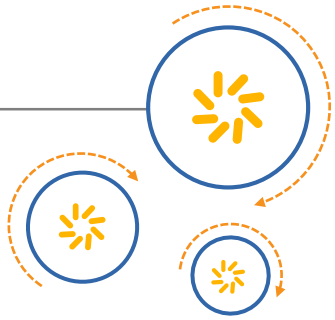
Qualcomm Technologies, Inc.



Geofencing Reference Guide

80-NB758-1 E

August 24, 2015

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

Revision history

Revision	Date	Description
A	July 2012	Initial relase
B	September 2013	Numerous changes were made including the addition of Geofence 3.0; it should be read in its entirety
C	October 2014	Added Geofence 3.0.1 and 3.1; changes cover WWAN motion classification enhanced Wi-Fi motion detector and proximity Geofence indication
D	January 2015	Added information regarding Geofence use of RF Context Data and persistent storage
E	August 2015	Numerous changes were made including the addition of Geofence 3.3; it should be read in its entirety

Note: There is no Rev. I, O, Q, S, X, or Z per Mil. standards.

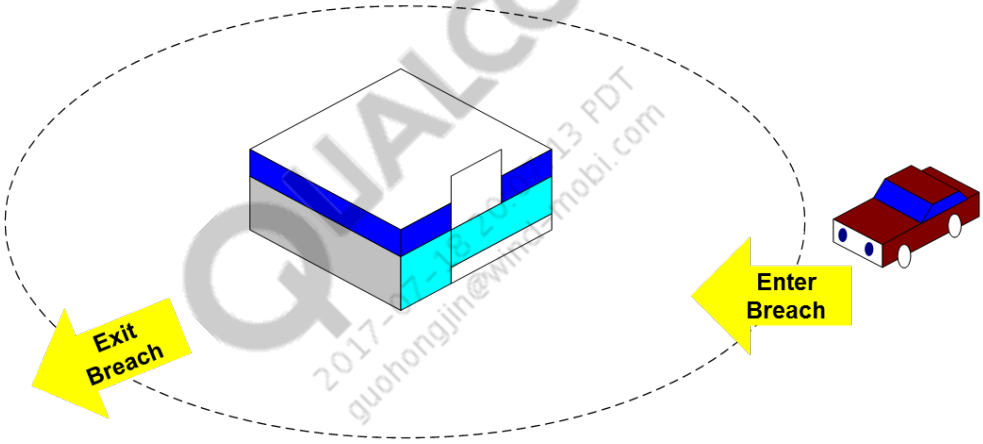
Contents

1 Introduction

1.1 Purpose

This document provides an overview of geofencing, including architecture, configuration, and call flows. The document is for OEMs, carriers, and partners using the low power and high responsiveness and availability of Qualcomm® IZat™ location services geofencing.

A geofence is a virtual perimeter on a geographic area using a location-based service. When a geofencing device enters or exits the area, a notification is generated.



1.2 Conventions

Function declarations, function names, type declarations, attributes, and code samples appear in a different font, for example, `#include`.

1.3 Technical assistance

For assistance or clarification on information in this document, submit a case to Qualcomm Technologies, Inc. (QTI) at https://createpoint.qti.qualcomm.com/.

If you do not have access to the CDMATech Support website, register for access or send email to support.cdmatech@qti.qualcomm.com.

2 Geofence management and timeline

2.1 How geofences are managed

Geofences can be Mobile-Originated (MO) or Mobile-Terminated (MT). The core geofence task/logic is independent of how the geofence is set.

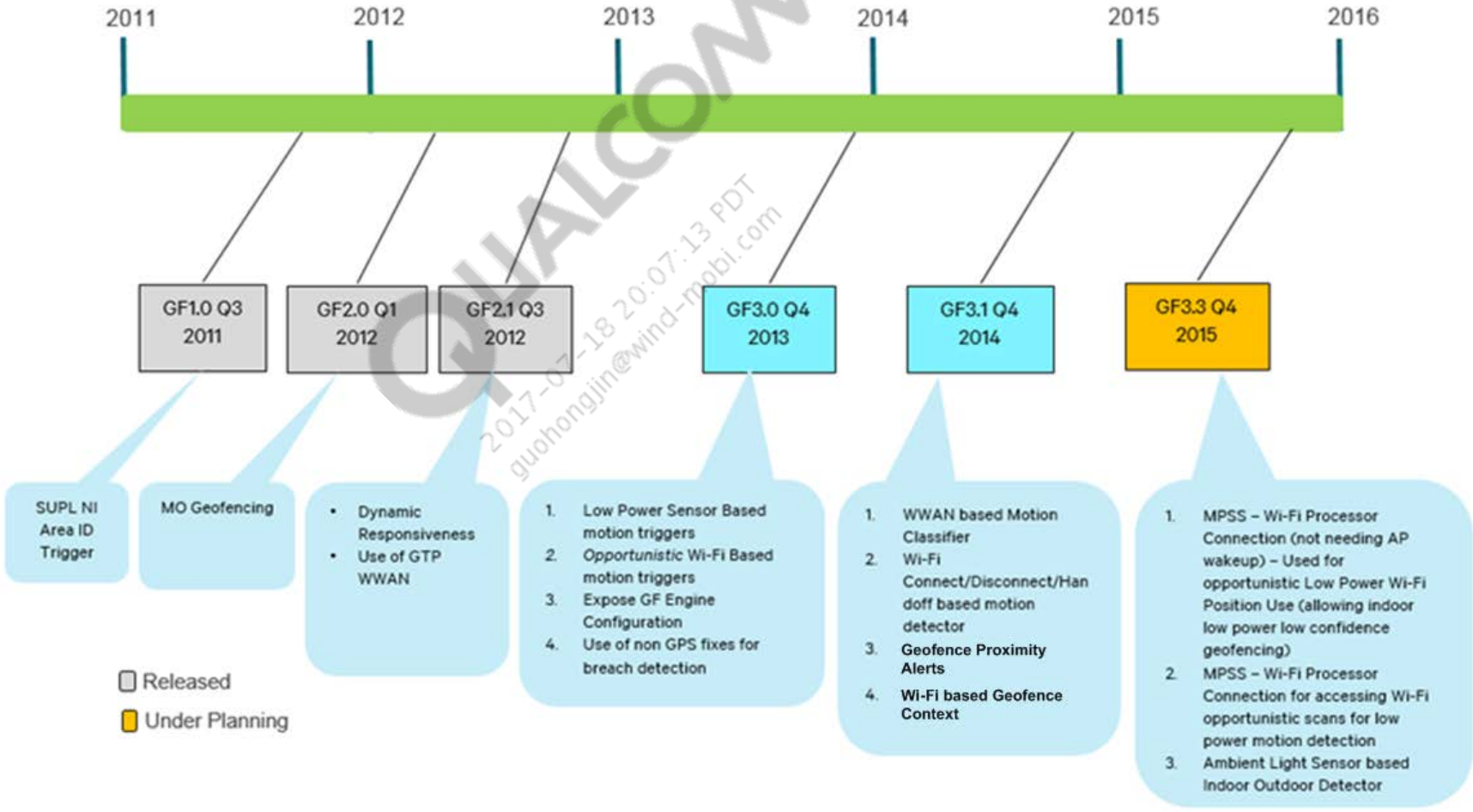
MO includes the following:

- MDM – Geofences added or deleted by Loc API (QTI-provided API on MDMs)
- MSM™
  - Geofences added or deleted by Android™ AddProximityAlert()
  - Geofences added or deleted by Google Play Services API

MT includes geofences added or deleted by network side apps via MT protocol, that is, OMA SUPL 2.0 MT Area Event Triggers.

2.2 IZat geofencing timeline – Major releases

The following figure shows a brief timeline of the IZat geofencing solution, including which features have been added already and which are expected to be added in future releases.



3 Modem and low-power processor-based implementation

3.1 Low-power geofence implementation

A low-power geofence task within the modem provides core geofencing event detection capability. The geofence task uses algorithms to provide optimal power usage and geofence event detection. In most cases, these algorithms cannot be run at an application level. The algorithms are as follows:

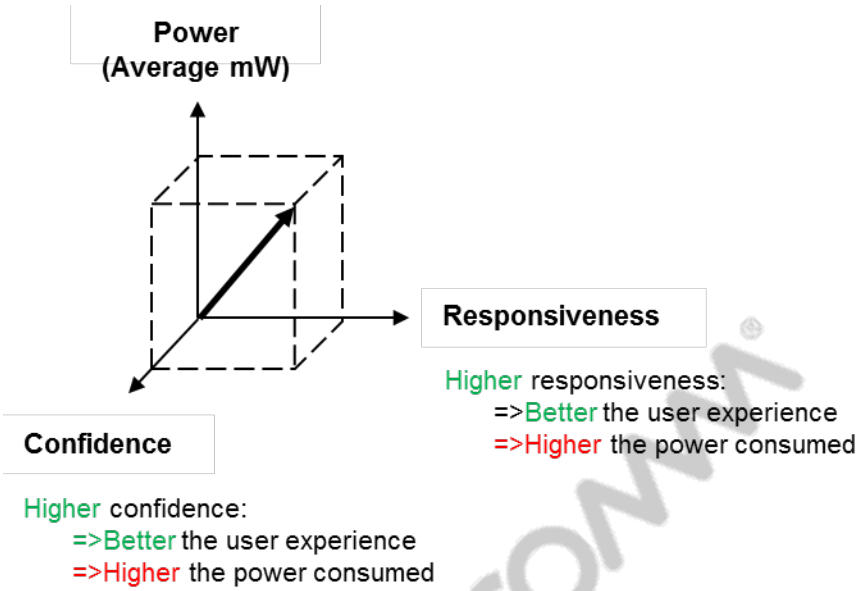
- Use of Area IDs (from SUPL 2.0) to minimize invocation of high precision (GNSS) fix
- Optimal rate at which to invoke GNSS fixes (when needed) to minimize power usage
- Distance-based backoff when no cell database list, e.g., Area ID list in SUPL 2.0, is available
- Use of auxiliary information, for example, GTP WWAN, sensors, to reduce the need for a GNSS fix
- Use of Zero Power Positioning and GTP WWAN planned as a trial feature in Q1 2012 package
- Sensor use under planning for a future release

The SUPL 2.0 protocol module uses the geofence task as of the GF2.0 Q3 2011 package. Benefits of this approach were made available to all applications via HLOS side APIs and customer APIs via the GF2.0 Q1 2012 package.

3.2 Geofence performance

Responsiveness describes how soon a device can recognize that it has entered or left a geofence. There is a delay tolerance for detecting a geofence breach compared to the time when the true breach occurred. The lower the responsiveness, the higher the probability for a missed geofence breach event and the user experience and the power consumed are lower. Valid values are low, med, and high.

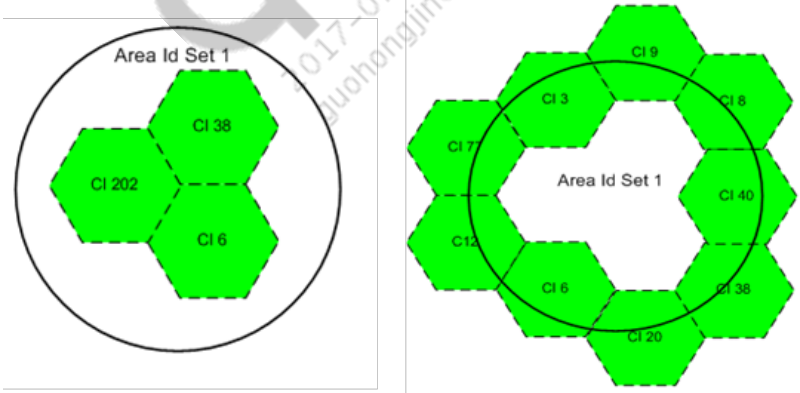
Confidence describes how accurate the detection is when entering and leaving an event for a geofence. Confidence affects the use of high-precision fix requests. The lower the confidence, the higher the probability for a false geofence breach and the user experience and the power consumed are lower. Valid values are low, med, and high.



3.3 Power optimization algorithms

Several algorithms are used to optimize power:

- Area ID-based power optimization determines when to perform position fixes and when to go dormant.



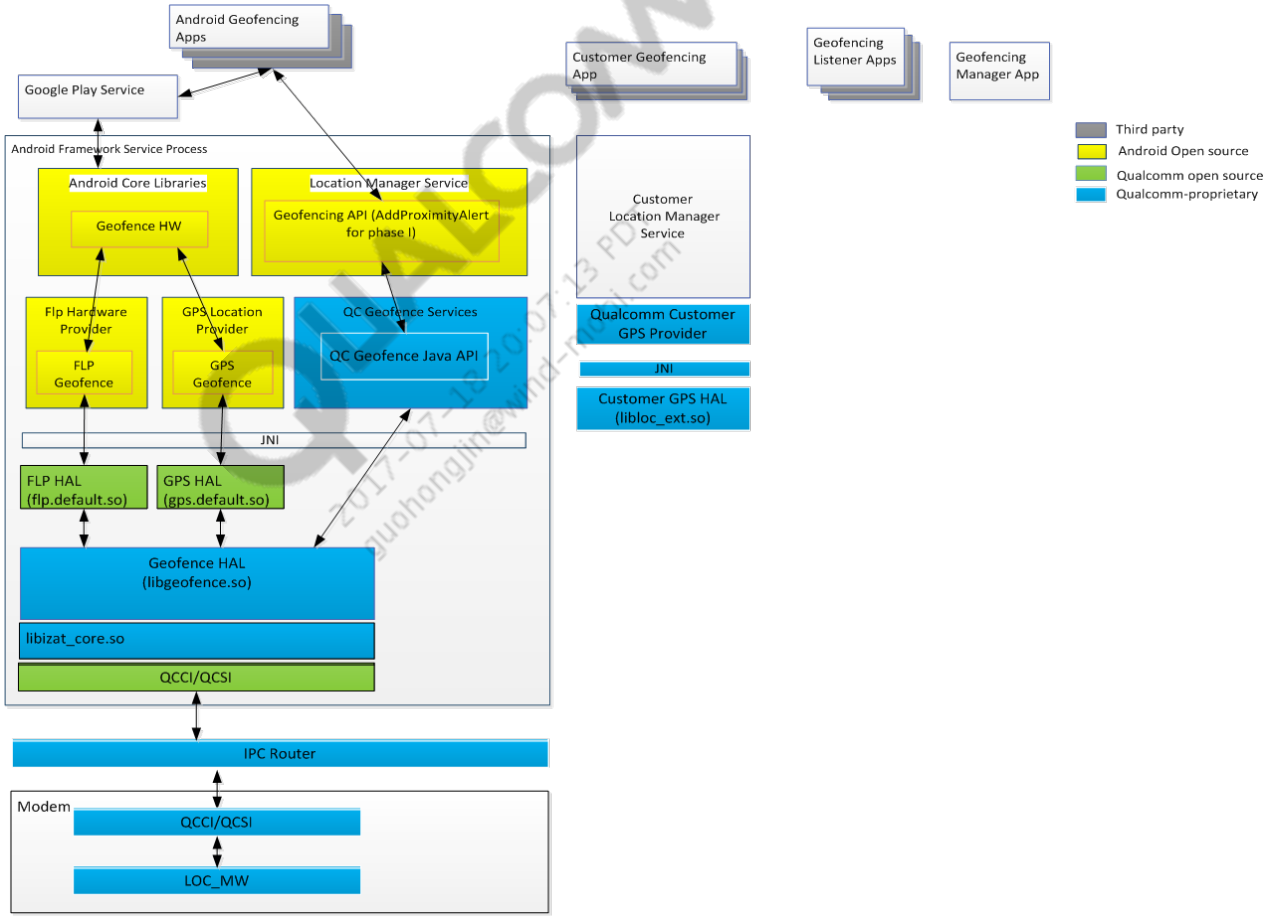
- Distance-based backoff calculates the rate of position fixes depending on the distance of the handset from the border of the geofence.
- Hysteresis handling uses hysteresis to avoid frequent breach reports when the handset is frequently criss-crossing across the border of the geofence.
- Handling challenging GPS environment performs exponential backoff when in a challenging GPS environment until it is detected that the handset has exited the challenging environment.
- DPO-based tracking saves power by detecting beneficial times to enter and exit DPO tracking. This algorithm uses the dynamic power optimization feature of the GNSS engine instead of doing single-shot fixes.

- Advanced distance-based backoff uses cell change events to gate the use of GNSS fixes.
- Motion detection using sensors, Wi-Fi, and WWAN uses sensors, Wi-Fi scan measurements/Wi-Fi events, and WWAN measurements for motion detection to reduce the number of GNSS fixes.
- Context-based backoff learns and uses Wi-Fi context to gate the use of GNSS fixes.

NOTE: For a future roadmap, see Section 2.2.

4 Geofence Android and Windows Phone architecture

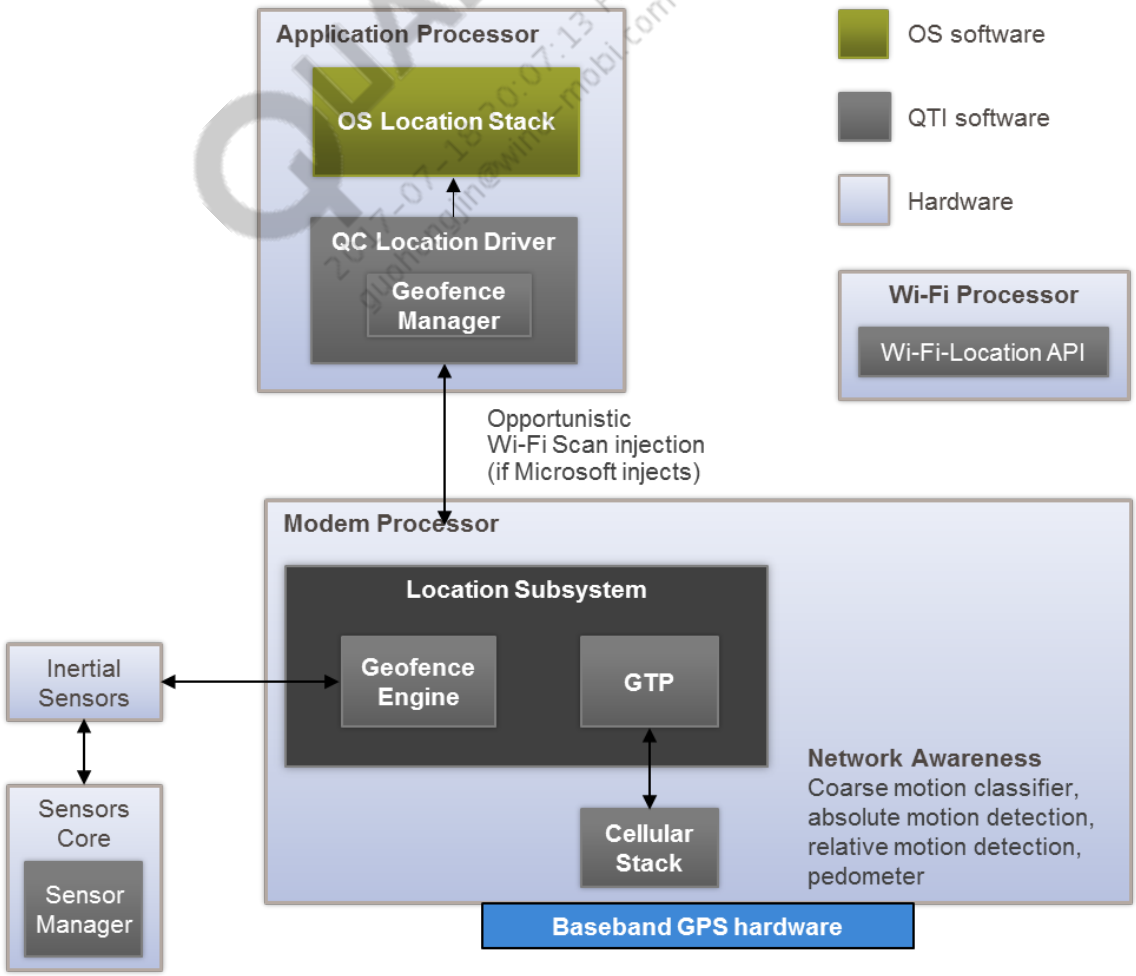
4.1 Geofence Android architecture



Geofence API options

Description	Control of geofence engine	Configurability of geofence parameters
Google Play Services/FLP Geofencing APIs	Partial control – Current Google Play Services/FLP implementation is to defer to IZat low-power geofencing, then take over servicing of geofence when IZat GF is unable to determine GF status; in the future, Android could adjust the “deferral logic”	Limited to Android API configuration options
Proximity Alert API	Full control – Geofences are fully run within IZat low-power Geofencing.	Limited to Android API configuration options
QMI-LOC	Full control – Geofences are fully run within IZat low-power geofencing.	Enhanced, including configurations for confidence and responsiveness; additional options might be possible in the future, for example, polygon

4.2 Geofence architecture on Windows Phone 8.1



5 Geofence 3.x

5.1 Geofence 3.0

Geofence 3.0 provides less power consumption using sensor and opportunistic Wi-Fi scan results (fewer GNSS-based position requests). It requires an enabled QTI SSC™ (Snapdragon™ Sensor Core) for low-power sensor (accelerometer-based) motion detection and needs a physical sensor (accelerometer) with FIFO buffering capability for optimal power savings.

Geofence 3.0 injects opportunistic, periodic Wi-Fi scans using a listener for Wi-Fi scans when the Access Point (AP) wakes up. Geofencing does not explicitly wake up the AP for these scans, and hence powerwise, these scans are free for geofencing.

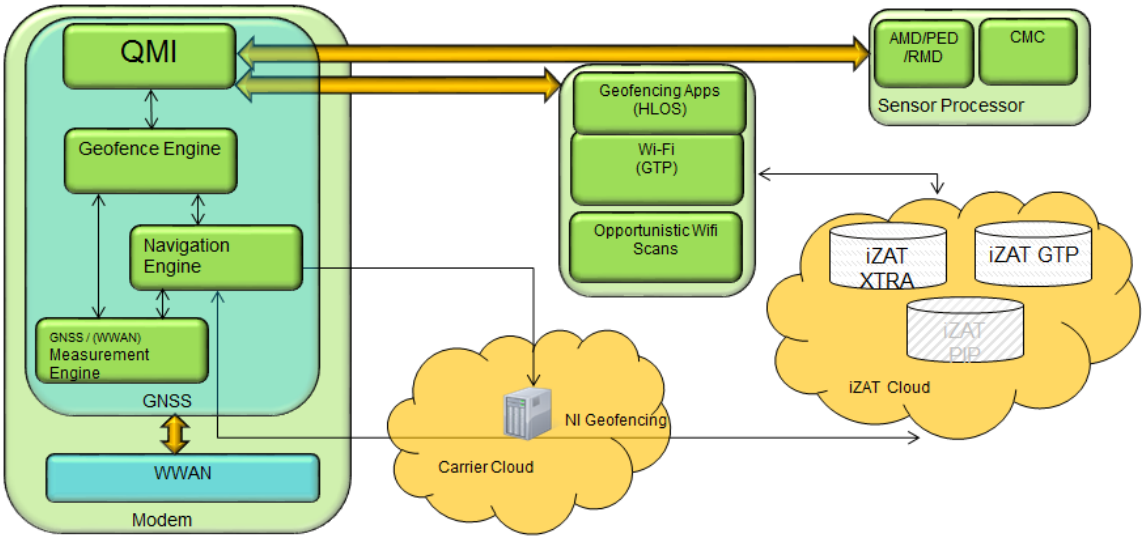
Geofence 3.0 includes ultrahigh responsiveness for applications requiring breach notifications with responsiveness of 1 sec or less. The geofence engine configuration uses sensors in geofencing and On Demand Coarse Position Injection (ODCPI) when GPS is unavailable.

For non-GPS fixes, Geofence 3.0 uses the following:

- GTP WWAN fixes
- Wi-Fi-based ODCPI fixes when GPS is not available

Higher power consumption is implied and hence, used only when GPS is not available; use of ODCPI is limited to gate power consumption.

Architecture



5.2 Geofence 3.0.1

Geofence 3.0.1 provides enhancements to improve breach latencies for high responsiveness geofence. It also provides better GNSS QoS management for power optimization, that is, it manages GNSS QoS requirement for a GNSS fix to bring in power optimization

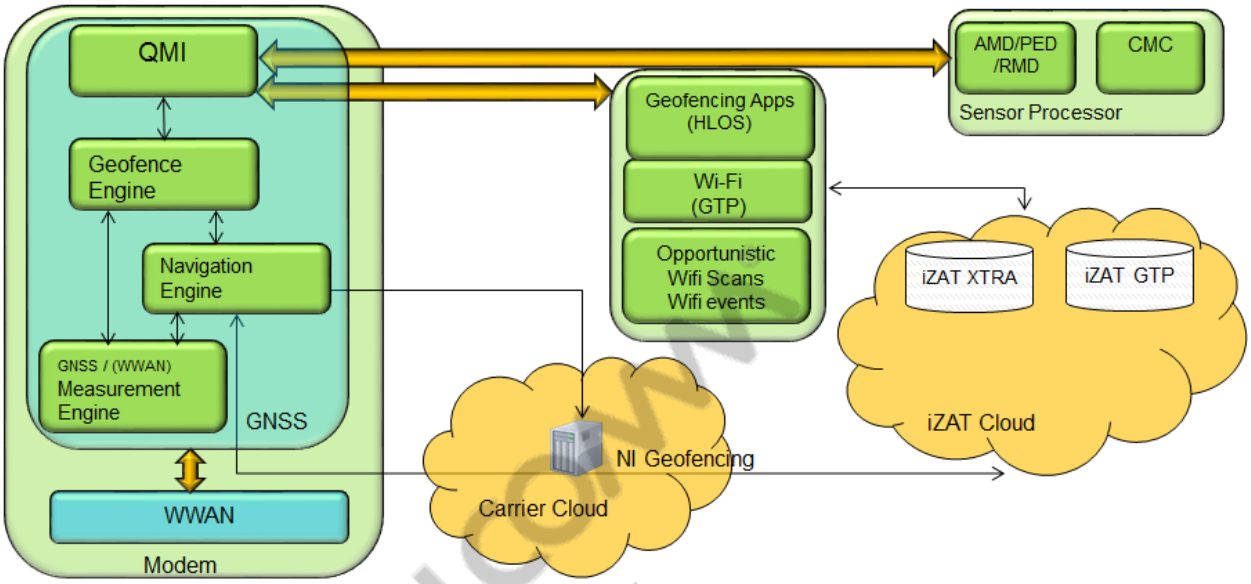
Geofence 3.0.1 allows configuration of various aspects of the geofencing engine through QMI and NV. See Chapter 6 for details.

5.3 Geofence 3.1

Geofence 3.1 includes many improvements:

- Enhanced Wi-Fi motion detection
- Better power and performance tradeoff using opportunistic Wi-Fi events from HLOS
- Support of Wi-Fi context
- Provides better responsiveness using Wi-Fi Context
- Future geofencing releases will support other contextual information
- Geofencing 3.1 stores the context in RAM and is deleted once the phone reboots
- WWAN motion classification
- Brings in power optimization using WWAN measurements; supported for LTE and WCDMA
- Proximity detection
- Brings in new capability to register indication for proximity to a geofence

Architecture



5.4 Geofence 3.3

Background engine enhancements supporting Geofence 3.3 are listed. Geofence 3.2 was an internal release with the architecture changes detailed in the following figure.

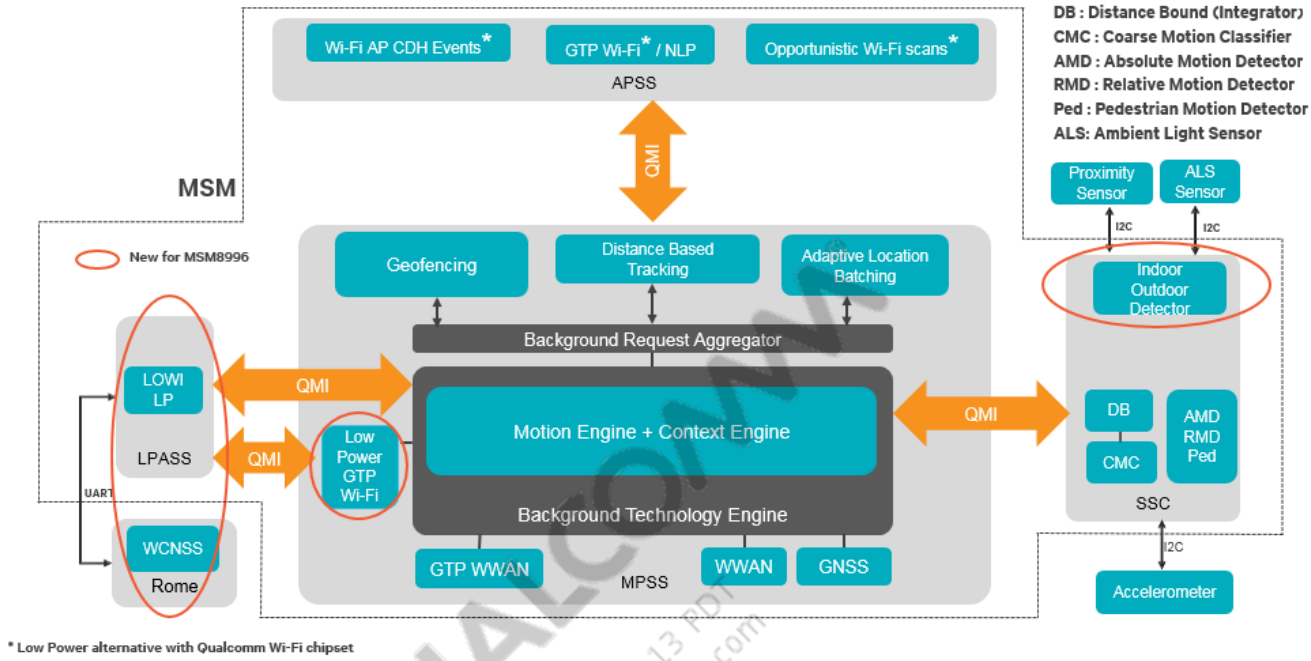
- Opportunistic/Snoop low power Wi-Fi discover scan – HLOS offload Wi-Fi discovery scans to the Wi-Fi processor in certain conditions. When scans are offloaded, no opportunistic scans are available from the application processor. Wi-Fi scans are used for motion detection purposes in the background engine and can result in significant energy savings by deferring the use of GNSS when there is limited motion.

  Android example – The AP offloads scans when the device is not associated with an AP (Wi-Fi is on). In this case, snoop scans are received every 10 to 18 sec in MPSS directly from WCNSS.

- Opportunistic low power GTP Wi-Fi positioning use – Background engine uses the low power GTP Wi-Fi fix whenever the fixes are made using opportunistic Wi-Fi discovery scans. The advantage is that it allows further deferring of the use of GNSS fixes when outdoors. When indoors, it provides increased positioning availability at low power, which helps in better responsiveness for geofences and higher availability for location batching.

- Ambient light sensor and proximity sensor based indoor outdoor detector – Low power mechanism to determine when the devices moves out from indoor (GNSS denied case) to outdoor (GNSS available case). This helps to provide better Geofence exit responsiveness and higher accuracy batching fixes at low power.

Architecture



6 Geofence configurations

6.1 Geofence GNSS position QoS session timeout

- NV item – 71563
- Default – 30 sec; the value can only be set between min 10 and max 40
- Description – This NV item is used by the geofencing engine as session timeout while requesting a GNSS fix. This NV item impacts power usage, as it can affect the engine on time for GNSS fixes requested for geofencing.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV: GNSS_POSITION_SESSION_TIMEOUT
- NV available from Geofencing 3.0

6.2 Geofence GNSS unavailable indication timeout

- NV item – 71555
- Default – 40 sec
- Description – This NV item is used by the geofencing engine as a timeout, after which it is required to send a GNSS Unavailable QMI indication to the client when under bad GNSS environment.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV: GNSS_UNAVAILABLE_INDICATION_TIMEOUT
- NV available from Geofencing 3.0

6.3 Geofence GNSS max position uncertainty accepted

- NV item – 72514
- Default – 100 m
- Description – This NV item is used to configure the maximum position uncertainty in the GNSS position fix accepted by the geofencing engine when detecting breaches. The position uncertainty value should be the 99% converted HEPE.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV: GNSS_POSITION_MAX_PUNC_ACCEPTABLE
- NV available from Geofencing 3.0

6.4 Geofence motion detection sources

- NV item – 71562
  - Bit 0 – Enable or disable sensors-based motion classification; default: 0 (disable)
  - Bit 1 – Enable or disable Wi-Fi-based motion detection; default: 1 (enable)
  - Bit 2 – Enable or disable WWAN-based motion classification; default: 1 (enable)
- Description – This NV item enables or disables different sources for motion classifications. When turning on sensor-based motion detection, OEMs must check whether the sensor in use supports FIFO. With FIFO support, OEMs can see geofencing power benefits.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV QMI_LOC_MOTION_DETECTION_SOURCE_MASK
  - QMI_LOC_MOTION_DETECTION_SOURCE_SENSORS
  - QMI_LOC_MOTION_DETECTION_SOURCE_WIFI
  - QMI_LOC_MOTION_DETECTION_SOURCE_WWAN
- NV available from Geofencing 3.0

NOTE: This NV item should be changed to disable all motion sensing while running SUPL Area-ID test cases on simulated test environment; for example, Spirent.

6.5 Geofence position sources

- NV item – 71573
  - Bit 0 – Enable or disable ODCPI
- Default
  - Geofencing 3.0 – 0 (disable)
  - Geofencing 3.1 and later – 1 (enable)
- Description – This NV item is used to configure position sources that geofencing can use.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV ENABLE_CPI_USAGE
- NV available from Geofencing 3.0

6.6 Geofence medium responsiveness backoff

- NV item – 72569
- Default – 120 sec
  - If the value is configured for less than 30 sec, the value is set at 30 sec
  - If the value is configured for more than 600 sec, the value is set at 600 sec
- Description – This NV item configures the responsiveness value in seconds that geofencing engine shall use for all medium responsiveness geofences.

- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV MEDIUM_RESPONSIVENESS_VALUE
- NV available from Geofencing 3.0.1

NOTE: If the medium responsiveness value is changed, the responsiveness of the existing medium responsiveness geofence does not change until the next position fix, which is based on the previous medium responsiveness setting.

6.7 Geofence CPI request rate

- NV item – 72559
- Default – 300 sec (5 min)
- Description – This NV item configures the minimum seconds geofencing engine shall wait between two Coarse Position Injection (CPI) requests. The requests are further gated by motion sensing.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV CHAL_GNSS_ENV_MIN_CPI_WAIT_INTERVAL
- NV available from Geofencing 3.0.1

6.8 Geofence challenging GPS environmental-based backoff

- NV item – 72570
- Default min – 30 sec
- Default max – 960 sec (16 min)
- Description – This NV item configures the behavior of GPS fix tries by the geofencing engine when a challenging GPS environment is detected.

  The geofencing engine follows an exponential backoff between GPS fix attempts when in a challenging GPS environment. The exponential backoff starts from the Challenging GPS Env Backoff Min value and doubles every time a GPS position fix fails, until the exponential backoff value reaches Challenging GPS Env Backoff Max, after which the exponential backoff stays at that value.
- QMI control – NA
- NV available from Geofencing 3.0.1

6.9 Geofence challenging GPS environmental motion sensing distance

- NV item – 72572
- Description – This NV item is used to configure the distance in meters that the geofencing engine shall accumulate for before trying a GNSS or CPI fix when in a challenging GPS environment.

- Motion sensing distance for CPI
  - Default – 50 m
  - Description – This is the minimum distance in meters that the geofencing engine should accumulate before trying another CPI fix when in a challenging GPS environment.
- Motion sensing distance for GPS
  - Default – 50 m
  - Description – This is the minimum distance in meters that the geofencing engine should accumulate before trying another GPS fix when in a challenging GPS environment.
- QMI control – NA
- NV available from Geofencing 3.0.1

6.10 Geofence motion state speed

- NV item – 72571
- Description – This NV item is used to configure the motion state speeds in meters per second that geofencing shall use during distance accumulation.
- Walk
  - Default – 3 m/s
  - Description – This is the speed in meters per second that the geofencing engine uses for accumulating distance when pedestrian walk motion is detected.
- Run
  - Default – 8 m/s
  - Description – This is the speed in meters per second that the geofencing engine uses for accumulating distance when pedestrian run motion is detected.
- QMI control – QMI_LOC_SET_GEOFENCE_ENGINE_CONFIG_REQ_MSG: Optional TLV QMI_LOC_GEOFENCE_MOTION_STATE_CONFIG_STRUCT
- NV available from Geofencing 3.0.1

6.11 Geofence use network-assisted fixes

- NV item – 72535
- Default – 0 (disabled)
- Description – This NV item is used to enable or disable the GM engine to use network-assisted fixes for breach detection. The network-assisted fixes include MSA, AFLT fixes, etc.
- QMI control – NA
- NV available from Geofencing 3.0.1

6.12 Geofence high responsiveness

- NV item – 72511
- Default – 1 (enabled)
- Description – This NV item is used to enable high responsiveness enhancement to improve breach detection latency at a cost of increased power when near the geofence boundary and when handset is detected entering the geofence.
- QMI control – NA
- NV available from Geofencing 3.0.1

6.13 Geofencing LOWI registration enable

- NV item – 73652
- Default value – 1
- Description – This NV item is used to register geofencing as a client to LOWI service on LPASS. Geofencing uses the LOWI LP for Wi-Fi scans, connect, disconnect, or handover events, etc.
- QMI control – NA
- NV available from Geofencing 3.3

6.14 Geofencing LOWI subscription mask

- NV item – 73653
- Default value – 0x1
- Description – This NV item is used to subscribe to different services supported on LOWI LP. Currently subscribed to snoop scans from LOWI only. But there are other services supported on LOWI as well such as discovery scans, Wi-Fi connect, disconnect, or handover events, etc., which could be used in the future.
  - Value
    - Bit 0 – Register for snoop scans from LOWI
- QMI control – NA
- NV available from Geofencing 3.3

6.15 Geofencing LOWI registration config

- NV item – 73654
- Default value – 0x1
- Description – This NV is used to configure how GM registers with LOWI service on LPASS.
- NV available from Geofencing 3.3

- This NV has two fields:
  - Enable timer mask
    - Range – 0 – 0xFFFFFFFF
    - Value
      - Bit 0: Enable short-term retry timer
      - Bit 1 – Enable long-term retry timer
      - Default value – 0x3
    - Description – If the LOWI registration fails from GM, this NV is used to configure how to retry the re-registration attempts with LOWI. There are two timers for this purpose:
      - Short-term retry timer – This timer tries aggressively for retries configured by NV with a periodicity of 10 sec between the retries
      - Long-term retry timer – When this timer is enabled , if the short-term registration retries fail, this timer tries less aggressively for LOWI registration. The periodicity is not configurable.
      - QMI control – NA
  - Short-term timer max retry count
    - Range – 0 to 50
    - Units – NA
    - Default value – 12
    - Description – Short-term retry timer uses the configured value to try LOWI registration retries
    - QMI control – NA

6.16 Geofencing filter WLAN frequencies mask

- NV item – 73722
- Default value – 0x1
- Description – This NV is used to filter and accept the requested WLAN frequencies by GM and filter out the remaining ones. The WLAN frequencies may be injected from HLOS, LOWI, or other capable sources.
- Value
  - 0 – Disable GM filtering of WLAN frequencies. Accept all frequencies. No filtering. This value should not be used.
  - 0x1 – Enable GM filtering and accept 2.4 GHz band from the WLAN frequencies
  - 0x2 – Enable GM filtering and accept 5 GHz band from the WLAN frequencies
- QMI control – NA
- NV available from Geofencing 3.3

6.17 Geofencing indoor outdoor sensor configuration switches mask

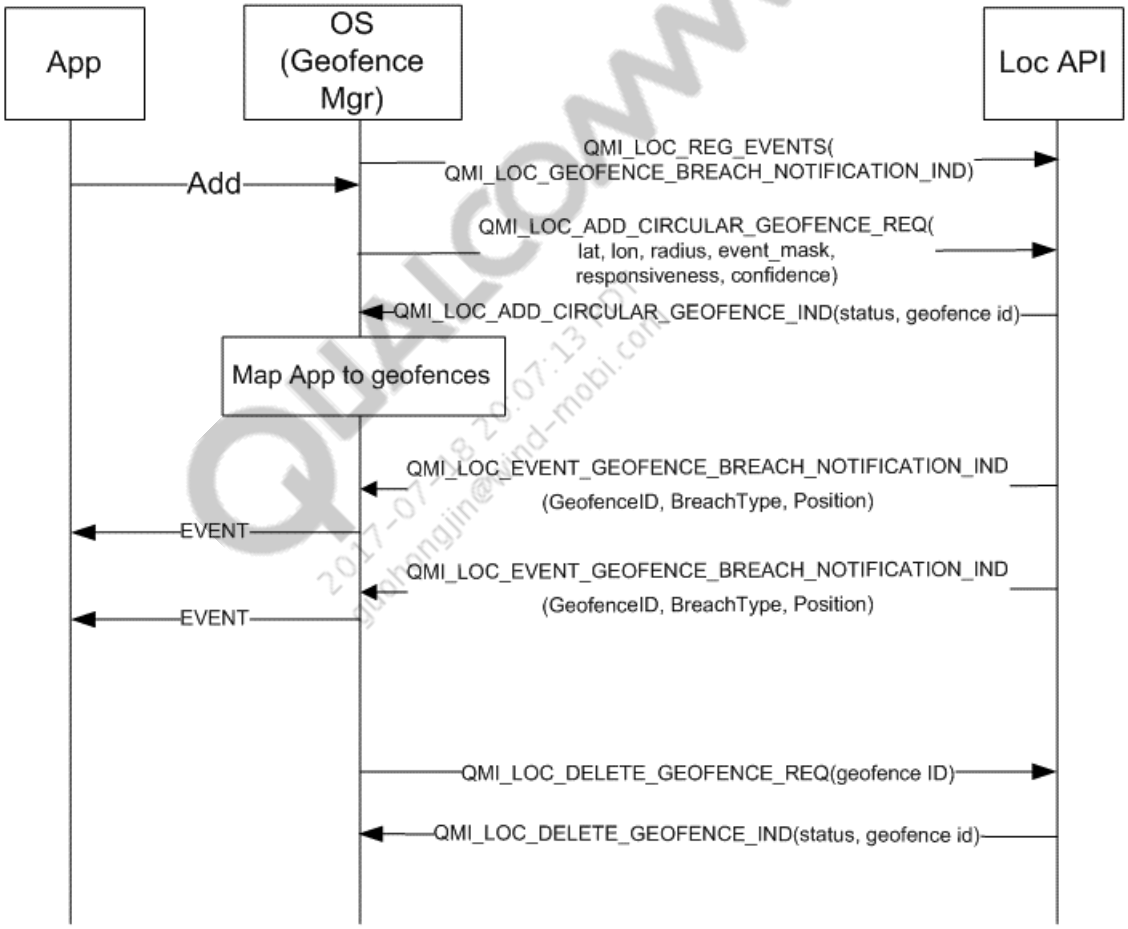
- NV item – 73692
- Default value – 0x0 (disabled)

Description – This NV item is a bit mask used to set configuration switches for geofencing indoor outdoor detection feature. A bit value of 1 is treated as on and a bit value of 0 is treated as off.

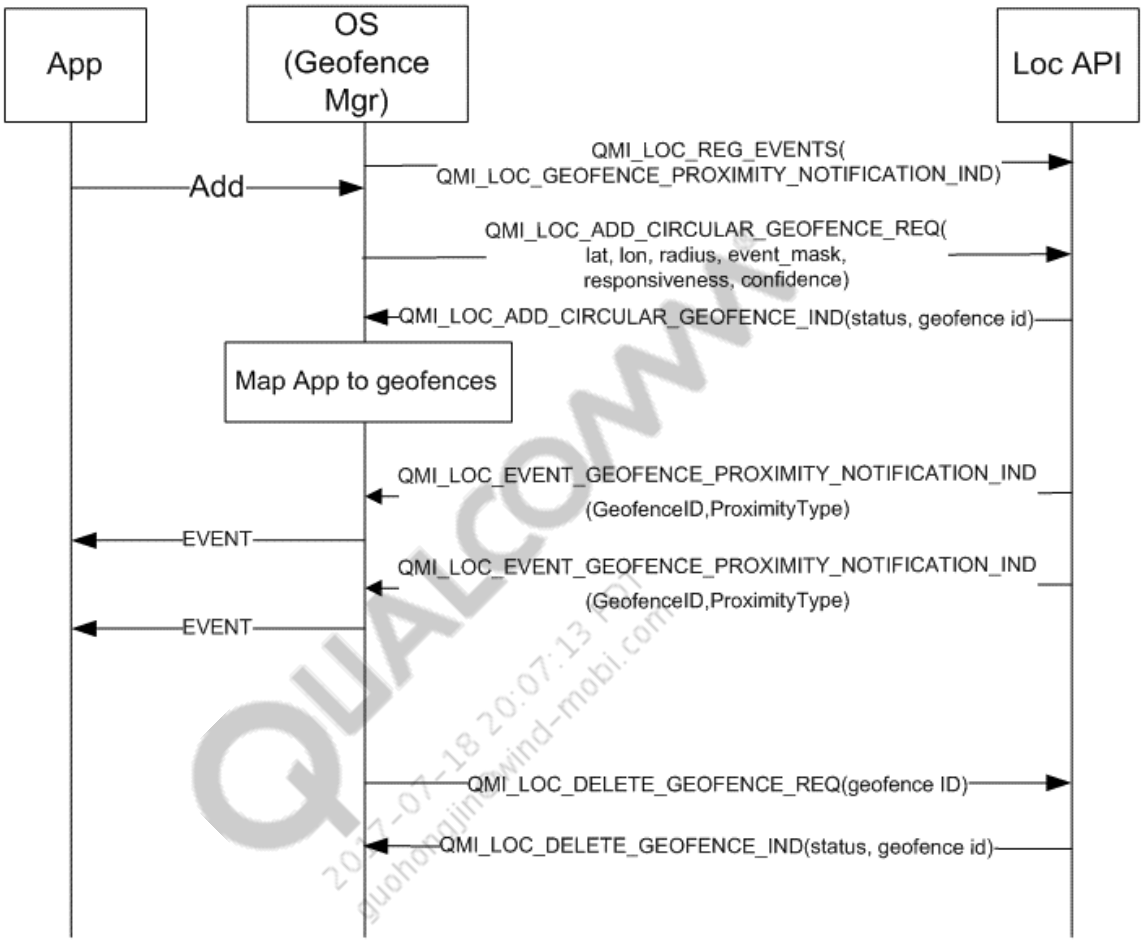
- Value
  - 0x0 – Disable the ambient light sensor-based indoor outdoor detection
  - 0x1– Enable the ambient light sensor-based indoor outdoor detection
- NV available from Geofencing 3.3

7 API and call flows

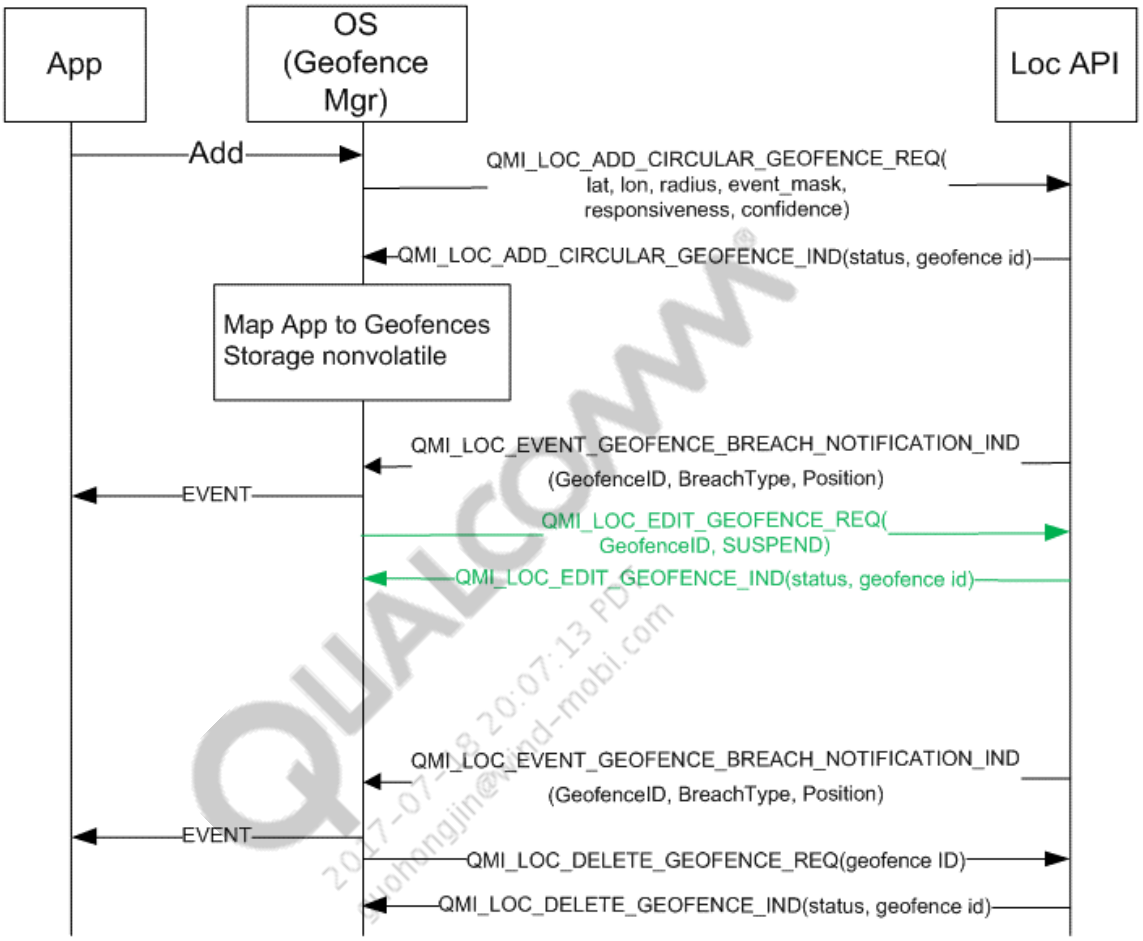
7.1 Add, delete, and geofence breach indication



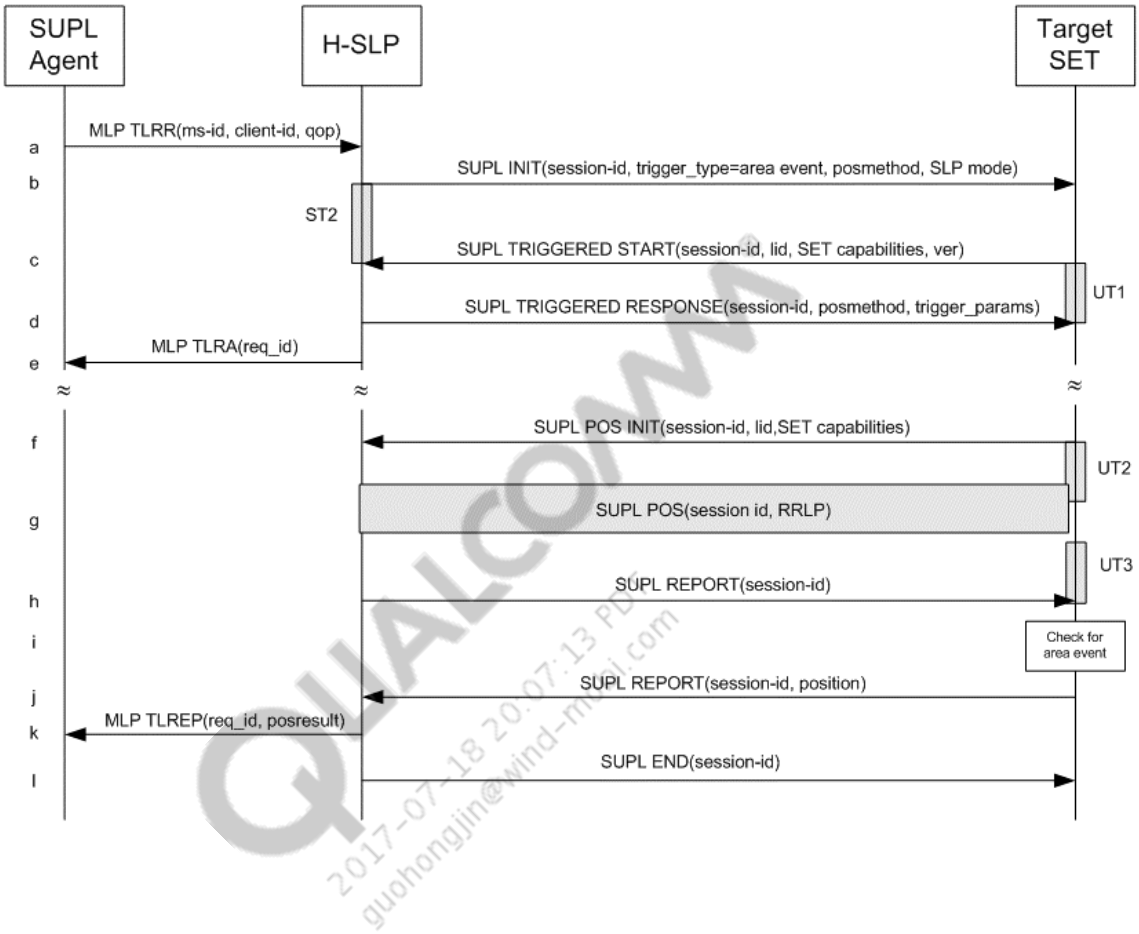
7.2 Add, delete, and geofence proximity indication



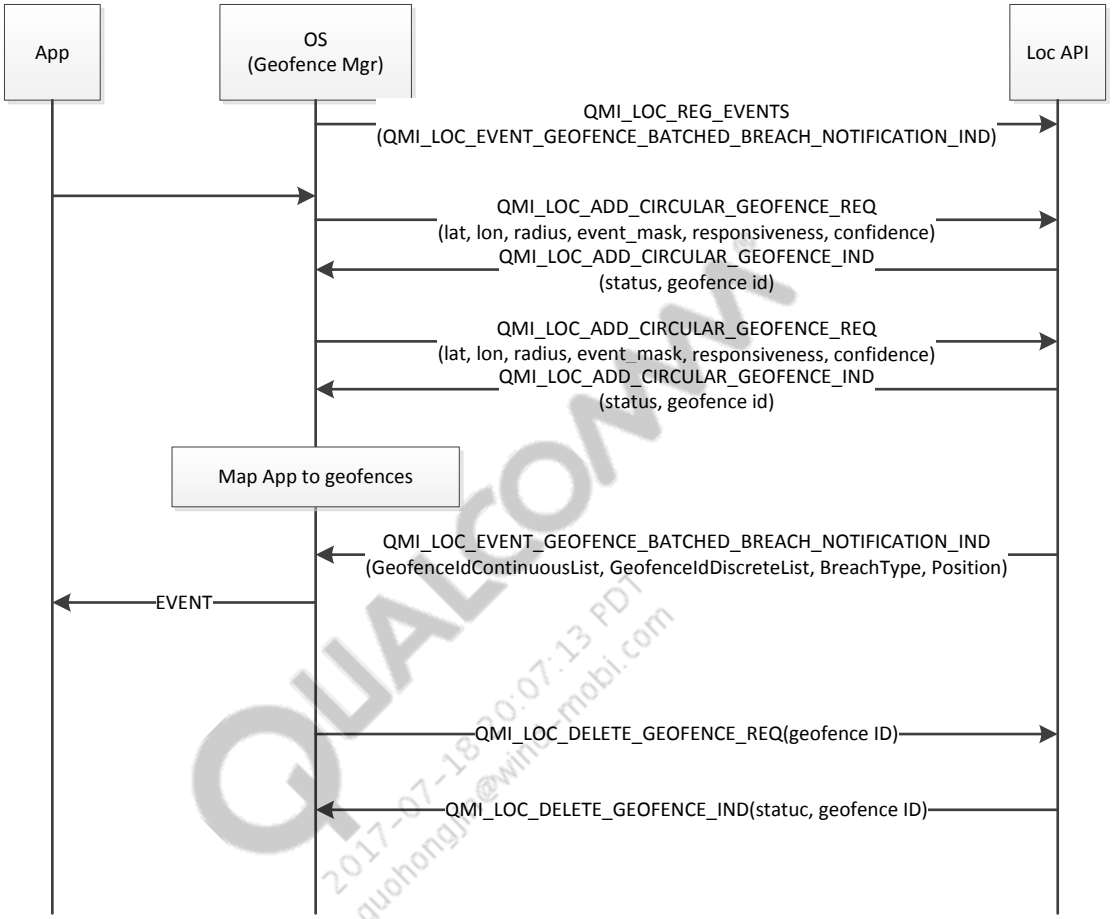
7.3 Edit a geofence



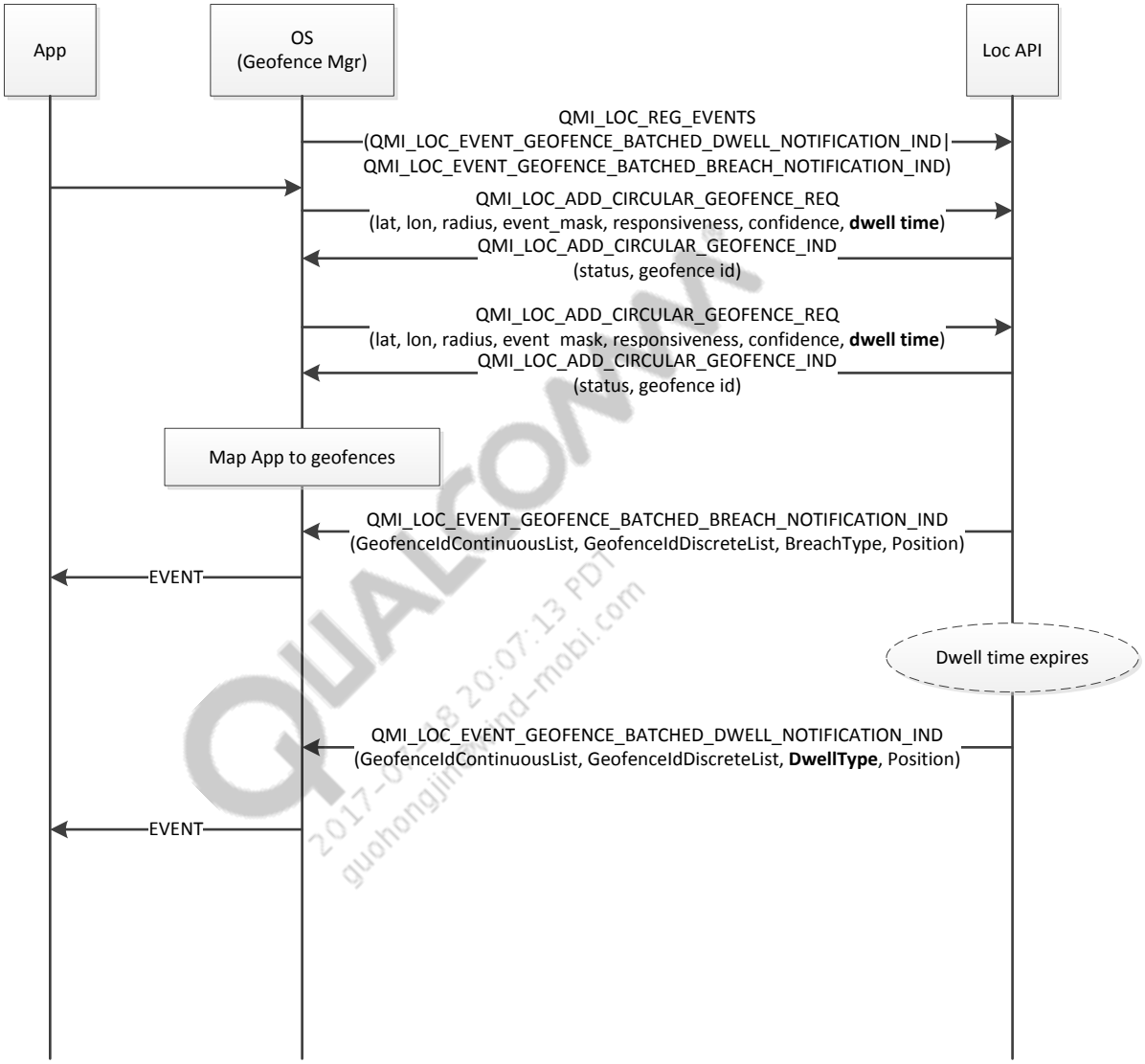
7.4 SUPL2.0 NI geofence implementation



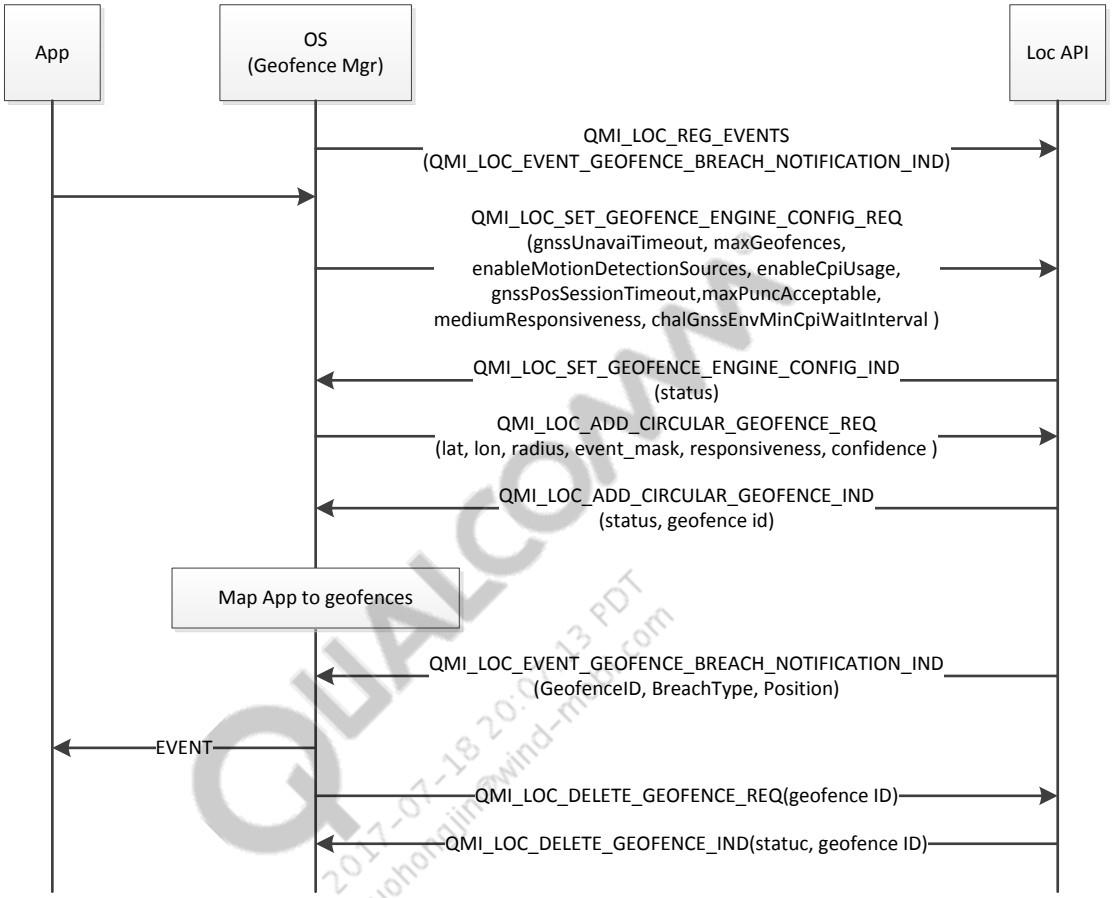
7.5 Geofence batch breach notification



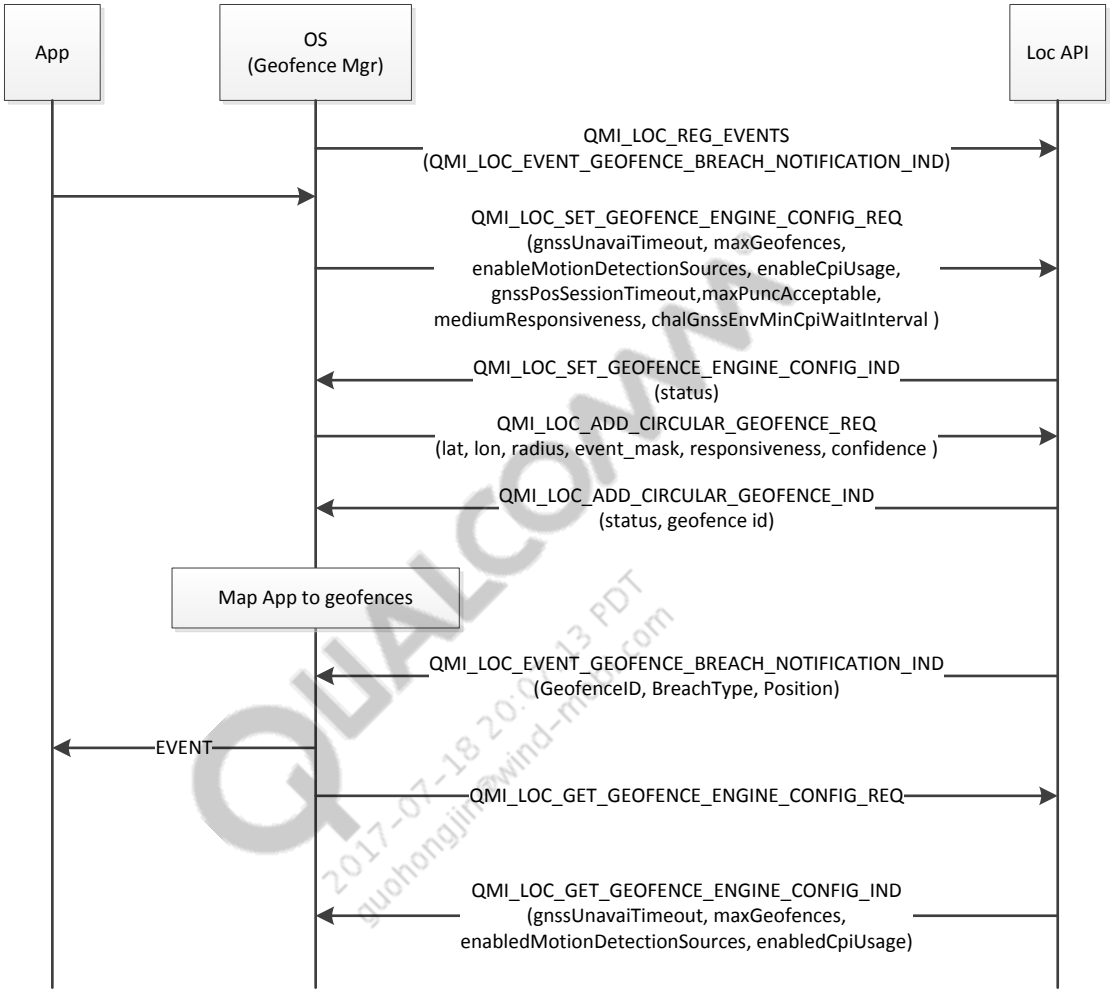
7.6 Geofence batch dwell notification



7.7 Set geofence engine configuration



7.8 Get geofence engine configuration



7.9 Geofence API details

Commands	Request	Response (indication)
QMI_LOC_ADD_CIRCULAR_GEOFENCE	▪ Lat, long, radius ▪ event_mask ▪ Responsiveness ▪ Confidence	▪ Status ▪ Geofence ID
QMI_LOC_QUERY_GEOFENCE	▪ Geofence ID	▪ Origin – Network, device ▪ PositionWrtGeofence – Inside, outside ▪ Geofence parameters – Lat, long, radius ▪ State (active/suspend)

Commands	Request	Response (indication)
QMI_LOC_EDIT_GEOFENCE_REQ	▪ Geofence ID ▪ State (Active/Suspend) ▪ Breach mask – Entering, leaving	▪ Geofence ID ▪ Status ▪ Failed parameters
QMI_LOC_GET_GEOFENCE_LIST		▪ Status ▪ List of geofences
QMI_LOC_SET_GEOFENCE_ENGINE_ CONFIG_REQ	▪ Status ▪ GNSS unavailable indication timeout ▪ Max geofences to be programmed ▪ Motion detection sources to be enabled ▪ Enable/Disable CPI usage ▪ GNSS position session timeout ▪ GNSS max punc acceptable ▪ Medium responsiveness value of geofences ▪ Challenged GNSS environment minimum CPI wait interval ▪ Set motion state speed for different motion states	▪ Status
QMI_LOC_GET_GEOFENCE_ENGINE_ CONFIG_REQ	▪ Transaction ID	▪ Status ▪ GNSS Unavailable Indication Timeout ▪ Max geofences programmed ▪ Enabled motion detection sources ▪ Status of CPI usage

Notifications	Values
EVENT_GEOFENCE_BREACH_NOTIFICATION	▪ GEOFENCE_BREACH_TYPE_ENTERING ▪ GEOFENCE_BREACH_TYPE_LEAVING
EVENT_GEOFENCE_PROXIMITY_NOTIFICATION	▪ GEOFENCE_PROXIMITY_TYPE_IN ▪ GEOFENCE_PROXIMITY_TYPE_OUT

Notifications	Values
EVENT_NI_GEOFENCE_NOTIFICATION	▪ ADDED ▪ DELETED ▪ EDITED
EVENT_GEOFENCE_GEN_ALERT_IND	▪ GEOFENCE_GEN_ALERT_GNSS_ UNAVAILABLE ▪ GEOFENCE_GEN_ALERT_GNSS_ AVAILABLE ▪ GEOFENCE_GEN_ALERT_OOS ▪ GEOFENCE_GEN_ALERT_TIME_INVALID
EVENT_GEOFENCE_BATCHED_BREACH_NOTIFICATION_ IND	▪ GEOFENCE_BREACH_TYPE_ENTERING ▪ GEOFENCE_BREACH_TYPE_LEAVING ▪ GEOFENCE ID CONTINUOUS LIST ▪ GEOFENCE ID DISCRETE LIST
EVENT_GEOFENCE_BATCHED_DWELL_NOTIFICATION_ IND	▪ GEOFENCE_DWELL_TYPE_ENTERING ▪ GEOFENCE_DWELL_TYPE_LEAVING ▪ GEOFENCE ID CONTINUOUS LIST ▪ GEOFENCE ID DISCRETE LIST

A References

A.1 Related documents

Title	Number
Qualcomm Technologies, Inc.	
Optimized Geofence Management on Qualcomm Platforms	80-NB607-1

A.2 Acronyms and terms

Acronym or term	Definition
AP	Access Point
CPI	Coarse Position Injection
MO	Mobile-Originated
MT	Mobile-Terminated
ODCPI	On Demand Coarse Position Injection
SSC	Snapdragon™ Sensor Core