflow)

Actor: Hätäkeskuslaitos Operator (Duty Officer)
Goal: Verify an incoming FDF threat on the operator console, obtain four-eyes confirmation from a second operator, and dispatch the alert to all channels within 30 seconds



DIAGRAM

Steps

1. FDF air surveillance detects a threat and sends a signed threat object to Hälytin's intake
2. Hälytin's backend verifies the cryptographic signature and sanity-checks the threat data (position, altitude, velocity within expected ranges)
3. If verification passes, the threat is surfaced on the Hätäkeskuslaitos operator console with an audible alert tone
4. Operator sees the threat displayed on a map with the track (past and projected), current altitude, velocity, and FDF classification (drone, missile, hostile aircraft, unknown)
5. Console shows the proposed affected area as a polygon (municipality boundary or finer geometry based on FDF track projection) and the population estimate in that area from public statistics
6. Operator reviews the pre-translated alert text in Finnish, Swedish, and English; all text has been pre-approved by Sisäministeriö
7. Operator evaluates whether the threat is valid (not a test, not a spurious track, not a system error)
8. If the threat is invalid, the operator clicks 'Reject', enters a reason (e.g., 'duplicate track', 'false positive'), and closes the incident; the rejection is logged
9. If the threat is valid, the operator determines the alert severity: Test/Exercise alert (single operator can confirm) or Live Air-Threat alert (requires four-eyes confirmation)
10. For Test/Exercise alerts, the operator clicks 'Confirm' to authorize dispatch
11. For Live Air-Threat alerts, the operator clicks 'Request Confirmation', which sends a notification to a second operator (supervisor or peer) at another console
12. The second operator receives the confirmation request, reviews the same threat map, affected area, and proposed alert text
13. The second operator either clicks 'Confirm' (four-eyes confirmation complete) or 'Reject' (incident closed, reason logged)
14. Once confirmation is obtained (single or four-eyes), the dispatch signal is sent to all channels simultaneously
15. App push notifications are queued for delivery to all devices in the affected area through Apple Push Notification Service (iOS) and Firebase Cloud Messaging (Android)
16. SMS is queued for delivery through mobile carrier gateways to phones in the affected area
17. A broadcast trigger is sent to Yle for radio and television interruption
18. The Hälytin website and teletext page 112 are updated with the alert banner
19. Operator console shows a loading indicator while all channels acknowledge receipt
20. Once all channels have acknowledged (or timed out after 10 seconds), the console displays 'Alert dispatched - delivery confirmed' or 'Alert dispatched - SMS channel failed, retrying' if a channel is slow
21. Operator can now click 'Stop Alert' (to abort the incident) or 'Send Update' (if FDF provides new track data that changes the affected area) without additional confirmation

Key Decisions

- **Four-eyes confirmation is mandatory for live air-threat alerts** — The workflow enforces this; no role can bypass it, regardless of time pressure or seniority

- **Test/Exercise alerts require only single-operator confirmation** — This allows frequent drills without operational friction while maintaining human-in-the-loop
- **Affected area is determined by FDF track projection, not by operator choice** — The operator cannot manually expand or shrink the alert area; this prevents operator error from creating false alarms
- **All channels dispatch simultaneously** — The user experience is "all channels fire as close to simultaneously as physics allows"; no staggered dispatch that might cause confusion
- **Dispatch is irreversible but stoppable** — Once sent, the alert cannot be unsent, but the operator can send a stop/correction alert immediately if new information arrives

Accessibility Notes

- Operator console is designed for use by a tired operator at 3am under stress; every control is large, clearly labeled, and in consistent position
- Map uses high-contrast colors (red for affected area, blue for threat track) with no color-only indicators
- Font size is at least 14pt for all text; critical information (threat type, affected area, population) is in 18pt+ bold
- Confirmation buttons are large (48x48 points minimum) and use distinct colors: green for 'Confirm', red for 'Reject', orange for 'Request Confirmation'
- Keyboard shortcuts are available for all critical actions (C for Confirm, R for Reject, U for Update) for operators who prefer keyboard navigation
- Audio alert tone is distinctive and non-intrusive (not startling); volume can be adjusted in settings

Error Recovery

- If a channel fails to acknowledge dispatch (e.g., SMS gateway timeout), the console shows the failure and the operator can click 'Retry' to re-send to that channel only
- If the second operator does not confirm within 60 seconds, the console shows a timeout warning; the first operator can click 'Escalate to Supervisor' to route to a supervisor for expedited confirmation
- If the operator accidentally clicks 'Confirm' on an invalid threat, they can immediately click 'Stop Alert' to send a cancellation; the stop is logged with the reason
- If the FDF signature verification fails (malformed or unsigned threat), the threat is rejected automatically and logged; the operator is notified that the threat could not be verified
- If the operator console loses network connectivity, it enters offline mode and displays cached threat data; once connectivity is restored, any pending confirmations are re-sent

Install and Configure Hälytin

Actor: Finnish Resident
Goal: Download the Hälytin app, complete onboarding, grant required permissions, and be ready to receive air-threat alerts in under 2 minutes

DIAGRAM

Steps

1. User visits halytin.fi or navigates to Hälytin in Apple App Store or Google Play Store
2.

Taps 'Install' (iOS) or 'Get' (Android) button to begin download

3. App downloads and installs in background; user sees progress indicator
4. User launches Hälytin for the first time and sees welcome screen explaining the app's single purpose: air-threat alerts
5. If user is unfamiliar with the app's function, they can tap 'How it works' to read a plain-language explanation with a map showing how alerts work; they return to the welcome screen
6. User selects their preferred language from a dropdown: Finnish, Swedish, or English
7. User taps 'Continue' and sees the location permission request
8. If user denies location permission, they see a warning explaining that location is needed for accurate, targeted alerts; they can grant permission or continue without it (system will use coarse location from cell tower or municipality)
9. User sees the notification permission request
10. If user denies notifications, they see a warning that notifications are required for alerts to work; they can grant permission or continue with notifications disabled (alerts will still be available in the app, but push notifications will not fire)
11. User is offered accessibility options: high contrast mode, large text, vibration-only mode (for deaf users), or screen-reader compatibility
12. User selects accessibility preferences or skips this step
13. User taps 'Finish Setup' and is taken to the main threat map screen showing 'All clear' status
14. System displays confirmation message: 'You're protected - ready to receive alerts'
15. User can screenshot the confirmation screen to share with others or close the app; onboarding is complete

Key Decisions

- **Language selection is mandatory** — User must choose one of the three supported languages before proceeding; this ensures alerts are always in the user's preferred language
- **Location permission is strongly encouraged but not mandatory** — Without location, alerts will reach the user but targeting precision degrades to cell-tower or municipality level; the system still functions
- **Notification permission is strongly encouraged but not mandatory** — Without notifications enabled, the user must manually open the app to see alerts; the system logs this as a degraded-reach scenario
- **Accessibility options are optional but discoverable** — Users who need them can find them; users who don't can skip without friction
- **Onboarding must complete in under 2 minutes** — Every screen has a clear forward path; no required scrolling or hidden settings

Accessibility Notes

- Welcome screen text is large (18pt minimum) and uses high-contrast colors
- All buttons are 48x48 points minimum for touch accessibility
- Permission request screens include screen-reader-friendly explanations of why each permission is needed
- Vibration-only mode is available for deaf users; alerts will vibrate and show visual notifications without sound
- High-contrast mode inverts colors for users with low vision

- Language selection uses native script (Finnish, Swedish, English) with no abbreviations
- The 'How it works' explainer uses simple sentences, active voice, and a visual map example

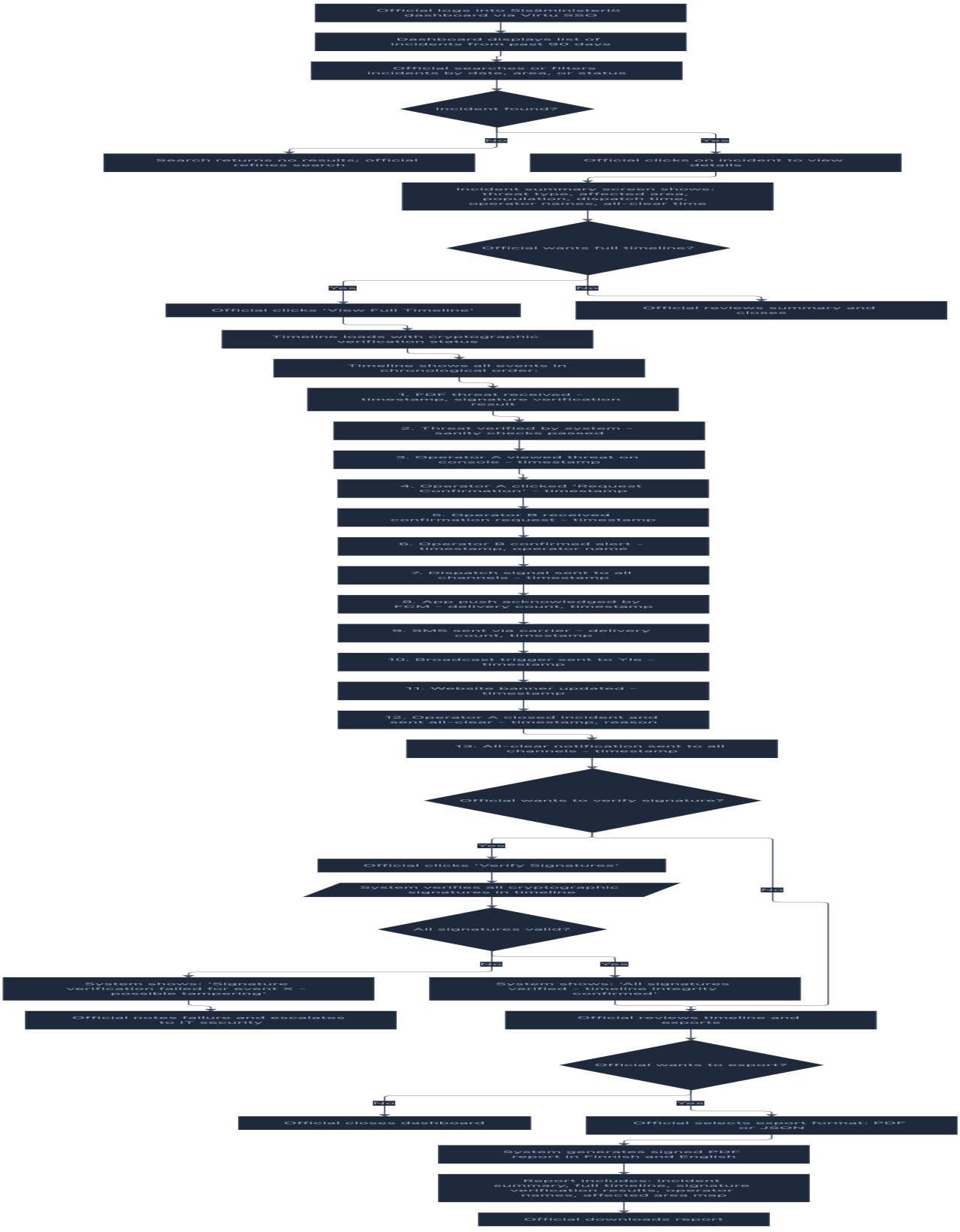
Error Recovery

- If the app crashes during installation, the user can restart the installation from the app store; the system does not require re-download
- If permission requests are denied, the user can change them later in iOS Settings or Android Settings; the app will prompt them on the next launch
- If the app fails to connect to the backend during onboarding, it enters offline mode and allows the user to complete setup; the app will sync once connectivity is restored

Review Post-Incident Timeline

Actor: Sisäministeriö Preparedness Official

Goal: Access a complete, signed audit trail of an incident from FDF detection through all-clear notification to verify system integrity, operator performance, and channel delivery



Steps

1. Sisäministeriö preparedness official accesses the Hälytin post-incident review dashboard via a secure web interface
2. Official authenticates using Virtu SSO (Finnish public-sector identity infrastructure)
3. Dashboard displays a list of all incidents from the past 90 days, sorted by date (most recent first)
4. Official searches or filters incidents by date range, affected area, threat type, or status (completed, aborted, false alarm)
5. Once the incident of interest is found, the official clicks on it to view the incident summary
6. Incident summary screen displays: threat type (drone, missile, hostile aircraft, unknown), affected area (municipality or polygon), population estimate, dispatch timestamp, names of confirming operators, all-clear timestamp, and incident status (completed/aborted/false alarm)
7. Official can review the summary and close, or click 'View Full Timeline' to see the detailed audit trail
8. Full timeline loads and displays a cryptographic verification status indicator at the top: 'Timeline integrity verified' (green) or 'Signature verification failed' (red)
9. Timeline displays all events in strict chronological order:
    - FDF threat received (timestamp, signature verification result)
    - Threat verified by system (sanity checks passed, no replay detected)
    - Operator A viewed threat on console (timestamp)
    - Operator A clicked 'Request Confirmation' (timestamp)
    - Operator B received confirmation request (timestamp)
    - Operator B confirmed alert (timestamp, operator name)
    - Dispatch signal sent to all channels (timestamp)
    - App push acknowledged by FCM (delivery count, timestamp, sample of device tokens that received the alert - anonymized)
    - SMS sent via carrier (delivery count, timestamp, carrier name)
    - Broadcast trigger sent to Yle (timestamp)
    - Website banner updated (timestamp)
    - Operator A closed incident and sent all-clear (timestamp, reason)
    - All-clear notification sent to all channels (timestamp, delivery counts)
10. Official can click on any event in the timeline to see additional details (e.g., exact alert text, affected area polygon, FDF threat object payload)
11. Official can click 'Verify Signatures' to trigger cryptographic verification of all signatures in the timeline
12. System verifies each signature using the corresponding public keys (FDF key for threat signature, operator certificate for confirmation signature, system key for dispatch and all-clear signatures)
13. If all signatures are valid, the system displays: 'All signatures verified - timeline integrity confirmed' (green indicator)
14.

If any signature is invalid, the system displays: 'Signature verification failed for event X - possible tampering' (red indicator with details)

15. If signatures fail verification, the official notes the failure and escalates to Taiga IT security or Hätäkeskuslaitos security team
16. Official can export the full timeline as a signed PDF report (bilingual FI/EN) or as structured JSON
17. PDF report includes: incident summary, full timeline with all events and timestamps, signature verification results, operator names, affected area map, and population estimate
18. Report is signed by Hälytin and can be verified against Hälytin's public key
19. Official downloads the report for archival, parliamentary oversight, or public disclosure
20. Official closes the dashboard

Key Decisions

- **Timeline is immutable and append-only** — Events cannot be added, removed, or reordered; this prevents any post-hoc manipulation of the incident record
- **All signatures are cryptographically verified** — The official can confirm that every event in the timeline is authentic and has not been tampered with
- **Operator names are displayed** — This ensures accountability; every confirmation is attributed to a named operator
- **Delivery counts are aggregated, not per-user** — This protects user privacy while giving officials visibility into channel effectiveness
- **Timeline is exportable in multiple formats** — PDF for human review and archival; JSON for machine parsing and statistical analysis

Accessibility Notes

- Timeline is displayed in a table with clear column headers: Event, Timestamp, Details, Status
- Events are color-coded: green for successful events (verification passed, delivery confirmed), yellow for partial success (one channel failed), red for failures (signature invalid)
- Timestamp format is ISO 8601 with timezone (e.g., 2027-02-15T14:32:45+02:00) for clarity
- Official can toggle between Finnish and English for the full interface and reports
- PDF reports include a digital signature and a QR code that links to the incident details for verification
- Timeline can be downloaded as a CSV file for import into spreadsheet tools for further analysis

Error Recovery

- If the official's SSO session expires, they are prompted to re-authenticate; the timeline view is preserved
- If signature verification fails due to a missing public key (e.g., FDF key has been rotated), the system displays an error and the official can request the updated key
- If the timeline fails to load (database error, network timeout), the official sees a retry button and can try again
- If the export fails (file system error, PDF generation timeout), the official is notified and can try again or contact support
-

If the official accidentally closes the timeline view, the incident remains in the system and can be reopened by searching for it again