Device Apps Network Efficiency Requirements

Candidate Version 1.0 – 07 May 2013

Open Mobile Alliance

OMA-RD-DANE-V1_0-20130507-C

Contents

Figures

Tables

1. Scope (Informative)

This document defines the requirements for the OMA Device Apps Network Efficiency (DANE) Enabler V1.0.

The aim of the OMA DANE V1.0 RD is to define requirements for supporting the following:

- Definition of a set of Device APIs to be exposed to Device Apps by a Device Service Optimizer; through those APIs authorized Apps will register to the DSO declaring their needs in terms of QoS, tolerance to delay etc.;
- Definition of mapping rules (applied by the Device Service Optimizer) between Apps requesting a particular QoS, the related IP flows and network interfaces on Device.

OMA DANE V1.0 RD includes also requirements for future releases of DANE Enabler:

- Definition of a solution identifying all Apps present on the device and their impacts on the network in terms of signalisation and shaping the signalling traffic they generate based on categorisation.

2. References

2.1 Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[3GPP TS 23.203] "Policy and charging control architecture", 3rd Generation Partnership Project (3GPP), URL/http://www.3gpp.org/ftp/Specs/archive/23_series/23.203/

[3GPP TS 23.207] "End-to-end Quality of Service (QoS) concept and architecture", 3rd Generation Partnership Project (3GPP), URL:http://www.3gpp.org/ftp/Specs/archive/23_series/23.207/

[3GPP TS 29.213] "Policy and Charging Control signalling flows and QoS parameter mapping", 3rd Generation Partnership Project (3GPP), URL:http://www.3gpp.org/ftp/Specs/archive/29_series/29.213/

[DMPRO] "OMA Device Management Protocol", Version 1.3. Open Mobile Alliance™. OMA-TS-DM_Protocol-V1_3, URL:http://www.openmobilealliance.org/

[DMARCH] "OMA Device Management Architecture", Version 1.3, Open Mobile Alliance™ OMA-AD-DM-V1_3, URL:http://www.openmobilealliance.org/

[OpenCMAPI] "OMA OpenCMAPI", Version 1.0. Open Mobile Alliance™, OMA-TS-OpenCMAPI-V1_0-20120619-C, URL: http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.9, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_9, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Device App	An application running in the device that uses device/network resources
Device Service Optimizer	An entity residing in the device, managing the interaction between Device Apps and device/network resources
PCRF	See [3GPP TS 23.203]

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
App	Application
DM	Device Management
DSO	Device Service Optimizer
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GBR	Guaranteed Bit Rate
IP	Internet Protocol
OMA	Open Mobile Alliance
PCRF	Policy and Charging Rules Function
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RN_API	Apps Registration and Events Notification API
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity

4. Introduction (Informative)

Smartphones and Tablets Devices have completely reshaped the nature of Mobile Services, having become the drivers of the industry growth: Devices and their ecosystem (on-line Stores) offer thousands of Services, in the form of Apps running on such popular Terminals. Device owners (and then the Mobile Customers) tend to install and use many Apps, but Apps are very often unable to take advantage of Network resources/capabilities Providers can offer

Apps' behaviour, with respect to Wireless Network capabilities exploitation, is often not rational and left to chance, resulting in less Apps' quality, less Customers satisfaction and waste of wireless resources

In this context, OMA DANE Enabler is a Device enabler in charge to optimize Device Apps QoE, exposing relevant Device APIs and collaborating with Wireless Networks Policy Managers.

Moreover as many apps are not optimized and are strongly impacting cellular networks in particular signalling, future release of OMA DANE Enabler will deal with all aspects related to Network Efficiency and impacts of Apps on the signalisation by identifying all applications, classifying them in categories and will apply mechanisms to reduce the impacts of these applications on the network saving consequently significant battery life of the device.

4.1 Version 1.0

This document defines the requirements for the OMA Device Apps Network Efficiency (DANE) Enabler Version 1.0, defining:

- Apps Registration and Events Notification API (API to be exposed by the DANE "Device Service Optimizer", i.e., a component running on Devices and offering the whole set of DANE functionalities; such API shall be consumed by authorized Device Apps);
- The DSO behaviour to respond accordingly upon reception of a request from Device Apps through specific APIs;
- How the DSO requires a dedicated bearer to the network, i.e., the DSO will interact with the 3GPP PCRF (through Rx interface or through a more generic QoS API exposed by the Mobile Network) in order to establish a dedicated bearer for the Device and in particular for a specific IP flow; in case of non-3GPP access, the interaction may be towards an alternative Policy Manager;
- DSO Measurements functionality and the Events Notification side of the API: when a Device App performs a successful registration to the DSO (through the Apps Registration and Events Notification API), the App also subscribes to "QoS level change" Event Notification;
- Policies to manage requests from Device Apps.

4.2 Future Version

After version 1.0, future version of the DANE Enabler will address the following aspects:

- Identification of the applications present on the device, classification in lists organized by different categories or profiles defined accordingly to their impacts on the network signalisation and management of these lists.
- Shaping of network signalisation traffic of the Apps present (per Apps or per category).

5. Device Apps Network Efficiency release description (Informative)

The core of DANE will be the Device Service Optimizer (DSO), as shown in Figure 1. Authorized Apps (running in the device) will interact with the DSO through a set of Device APIs in order to (for example):

- Get assigned a premium/real-time QoS;
- Indicate the preferred access network (Wi-Fi, 3GPP, …);
- Indicate how many IP flows the App is going to request;
- Indicate the delay the App may manage (e.g., for the second IP flow the App is delay-tolerant up to 15min).

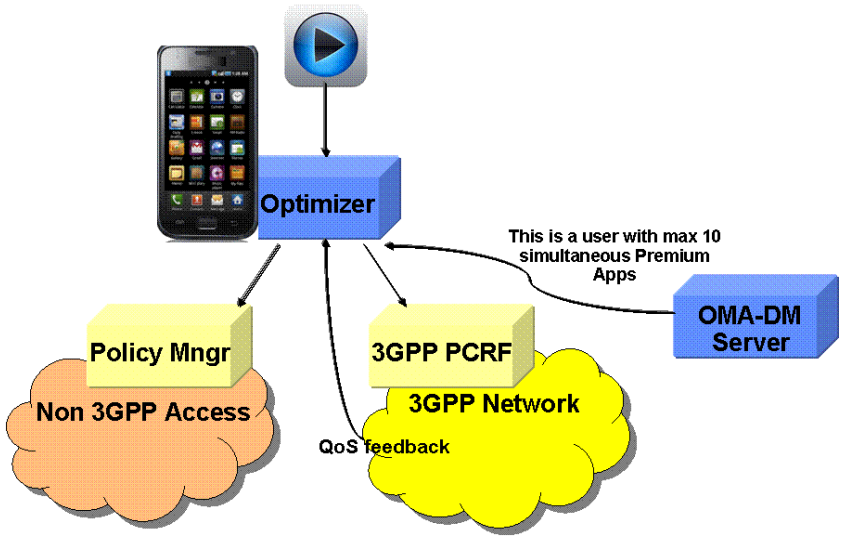

Figure 1: High level architecture for the DANE Enabler

Having received the request of an authorized App through the Device APIs, the DSO will react consequently to what is declared in such request. As shown in the figure, in case of 3GPP network, the DSO will interact with the 3GPP PCRF (through Rx interface or through a more generic QoS API exposed by the Mobile Network) in order to establish a dedicated bearer for the Device and in particular for a specific IP flow; in case of non-3GPP network, DSO behaviour to interact with the QoS Policy Management is for further study.

Even though an App can possess valid credentials and be able to contact the DSO through the Device APIs, does not mean that all the requests from that App will be granted by the DSO. A policy will regulate, for instance, how many simultaneous highest QoS levels the Device (i.e., the DSO) can successfully request to the Network and if that number is exceeded then the latest App request will be denied with a consistent reason field. The policy mentioned in this example may be formalized as an OMA-DM Management Object and received from the DSO by a remote OMA-DM Server (see [DMARCH]) managed by the Mobile Operator.

5.1 End-to-end Service Description

The DANE Enabler is aimed to deliver to market a reference solution to let Device Apps be more efficient in the usage of Network resources, while satisfying Customers' needs for increased QoE. It will provide to Apps Developers a simple way to increase Apps performances. The benefits of such mechanism, implemented accordingly to the OMA DANE, are for all involved players:

- Customers:
    - Device Apps have higher performances and reliability

  - Better Battery life

- Applications Developers
  - Developers will not have to worry about how the Apps will interact with the mobile network QoS. The DSO will ensure a proper functioning accordingly to the QoS mechanism available from the network.
- Device and OS Vendors
  - Apps compliant to DANE Enabler will take advantage of available QoS enhancing capabilities from the network through an API exposed by the DSO.
- Operators
  - Operators will benefit from the fair use of network resources by all Apps on Devices.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Release
DANE-HLF-001	The DANE Enabler SHALL include a Device Service Optimizer (DSO). Note: The role of the DSO may be revisited during the architecture and technical specs design.	1.0
DANE-HLF-002	The DANE Enabler SHALL support Apps Registration and Events Notification.	1.0
DANE-HLF-003	The DANE Enabler SHALL support QoS measurements and events notification.	1.0
DANE-HLF-004	The DANE Enabler SHALL, at minimum, support DSO interaction with the PCRF, where applicable.	1.0
DANE-HLF-005	The DANE Enabler SHALL support policy regulating DSO behaviour.	1.0
DANE-HLF-006	The DANE Enabler SHALL be able to support identification and classification in a list of the applications present on the device and the management of the list. **Informational Note:** The required functionality of this requirement is as specified in requirements listed in section 6.7	For Future Release
DANE-HLF-007	The DANE Enabler SHALL be able to manage the impacts in terms of signalisation of the Apps present. **Informational Note:** The required functionality of this requirement is as specified in requirements listed in section 6.8	For Future Release

Table 1: High-Level Functional Requirements

6.1.1 Security

6.1.1.1 Authentication

Label	Description	Release
DANE-ATH-001	The DANE Enabler SHALL support a mechanism to authenticate Device Apps	1.0
DANE-ATH-002	The DSO MAY support digital certificate as credential to authenticate Device Apps. Informational Note: The role of DSO may be revisited during the architecture phase.	1.0

Table 2: High-Level Functional Requirements - Authentication Items

6.1.1.2 Authorization

Label	Description	Release
DANE-ATZ-001	The DANE Enabler SHALL support a mechanism to authorize Device Apps to consume the RN_API	1.0
DANE-ATZ-002	The DANE Enabler MAY support the authorisation of the device user (e.g., through the device User Interface) to use the Applications Network Efficiency mechanism including the analysis of data.	For Future Release

Table 3: High-Level Functional Requirements - Authorization Items

6.1.1.3 Data Integrity

Label	Description	Release
DANE-DIN-001	The DANE Enabler SHALL support data integrity for all data transferred from the Device Apps to the DSO, and vice versa.	1.0

Table 4: High-Level Functional Requirements - Data Integrity Items

6.1.1.4 Confidentiality

Label	Description	Release
DANE-CON-001	The DANE Enabler SHALL support data confidentiality that ensures information transferred from the Device Apps to the DSO, and vice versa, is not made available or disclosed to any unauthorised entity, or process.	1.0
DANE-CON-002	The DANE Enabler SHALL support data confidentiality (including for any statistics collected), as applicable.	1.0

Table 5: High-Level Functional Requirements - Confidentiality Items

6.2 Apps Registration and Events Notification API Requirements

Label	Description	Release
DANE-RN_API-001	The DSO SHALL expose a Device API (referred to as "Apps Registration and Events Notification API", RN_API), to be used by authorized Apps running on the Device.	1.0
DANE-RN_API-002	The DSO SHALL support receiving registration requests from Device Apps aiming at exploiting the RN_API.	1.0
DANE-RN_API-003	The DSO SHALL be able to recognize and manage, in a registration request from a Device App, some specific relevant parameters, at minimum (refer to [3GPP TS 23.203], [3GPP TS 23.207], [3GPP TS 29.213]): • an identifier of the Device App requesting the registration • and for each IP flow that will be generated by the Device App requesting the registration: o an identifier of the IP flow (unique on a per Device App basis); o the destination URL; o the QoS level requested for the IP flow, as one of the following parameters: ▪ "GBR_ConversationalVoice" ▪ "GBR_ConversationalVideo" ▪ "GBR_RealTimeGaming" ▪ "GBR_BufferedStreaming" ▪ "Non-GBR_Signaling" ▪ "Non-GBR_TCP-based" o the preference for Wi-Fi connection (Boolean parameter); o the tolerance to postponed connection to target Server (parameter expressed in minutes); o the shaping method, as one of the following parameters: ▪ "Push Server" ▪ "Network Socket Request Manager" ▪ "Other".	1.0
DANE-RN_API-004	The DSO SHALL be able to respond (accept/reject) to Device Apps registration request based on Service Provider's policy (e.g., number of registered Apps, IP flows and related QoS levels)	1.0
DANE-RN_API-005	The DSO SHALL respond with an error condition (or otherwise negative, or non-supportive) indication to any requests received from a Device App that is non-authorised. **Informational Note**: The role of DSO may be revisited during the architecture and technical specs design.	1.0

Table 6: Apps Registration and Events Notification API Requirements.

6.3 Device Service Optimizer Functional Requirements

Label	Description	Release
DANE-DSO-001	Whenever receiving a registration request from an authorized Device App (and such request satisfies Service Provider's policy), the DSO SHALL be able to manage the IP flows through: • the Wi-Fi module of the device, if the preference for Wi-Fi connection (Boolean parameter) was indicated in the registration request and a Wi-Fi connection is available; • the 3GPP module of the device, if the preference for Wi-Fi connection (Boolean parameter) was not indicated in the registration request. **Note**: In case there is a connection manager (such as, the OMA OpenCMAPI Enabler [OpenCMAPI]) implemented on the device, care must be taken to manage any conflicting control conditions (i.e., IP flows, etc.) and ensure compatibility.	1.0
DANE-DSO-002	For IP flows to be managed through the 3GPP module of the device, the DSO SHALL associate an IP flow to an already established bearer if and only if such bearer satisfies the QoS level indicated by the Device App in the registration request for that IP flow.	1.0
DANE-DSO-003	For IP flow to be managed through the 3GPP module of the device, if there is no established bearer with the requested QoS level, the DSO SHALL interact with the appropriate network element (e.g., trigger the 3GPP Network PCRF, using a QoS API) in order to establish a dedicated bearer for the device and in particular for that IP flow ([3GPP TS 23.203], [3GPP TS 29.213]).	1.0
DANE-DSO-004	The DSO MAY be responsible of mapping IP flows to dedicated bearers for uplink traffic ([3GPP TS 23.203]).	1.0

Table 7: Device Service Optimizer Functional Requirements.

6.4 QoS Measurements and Events Notification Requirements

Label	Description	Release
DANE-ME&N-001	The DSO SHALL be able to retrieve information about the actual QoS level (e.g., one-way delay, jitter, packet loss) for each IP flow specified in an authorized App's registration request,	1.0
DANE-ME&N-002	The DSO SHALL be able to notify the registered Apps at least of the following event: • The actual QoS level (cfr. DANE-ME&N-001) of one or more IP flows is lower than the one requested by the registered App; • In case no QoS mechanism is available from the network, the DSO SHALL respond "The network cannot satisfy the request for a specific QoS".	1.0

Table 8: Measurements and Events Notification Requirements.

6.5 DSO-PCRF Interface Requirements

Label	Description	Release
DANE-PCRFint-001	If the DSO detects to have to establish a new dedicated bearer (cfr. DANE-DSO-003), then it SHALL send to Network PCRF a request containing at least the following parameters ([3GPP TS 23.203], [3GPP TS 29.213]): • Mobile user ID • one or more IP flows sockets • the desired QoS level for each IP flow Note: DSO support of non-3GPP PCRF QoS mechanisms (such as, in Wi-Fi QoS and other schemes) is for further study. Specific proposals addressing non-3GPP QoS mechanisms may be proposed during the architecture and technical specs design. In case there are no QoS mechanisms available, the Device App shall work normally accordingly to its design (i.e., without the benefit of any optimization by the 3GPP PCRF).	1.0

Table 9: DSO-PCRF Interface Requirements.

6.6 Policy regulating DSO behaviour requirements

Label	Description	Release
DANE-POL-001	The DSO SHALL be able to accept / reject registration requests by Device Apps with valid credentials, but additionally they should meet some internal policy criteria.	1.0
DANE-POL-002	The DSO SHALL be able to receive the policy which regulates DSO behaviour by a remote server operated by a Service Provider (e.g., an OMA-DM Server compliant, see [DMPRO] and [DMARCH]).	1.0
DANE-POL-003	If the policy is obtained from an OMA-DM server, then the DSO behaviour policy SHALL be defined accordingly to operations of OMA-DM ([DMPRO], [DMARCH]).	1.0
DANE-POL-004	The policy SHALL include a parameter specifying the max number of Device Apps allowed to simultaneously send a registration request to the DSO.	1.0
DANE-POL-005	The policy SHALL include a parameter specifying the max number of registration requests to DSO allowed for a certain authorized Device App.	1.0
DANE-POL-006	Device Apps SHALL be univocally identified by App IDs.	1.0
DANE-POL-007	The policy MAY include the list of Device Apps authorized to send registration requests to the DSO.	1.0
DANE-POL-008	The policy SHALL include a parameter specifying the max cumulative QoS level (i.e., the sum of requested IP flows' QoS levels) allowed for a certain App ID.	1.0
DANE-POL-009	The policy SHALL include a parameter specifying the max cumulative QoS level allowed for a Device.	1.0

Table 10: Policy regulating DSO behaviour Requirements.

6.7 Apps Identification Functional Requirements

This section identifies the requirements for identifying and classifying applications on the device.

Label	Description	Release
DANE-Apps-001	The DANE Enabler SHALL be able to identify all applications present on the device and classify them in different groups or categories (e.g., social network, streaming, new Application…). **Informational Note:** The exact classification will be done during the technical specs design.	For Future Release

Label	Description	Release
DANE-Apps-002	The DANE Enabler SHALL be able to create different Apps Type profiles corresponding to the behaviour of Apps in term of Network Signalisation (e.g., hearth beat frequency, long live TCP connections, pulling notification …) and to match this profile with the different Applications categories. **Informational Note:** The list of the parameters to be part of an Apps Type profile will be established during the technical specs design.	For Future Release
DANE-Apps-003	The DANE Enabler SHALL classify every application into a specific category.	For Future Release
DANE-Apps-004	The DANE Enabler SHALL be able to manage the list of applications within the groups or between the group (e.g., move an application from one list to another or delete the application from the list)	For Future Release

Table 11: Apps Identification Functional Requirements.

6.8 Apps Network Efficiency Management Functional Requirements

This section identifies the requirements related to management of the Network Efficiency of the Apps.

Label	Description	Release
DANE-ANEM-001	The DANE Enabler SHALL support a mechanism to monitor and analyse different Apps elements in term of Network signalisation impacts (e.g., heart beat frequency, long live TCP connections, polling notification …). **Informational Note**: The list of the parameters to be monitored will be established during the technical specs design.	For Future Release
DANE-ANEM-002	The DANE Enabler SHALL be able to classify, or re-classify, an application from the category "New application" to the corresponding "Apps Type profile" at any time, as appropriate.	For Future Release
DANE-ANEM-003	The DANE Enabler SHALL be able to set up specific rules for shaping the different Apps network signalisation for a specific App, specific category, or all Apps.	For Future Release
DANE-ANEM-004	The DANE Enabler SHOULD be able to apply different rules based on different events and network conditions (e.g., roaming, battery status low…).	For Future Release
DANE-ANEM-005	The DANE Enabler MAY be able to retrieve some status information (e.g., roaming status, battery…) from [OpenCMAPI].	For Future Release
DANE-ANEM-006	The DANE Enabler MAY be able to configure the network signalling parameters (e.g., frequency of heart beat messages) applicable to different applications.	For Future Release
DANE-ANEM-007	The DANE Enabler SHALL be able to provide statistics information related to the different Apps Network signalisation elements (e.g., per Apps, per categories…).	For Future Release

Table 12: Apps Network Efficiency Management Functional Requirements.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-DANE-V1_0	04 Jan 2013	All	First baseline
	18 Feb 2013	1, 3.2, 3.3, 4, 5, 6	Incorporates the following inputs: - OMA-REQ-DANE-2013-0003R03-CR_Registration_and_Notification_API - OMA-REQ-DANE-2013-0004R02-CR_DSO_inner_logics - OMA-REQ-DANE-2013-0005R01-CR_DSO_Measurements_and_Events_Notification - OMA-REQ-DANE-2013-0006R01-CR_DSO_PCRF_interface - OMA-REQ-DANE-2013-0007R01-CR_Scope_section - OMA-REQ-DANE-2013-0008R01-CR_Introduction_section - OMA-REQ-DANE-2013-0009R01-CR_End_to_end_Service_Description_section
	21 Feb 2013	6.6	Incorporates the following inputs: - OMA-REQ-DANE-2013-0010R01-CR_DSO_policy
	28 Mar 2013	2.1, 3.3, 4.1, 6.1, 6.1.1,	Incorporates the following inputs: - editing online during the REQ CC on 28 March 2013-04-03 (see RDRR) - OMA-REQ-DANE-2013-0013R01-CR_RDRR_Security_comments_resolution - OMA-REQ-DANE-2013-0014R01-CR_Section_6_2_non_authorised_apps View previous versions - OMA-REQ-DANE-2013-0015R02-CR_References - OMA-REQ-DANE-2013-0016-CR_Abbreviations
	18 Apr 2013	All	Incorporates the following inputs: - OMA-REQ-DANE-2013-0019R02-CR_RDRR_DTAG_Comments_Resolution - OMA-RDRR-DANE-V1_0-20130418-D
	25 Apr 2013	All	Editorial clean-up (spell check, alignment of table indentations, adding apostophe after e.g. and i.e.).
Candidate Version OMA-RD-DANE-V1_0	07 May 2013	N/A	Status changed to Candidate by TP Ref #OMA-TP-2013-0120-INP_DANE_V1_0_RD_for_Candidate_approval