UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NUMBER | FILING or 371(c) DATE | GRP ART UNIT | FIL FEE REC'D | ATTY.DOCKET.NO | TOT CLAIMS | IND CLAIMS |
|---|---|---|---|---|---|---|
| 61/387,247 | 09/28/2010 | | 220 | RALEP038+ | | |

**CONFIRMATION NO. 2260**

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

**FILING RECEIPT**

*OC000000044053178*

Date Mailed: 10/26/2010

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

**Applicant(s)**

Gregory G. Raleigh, Woodside, CA;

**Power of Attorney:**
Michael Schallop--44319

**If Required, Foreign Filing License Granted:** 10/18/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/387,247**

**Projected Publication Date:** None, application is not eligible for pre-grant publication

**Non-Publication Request:** No

**Early Publication Request:** No
**Title**

SECURED DEVICE DATA RECORDS

## PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international

patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

## LICENSE FOR FOREIGN FILING UNDER

## Title 35, United States Code, Section 184

## Title 37, Code of Federal Regulations, 5.11 & 5.15

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Doc Code: **TR.PROV**
Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)
Approved for use through 06/30/2010 OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

## Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

### Inventor(s)

Inventor 1 — Remove

| Given Name | Middle Name | Family Name | City | State | Country |
|---|---|---|---|---|---|
| Gregory | G. | Raleigh | Woodside | CA | US |

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. — Add

| | |
|---|---|
| **Title of Invention** | SECURED DEVICE DATA RECORDS |
| Attorney Docket Number (if applicable) | RALEP038+ |

### Correspondence Address

Direct all correspondence to (select one):

| | |
|---|---|
| ◉ The address corresponding to Customer Number | ○ Firm or Individual Name |
| Customer Number | 21912 |

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

◉ No.

○ Yes, the name of the U.S. Government agency and the Government contract number are:

Doc Code: **TR.PROV**
Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)
Approved for use through 06/30/2010 OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

## Entity Status

Applicant claims small entity status under 37 CFR 1.27

◯ Yes, applicant qualifies for small entity status under 37 CFR 1.27

◉ No

## Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

## Signature

Please see 37 CFR 1.4(d) for the form of the signature.

| | | | | | |
|---|---|---|---|---|---|
| Signature | /Michael J. Schallop/ | | | Date (YYYY-MM-DD) | 2010-09-28 |
| First Name | Michael J. | Last Name | Schallop | Registration Number (If appropriate) | 44319 |

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

# Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or paten. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, t o a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



# Request For Information for Advanced Wireless Services Chipsets

Version 1



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

Table of Contents

Instructions to Prospective Suppliers of Chipsets for Wireless Carrier Advanced Wireless Services ..... 5

AWSP Chipset RFI Response Timeline ..... 6

AWSP Chipset RFI Response Submission Checklist Proposal checklist: ..... 7

1 Technical Overview of Embedded Device Data Record Processor for Advanced Wireless Services ..... 8

1.1 Introduction ..... 8

1.2 Summary of AWSP Development and Certification Process For Embedded DDR Processor Chipsets ..... 9

1.3 DDR Processor Overview ..... 10

1.4 Overview of AWSP Chipset Secure Image Programming, Secure Boot, Secure Execution and Secure Firmware Update Requirements ..... 13

1.5 AWSP Chipset DDR Processor Implementation Alternatives ..... 15

2 Embedded DDR Processor Implementation on a Smart Phone Application Processor (APU) Chipset ..... 18

2.1 Security requirements for APU ..... 21

2.2 Examples of Suitable APU Chipset SEE Implementation Techniques ..... 22

3 Embedded DDR Processor Implementation on a 3G/4G Wireless Modem Chipset ..... 23

3.1 Security requirements for MPU ..... 28

3.2 Examples of Suitable MPU Chipset SEE Implementation Techniques ..... 28

4 Embedded DDR Processor on a Smart Phone Application Chipset Combined with Data Path Security Verifier on a 3G or 4G Wireless Modem Chipset ..... 29

4.1 Security requirements for APU ..... 31

4.2 Examples of Suitable APU Chipset SEE Implementation Techniques ..... 32

5 Appendix A: APU Chipset Requirements Overview ..... 33

5.1 Below is basic APU specification requirements ..... 33

5.2 Intel Atom (e.g., Z5xx, Z6xx, D4xx, D5xx series) based solution ..... 33

5.3 ARM based solution ..... 33

6 Appendix B: Modem Chipset Requirements Overview ..... 34

6.1 Below is basic MPU specification requirements ..... 34

6.2 EVDO Chipset based solution ..... 34

6.3 HSPA Chipset based solution ..... 34

6.4 LTE Chipset based solution ..... 34

7 Appendix C: Timeline for AWSP Chipset Certification Program ..... 35
8 Appendix D: DDR Processor Proposal Submission Guidelines and Table of DDR Chipset Supplier Questions ..... 36
8.1 Proposal Submission Guidelines ..... 36
8.2 DDR Chipset Supplier Questionnaire ..... 37
9 Appendix E: Alternative Functionality and Location for DDR Processor ..... 39
9.1 Alternative for Stand Alone Chip or SIM Implementation of DDR Processor with Modem Processor Implementation of Data Path Security Verification ..... 39
9.2 Alternative APU DDR Processor Locations That Involve Network Access Policy Enforcement at Higher Levels of the Network Stack ..... 41
10 Appendix F: Additional Description of Selected Aspects of DDR Processor Functional Operation ..... 43
10.1 DDR Firmware Installation, Security Credential Configuration and Update ..... 43
10.2 Mail Box Communication Channel between Service Processor and DDR Processor ..... 44
10.3 DDR Processor Record Generator ..... 45
10.4 Upon Reset and/or Powering up DDR Processor Access Controller ..... 46
10.5 DDR Processor Network Busy State Monitor ..... 47
10.6 Binding and Securing the Secure Communication Channel Between the DDR Processor and the Service Controller ..... 47
10.7 Binding and Securing the Secure Communication Channel Between the DDR Processor and the DPSV In An APU/MPU Implementation ..... 48
10.8 Security requirements for OEM programming of DDR Processor ..... 49
10.8.1 Code Signing ..... 49
10.8.2 Random seed for DDR Device Private Key ..... 49
10.8.3 DDR Device Cert ..... 49



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

## List of Figures

Figure 1: Advanced Wireless Service Platform End to End DDR Reporting and Processing System ..... 9
Figure 2: Process for Booting, Executing and updating the DDR Firmware ..... 14
Figure 3: AWSP Chipset Embedded DDR Processor Options ..... 14
Figure 4: APU Implementation (option-1) with Embedded DDR Processor, Modem Bus Driver and Modem Physical Bus in Date Path Security Zone ..... 15
Figure 5: High Level Diagram of Secure Embedded DDR Processor in APU Implementation (option-1) ..... 16
Figure 6: Details of Secure Embedded DDR Processor in SEE APU Implementation with Modem Bus Driver (option-1) ..... 17
Figure 7: MPU Implementation (option-2) with Embedded DDR Processor and Modem Data Path From DDR Processor to Network in Zone of Data Path Security ..... 20
Figure 8: High Level Diagram of Embedded Secure DDR Processor in MPU Implementation (option-2) ..... 21
Figure 9: Details of Embedded Secure DDR Processor in SEE MPU Implementation (option-2) ..... 22
Figure 10: APU & MPU Implementation (option-3) with Embedded DDR Processor and Modem Data Path From DDR Processor to Network in Zone of Data Path Security ..... 24
Figure 11: Details of Combined APU DDR Processor and MPU Data Path Security Verifier (option-3) ..... 26
Figure 12: Details of Combined SIM DDR Processor and MPU Data Path Security Verifier ... 33
Figure 13: Secure Boot Sequence Flowchart ..... 44
Figure 14: Passing DDR Service Processor Mailbox Messages between Secure and Unsecure Memory Regions ..... 45
Figure 15: DDR Processor Service Controller Session Authentication and Verification Process Flowchart ..... 46



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

The Advanced Wireless Service Platform (AWSP) is an enhanced networking technology platform that adds new internet and data service capabilities to Wireless Carrier's 4G, 3G, 2G and Roaming Partner network assets. In AWSP the wireless devices, chipsets, firmware and software play an enhanced role in wireless network service policies for charging, access control and service notification. AWSP will support a wide range of services, devices and applications for the consumer, enterprise and machine to machine (M2M) markets. The device types that will be supported by AWSP include the following:

- 4G and 3G smart phones
- 4G and 3G feature phones
- 4G and 3G USB dongles and cards
- 4G-to-WiFi and 3G-to-WiFi bridge devices
- 4G and 3G notebook and netbook computing devices
- 4G and 3G slate computing devices
- Other 4G and 3G consumer electronics devices (cameras, personal navigation devices, music players, home power meters, etc)
- M2M devices (various types of consumer and industrial devices with minimal UI capabilities such as geo-location tracking devices, parking meters, vending machines, etc)

The Device Data Record Processor (DDR Processor) is a key element in the AWSP architecture. The DDR Processor consists of firmware that is integrated into a secure hardware execution environment within an AWSP chipset. The purpose of the AWSP Chipset Certification Program is to qualify chipsets for proper services delivery over AWSP. The list of chipset suppliers that pass the AWSP Chipset Certification Program will be provided by Wireless Carrier to device OEMs as AWSP certified chipsets. All devices that receive AWSP enhanced services will be required to have AWSP approval.

The Purpose of this Request For Information for Advanced Wireless Services Chipsets (AWSP Chipset RFI) is to solicit interest, feedback and preliminary indication of the following:

- Indication of interest in supplying AWSP certified chipsets to Wireless Carrier device OEMs
- The proposal summary document titled "Design Overview for APU (MPU) Chipset With Embedded DDR Processor Capabilities" (see Appendix D of the Technical Overview of the Embedded Device Data Record Processor for Advanced Wireless Services)
- Preliminary indication of compliance with DDR Processor chipset requirements
- Answers to questions listed in the DDR Chipset Supplier Questionnaire (see Appendix D of the Technical Overview of the Embedded Device Data Record Processor for Advanced Wireless Services)
- Preliminary indication of compliance with the AWSP chipset certification timeline
- Feedback on suggested improvements in DDR Processor Secure Execution Environment (SEE) implementation or certification processes described in more detail below.

Prospective chipset suppliers are encouraged to respond to this AWSP Chipset RFI if there is an interest in supplying chipsets to OEMs who will build Wireless Carrier AWSP devices.

## AWSP Chipset RFI Response Timeline

| | |
|---|---|
| October 20, 2010 | AWSP Chipset RFI issued |
| November 20, 2010 | Initial responses due |
| November 14 - December 14, 2010 | Prospective supplier discussions |
| January 14, 2011 | Down selection complete |
| July 14, 2011 | First chipsets enter DDR approval testing and begin integration into OEM 4G and 3G production devices |
| November 14, 2011 | First chipsets with DDR Processor approved for production services |
| January 14, 2012 | Volume device shipments |

## AWSP Chipset RFI Response Submission Checklist

### Proposal checklist:

1. Proposal for a chipset that will support one or more of the three main implementation approaches for an APU or modem chipset with secure DDR Processor.
2. Completed AWSP Chipset proposal questionnaire listed in the Table of Questions in Appendix D.
3. Detailed chipset specifications for proposed baseline chipset(s)
4. Description of supplier wireless chipset product line, current market design wins and most recent 4 quarters of production volume in similar applications.
5. Description of current supplier chipsets in use in 3G or 4G wireless handsets or similar device applications.
6. Chipset pricing starting in CY 2010 with volume increments of 1M, 5M, 10M, 25M and 50M.

Proposal discussion must include sufficient detail to allow a technical evaluation of the all aspects of the supplier's chipset identified in the AWSP Chipset RFI Table of Questions in Appendix D.

# 1 Technical Overview of Embedded Device Data Record Processor for Advanced Wireless Services

## 1.1 Introduction

This technical overview is intended to provide an introduction to the chipset requirements necessary to support the Wireless Carrier Request For Information Regarding Advanced Wireless Services Chipsets (AWSP Chipset RFI). The requirements outlined herein involve integrating a secure Device Data Record Processor (DDR Processor) in chipsets that are certified and approved for operation with the Wireless Carrier AWSP.

AWSP is an enhanced networking technology platform that adds new internet, data, voice over IP and video over IP service capabilities to Wireless Carrier's 4G, 3G, 2G and Roaming Partner network assets. In AWSP wireless devices, chipsets, firmware and software play an enhanced role in enforcing service policies for access service charging; network access control and traffic control; and service notification. The DDR Processor is a key element in the AWSP architecture and is operated in a secure chipset environment as outlined herein.

This document contains the following information:

- Overview of requirements for secure firmware execution environment, nonvolatile memory, and application space communication necessary to support secure operation of the DDR Processor
- Overview of DDR operation
- Overview of APU chipset requirements (Appendix A)
- Overview of MPU chipset requirements (Appendix B)
- Timeline for the DDR Certification Program (Appendix C)
- Prospective chipset supplier Questionnaire Table (Appendix D)
- Additional implementation alternatives for DDR Processor (Appendix E)
- Selected details of DDR Processor implementation and operation (Appendix F)

The information contained herein is not intended as a detailed specification for the DDR Processor or as a detailed specification for the chipset requirements necessary to support the DDR Processor. A more detailed document set ("AWSP System Overview", "Device Data Record Processor Chipset Specifications", "Service Processor Overview", "Service Controller Overview") will be provided to prospective chipset suppliers selected for continued discussions following the AWSP Chipset RFI down-selection process.

The plan for implementing the DDR Processor in production OEM devices is to select a subset of the chipset supplier community to help develop and field AWSP-certified products. Once the initial production launch is complete, additional chipset suppliers may then be solicited. As outlined below, the estimated production launch timeline for devices with AWSP approved chipsets is early in the first calendar quarter of 2012.

## 1.2 Summary of AWSP Development and Certification Process For Embedded DDR Processor Chipsets

An Approved Chipset Partner is a chipset supplier whose response to the AWSP Chipset RFI is accepted through down selection process, and the chipset supplier becomes part of the Wireless Carrier AWSP Chipset Certification Program.

During the chipset development phase of the AWSP Chipset Certification Program, ItsOn, a Wireless Carrier AWSP technology supplier (Firmware Supplier), will deliver the DDR firmware described in this document to Approved Chipset Partners. The DDR firmware license materials provided to the Approved Chipset Partner will include the DDR Firmware Developers Kit (DDR FDK). The DDR FDK includes firmware code (written in C), detailed DDR Processor specifications, detailed chipset SEE specifications, DDR Processor chipset test criteria, and DDR Processor chipset certification procedures. The Approved Chipset Partner will integrate the DDR firmware into a Chipset Certification Device (CCD) that includes the chipset submitted to the AWSP Chipset Certification Program.

The CCD will be one of:

(1) an Approved Chipset Partner chipset Board Support Package (BSP) for a smart phone/feature phone device that includes the chipset submitted to the AWSP Chipset Certification Program, or

(2) a smart phone/feature phone device that includes the Approved Chipset Partner chipset submitted to the AWSP Chipset Certification Program

The first Operating System (OS) the Approved Chipset Partner will use for the AWSP Chipset Certification Program will be either Linux or Android. The timeline for additional DDR Processor OS certifications will be mutually agreed upon. The Approved Chipset Partner will receive support from the Firmware Supplier to integrate certain enhanced functionality into the CCD OS build. The enhanced functionality will include integration of a Service Processor kernel program and application. As part of the DDR firmware license, the Firmware Supplier will provide the Approved Chipset Partner with a Service Processor Software Developers Kit (SP SDK). The SP SDK will include all the software and descriptive information required to integrate the SP SDK kernel program and application software into device OEM. The Approved Chipset Partner CCD will connect to either Wireless Carrier's 3G (EVDO) network or Wireless Carrier's 4G LTE network using a mutually agreeable WWAN wireless modem chipset already certified for operation on Wireless Carrier's network.

## 1.3 DDR Processor Overview

The DDR Processor is implemented within secure firmware embedded in either the applications processor unit (APU) or the modem processor unit (MPU). The DDR Processor is part of the device firmware build installed by the OEM at time of manufacture. The DDR Processor monitors incoming and outgoing IP packets and gathers statistics called “device data records” (DDRs). A DDR is, in part, a record of the amount of data transmitted or service usage consumed along an IP flow, where an IP flow is defined by source address, destination address, source port, destination port and protocol type. In some applications DDRs also include other types of classification for network service usage. DDRs are used in 2G, 3G and 4G in both home and roaming network conditions for various service usage accounting, access control and service policy enforcement verification functions.

Figure 1 shows a high level diagram of the end-to-end DDR system. In the diagram the three DDR implementation options that are available to the prospective chipset supplier for securely embedding DDR Processor firmware and functionality into an APU chipset or an MPU chipset are shown. Each of these three options is described at a high level in the next section and more detailed discussion for each option is provided in sections that follow.

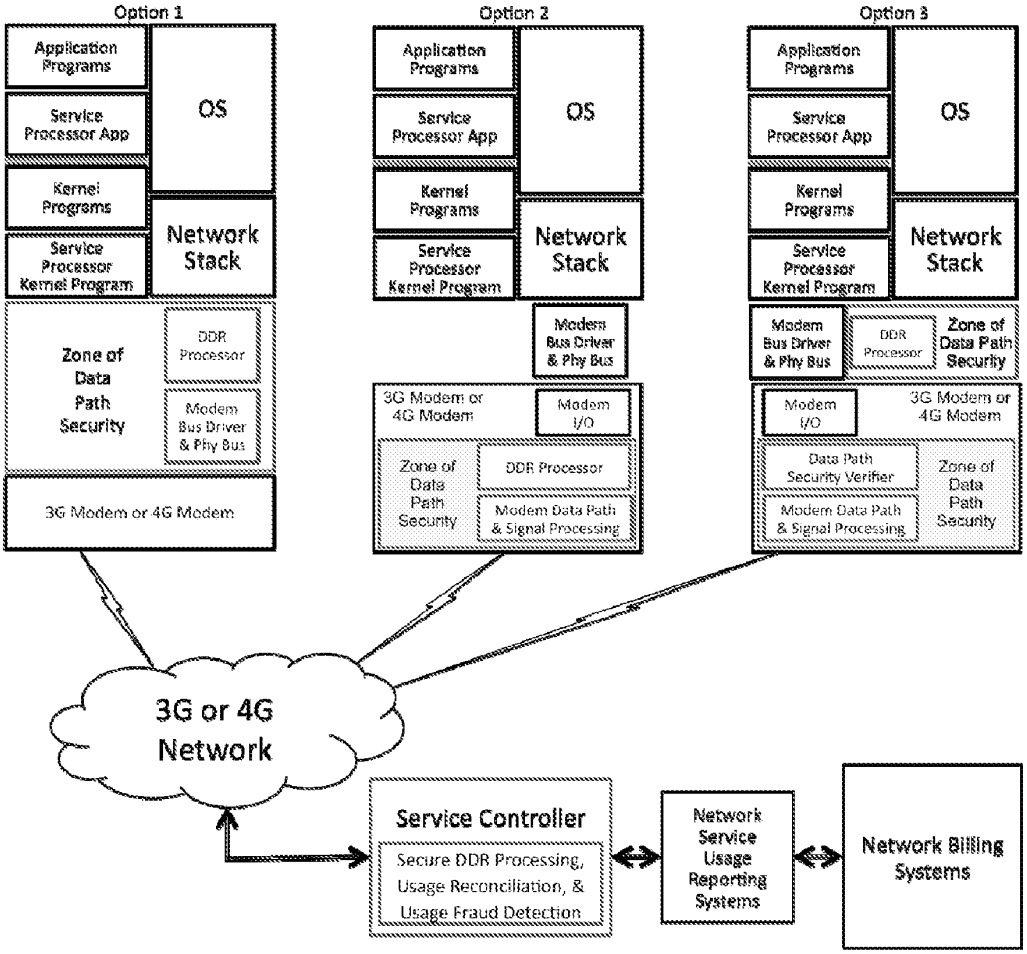



**Figure 1: Advanced Wireless Service Platform End to End DDR Reporting and Processing System**

The Service Controller is an AWSP network server cloud system that is used to:

(i) collect device service usage reports
(ii) manage certain aspects of device based network service policy
(iii) ascertain the Network Busy State (NBS) for the various base stations on the network
(iv) manage the user notification and service plan selection UI processes configured on the device and
(v) manage certain aspects of service fraud protection



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

The Service Controller communicates with the two device-based elements of the AWSP system: the DDR Processor and a Service Processor. The Service Processor consists of an application space (or framework space) program and a kernel space (or driver space) program, both running in the OS partition on the APU. The Service Processor performs various functions for the carrier network including collecting network busy state (NBS) information (see below), service usage classification and reporting, certain network service policy enforcement functions, certain user notification functions and roaming access policy enforcement functions. In some devices the Service Processor also logs and reports device service usage information that assists the carrier in determining how to provide the user with optimized services, information or content. The Service Processor is not in general in the secure region and therefore, unlike the DDR Processor, does not have a direct impact on the AWSP chipset requirements. Consequently, the discussion regarding Service Processor functionality in the remainder of this document is limited to the information required to understand the basic operation of the DDR Processor to assist the prospective supplier in responding to the AWSP Chipset RFI. Additional information on Service Processor operation, Service Controller operation and AWSP system operation will be available to suppliers who enter the AWSP Certification Program.

The DDR Processor communicates DDRs to the Service Controller server cloud located on the network. This remote server cloud is accessed via the internet or the carrier network. The DDR Processor does not send DDRs directly to the Service Controller but instead forwards the DDRs to the Service Processor. The Service Processor then relays the DDRs to the Service Controller along with additional service usage reports and other service policy management and user notification communications generated by the normal operation of the Service Processor. The APU OS execution environment is not considered secure or trusted even though the Service Processor is protected by the OS and other security elements within the system. In addition, the network data path between the DDR Processor to the Service Processor is not considered to be secure or trusted and neither is the data path between the Service Processor and the Service Controller. Therefore the DDR Processor and the Service Controller use cryptographic techniques to provide a secure link from the DDR Processor to the Service Controller. The DDR Processor is considered secure and trusted due to the design options described herein. Securing the service usage monitoring and control performed by the DDR Processor on the 3G or 4G network data path, and securing the DDR reporting channel from the DDR Processor to the Service Controller is the principle objective of the AWSP Chipset Certification Program.

An Access Controller function within the DDR Processor is employed as described below to ensure that if the DDR flow is tampered with or blocked, then the device network access data path connection managed by the DDR Processor is restricted down to only those network destinations required to manage the DDR Processor communication with the Service Controller. The DDR Processor Access Controller gets feedback from the Service Controller to restrict access or allow full access. The restricted access list (e.g. list of host names, IP addresses, etc.) is either pre-provisioned within the DDR Processor SEE or is configured through the secure path as described in more detail herein.

Secure, reliable and trusted transmission of DDRs from the DDR processor is ensured by the following three DDR reporting system design aspects:

1. The DDR Processor firmware is securely loaded and executed in a Secure Execution Environment (SEE)
2. The data path between the DDR Processor to the 3G or 4G network modem antenna connection is secured to prevent fraudulent software or firmware from forming data paths that circumvent the DDR Processor data path processing
3. The DDRs transmitted from the DDR Processor to the Service Controller are integrity-checked in a manner that protects them from being tampered with or replayed
4. An authentication process between the DDR Processor and the Service Controller combined with a set of unique DDR report sequence identifiers and authentication session keep alive timers are used to maintain and confirm the secure connection between the DDR Processor and the Service Controller. If the secure session or the flow of DDR records between the DDR Processor and the Service Controller are interrupted, then the Access Control function in the DDR Processor restricts access modem (3G or 4G) data path to the network destinations necessary to re-establish a securely authenticated session between the DDR and the Service Controller.

The DDR processor also contains a secure Network Busy State Monitor function (NBS Monitor). The NBS Monitor logs and reports various network and modem performance parameters and also computes and reports a measure of network congestion called “Network Busy State” (NBS). NBS is a measure that indicates the level of network congestion at a give base station sector over a given measurement interval. All of this information is included in a network busy state report (NBSR) that is part of the DDR message reports sent to the Service Controller via the Service Processor.

Additional functional descriptions of selected DDR Processor features are provided in Appendix F.

## 1.4 Overview of AWSP Chipset Secure Image Programming, Secure Boot, Secure Execution and Secure Firmware Update Requirements

The DDR Processor system requires a dedicated Secure Execution Environment (SEE) within the APU or modem chipset. The SEE provides for secure, trusted generation of device data records as described in subsequent sections herein. The basic functionality of the SEE is described below.

The SEE is a secure memory execution partition that cannot be accessed by any external program, bus or device port. The partition includes code space and data space. A Secure Boot Loader executes within the SEE. The only other code images allowed to execute in the SEE are secure images, meaning digitally-signed images whose signature is verified by the Secure Boot Loader. At time of device manufacture, the Secure Boot Loader is programmed into nonvolatile memory in the on-chip SEE. The Secure Boot Loader fetches a secure image from nonvolatile memory and installs it in the SEE in a trusted and secure manner. The Secure Boot Loader is the only element capable of loading an image into the SEE.

The DDR Processor is a secure image. The remainder of this section describes how the DDR Processor is installed by the Secure Boot Loader into the SEE. Installation of other secure images is similar.

The DDR Processor image is digitally signed by the device OEM. The Secure Boot Loader verifies the signature using the Boot Loader Verification Key and rejects the image if the signature is invalid. The Boot Loader Verification Key is a 2048-bit RSA public key embedded within the Secure Boot Loader image.

Typically, the signed DDR Processor image is stored in the off-chip nonvolatile memory. Alternatively, it is preferred to store the signed DDR Processor image in on-chip nonvolatile memory, but the typical on-chip storage capacity of most chipsets is too constrained to store this image so off-chip storage may be used. If the prospective chipset supplier's chipset product line allows for storage of the entire DDR Processor image in on-chip nonvolatile memory (e.g. OTM memory) this should be highlighted in the AWSP Chipset RFI response.

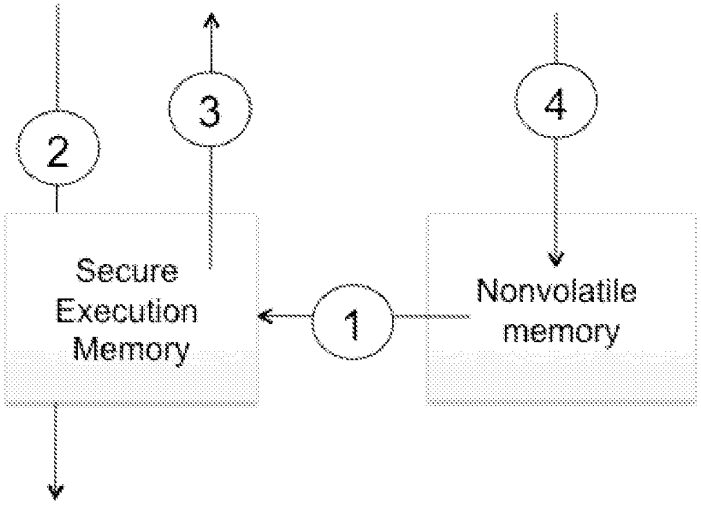



Figure 2: Process for Booting, Executing and updating the DDR Firmware

1. When the device boots, the Secure Boot Loader fetches the DDR Processor image from nonvolatile memory, installs it in the SEE, and executes it. During installation, and prior to execution, the Secure Boot Loader verifies the digital signature of the DDR Processor image using the Boot Loader Verification Key. If the signature is invalid, execution does not occur; an error message is sent to the Service Controller via the Service Processor, and the Secure Boot Loader attempts to fall back to a previously stored image (see below for more detail).
2. The data path from the non-secure OS stack elements to the modem(s) being monitored and controlled by the DDR Processor must pass into the SEE and be made available to the DDR Processor. Once the OS stack data destined for the modem is transferred into SEE memory, the secure DDR Processor program analyzes and acts on the data destined for the modem as described in the sections that follow. The DDR Processor must have a secure data interface from the SEE to the modem data path. There cannot be any data path that can circumvent the SEE and "sneak around" the DDR Processor. Examples of secure execution partition and

data interface solutions that might be proposed by a prospective chipset supplier include a "Trusted-API", "ARM Trust Zone", "Intel Smart & Secure", or a custom solution or proprietary solution specific to the chipset supplier.

3. A communication channel (or "DDR mail box") provides communication between the DDR Processor program running in the SEE to a Service Processor application program running in the non-secure OS environment (application/user space).
    a. Example options for the DDR mailbox (note that other proposed DDR mailbox methods are invited and these are just examples):
        i. Shared memory using DMA channels
        ii. Logical channels (endpoints) within modem bus driver (e.g. USB interface) between APU and MPU
            1. Piggyback channels on top of an already exiting logical channel between APU and MPU
4. The DDR Processor firmware image is updated using the OEM processes supported by the chipset supplier for over the air (OTA) and over the network (OTN) update of the chipset nonvolatile memory firmware image provided to device OEMs. It is envisioned that the DDR Processor will be stored along with other chipset firmware drivers loaded by the device at boot. The DDR Processor requires enough nonvolatile memory space to accommodate at least two images, one image that is currently running and a new downloaded image. The maximum size of each image is 0.5 MB. The Secure Boot Loader includes a firmware image switch to use the new image once download is complete. The image switch function includes a fallback system to switch back to the current image if the new image has an invalid signature, or if the new image is older than the current image as indicated by revision numbers contained within each image. The current image is retained at least until the new image has been accepted by the Secure Boot Loader.

## 1.5 AWSP Chipset DDR Processor Implementation Alternatives

The DDR Processor may be implemented in one of three configurations:

1. Integration into the APU chipset SEE and nonvolatile memory. The DDR Processor is securely implemented on the 2G, 3G or 4G modem data path directly below the modem driver data path processing function and above the modem bus driver data path processing function (typically USB driver, SDIO driver or similar bus driver function). The entire data path below the DDR Processor through the modem bus driver and through the 2G, 3G or 4G network modem is secured to prevent data paths that circumvent the DDR Processor data path processing.

2. Integration into the 2G, 3G or 4G MPU chipset SEE and nonvolatile memory. The DDR Processor is securely implemented on the 2G, 3G or 4G modem data path just below the modem bus driver and logical channel interface and the entire data path below the DDR Processor to the 2G, 3G or 4G network is secured to prevent data paths that circumvent the DDR Processor data path processing.

3. Integration into the APU chipset SEE and nonvolatile memory. The DDR Processor is securely implemented on the 2G, 3G or 4G modem data path somewhere below the OS stack and above the modem bus driver. Rather than securing the entire data path below the DDR Processor through the modem bus driver and through the 2G, 3G or 4G network modem, the data path between the DDR Processor and the modem wireless network access connection is secured by integrity-checking the data that streams between the DDR Processor and a Data Path Security Verifier (DPSV) function. Any data path information that is not properly accounted for and integrity-checked is not conducted to or from the wireless network connection. This eliminates the need to secure APU firmware, hardware and data path elements other than the DDR Processor itself.

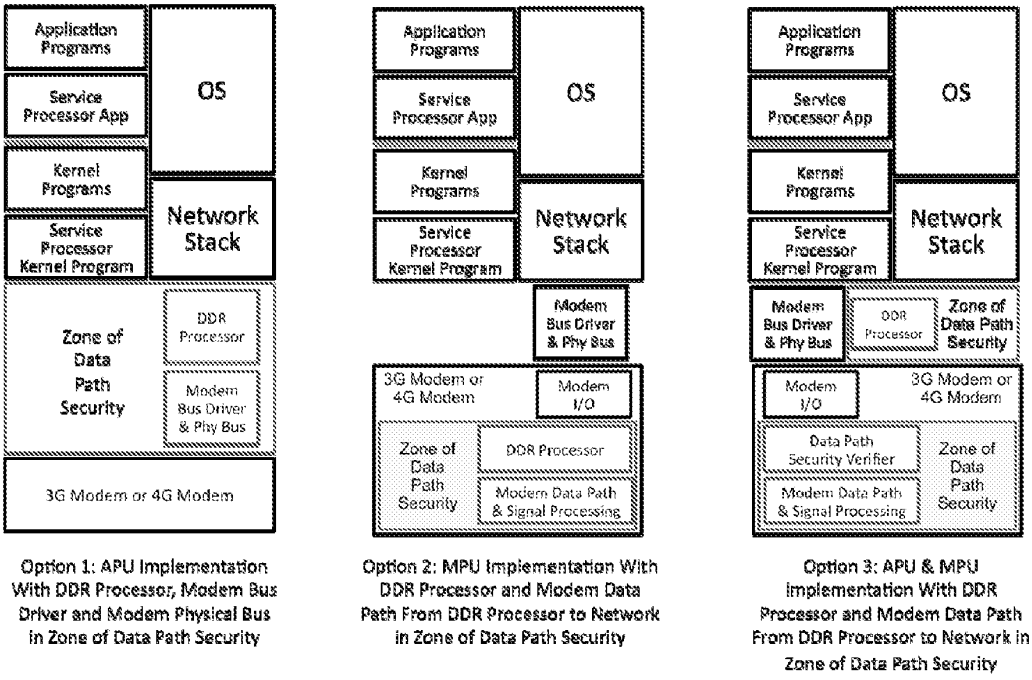



Figure 3: AWSP Chipset Embedded DDR Processor Options

Figure 3 shows the three listed options for Secure DDR firmware embedding in AWSP chipsets. Each option is described briefly below to provide a frame of reference for the implementation options. Further detail for each implementation option is then provided in the sections that follow. Prospective chipset suppliers who wish to respond to the AWSP Chipset RFI are required to propose supplying a chipset with at least one of the three APU or MPU implementations listed above. If the prospective supplier feels that there are tradeoffs that warrant further discussion and analysis, the supplier is encouraged to propose more than one implementation with a discussion of the tradeoffs.

The prospective chipset supplier is invited to comment on the relative advantages and merits of an APU implementation as in option 1, an MPU implementation as in option 2, or a combined APU/MPU implementation as in option 3. Comments are also welcome from the prospective chipset supplier on proposed implementations for one of the alternative secure partition configurations outlined in Appendix E, or some other implementation alternative that the supplier may wish to propose. However, any alternative implementation proposed by the chipset supplier must be in addition to a proposal to implement at least one of the three "first to market" options listed above.

## 2 Embedded DDR Processor Implementation on a Smart Phone Application Processor (APU) Chipset

The primary motivation for supporting APU based solution is to provide a single secure DDR Processor location on the 2G, 3G or 4G network data path that provides for service usage monitoring and access control for multiple wireless modems. A second motivation for the APU based solution is to allow prospective APU chipset suppliers who may not necessarily have WAN modem technology to participate in the AWSP device market. A third motivation for the APU implementation is that it is typically easier to enable OTA and OTN firmware updates for APU implementations as compared to MPU implementations.

In this first DDR Processor chipset implementation option shown in the figure below, the DDR Processor is embedded into the APU chipset SEE and nonvolatile memory. Along with the DDR Processor SEE, the secure data path environment (Zone of Data Path Security) must include the modem bus driver and physical bus. Provided that the modem bus driver and the physical bus to the modem are secured against (or otherwise inaccessible to) fraudulent software or firmware attempting to circumvent the DDR Processor, the modem itself need not be secured.

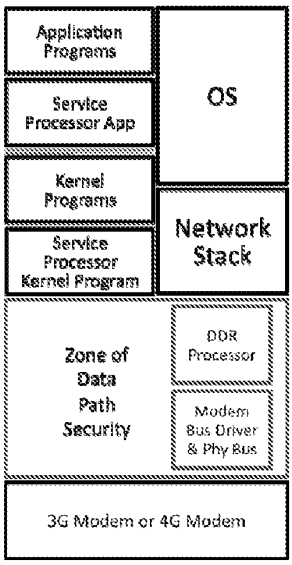



**Figure 4: APU Implementation (option-1) with Embedded DDR Processor, Modem Bus Driver and Modem Physical Bus in Date Path Security Zone**

In figure 4, the DDR Processor is securely implemented on the 2G, 3G or 4G modem data path directly below the modem driver data path processing function and above the modem bus driver data path processing function (typically USB driver, SDIO driver or similar bus driver function). The entire data path below the DDR Processor through the modem bus driver and through the 2G, 3G or 4G modem is secured to prevent data paths that circumvent the DDR

Processor data path processing. This means that the modem bus driver must either be secured in the DDR SEE or its own SEE, or the modem bus driver code and data path must be inaccessible to software or firmware on the APU that could circumvent the DDR Processor.

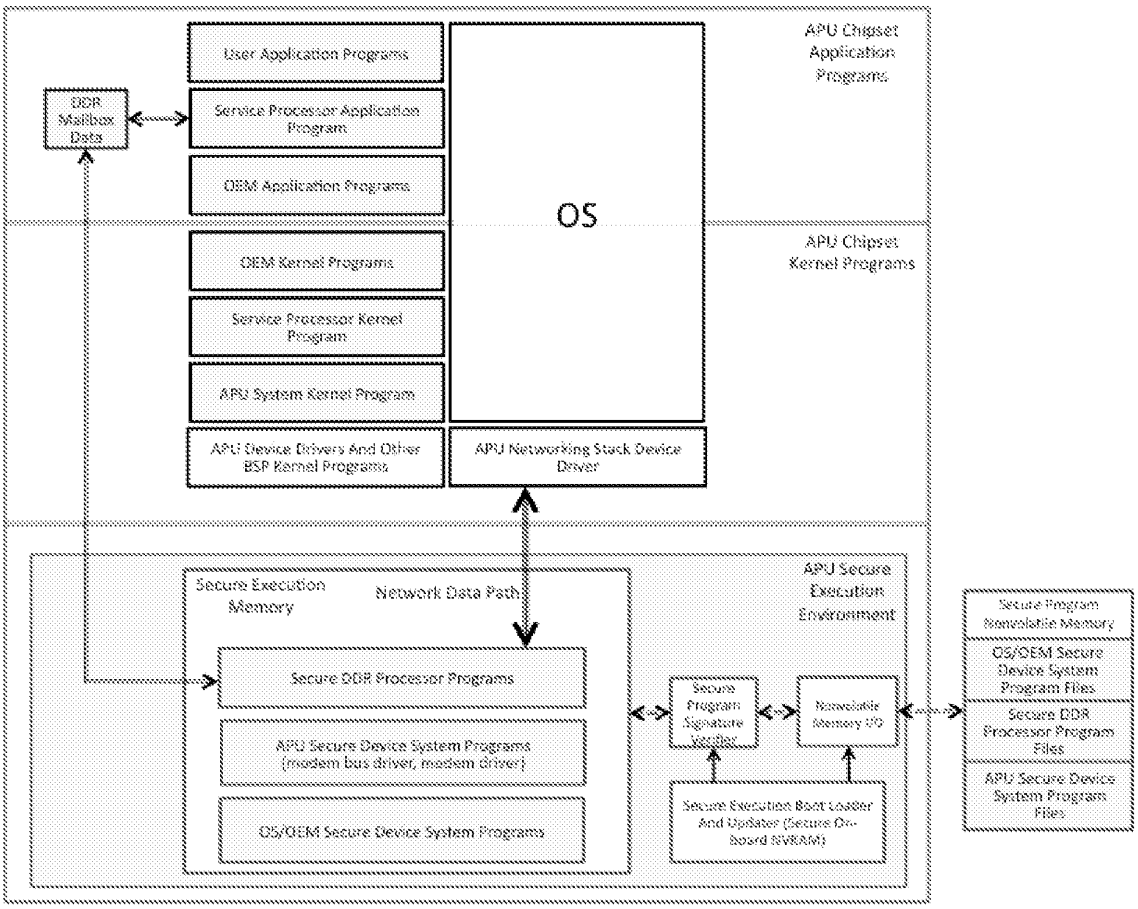



**Figure 5: High Level Diagram of Secure Embedded DDR Processor in APU Implementation (option-1)**

Figure 5 shows the major functional blocks within an APU based solution where the DDR processor resides in the APU's SEE together with other APU secure programs and the DDR processor's communication channel to the Service Processor application program is via a shared mailbox (e.g., a shared memory). It also shows the interface to the non-volatile memory (for SW downloads) with the presence of secure boot code to ensure that all secure codes are first digital signature verified before download is considered complete. The data path is a separate interface where data frames are sent to the secure environment for the DDR processor to gain access and perform DDR usage measure in addition to controlling limited or unlimited network access.

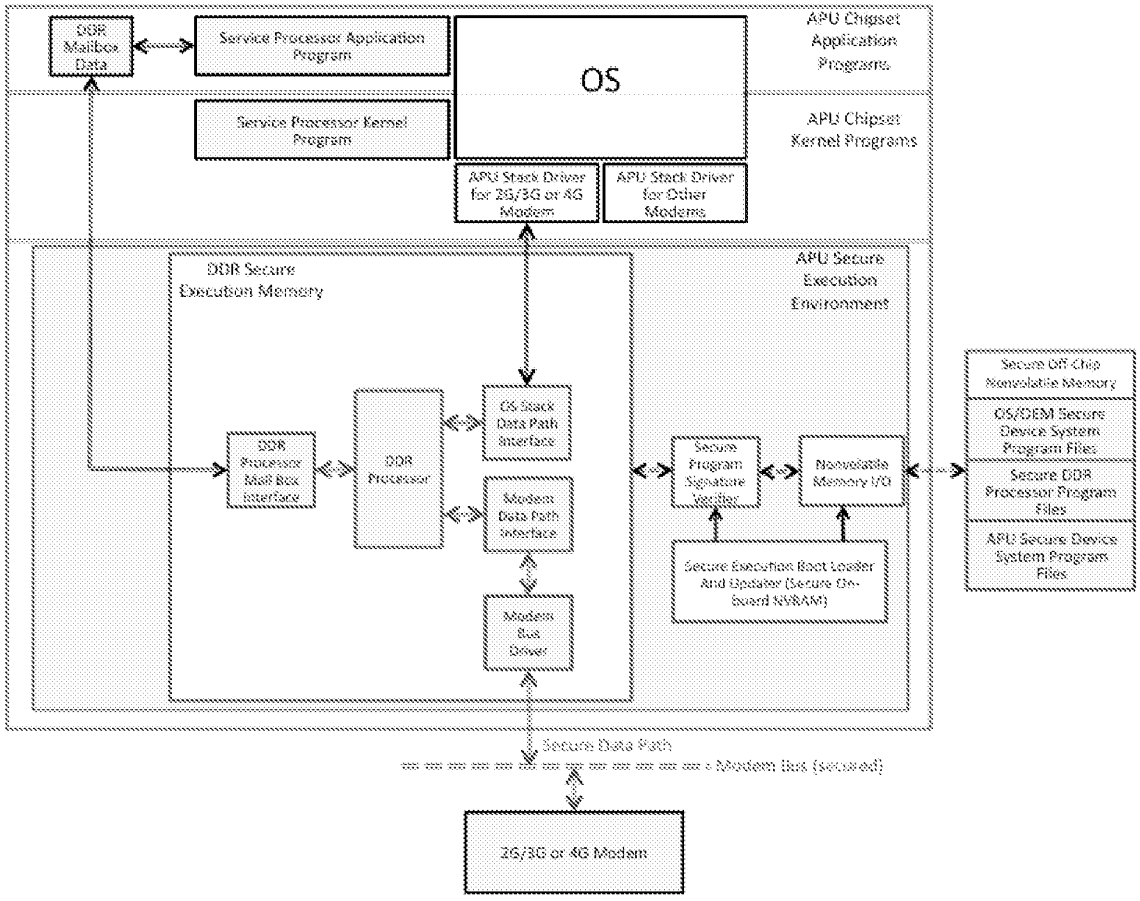



**Figure 6: Details of Secure Embedded DDR Processor in SEE APU Implementation with Modem Bus Driver (option-1)**

Figure 6 shows more detail on how the DDR Processor can be implemented in an APU secure operating environment along with the 2G, 3G or 4G modem bus driver. The DDR processor monitors IP packets going to and from the modem bus driver (e.g. USB driver/controller).

As described above and in section 1 and Appendix F, the secure boot loader pulls in the DDR Processor and modem bus driver images from nonvolatile memory into the execution memory within SEE to run (after code signature is verified). The DDR Processor and modem bus driver image and other secure images are all part of secure boot load to be signature verified before they can run.

The DDR Processor sits in line with the 2G, 3G or 4G modem data path and all traffic between the OS stack and the 2G, 3G or 4G network is monitored by the DDR Processor. There is a DDR Processor OS stack data interface that bridges between the DDR secure execution environment (SEE) and the unsecure OS stack in the kernel. There is also a DDR Processor modem data path interface that similarly connects the DDR Processor to the modem data path fed by the modem

bus driver. The reason the DDR must be in line on the data path and not simply a clone/monitor/drop function is that the DDR Processor is required to implement the Access Controller function to maintain the integrity of network access in the event that the DDR reports are tampered with or blocked from reaching the Service Controller, or the DDR Processor is tampered with, or the Service Processor is tampered with.

Three of the key aspects of all AWSP Chipset RFI responses that will be closely evaluated for APU solutions are:

1. How the APU chipset SEE is constructed.
2. Vulnerability assessment for APU SEE program or memory attacks by software or firmware operating outside the APU SEE. What must a hacker do to install or modify software in the DDR SEE? Does installing or modifying software in the DDR SEE require a hardware modification or can it be done with firmware or software modifications that can be accomplished without modifying or tampering with hardware?
3. How are the data communication channels securely formed between programs operating in the APU SEE and programs operating in the unsecure environments on the APU?
4. How does the APU protect the modem bus from other applications and drivers? What are the vulnerabilities associated with the architecture?

There is also a mailbox function that passes data between the secure DDR SEE and the unsecure Service Controller application. This mailbox may be implemented in a variety of ways including the examples provided in section 1 and Appendix F.

Additional functional description of selected DDR Processor features and APU implementation details are provided in section 1 and Appendix F.

### 2.1 Security requirements for APU

The DDR Processor and USB driver must execute in a secure environment on the smart phone application processor chipset. The secure environment must guarantee the following:

- No unauthorized ability to replace or modify the DDR Processor code or modem bus driver/controller code (e.g. USB driver/controller).
- The data path from the DDR Processor to the physical modem bus driver (e.g. USB port) must be isolated from firmware outside the secure environment. That is, no firmware outside the secure environment has the ability to affect the accurate gathering of statistics by the DDR processor.
- No ability for code other than the DDR Processor to access sensitive crypto storage such as keys. This includes shielding sensitive storage from debug monitors, etc.

APU firmware must not have bugs that might allow the secure environment to be circumvented. This applies to all APU firmware, not just the DDR Processor. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

## 2.2 Examples of Suitable APU Chipset SEE Implementation Techniques

Here are two examples of a suitable secure environment. These examples are for illustration only; compliant implementations are not restricted to be one of these.

Example 1. A conventional CPU with upgradeable firmware. The firmware might be held in nonvolatile memory, or it might be in flash memory that has means to reprogram the flash. The firmware is installed at time of manufacture and by design provides a compliant secure environment. Rigorous quality-assurance testing is required to ensure that bugs are unlikely to provide a means for compromising the secure environment. A new firmware image will be accepted for installation only if it has a valid digital signature. Version control checking should be included to prevent rollback to older versions. The firmware that validates the signature and version resides in firmware that may or may not be upgradeable.

Example 2: A security-partitioned CPU such as ARM “Trustzone” or Intel “Smart & Secure” (or another suitable substitute including potentially supplier custom security environment CPU partitioning techniques). The DDR Processor, modem bus driver (e.g. USB driver/controller), and any intervening code run in Trustzone’s (or Smart & Secure’s) secure mode. A secure boot procedure enforces the requirement that the DDR Processor, modem bus driver (e.g. USB driver/controller), and intervening code be contained in a digitally signed, version-controlled code image. Hardware firewalls shield sensitive crypto storage from normal-mode firmware. Also, the firewalls ensure that normal-mode firmware cannot tamper with the data path between the DDR Processor and the physical modem bus driver (e.g. USB port), thus preventing interference with the gathering of statistics.

# 3 Embedded DDR Processor Implementation on a 3G/4G Wireless Modem Chipset

In an MPU implementation, the DDR processor resides in the modem block with other secure modem data path processing code and hardware functions. The primary motivation for supporting an MPU-based secure DDR Processor implementation is that once the data path below the modem bus driver interface is secured, it is relatively difficult to hack the device to create a data path that reaches the network by circumventing the DDR Processor. A second motivation is that for some MPU chipset families it can be more straightforward to implement a secure execution environment, secure boot loader and secure nonvolatile memory as compared to implementing the same functions in some APU families that do not have standard hardware security partition features such as “ARM Trust Zone”, “Intel Smart & Secure”. A third advantage is that an MPU implementation also has less interaction with the OS kernel builds than in the case of an APU implementation.

A disadvantage of the MPU DDR Processor implementation is that the modem processor environment may not have a CPU with the same performance and secure execution memory space as an APU solution. This disadvantage has been greatly mitigated by designing and optimizing the DDR Processor firmware so that the code memory size is small and the CPU performance requirement is very minimal even for relatively low powered modem processor chipset CPUs. A final disadvantage that has been considered is that the OTA and OTN update process may be more complex than that achieved by certain APU chipset suppliers and their OEMs.

The prospective AWSP APU or MPU chipset supplier is invited to comment on the relative advantages and disadvantages of an MPU and APU implementation.



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

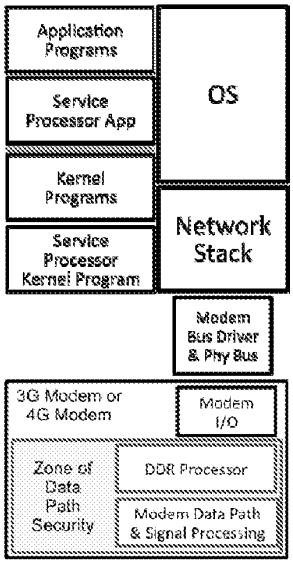



**Figure 7: MPU Implementation (option-2) with Embedded DDR Processor and Modem Data Path From DDR Processor to Network in Zone of Data Path Security**

In this second DDR Processor chipset implementation option shown in the figure 7, the DDR Processor is embedded into the 3G or 4G MPU chipset SEE and nonvolatile memory. As shown in the above figure, to ensure that fraudulent software or firmware cannot circumvent the DDR Processor, the Zone of Data Path Security must include the DDR Processor along with the modem data path processing and the modem signal processing that occurs between the DDR and the antenna.

The DDR Processor is securely implemented on the 3G or 4G modem data path just below the modem bus driver and logical channel interface and the entire data path below the DDR Processor to the 3G or 4G network is secured to prevent data paths that circumvent the DDR Processor data path processing.

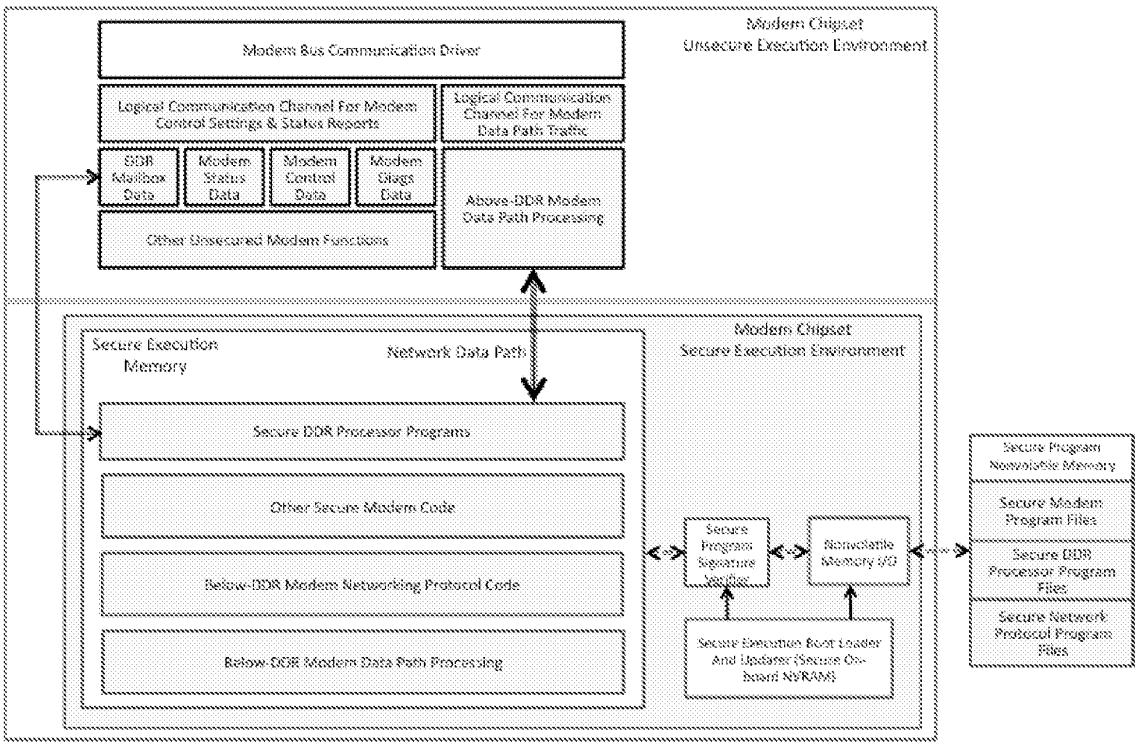



**Figure 8: High Level Diagram of Embedded Secure DDR Processor in MPU Implementation (option-2)**

Similar to the APU based solution, figure 8 shows the major functional blocks within a Modem based solution where the DDR processor resides in the modem's SEE together with other modem secure codes and the DDR processor's communication channel to the Service Processor application program is via a shared mailbox (e.g., serviced by a USB endpoint). This interface can either use a separate logical communication channel or be piggybacked on top of an already existing logical communication channel between APU and MPU. Note that the recipient of the DDR mailbox data shown in this diagram is the Service Processor Application code.

The figure 8 also shows the interface to the non-volatile memory (for SW downloads) with the presence of secure boot code to ensure that all secure codes are first digital signature verified before download is considered complete. The data path is a separate interface where data frames are sent to the secure environment for the DDR processor to gain access and perform DDR usage measure in addition to controlling limited or unlimited network access.

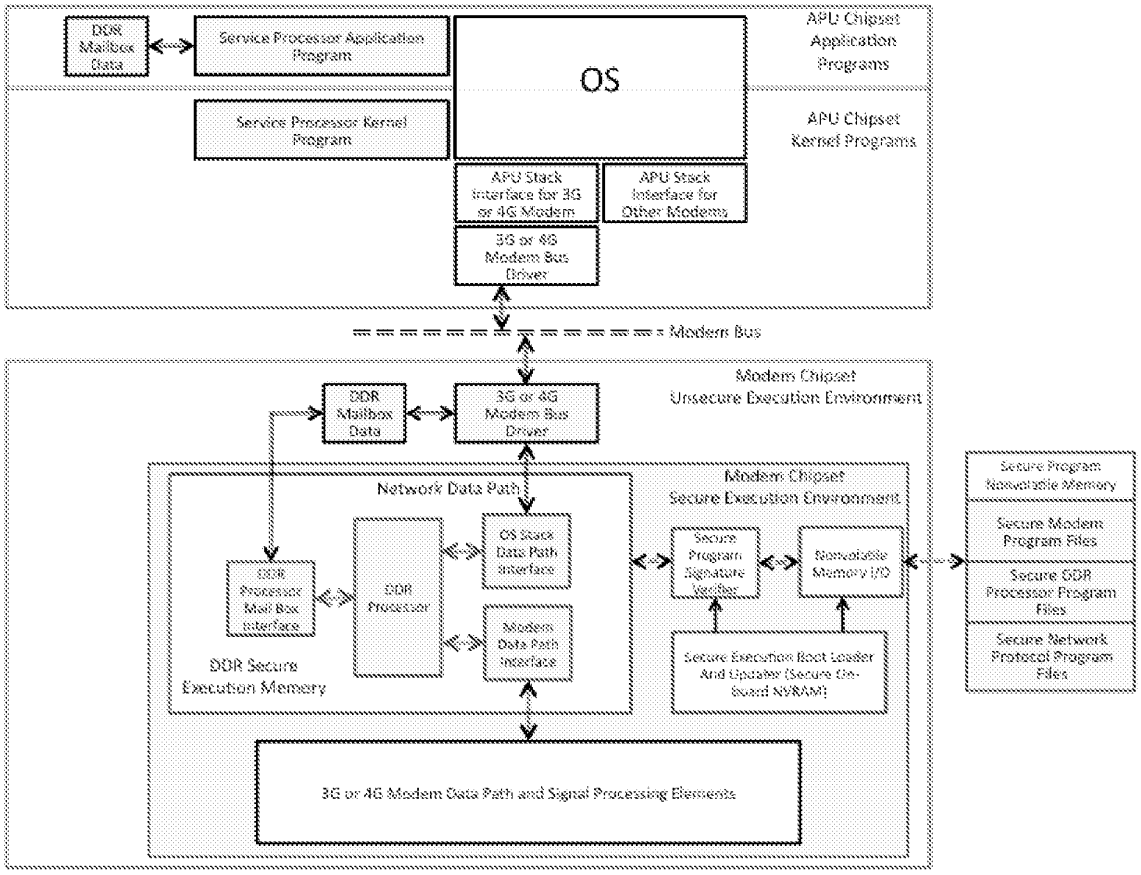



**Figure 9: Details of Embedded Secure DDR Processor in SEE MPU Implementation (option-2)**

Figure 9 shows more detail on how the DDR Processor is implemented in an MPU secure operating environment where the data path through the 3G or 4G modem network processing and signal processing is secured up to the antenna from access from software or firmware other than the DDR Processor.

The secure boot loader process operates as described in sections 1 and 2 and Appendix F. The DDR Processor is in line on the data path as described in sections 1 and 2 and Appendix F. There is a DDR Processor OS stack data interface that bridges between the DDR secure execution environment (SEE) and the (potentially) unsecure modem bus driver interface. There is also a DDR Processor modem data path interface that similarly connects the DDR Processor to the modem data path processing and the modem signal processing that occurs between the DDR and the antenna. As explained above and throughout, the reason the DDR must be in line on the data path and not simply a clone/monitor/drop function is that the DDR Processor is required to implement the Access Controller function to maintain the integrity of network access in the event that the DDR reports are tampered with or blocked from reaching the

Service Controller, or the DDR Processor is tampered with, or the Service Processor is tampered with.

Three of the key aspects of all AWSP Chipset RFI responses that will be closely evaluated for MPU solutions are:

1. How the MPU chipset SEE is constructed.
2. Vulnerability assessment for MPU SEE program or memory attacks by software or firmware operating outside the MPU SEE. What must a hacker do to install or modify software in the DDR SEE? Does installing or modifying software in the DDR SEE require a hardware modification or can it be done with firmware or software modifications that can be accomplished without modifying or tampering with hardware?
3. How do the data communication channels are securely formed between programs operating in the MPU SEE and programs operating in the unsecure environments on the MPU?

There is also a mailbox function that passes data between the secure DDR SEE and the unsecure Service Controller application. This mailbox may be implemented in a variety of ways with examples provided in section 1 and Appendix F.

Additional functional description of selected DDR Processor features and MPU implementation details are provided in section 1 Appendix F.

It is important to note that the secure region must be inclusive of all data path processing steps below the DDR processor and there cannot be any data path through the modem to the network that circumvents the DDR processor.

### 3.1 Security requirements for MPU

The DDR Processor must execute in a secure environment in order to guarantee that DDRs accurately reflect the device's usage of network bandwidth. The secure environment must guarantee the following:

- No unauthorized ability to replace or modify the DDR Processor code.
- No ability for code other than the DDR Processor to access sensitive crypto storage such as keys. This includes shielding sensitive storage from debug monitors, etc.
- No ability for any code to interfere with the accurate gathering of statistics by the DDR Processor.

MPU firmware must not have bugs that might allow the secure environment to be circumvented. This applies to all MPU firmware, not just the DDR Processor. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

### 3.2 Examples of Suitable MPU Chipset SEE Implementation Techniques

The examples of suitable secure execution environment (SEE) implementations in the modem processor CPU are the same as the application processor CPU. These examples are for illustration only; compliant implementations are not restricted to be one of these.

## 4 Embedded DDR Processor on a Smart Phone Application Chipset Combined with Data Path Security Verifier on a 3G or 4G Wireless Modem Chipset

In the third implementation option, the DDR Processor is embedded in a SEE APU chipset, and a Data Path Security Verifier (DPSV) is embedded in the MPU chipset. The purpose of the DPSV is to use cryptographic means to achieve a secure and trusted data path between the secure DDR Processor and the modem network antenna connection. This prevents a data connection between fraudulent software or firmware and the network without the need to secure the modem bus, the physical modem bus and the modem data path elements above the DPSV element.

By establishing a secure communication channel between the DDR Processor and the DPSV, a secure channel "binding" is created so that only network data path flows that are securely processed by the DDR Processor can reach the 3G or 4G modem connection to the wireless access network even if fraudulent software or firmware circumvents the DDR Processor by successfully gaining access to the modem bus interface. In the event that fraudulent software or firmware circumvents the DDR Processor and communicates intended unsecured data path information with the modem, the DPSV blocks the network data paths that are not processed and cryptographically secured by the DDR Processor.

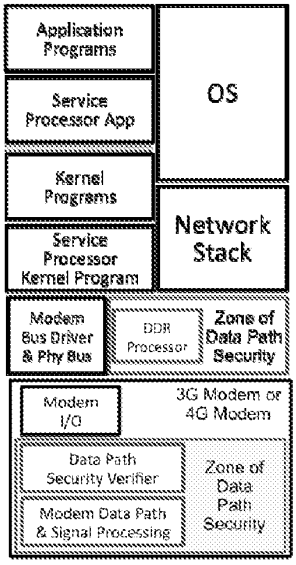



**Figure 10: APU & MPU Implementation (option-3) with Embedded DDR Processor and Modem Data Path From DDR Processor to Network in Zone of Data Path Security**

In this third DDR Processor chipset implementation option shown in the figure 10, the DDR Processor is embedded into the APU chipset SEE, and a second companion firmware image

called the Data Path Security Verifier (DPSV) is embedded into the 3G or 4G MPU chipset SEE. As also shown in the figure 10, to ensure that fraudulent software or firmware cannot circumvent the DDR Processor, there are two Zones of Data Path Security, one encompassing only the DDR Processor and the second one that includes the DPSV along with the modem data path processing and the modem signal processing that occurs between the DDR and the antenna (this second Zone of Data Path Security is similar to that of a modem-only implementation of the DDR Processor).

As mentioned above, the main motivation for option 3 is to provide an alternative that does not require securing the APU 3G or 4G Modem bus driver and physical bus. Some prospective AWSP APU chipset suppliers may consider it easier to create two firmware images and two Zones of Data Path Security rather than securing the data path between the DDR Processor SEE and the modem antenna connection. As compared to APU-based implementation option, the firmware for the APU is somewhat simplified and the security design work involved with securing the modem bus driver and physical bus are eliminated. As compared to MPU-based implementation, the modem firmware is also simplified. In some APU chipset architectures, it may be difficult to secure the data path from the DDR Processor through the modem bus driver, the modem physical bus and the modem itself.

A further motivation is that in some MPU chipsets there may be a need to simplify or reduce the size of the secure firmware program image required on the MPU. Simpler and smaller firmware can reduce the frequency of required updates or perhaps eliminate them altogether. Implementation option 3 reduces the firmware required on the MPU down to the DPSV which implements the simplified security function of binding the signed data path of the modem to the DDR Processor. This allows more complex data path processing by the DDR Processor to be implemented on the APU where (i) secure firmware execution memory is typically larger and CPU performance is typically higher, and (ii) the firmware update system is typically more capable and more flexible. There are also drawbacks with the option-3. The primary drawback is that firmware must be embedded in both the wireless network chipset (MPU) and the smart phone Application Processor (APU) chipset. Prospective AWSP chipset suppliers are invited to comment on these tradeoffs.

As shown in the figure 11, a first SEE is implemented on the APU chipset and this SEE needs to only contain the DDR Processor. A second SEE is implemented on the MPU chipset and this SEE needs to only contain the Data Path Security Verification (DPSV) program. The DPSV sits on the data path for the modem and its function is quite simple: the DPSV only passes data path information that is processed and acknowledged by the DDR Processor. The DPSV is “bound” to the DDR Processor so that it knows the signature of the DDR processor data path and it can receive acknowledgements from the DDR Processor.

A more detailed description of how the DDR Processor binds a secure data path channel to the DPSV, and how the DPSV ensures that all 3G or 4G modem network service usage is being properly monitored and processed, is provided in Appendix F.

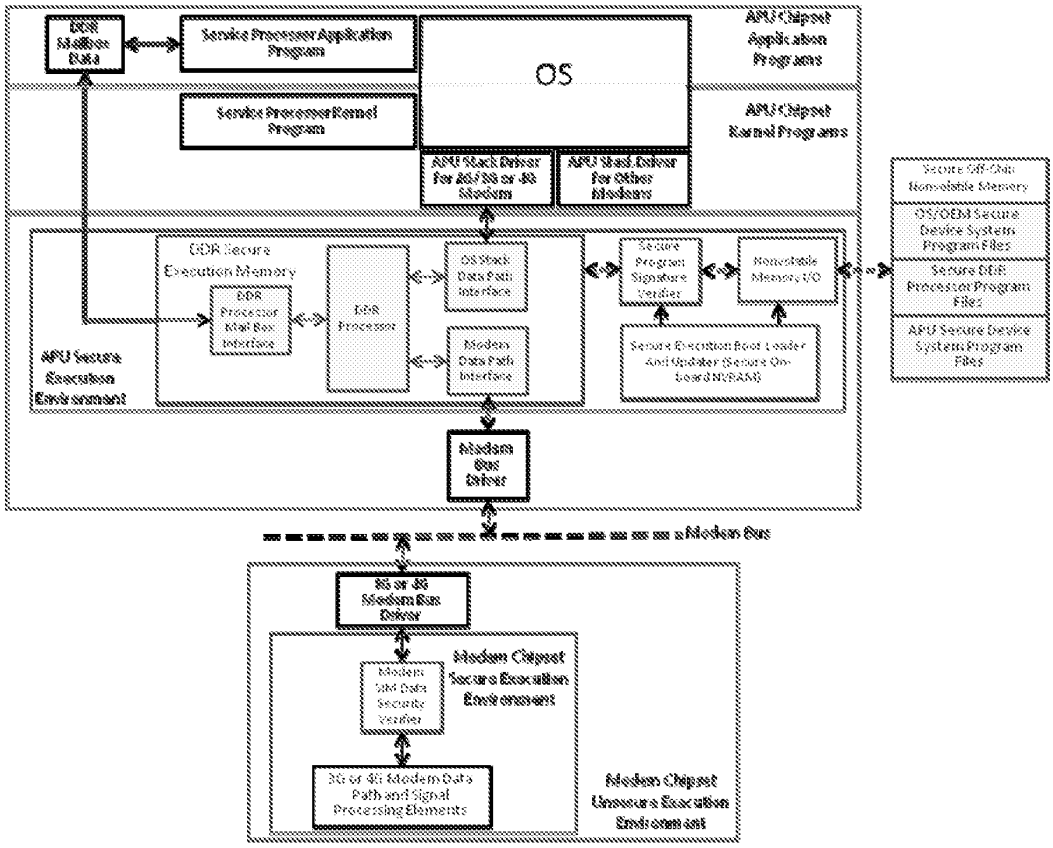



**Figure 11: Details of Combined APU DDR Processor and MPU Data Path Security Verifier (option-3)**

## 4.1 Security requirements for APU

The DDR Processor must execute in a secure environment on the smart phone application processor chipset in order to guarantee that DDRs accurately reflect the device's usage of Network bandwidth. The secure environment for the DDR Processor must guarantee the following:

- No unauthorized ability to replace or modify the DDR Processor code
- No ability for APU code other than the DDR Processor to access sensitive crypto storage such as keys. This includes shielding sensitive storage from debug monitors, etc.

APU firmware that executes in the secure environment must not have bugs that allow the secure environment to be circumvented. This applies to all APU firmware, not just the DDR Processor. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit

The DPSV must execute in a secure environment in order to guarantee that 3G or 4G modem data software or firmware that attempts to circumvent, tamper with or disable the DDR Processor is not allowed to gain network access through the modem. The secure environment for the DPSV must guarantee the following:

- No unauthorized ability to replace or modify the DPSV code.
- No ability for code other than the DPSV to access sensitive crypto storage on the modem SEE such as keys. This includes shielding sensitive storage from debug monitors, etc.
- No ability for any code to interfere with the proper crypto functions of the DPSV or communications between the DPSV and the DDR Processor.

MPU firmware must not have bugs that might allow the secure environment to be circumvented. This applies to all MPU firmware, not just the DDR Processor. For example, a common attack is buffer overflow, in which an attacker chooses inputs that cause an unchecked buffer to exceed its bounds, resulting in unintended behavior that the attacker can exploit.

### 4.2 Examples of Suitable APU Chipset SEE Implementation Techniques

Here are two examples of a suitable secure environment. These examples are for illustration only; compliant implementations are not restricted to be one of these.

# 5 Appendix A: APU Chipset Requirements Overview

## 5.1 Below is basic APU specification requirements

- Up to 3.0 M Byte Secure memory allocated to the DDR processor
- Up to 6.0 M Byte nonvolatile memory dedicated for the DDR processor; two 3.0 M Byte images
- Up to 3.0 MB non-secure memory for the Service Processor Application
- Less than 200KB for Kernel code
- Minimum CPU clock rate of 400MHz
- Minimum 16KB/16KB Data and Instruction cache
- Desirable, but not required: Common Hardware security blocks, i.e. AES, DES, RSA, Diffie-Hellman, SHA, random generator, etc.
- First supported OSes are Linux and Android. Other OSes; WM, Apple, Palm, and Symbian will follow

Some of the industry known APUs:

## 5.2 Intel Atom (e.g., Z5xx, Z6xx, D4xx, D5xx series) based solution

- Up to 2.13 GHz CPU clock rate with single or dual core processor
- 512KB L2 cache
- Intel Trusted Execution Technology including TPM support
- Up to 667 MHz Front Side Bus (FSB)
- Linux and Windows (Win7) OSes

## 5.3 ARM based solution

- ARM Cortex A9 CPU
- Up to 1+ GHz CPU clock rate
- 512KB L2 Cache
- ARM Trusted Zone Architecture
- Linux, Android, Symbian and Windows Mobile OSes

# 6 Appendix B: Modem Chipset Requirements Overview

## 6.1 Below is basic MPU specification requirements

- Up to 3.0 M Byte Secure memory allocated to the DDR processor
- Up to 6.0 M Byte nonvolatile memory dedicated for the DDR processor; two 3.0 M Byte images
- Minimum CPU clock rate of 400MHz
- Minimum 16KB/16KB Data and Instruction cache
- Desired, but not required: Common Hardware security blocks, i.e. AES, DES, RSA, Diffie-Hellman, SHA, random generator, etc.
- Ideally supporting Android OS or one of the well-known RTOS

Some of the industry known MPUs:

## 6.2 EVDO Chipset based solution

- ARM 11-based CPU architecture
- Up to 600 MHz CPU clock rate
- ARM Trusted Zone Architecture with many common hardware crypto blocks
- USB 2.0 mode support +PHY

## 6.3 HSPA Chipset based solution

- Snapdragon/ARM based CPU architecture
- Up to 800 MHz CPU clock rate
- ARM Trusted Zone Architecture with many common hardware crypto blocks
- USB 2.0 mode support +PHY

## 6.4 LTE Chipset based solution

- Snapdragon/ARM based CPU architecture
- Up to 1 GHz CPU clock rate
- ARM Trusted Zone Architecture with many common hardware crypto blocks
- USB 2.0 mode support +PHY

# 7 Appendix C: Timeline for AWSP Chipset Certification Program

This section will be completed later.

# 8 Appendix D: DDR Processor Proposal Submission Guidelines and Table of DDR Chipset Supplier Questions

## 8.1 Proposal Submission Guidelines

AWSP Chipset RFI response submissions should include a document titled Design Overview for APU (MPU) Chipset With Embedded DDR Processor Capabilities (Design Overview). The Design Overview should include the following sections:

1. Supplier's understanding of the key requirements of the embedded DDR Processor with a list of the key design requirements the supplier has identified as critical to proper secure operation of the DDR Processor.
2. Identification of which chipset(s) the supplier has selected for embedding the DDR Processor with a high level summary of chipset capabilities and existing smart phone market design wins.
3. Overview of supplier's chipset product line secure programming capabilities and features that support secure applications like the DDR Processor.
4. Overall description of supplier's specific design for embedding the DDR Processor.
5. Explanation of how the design creates a Secure Execution Environment for loading, verifying and executing the DDR processor.
6. Explanation of how the data path between the DDR Processor and the modem network access connection is protected from circumvention by fraudulent software.
7. Explanation of how the DDR Processor firmware, and any other data path firmware functions that must be protected are stored, loaded, booted and updated.
8. Description of the Chipset Certification Device that is proposed as the device platform for completing the chipset testing requirements in the AWSP Certification Program.
9. Proposed schedule for embedding the DDR Processor and passing the AWSP Certification Program.
10. Answers to the detailed questions in the DDR Processor Table of Questions.

## 8.2 DDR Chipset Supplier Questionnaire

**All Solutions**

1 What standard supplier's chipset version(s) are proposed as a baseline to support the AWSP chipset requirements?
2 Is an existing production chipset capable of providing the AWSP chipset requirements? If not, what design modifications are required and what is the estimated timeline for implementing the changes?
3 Which embedded DDR Processor design implementation option is proposed: option-1 (APU based implementation), option-2 (MPU based implementation), or option-3 (APU/MPU combo)?
4 Please provide a summary of the prospective suppliers perceived advantages and disadvantages of each of the three main DDR Processor implementation options described in the Technical Overview of the Embedded Device Data Record Processor for Advanced Wireless Services.
5 What OS is used in the chipset supplier's low level operating system?
6 How is the nonvolatile memory DDR Processor image proposed to be updated? Is this the same process used to update chipset images by the device OEM? Is the process OTA and OTN?
7 How is the secure execution environment implemented? Please provide a vulnerability assessment for SEE program or memory attacks by software or firmware operating outside the SEE. What must a hacker do to install or modify software in the DDR SEE? Does installing or modifying software in the DDR SEE require a hardware modification or can it be done with firmware or software modifications that can be accomplished without modifying or tampering with hardware?
8 How is the secure boot procedure implemented? Please provide a summary that includes the following: boot sequence from power-up/reset, to execution of the Secure Boot Loader, to installation of the DDR Processor and any other secure images; signature verification process, including description of actions taken when an invalid signature is encountered; secure image format, including locations of the signature and version control information.
9 How is the DDR Device Private key stored in nonvolatile memory? How is it protected from access by software or firmware operating outside the SEE? If there is space available in the nonvolatile memory to store additional private keys, please specify this.
10 How is RAM within the SEE protected from unauthorized access by software or firmware operating outside the SEE? Please specify the amount of such protected RAM within the SEE that is available to the DDR Processor.
11 How is the data path below the DDR Processor secured in the design?
12 How much secure execution code space (RAM) is available to the DDR Processor? Is it greater than 1 MB?
13 How much secure data transfer space (RAM) is available to the DDR Processor? Is it greater than 2 MB?
14 What is the processing speed of the CPU proposed to run the DDR Processor? How much of the CPU-cycle capacity (in %) is estimated to be available to the DDR Processor in a typical Android smart phone implementation?
15 Does CPU have either Data or Instruction cache or both? If so, What is the size of Data and Instruction cache?
16 Does the SEE make any crypto acceleration hardware available to the DDR Processor? Examples of such hardware include RSA, Diffie-Hellman, AES, SHA, random bit generator, etc.
17 Is a debug monitor or similar utility included? If so, how is it prevented from accessing protected storage in the SEE? How is it prevented from executing code in the SEE?
18 What are the secure data interface data transfer rates
19 What means is provided by which the DDR Processor can securely measure and report timestamps?

20 When the Factory Initialization (FI) routine of the DDR Processor is executed in the factory, how is the random seed from the tester input to the FI routine? How is the public key computed by the FI routine exported to the tester?

21 What is the implementation technique to provide a "logical" communication channel between DDR processor and Service Processor in the case of DDR processor being in MPU (e.g. USB endpoint)?

22 If the "logical" channel is piggybacked on a previously used channel, is there any implementation constraints, i.e. protocol, message size, message frequency, etc.?

**MPU Solution**

23 Does the CPU support Android OS? If not, does it support any well-known RTOS? Please provide necessary documentation for the RTOS.

**APU Solution**

24 Describe the hardware interface between the APU and MPU, e.g., is it a dedicated point to point connection or it is hub-based? Is the PHY interface between the APU and MPU being considered secure (e.g. no firmware/software can circumvent the secure data path accessing the MPU directly)?

25 Is the interface between MPU and APU point to point, meaning there is only one path to get to the MPU, for example through the assigned USB port?

# 9 Appendix E: Alternative Functionality and Location for DDR Processor

## 9.1 Alternative for Stand Alone Chip or SIM Implementation of DDR Processor with Modem Processor Implementation of Data Path Security Verification

In some applications it may be attractive to locate the DDR Processor on a standalone chipset that attaches to the APU or MPU chipset, such as a SIM card. This can be accomplished with an extension to option 3, the option for implementing an embedded DDR Processor on a smart phone APU chipset combined with a Data Path Security Verifier (DPSV) implemented on a 3G or 4G wireless Modem chipset. Option 3 is described above in section 4 with some detail also provided below in section 10. The fact that implementation option 3 does not require a hardware or firmware secure data path between the DDR Processor and the modem DPSV makes it possible to move the DDR Processor onto the SIM card (or other standalone security chipset) by adding a data path logical channel forwarding function on the APU and enabling the mailbox data communication function between the Service Controller and the DDR Processor to connect over the SIM data bus. In addition, the DDR Processor reports to the Service Controller can be secured with none of the system elements on the APU being secured in a hardware assisted secured execution environment (SEE).

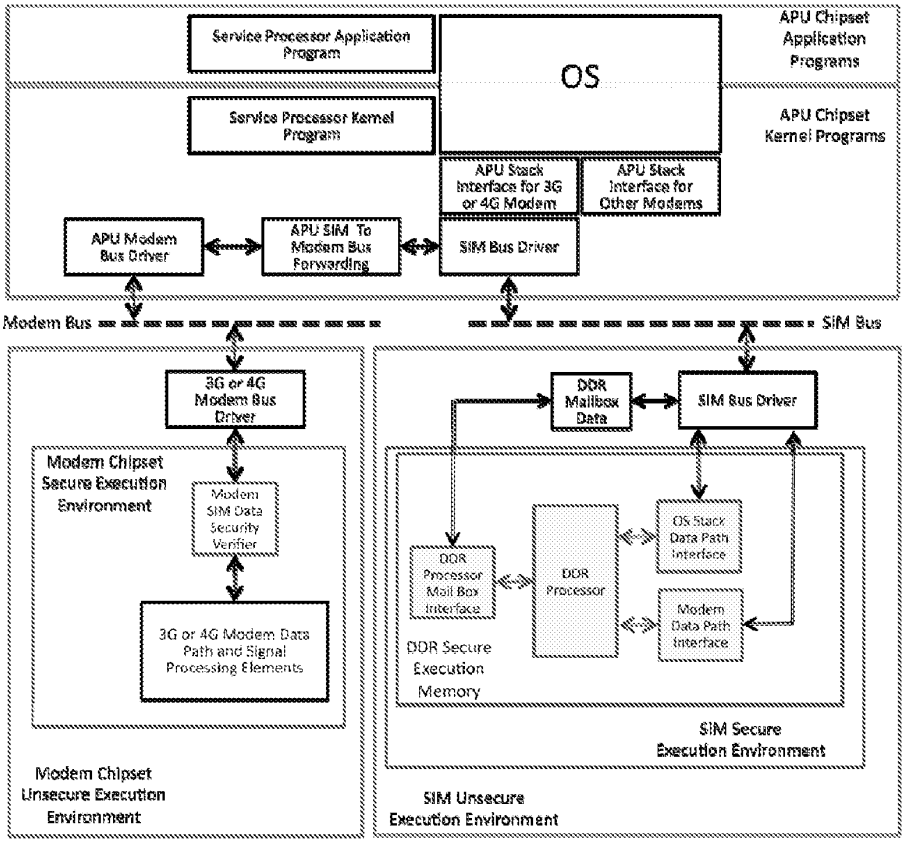



Figure 12: Details of Combined SIM DDR Processor and MPU Data Path Security Verifier



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

Referring to Figure 12, here is the SIM DDR and modem DPSV implementation alternative works:

1. The secure DDR Processor is located on the SIM in a similar manner as described for the MPU in section 3. A 3G or 4G modem network data path forwarding function and a SIM bus driver function are added to the APU. The secure DPSV is located in the modem exactly as described in section 3.
2. A first logical communication channel is created over the SIM bus between the Service Processor DDR mailbox on the APU and the DDR mailbox on the SIM, and this supports the communication between the Service Processor and the DDR Processor. A second logical data channel is created over the SIM bus between the OS networking stack and the DDR Processor and this is the logical channel intended for all OS networking stack communications with the 3G or 4G Network. A third logical communication channel is created between the SIM DDR Processor and the modem DPSV. This third logical communication channel is formed by forwarding data between the SIM bus interface located on the SIM, the SIM bus driver located on the APU, the SIM to modem bus forwarding function located on the APU, the modem bus driver located on the APU and the modem bus interface located on the modem.
3. The DPSV has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key.
4. The DDR processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key.
5. The DPSV and the DDR Processor exchange public keys and certs, then execute a key exchange process that authenticates each other and results in a secret, shared session key.
6. The DDR Processor receives upstream network data flows from the device OS networking stack and, using the session key, it appends an integrity check to each upstream data message that it sends to the DPSV. The DPSV blocks any upstream data path information that does not have a valid integrity check from the DDR Processor and informs the DDR Processor that it is receiving invalid upstream data so that the DDR Processor may inform the Service Controller of a possible fraud event.
7. The DPSV receives downstream network data flows and, using the session key, it appends an integrity check to each downstream data message that it sends to the DDR Processor. Each downstream data message is sequenced so that data messages cannot be blocked or replayed without being detected by the DDR Processor. If the DDR Processor receives a downstream data message with an invalid integrity check, the DDR Processor rejects the message and informs the Service Controller of a possible fraud event. The DDR Processor acknowledges each non-rejected downstream data message in the next upstream data message it sends to the DPSV. If the DPSV stops receiving downstream data message acknowledgements, it blocks downstream network data flows and informs the DDR Processor so that the DDR Processor may inform the Service Controller of a possible fraud event.
8. The DDR Processor securely sends DDR reports to the Service Controller by way of the Service Processor as described in previous sections. The DDRs transmitted from the DDR Processor to the Service Controller are integrity-checked and sequenced in a manner that cannot be tampered with or replayed.

9. An authentication process between the DDR Processor and the Service Controller combined with a set of unique DDR report sequence identifiers and authentication session keep-alive timers are used to maintain and confirm the secure connection between the DDR Processor and the Service Controller. If the secure session or the flow of DDR records between the DDR Processor and the Service Controller are interrupted, then the Access Control function in the DDR Processor restricts access of the 3G or 4G modem data path to the network destinations necessary to re-establish a securely authenticated session with between the DDR and the Service Controller.

## 9.2 Alternative APU DDR Processor Locations That Involve Network Access Policy Enforcement at Higher Levels of the Network Stack

Architecturally, there are alternative solutions where the DDR processor is located within a secure operating environment (SEE) at higher levels of the OS network stack than discussed herein in sections 1 through 4. There are advantages of locating the DDR Processor (or secured elements of the Service Processor) higher in the network stack. Certain key functions now performed by the Service Processor without hardware security might then be located in hardware secured execution memory. These key functions include 3G and 4G network data path processing and usage report functions, 3G and 4G network application access management and usage reporting functions and 3G and 4G service user notification and customer activity status functions.

As more advanced secure CPU partitioning technology is developed, it may soon become practical to implement large portions of the ItsOn Service Processor in hardware secured execution environments in the APU (or possibly MPU). Service Processor functions that would be advantageous to execute within a hardware secured execution environment include 3G and 4G network application access management and traffic processing that is more sophisticated, for example: (i) a secure application manager that differentially manages 3G and 4G application access according to network access policy set by the Service Controller and network busy state determined on the device and (ii) 3G and 4G network traffic that is classified and processed according to application ID, layer 7 destination as well as layer 3/4 destination and network busy state.

Securing these Service Processor functions can be attractive provided that: (i) the same level of security from hacking and malware that is available in the lower levels of stack processing can be achieved, (ii) the data path between the DDR Processor (and/or elements of the Service Processor) and the modem antenna connection can be secured from circumvention or tampering by device malware and (iii) there are sufficient memory and CPU cycles to execute the more sophisticated data path processing functions.

Prospective APU chipset suppliers are encouraged to propose alternative implementations of the DDR Processor located further up the networking stack, with an explanation of why the supplier believes such an implementation is desirable and feasible using the suppliers' chipset technology. However, any alternative implementation proposed by the chipset supplier must be in addition to a proposal to implement at least one of the three "first to market" options described in previous sections.

Prospective suppliers are reminded that all implementations of the DDR Firmware proposed must ensure that the data path through the DDR processor is secure in that there is no means available to other software or firmware that can be programmed by unauthorized users to circumvent or "sneak around" the DDR Processor data path to the 3G or 4G modem.

# 10 Appendix F: Additional Description of Selected Aspects of DDR Processor Functional Operation

## 10.1 DDR Firmware Installation, Security Credential Configuration and Update

Upon reset and/or power up, the system (APU and/or MPU, whichever the DDR is embedded on) starts by executing secure boot code. As part of this step the secure boot code is envisioned to configure system parameters (HW/firmware firewall resources, etc.) to establish the secure/normal region boundary and interfaces. The secure boot code also gets access to the root of trust (hidden to all other firmware/software) and begins to download and verify first its own public key (e.g. using hashing technique) and then download public keys of all secure codes. At this point the secure boot proceeds to download and verify digital signature of every secure software package before allowing normal software routines to be downloaded. This is normally done using “chain of trust” built on root of trust. If any digital signature fails, the secure boot stays looped in the idle state until it gets reset (watch dog timer expires, etc.) and/or platform is flashed with new image.

Also, when new secure software image is downloaded (image is stored in new area of the flash memory with a “secure” flag set) so that system goes back to reset state to have Secure boot reading the new image (based on the flag) and validate the digital signature before it becomes the current image from then on.

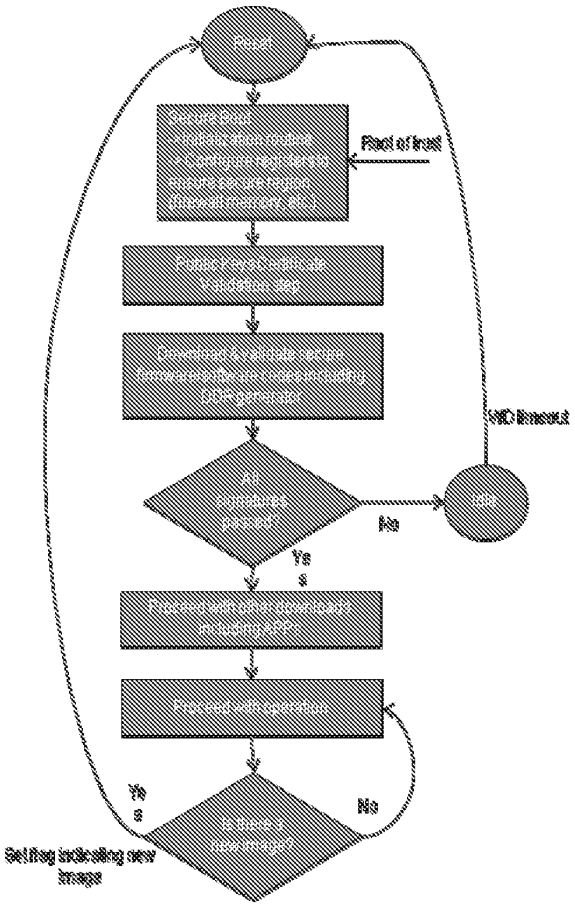


Figure 13: Secure Boot Sequence Flowchart

## 10.2 Mail Box Communication Channel between Service Processor and DDR Processor

As noted above there needs to be a logical communication channel between DDR processor and the Service Processor in order to send secure DDR message bundles to the Service Controller via Service Processor's Comm-Agent. This channel is referred to in the various diagrams as the "DDR Mailbox Data" block. For ease of implementation it is assumed that DDR processor does not have any IP address of its own hence can only send its message to Service Controller through Service Processor. In order to do that it needs to have this logical channel. The logical channel can be based on shared memory (normal region) architecture. Note that all DDR messages are encrypted and can only be decrypted by the Service Controller and no one else. Furthermore this logical channel can also be used for Service Controller to send down new DDR software updates.

In the case when the DDR processor is in the APU then the shared memory can be accessed via both Service Processor and DDR processor using APU's DMA engines. In the case when DDR processor is in the MPU then the modem interface is likely able to support additional logical channel (e.g. USB endpoint for 2G/3G/4G) to satisfy this requirement. If not the logical channel



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

can possibly be piggybacked on top of an existing "configuration and status channel" that provides the control channel between APU and MPU. Prospective chipset suppliers need to provide detailed implementation information on this logical channel (refer to AWSP Chipset RFI Questionnaire Table in Appendix D).

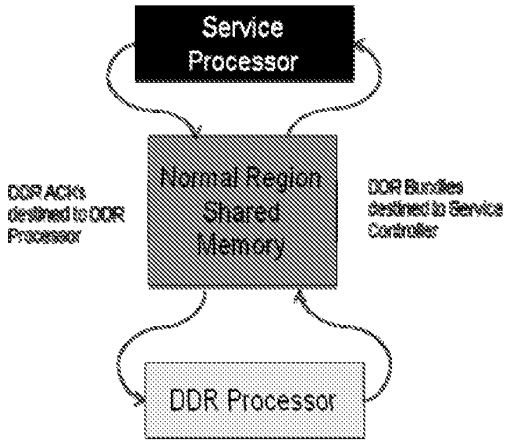



Figure 14: Passing DDR Service Processor Mailbox Messages between Secure and Unsecure Memory Regions

## 10.3 DDR Processor Record Generator

A DDR report spans a measurement period. Measurement periods are generally contiguous, meaning the next period begins immediately after the current period ends, with no traffic falling between periods. At the start of a period, all prior DDRs are deleted. During the period, the table of DDRs grows, since each observed IP flow creates an entry in the table. The period ends when either DDR storage exceeds a predefined threshold, or when a DDR report is requested by the Service Processor. DDR data not yet sent to the Service Processor application must remain in memory across power cycles, battery pulls, etc.

At the end of the measurement period, the DDR report is prepared by the DDR Processor and sent to the Service Processor. Crypto techniques are used to ensure that the contents of the report are kept private, and to ensure that any tampering with the DDR report will be detected by the Service Controller. The report includes timestamps that identify the start and end of the measurement period. Timestamps are calibrated and confirmed via a periodic handshake with the Service Controller to ensure that the DDR Processor time base has not been altered. Data compression is used to minimize the size of the report. Each DDR report message includes a sequence identifier that allows the Service Controller to determine if any DDRs have been blocked from the sequence. The report is stored by the Service Processor for subsequent forwarding to the Service Controller. Data stored by the Service Processor must remain in memory across power cycles, battery pulls, etc. The diagram below shows that the DDR generator resides in the modem where the secure DDR usage report is then sent to Comm-Agent within the Service Processor to be sent to the Service Controller.

## 10.4 Upon Reset and/or Powering up DDR Processor Access Controller

The DDR processor also contains Access Controller functionality. Upon power up and/or reset the Access Controller restricts the network access to only a few pre-configured IP addresses and/or host names including the Carrier services. The purpose of the Access Controller is to ensure that the Service Processor correctly delivers DDRs to the Service Controller. If the DDR flow is blocked or tampered with, the Access Controller blocks cellular wireless network access until the proper flow of DDRs is restored. The network access restriction is only applied to networks that have network access services maintained and managed by the network operator and this function is disabled for WiFi access not managed by the network operator.

Once modem is authenticated (via PPP session) via AAA, either after initial power up and/or after restoring from power save, the Access Controller is expected to restrict limited network access (based on set of IP addresses/host names, etc.) until it gets feedback from the service Controller to allow open access. Also, while traffic is running and DDR processor sending DDR records it continually expects to get secure DDR ACK frames to allow open access otherwise it enters “restrict access” state again (see chart below).

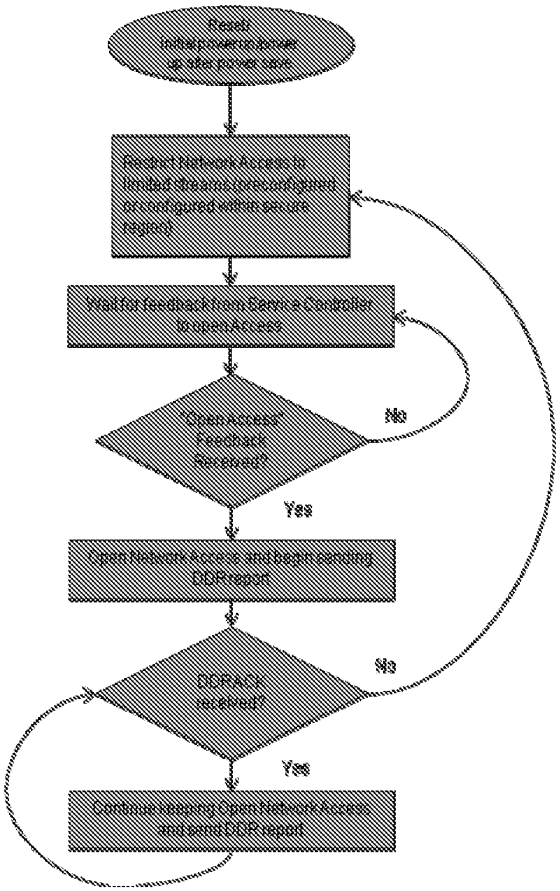



Figure 15: DDR Processor Service Controller Session Authentication and Verification Process Flowchart



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

### 10.5 DDR Processor Network Busy State Monitor

The Network Busy State Monitor (NBS Monitor) is a secure firmware program element in the DDR Processor that monitors, records and securely reports information on network busy state (or network congestion state) to the Service Controller for storage, network congestion analysis and service charging and control policy security purposes. The NBS Monitor performs the following basic functions within the SEE:

- Logs active network information (active network type, home/roaming, current carrier, base station, base station sector, etc)
- Monitors network access attempts and successes
- Monitors network speed
- Monitors round trip delay
- Monitors packet error rate
- Monitors modem performance parameters (RF channel, RF signal strength and variability, SNR, raw modem bit rate, raw modem bit error rate, channel bandwidth, etc)
- Implements algorithm to classify busy state of network
- Reports network busy state history within DDRs

### 10.6 Binding and Securing the Secure Communication Channel Between the DDR Processor and the Service Controller

Here is how the binding and data communication process works between the DDR Processor and the Service Controller:

The DDR Processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key.

1. The Service Controller has a unique private/public key pair. Its public key is well known and included in the DDR Processor code image.
2. The DDR Processor sends its public key and cert to the Service Controller, and the two execute a key exchange process that authenticates each other and results in a secret, shared session key.
3. The DDR Processor uses the session key to encrypt DDR reports it sends to the Service Controller and to append an integrity check to messages it sends to the Service Controller.
4. The Service Controller uses the session key to append an integrity check to messages it sends to the DDR Processor.



ItsOn and Headwater Partners I Proprietary and Confidential, Subject to NDA

### 10.7 Binding and Securing the Secure Communication Channel Between the DDR Processor and the DPSV In An APU/MPU Implementation

Here is how the binding and data communication process works between the DDR Processor and the DPSV:

1. The DPSV has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key.
2. The DDR processor has a unique private/public key pair and a digital certificate (cert) that attests to the authenticity of its public key.
3. The DPSV and the DDR Processor exchange public keys and certs, then execute a key exchange process that authenticates each other and results in a secret, shared session key.
4. The DDR Processor receives upstream network data flows from the device OS networking stack and, using the session key, it appends an integrity check to each upstream data message that it sends to the DPSV. The DPSV blocks any upstream data path information that does not have a valid integrity check from the DDR Processor and informs the DDR Processor that it is receiving invalid upstream data so that the DDR Processor may inform the Service Controller of a possible fraud event.
5. The DPSV receives downstream network data flows and, using the session key, it appends an integrity check to each downstream data message that it sends to the DDR Processor. Each downstream data message is sequenced so that data messages cannot be blocked or replayed without being detected by the DDR Processor. If the DDR Processor receives a downstream data message with an invalid integrity check, the DDR Processor rejects the message and informs the Service Controller of a possible fraud event. The DDR Processor acknowledges each non-rejected downstream data message in the next upstream data message it sends to the DPSV. If the DPSV stops receiving downstream data message acknowledgements, it blocks downstream network data flows and informs the DDR Processor so that the DDR Processor may inform the Service Controller of a possible fraud event.
6. The DDR Processor securely sends DDR reports to the Service Controller by way of the Service Processor as described in sections x and y. The DDRs transmitted from the DDR Processor to the Service Controller are integrity-checked and sequenced in a manner that can not be tampered with or replayed.
7. An authentication process between the DDR Processor and the Service Controller combined with a set of unique DDR report sequence identifiers and authentication session keep alive timers are used to maintain and confirm the secure connection between the DDR Processor and the Service Controller. If the secure session or the flow of DDR records between the DDR Processor and the Service Controller are interrupted, then the Access Control function in the DDR Processor restricts access of the 2G, 3G or 4G modem data path to the network destinations necessary to re-establish a securely authenticated session with between the DDR and the Service Controller.

### 10.8 Security requirements for OEM programming of DDR Processor

The discussion in this section does not have a direct impact on the AWSP chipset requirements. It is included to assist the prospective supplier in responding to the AWSP Chipset RFI.

#### 10.8.1 Code Signing

The DDR Processor code image is digitally signed by the device OEM. The signature is verified by the Secure Boot Loader using a fixed public key embedded within the Secure Boot Loader code image. This imposes the security requirement that the OEM operate a secure code-signing facility that preserves the secrecy of the fixed signing key. The OEM must ensure that only authorized personnel are able to access the code-signing facility and that they do so only for legitimate DDR Processor images.

#### 10.8.2 Random seed for DDR Device Private Key

At time of device manufacture, a private/public key pair called the DDR Device Key is assigned. The DDR Device Key is unique to each device and is used to establish a secure communications link to the Service Controller. The DDR Device Key is a Diffie-Hellman key pair with a 1024-bit modulus, 1024-bit base, and a 128-bit private exponent. The private exponent of the DDR Device Key (DDR Device Private Key) is unique to each device and stored in 128 bits of on-chip nonvolatile memory (e.g. OTP memory) in the SEE. The modulus and base are common to all devices and are embedded within the DDR Processor image. The public portion of the DDR Device Key (DDR Device Public Key) is not permanently stored; instead, it is calculated by the DDR Processor using the modulus, base, and private exponent.

The DDR Processor includes a “factory initialization” (FI) routine that is executed while the device is being initialized and tested at the factory. The FI routine generates the DDR Device Private Key and programs it into the nonvolatile memory of the SEE. The DDR Device Private Key never leaves the device and is accessible only to the DDR Processor. The FI routine computes the DDR Device Public Key and exports it to the factory tester.

The factory tester must provide a 128-bit random string to be used by the FI routine as a seed to generate the DDR Device Private Key. This requires that the factory tester include or have access to a high-quality random bit source. A suitable method is one of the software routines described in Appendix C of FIPS 140-2 (“deterministic random number generators”) seeded with the output of a hardware random source.

#### 10.8.3 DDR Device Cert

At the time of device manufacture, a digital certificate called the DDR Device Cert is assigned to the device. The DDR Device Cert is unique to each device and is used to establish a secure communications link to the Service Controller. The contents of the DDR Device Cert include the DDR Device Public Key. The DDR Device Cert is signed by the issuing certificate authority, and the signature is verified by the Service Controller when establishing a secure link. The DDR Device Cert is not sensitive information and may be stored in either on-chip or off-chip nonvolatile memory.

The OEM must issue a DDR Device Cert for the DDR Device Public Key exported by the FI routine. This imposes the security requirement that the OEM operates, or has access to, a certificate authority (CA).

If the OEM chooses to access an outsourced CA, then the OEM's primary obligation is to ensure that only authorized personnel are able to request certificates, and that they do so only for devices that have DDR Device Public Keys legitimately exported by the FI routine.

If the OEM chooses to operate a CA, the OEM has the additional obligation of maintaining the security of the CA, specifically, preserving the secrecy of the CA's fixed key that signs certificates.

| Electronic Patent Application Fee Transmittal | |
|---|---|
| **Application Number:** | |
| **Filing Date:** | |
| **Title of Invention:** | SECURED DEVICE DATA RECORDS |
| **First Named Inventor/Applicant Name:** | Gregory G. Raleigh |
| **Filer:** | Michael J. Schallop/Veronica Pula |
| **Attorney Docket Number:** | RALEP038+ |
| Filed as Large Entity | |

**Provisional Filing Fees**

| Description | Fee Code | Quantity | Amount | Sub-Total in USD($) |
|---|---|---|---|---|
| **Basic Filing:** | | | | |
| Provisional application filing | 1005 | 1 | 220 | 220 |
| **Pages:** | | | | |
| **Claims:** | | | | |
| **Miscellaneous-Filing:** | | | | |
| **Petition:** | | | | |
| **Patent-Appeals-and-Interference:** | | | | |
| **Post-Allowance-and-Post-Issuance:** | | | | |
| **Extension-of-Time:** | | | | |

| Description | Fee Code | Quantity | Amount | Sub-Total in USD($) |
|---|---|---|---|---|
| **Miscellaneous:** | | | | |
| | | | **Total in USD ($)** | **220** |

| Electronic Acknowledgement Receipt | |
|---|---|
| **EFS ID:** | 8513866 |
| **Application Number:** | 61387247 |
| **International Application Number:** | |
| **Confirmation Number:** | 2260 |
| **Title of Invention:** | SECURED DEVICE DATA RECORDS |
| **First Named Inventor/Applicant Name:** | Gregory G. Raleigh |
| **Customer Number:** | 21912 |
| **Filer:** | Michael J. Schallop/Veronica Pula |
| **Filer Authorized By:** | Michael J. Schallop |
| **Attorney Docket Number:** | RALEP038+ |
| **Receipt Date:** | 28-SEP-2010 |
| **Filing Date:** | |
| **Time Stamp:** | 16:20:29 |
| **Application Type:** | Provisional |

## Payment information:

| | |
|---|---|
| Submitted with Payment | yes |
| Payment Type | Deposit Account |
| Payment was successfully received in RAM | $220 |
| RAM confirmation Number | 2995 |
| Deposit Account | 500685 |
| Authorized User | |
| The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:<br>Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges) | |

## File Listing:

| Document Number | Document Description | File Name | File Size(Bytes)/ Message Digest | Multi Part /.zip | Pages (if appl.) |
|---|---|---|---|---|---|
| 1 | Provisional Cover Sheet (SB16) | RALEP038plus_Provisional_Coversheet_Efile.pdf | 1000032<br>c41df9ef959639af2332ff1e7dfad21cad55b5d4 | no | 3 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 2 | Specification | RALEP038plus_App.pdf | 2300882<br>279d226f6986c67b57ede9f24756786cd74b8e13 | no | 50 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 3 | Fee Worksheet (PTO-875) | fee-info.pdf | 29346<br>2444f716592184070d6c741f5d524167d8dd36b8 | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| | | **Total Files Size (in bytes):** | 3330260 | | |

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**
**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**
**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**
**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**