Qualcomm
TECHNOLOGIES, INC

EAP-SIM/AKA/AKA' Implementation using the QMI Authentication Service

Technical Memo

80-NA157-251 A

April 1, 2014

Confidential and Proprietary – Qualcomm Technologies, Inc.

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

Contents

Figures

Tables

Revision History

Revision	Date	Description
A	May 2014	Initial release.

1 Introduction

1.1 Purpose

This technical note provides a high-level description of how QMI clients on the applications processor can use QMI_AUTH service to perform authentication and session key distribution using Extensible Authentication Protocol (EAP) with Qualcomm modem devices.

The following EAP authentication mechanisms are supported via QMI_AUTH service:

- EAP-SIM [RFC 4186]
- EAP-AKA [RFC 4187]
- EAP-AKA' [RFC 5448]

1.2 Scope

This document is intended for licensees, infrastructure vendors, and mobile operators interested in the enablement of EAP authentication over WLAN and WWAN radio access technologies.

1.3 References

Reference documents are listed in Table 1-1. Reference documents that are no longer applicable are deleted from this table; therefore, reference numbers may not be sequential.

Table 1-1 Reference documents and standards

Ref.	Document	
Qualcomm Technologies		
Q1	*Application Note: Software Glossary for Customers*	CL93-V3077-1
Q2	*Qualcomm MSM Interface (QMI) Architecture*	80-VB816-1
Q3	*QMI AUTH For MPSS.BO.1.0, QMI Authentication Service Spec*	80-ND900-21
Q4	*QMI UIM For MPSS.BO.1.0, QMI User Identity Module Spec*	80-ND900-12
Standards		
S1	*Extensible Authentication Protocol (EAP)*	IETF RFC 3748
S2	*Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*	IETF RFC 4186
S3	*Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*	IETF RFC 4187
S4	*Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')*	IETF RFC 5448

1.4 Technical Assistance

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

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

1.5 Acronyms

For definitions of terms and abbreviations, refer to [Q1]. Table 1-2 lists terms that are specific to this document.

Table 1-2 Acronyms

Acronym	Definition
AKA	Authentication and Key Agreement
EAP	Extensible Authentication Protocol
IMSI	International Mobile Subscriber Identity
NAI	Network Access Identifier
QMI	Qualcomm messaging interface
SIM	subscriber identity module

2 Implementation

2.1 High Level Call Flow

The QMI_AUTH service provides authentication and session key distribution using the EAP mechanism. The service enables clients to use the wireless mobile station for EAP-SIM/AKA/AKA' authentication implemented as per [S1], [S2], [S3], and [S4].

NOTE: With this service, all EAP packets are packaged in QMI_AUTH messages and sent to the modem for processing. The processed EAP response from the modem can be forwarded by the QMI client to the EAP server through any radio access technology, e.g., WLAN. Refer to [Q3] for information about the QMI_AUTH service API.

Figure 2-1 illustrates a sample QMI_AUTH call flow.

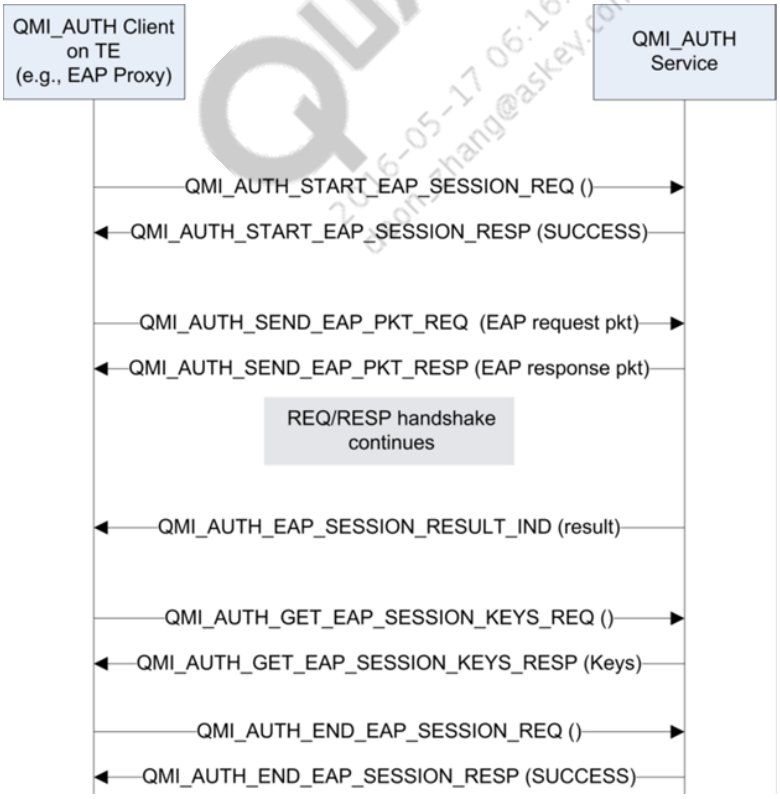

Figure 2-1 QMI_AUTH sample call flow

A QMI_AUTH service client must be created to enable QMI_AUTH services on a Qualcomm modem. This client, which resides on the applications processor, is then capable of invoking a series of functions that enable EAP authentication on the modem.

2.2 QMI_AUTH Service Initialization

Figure 2-2 illustrates the QMI_AUTH service initialization required during power up

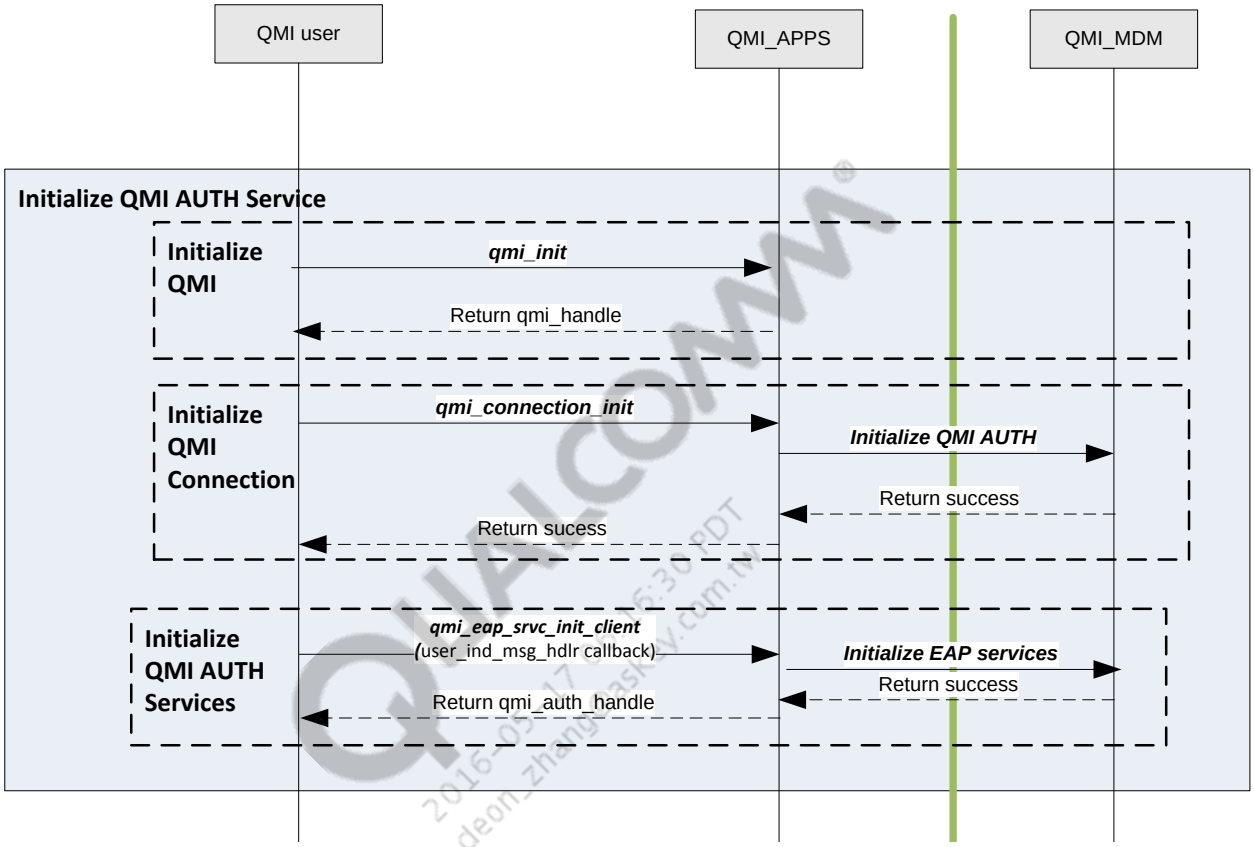

Figure 2-2 QMI_AUTH service power-up initialization

When the QMI_AUTH service power-up initialization procedure is complete, the QMI_AUTH service is ready to accept new client registration and new EAP session initiation requests.

2.3 QMI_UIM Service Initialization and Usage to Retrieve IMSI

The QMI_UIM service can be initialized during power up. Once the QMI_UIM service is initialized, QMI_UIM service clients can use the function shown in

to retrieve the IMSI. An IMSI-based NAI can then be formulated, which enables QMI_AUTH service clients to perform EAP-SIM/AKA/AKA' authentication. See [Q4] for QMI UIM service details.

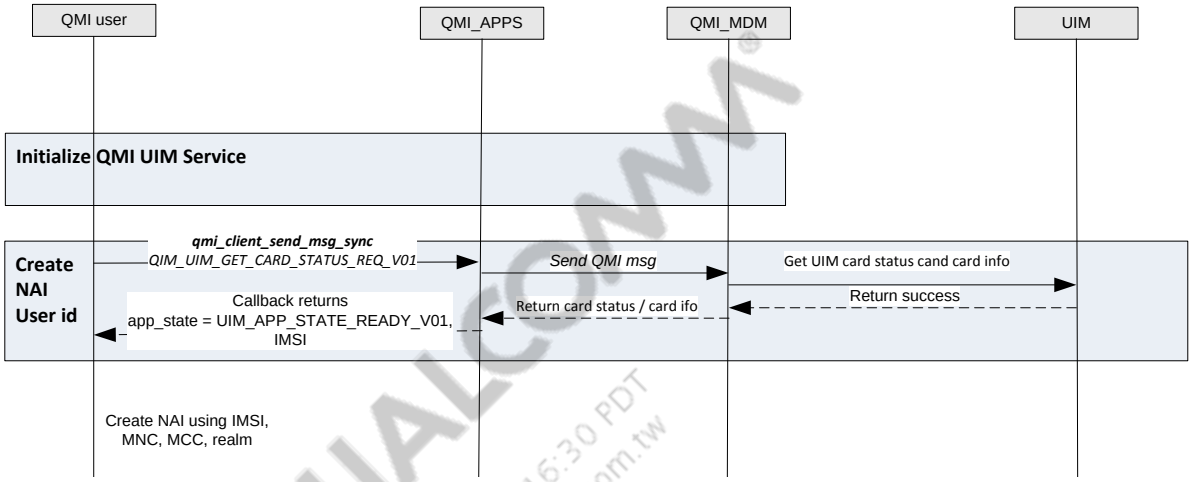

Figure 2-3 QMI_UIM service initialization, retrieving and creating IMSI-based NAI

2.4 EAP-SIM Full Authentication

Figure 2-4 illustrates a sample set of call flows for an EAP-SIM full authentication procedure per [S2]. These call flows were created using the QMI_AUTH service APIs and the IMSI-based NAI retrieved as per [Q3].

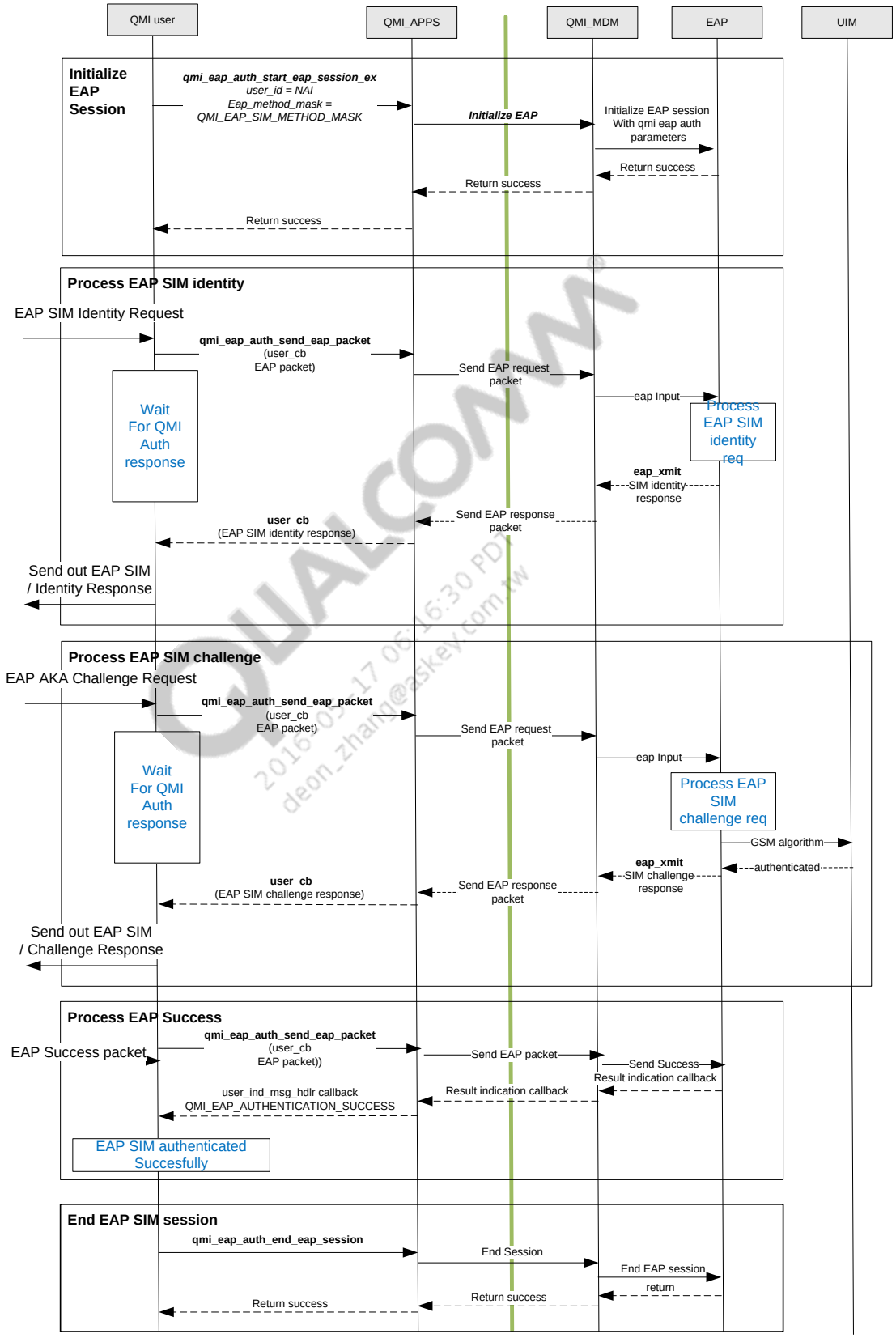

Figure 2-4 EAP-SIM session negotiation using the QMI_AUTH service

2.5 EAP-AKA Full Authentication

Figure 2-5 illustrates a sample set of call flows for an EAP-AKA full authentication procedure (per [S3]) using the QMI_AUTH service APIs [Q3] and the retrieved IMSI-based NAI.

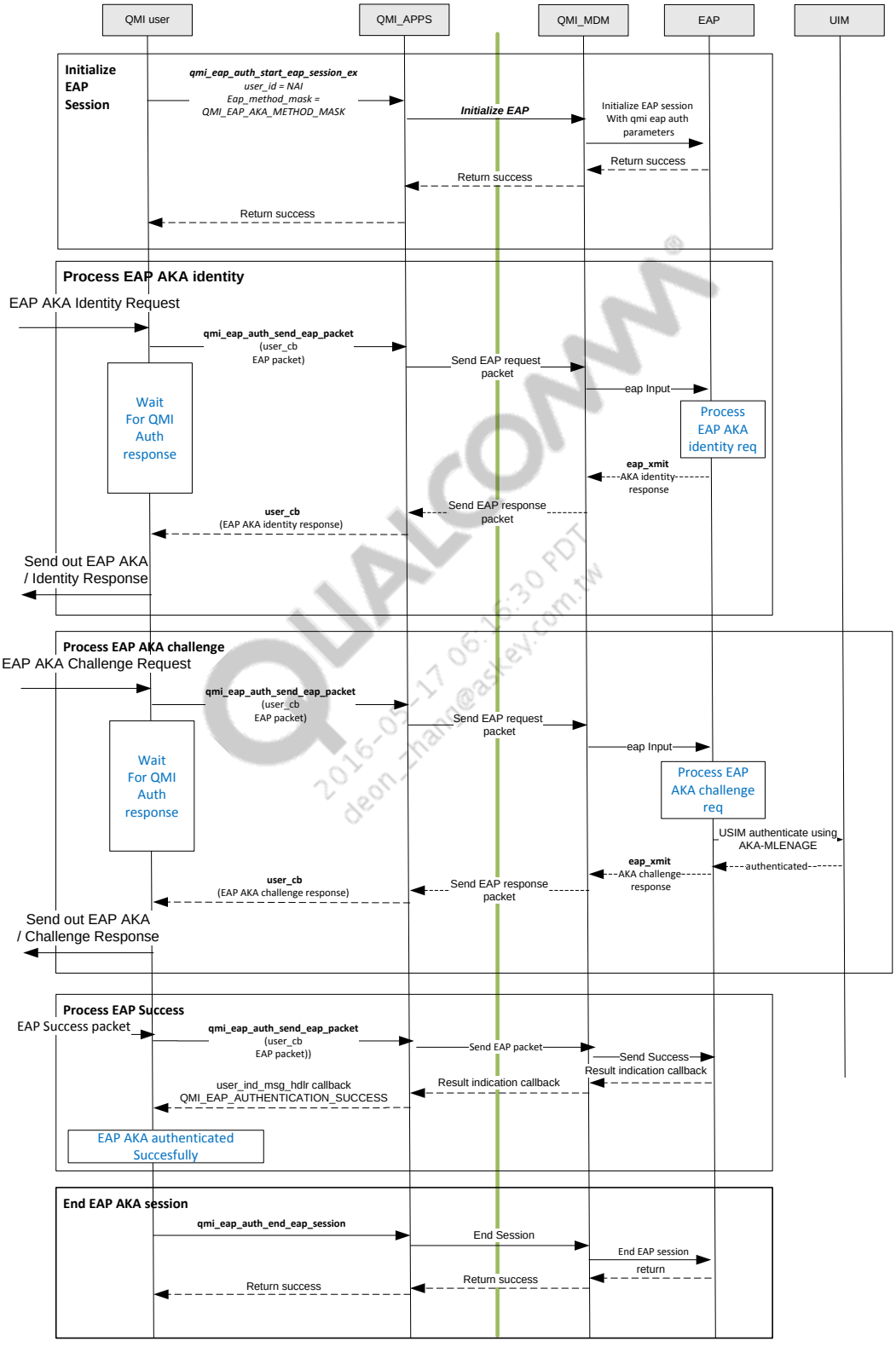

Figure 2-5 EAP-AKA session negotiation using QMI_AUTH service

2.6 EAP-AKA' Full Authentication

Figure 2-6 illustrates a sample set of call flows for an EAP-AKA' full authentication procedure per [S4]. These were created using the QMI_AUTH service APIs and the IMSI-based NAI retrieved as per [Q3].

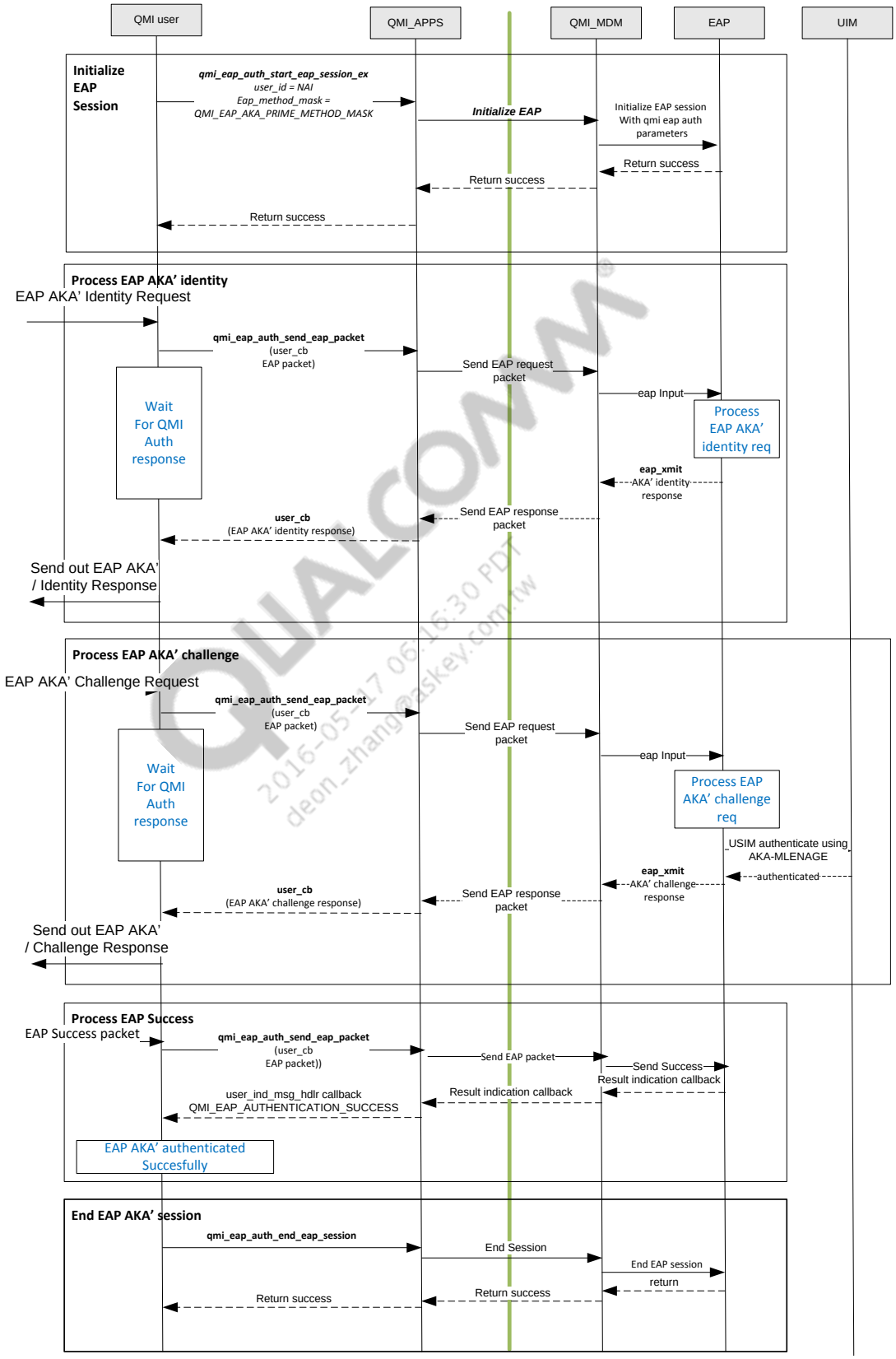

Figure 2-6 EAP-AKA' session negotiation using QMI_AUTH service

2.7 Support For Additional Functionality

Without the additional overhead of processing the EAP protocol packets, the QMI_AUTH service provides a unique way of EAP SIM/AKA/AKA' session negotiation. The QMI_AUTH service client having provisioned a QMI_AUTH EAP session client can retrieve the incoming EAP packet and transmit an outgoing EAP packet response back to the server with minimal processing.

In conjunction with the modem implementation of EAP, the QMI_AUTH service also supports:

- Fast re-authentication procedures for EAP-SIM/AKA/AKA'
- User anonymity (pseudonym) for EAP-SIM/AKA/AKA'
- Result indications for EAP-SIM/AKA/AKA'