International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.7

(08/2010)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services

Recommendation ITU-T J.366.7

Recommendation ITU-T J.366.7

IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services

Summary

Recommendation ITU-T J.366.7 specifies the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system as modified for use in cable networks.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.366.7	2010-08-29	9

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T J.366.7

IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services

1 Scope

This Recommendation specifies the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system as modified for use in cable networks.

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

Because this Recommendation indicates modifications from the ETSI specification [ETSI TS 133.203], the structure of the Recommendation does not follow normal ITU-T practice, so as to ease the task of the reader to correlate the two documents.

The modifications to the access security for IP-based services specification [ETSI TS 133.203] are shown in clause 6.

2 References

[ETSI TS 133.203] ETSI TS 133.203 V6.9.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the terms defined in [ETSI TS 133.203].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the abbreviations provided in [ETSI TS 133.203].

5 Conventions

This Recommendation uses the conventions provided in [ETSI TS 133.203].

6 Modifications to [ETSI TS 133.203]

Modifications introduced by this Recommendation are shown in revision marks. Unchanged text is replaced by ellipsis (…). Some parts of unchanged text (section numbers, etc.) may be kept to indicate the correct insertion points.

…

2 References

…

[25] 3GPP TR 33.978: "*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Aspects Of Early IMS*".

[26] IETF RFC 5626 (2009), *Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)*.

[27] OMA WAP-211-WAPCert, 22.5.2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-211-wapcert-20010522-a.pdf.

[28] IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

[29] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[30] OMA WAP-219-TLS, 4.11.2001, http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf.

[31] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

…

3.3 Abbreviations

…

SIP Session Initiation Protocol

TLS Transport Layer Security

4 Overview of the security architecture

…

The mechanisms specified in this technical specification are independent of the mechanisms defined for the CS- and PS-domain.

An independent IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IMS would continue to be protected by it's own security mechanism. As indicated in figure 1 the P-CSCF may be located either in the Visited or the Home Network. The P-CSCF shall be co-located within the same network as the GGSN, which may reside in the VPLMN or HPLMN according to the APN and GGSN selection criteria, cf. TS 23.060 [10].

NOTE – The text in this specification applies to both IPsec and TLS-based access security unless otherwise noted.

P-CSCF in the Visited Network.

• • •

5.1 Secure access to IMS

5.1.1 Authentication of the subscriber and the network

• • •

The AKA-protocol is a secure protocol developed for UMTS and the same concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA.

NOTE – Although the method of calculating the parameters in UTMS AKA and IMS AKA are identical, the parameters are transported in slightly different ways. In UMTS, the UE's response RES is sent in the clear, while in IMS RES is not sent in the clear but combined with other parameters to form an authentication response and the authentication response is sent to the network (as described in RFC 3310 [17]).

An optional mechanism for authentication is SIP Digest. It is also a challenge response protocol, and operates in a similar manner to IMS AKA. An authentication vector containing authentication information is sent from the Home Stratum to the Serving Network. The serving network uses the authentication information in an authentication vector to authenticate the UE.

The Home Network authenticates the subscriber at anytime via the registration or re-registration procedures.

• • •

5.1.3 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation.

The following mechanisms are provided at SIP layer: for IPsec-based access security:

1) The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in clause 7.

2) The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1.

The following mechanisms are provided for TLS-based access security:

1) Negotiation of TLS related confidentiality protection features shall take place at the TLS layer as specified in clause 7.1.2.

2) The UE shall always offer TLS cipher suites for P-CSCF to be used for the session, as specified in RFC 2246 [31].

3) The P-CSCF shall decide whether the TLS cipher suites are used. If used, the UE and the P-CSCF shall agree on TLS cipher suites at the TLS layer as specified in RFC 2246 [31].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling, as specified in clause 6.3.

The following mechanisms are provided for IPsec-based access security-:

1) The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session, as specified in clause 7.

2) The UE and the P-CSCF shall agree on security associations, which include the integrity keys, that shall be used for the integrity protection. The mechanism is based on IMS AKA and specified in clause 6.1.

3) The UE and the P-CSCF shall both verify that the data received originates from a node, which has the agreed integrity key. This verification is also used to detect if the data has been tampered with.

4) Replay attacks and reflection attacks shall be mitigated.

The following mechanisms are provided for TLS-based access security:

1) Negotiation of TLS-related integrity protection features shall take place at the TLS layer.

2) The use of TLS cipher suites with NULL integrity protection (or HASH) shall not be allowed.

3) The UE and the P-CSCF shall both verify that the data received originates from each other according to RFC 2246 [31]. This verification is also used to detect if the received data has been tampered with.

4) Replay attacks and reflection attacks shall be mitigated.

Integrity protection between CSCFs and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

NOTE 1 – TLS is mandatorily supported by SIP proxies according to RFC 3261 [6], and operators may use it to provide confidentiality and integrity inside their networks instead of or on top of IPsec, as the intra-domain Za interface is optional, and TLS may also be used between IMS networks on top of IPsec. It should be pointed out, that the 3GPP specifications do not provide support for TLS certificate management in a fashion similar to TS 33.310 (NDS/AF) [24] nor do they ensure backward compatibility with Release 5 CSCFs nor interoperability with other networks which do not use TLS, in case TLS is used by Release 6 CSCFs. These management and capability issues need then to be solved by manual configuration of the involved operators.

• • •

6.1 Authentication and key agreement

The One scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. figure 1. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. TS 23.228 [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g., keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in TS 33.102 [1]. The ISIM and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in TS 33.102 [1]. The AMF field can be used in the same way as in TS 33.102 [1].

An additional scheme for authentication is SIP Digest as specified in RFC 3261 [6]. SIP Digest achieves mutual authentication between the UE and the HN. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI. The HSS and the UE share a

preset secret associated by the IMPI. The generation of the authentication challenge shall be done in the same way as specified in RFC 3261 [6] and this document.

The HN shall choose the appropriate scheme for authenticating an IM subscriber based on the authentication algorithm parameter received from the UE in the initial register request. To mitigate bid down attacks, the HN may specify the lowest acceptable authentication algorithm to be used for authenticating an IM subscriber.

~~Furthermore~~If IPsec based access security is used, two pairs of (unilateral) security associations (SAs) are established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only two pairs of SAs shall be active between the UE and the P-CSCF. These two pairs of SAs shall be updated when a new successful authentication of the subscriber has occurred, cf. clause 7.4.

If both the UE and the P-CSCF support TLS, a server side authenticated TLS session may be established between the UE and the P-CSCF before the first SIP message is sent. If a TLS session is established prior to the initial register, the TLS session will exist until de-registration of the UE. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. If a TLS session is established, only one TLS tunnel shall be active between the UE and the P-CSCF.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g., belonging to same or different service profiles. Regarding the definition of service profiles cf. TS 23.228 [3].

6.1.1 Authentication of an IM-subscriber

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e., the S-CSCF, cf. figure 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.

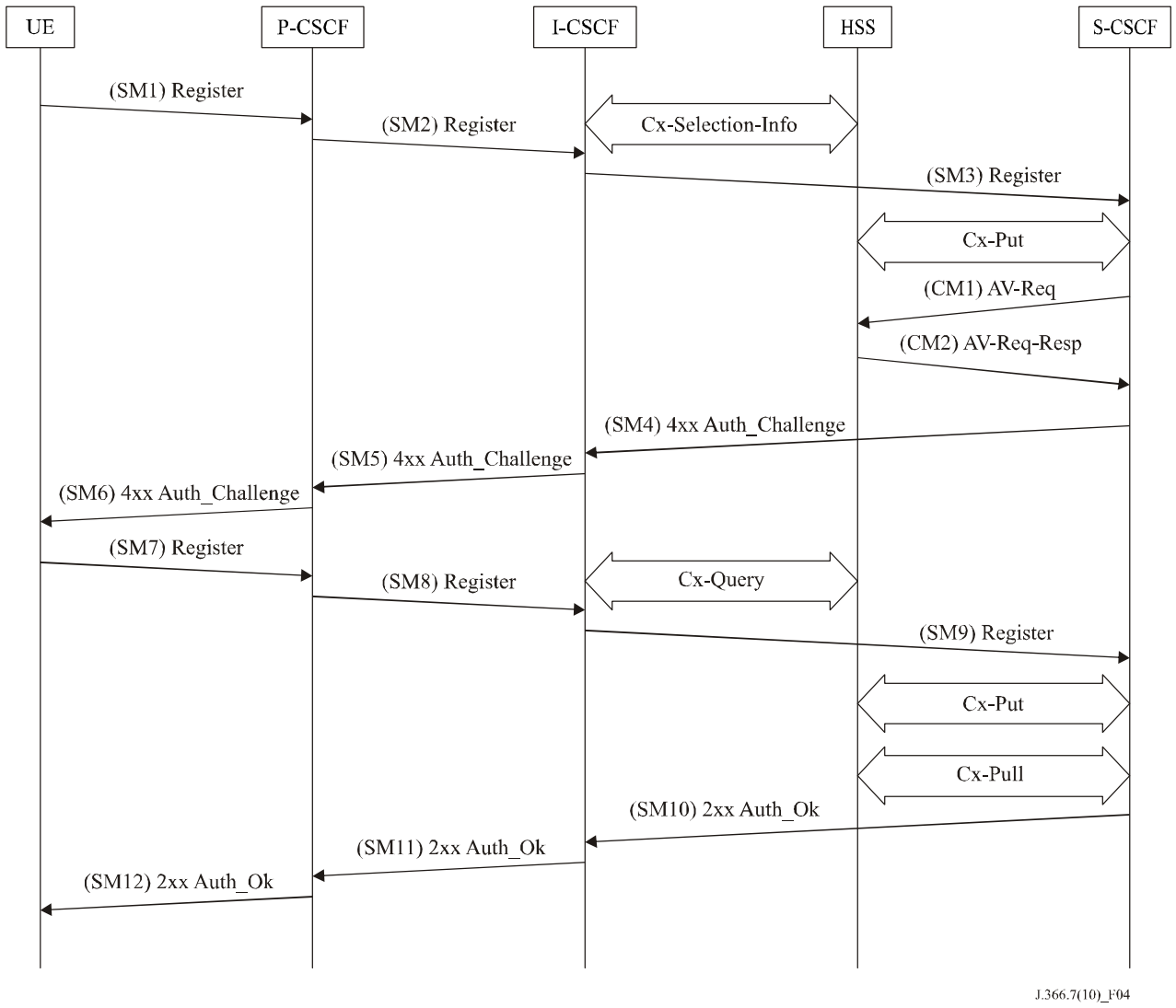

Figure 4 – The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

The detailed requirements and complete registration flows are defined in TS 24.229 [8] and TS 24.228 [11].

SMn stands for SIP Message n and CMm stands for Cx message m which has a relation to the authentication process:

IMS AKA based SM1:
REGISTER(IMPI, IMPU)
SIP Digest based SM1:
REGISTER(IMPI, IMPU, algorithm)

The UE adds the algorithm parameter in Authorization header to the initial register message SM1, in order to inform HN what type of challenge to create.

In SM2 and SM3 the P-CSCF and the I-CSCF respectively forwards the SIP REGISTER towards the S-CSCF.

After receiving SM3, if the IMPU is not currently registered at the S-CSCF, the S-CSCF needs to set the registration flag at the HSS to initial registration pending. This is done in order to handle mobile terminated calls while the initial registration is in progress and not successfully completed. The registration flag is stored in the HSS together with the S-CSCF name and user identity, and is used to indicate whether a particular IMPU of the user is unregistered or registered at a particular

S-CSCF or if the initial registration at a particular S-CSCF is pending. The registration flag is set by the S-CSCF sending a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF shall leave the registration flag set to *registered*. At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

Upon receiving the SIP REGISTER the S-CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S-CSCF has no valid AV then the S-CSCF shall send a request for AV(s) to the HSS in CM1 together with the number m of AVs wanted where m is at least one.

CM1:
Cx-AV-Req(IMPI, m)

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF using CM2. The authentication vectors are ordered based on sequence number. For IMS AKA, each ~~Each~~ authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each IMS AKA authentication vector is good for one authentication and key agreement between the S-CSCF and the IMS user. For the SIP Digest-based authentication, the authentication vector consists of the qop (quality of protection) value, the authentication algorithm, opaque, realm, and a hash, called H(A1), of the username, realm, and password. Refer to RFC 2617 [12] for additional information on the values in the authentication vector for SIP Digest based authentication.

IMS AKA based CM2:
Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,....,RANDn||AUTNn||XRESn||CKn||IKn)
SIP Digest based CM2:
Cx-AV-Req-Resp(IMPI, qop, algorithm, opaque, realm, H(A1))

When the S-CSCF needs to send an authentication challenge to the user, it selects the next authentication vector from the ordered array, i.e., authentication vectors in a particular S-CSCF are used on a first-in / first-out basis.

For IMS AKA, the~~The~~ S-CSCF sends a SIP 4xx Auth_Challenge i.e., an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P-CSCF. RFC 3310 [17] specifies how to populate the parameters of an authentication challenge. The S-CSCF also stores the RAND sent to the UE for use in case of a synchronization failure.

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S-CSCF to re-use a AV. Therefore no AV shall be sent more than once.

For SIP Digest-based authentication, the S-CSCF stores H(A1), and then sends a SIP 4xx Auth_Challenge i.e., an authentication challenge towards the UE including the challenge nonce and in SM4. The qop, algorithm, and opaque parameters shall be present. The nonce shall be 32 octets ASCII hexadecimal encoded and shall be calculated following the procedures defined in RFC 1750 [28]. The S-CSCF shall have the capability to support next-nonce. The S-CSCF shall have the capability to set time-limits and reuse count limits on the nonce.

NOTE – This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

IMS AKA based SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)
SIP Digest based SM4:
4xx Auth_Challenge(IMPI, nonce, qop=auth and/or auth-int, algorithm, opaque)

For IMS AKA, when ~~When~~ the P-CSCF receives SM5, it shall store the key(s) and remove that information and forward the rest of the message to the UE; for SIP Digest, the P-CSCF shall forward the message to the UE, i.e.,

IMS AKA based SM6:
4xx Auth_Challenge(IMPI, RAND, AUTN)
SIP Digest based SM6:
4xx Auth_Challenge(IMPI, nonce, qop=auth and/or auth-int, algorithm, opaque)

For IMS AKA, upon~~Upon~~ receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in TS 33.102 [1]. If both these checks are successful the UE uses RES and some other parameters to calculate an authentication response. This response is put into the Authorization header and sent back to the registrar in SM7. RFC 3310 [17] specifies how to populate the parameters of the response. It should be noted that the UE at this stage also computes the session keys CK and IK.

For SIP Digest, upon receiving the challenge, the UE shall calculate a cnonce of 16 binary octets following the procedures defined in RFC 1750 [28]. To calculate the response, the UE shall choose a qop value from the values received from the S-CSCF. The UE shall use nonce, cnonce, nc and qop to calculate an authentication response per RFC 3261 and thus RFC 2617. This response is also put into the Authorization header and sent back to the registrar in SM7.

IMS AKA based SM7:
REGISTER(IMPI, Authentication response)
SIP Digest based SM7:
REGISTER(IMPI, response, cnonce, qop=auth or auth-int, digest-uri, nonce-count)

The P-CSCF forwards the authentication response in SM8 to the I-CSCF, which queries the HSS to find the address of the S-CSCF. In SM9 the I-CSCF forwards the authentication response to the S-CSCF.

For IMS AKA, upon ~~Upon~~ receiving SM9 containing the response, the S-CSCF retrieves the active XRES for that user and uses this to check the authentication response sent by the UE as described in RFC 3310 [17]. For SIP Digest, the S-CSCF calculates the expected response using H(A1) and other parameters (e.g., nonce, cnonce, qop) and uses this to check against the response sent by the UE as specified in RFC 3261 [6]. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. If the IMPU was not currently registered, the S-CSCF shall send a Cx-Put to update the registration-flag to *registered*. If the IMPU was currently registered the registration-flag is not altered.

It shall be possible to implicitly register IMPU(s). (see clause 4.3.3.4 in TS 23.228 [3]). All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

When an IMPU has been registered this registration will be valid for some period of time. Both the UE and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable without interruptions. A successful registration of a previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

If the user has been successfully authenticated, the S-CSCF sends a SM10 SIP 2xx Auth_OK message to the I-CSCF indicating that the registration was successful. For SIP Digest, the 2xx Auth_OK message contains the Authentication-Info header with a response digest as specified in RFC 3261 [6]. The response digest allows the UE to authenticate the HN. The Authentication-Info header should contain the nextnonce parameter. In SM11 and SM12 the I-CSCF and the P-CSCF respectively forward the SIP 2xx Auth_OK towards the UE.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with an incorrect authentication response in order to make the HN de-register the IMPU. For this reason a subscriber, when registered, shall not be de-registered if it fails an authentication.

For IMS AKA, the ~~The~~ lengths of the IMS AKA parameters are specified in clause 6.3.7 of TS 33.102 [1].

6.1.2 Authentication failures

6.1.2.1 User authentication failure

In this case the authentication of the user should fail at the S-CSCF due an incorrect response (received in SM9). However, for IMS AKA, if the response is incorrect, then the IK used to protect SM7 will normally be incorrect as well, which will normally cause the integrity check at the P-CSCF to fail before the response can be verified at S-CSCF. In this case SM7 is discarded by the IPsec layer at the P-CSCF.

If the integrity check passes but the response is incorrect, the message flows are identical up to and including SM9 as a successful authentication. Once the S-CSCF detects the user authentication failure it should proceed in the same way as having received SM9 in a network authentication failure (see clause 6.1.2.2).

For SIP Digest, if the S-CSCF detects the user authentication failure, and the nonce used by UE is incorrect, the S-CSCF should send a new 401 (Unauthorized) message to the UE, using the stale parameter to inform the UE that the Digest response was calculated correctly (the username/password were correct), but the nonce is invalid. An invalid nonce may have been used outside local policy time-limits, or may have been used more times than local policy allows.

For SIP Digest, once the S-CSCF detects the user authentication failure, it shall set the registration-flag in the HSS to unregistered, or Not registered if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF does not update the registration flag.

CM3:
Cx-AV-Put(IMPI, Clear S-CSCF name)

The HSS responds to CM3 with a Cx-Put-Resp in CM4.

In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed. No security parameters shall be included in this message.

SM10:
SIP/2.0 4xx Auth_Failure

6.1.2.2 Network authentication failure

In this clause the case when the authentication of the network is not successful is specified. For IMS AKA, when~~When~~ the check of the MAC in the UE fails the network cannot be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM6.

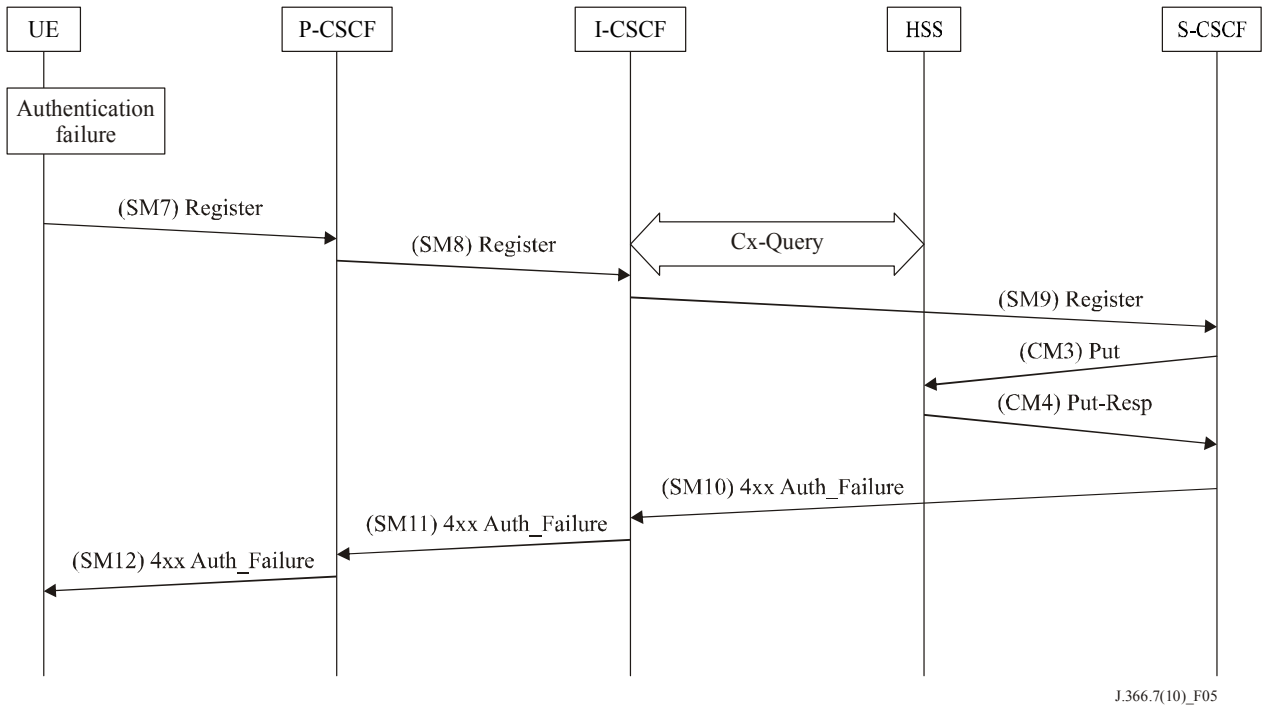

Figure 5

The UE shall send a Register message towards the HN including an indication of the cause of failure in SM7. The P-CSCF and the I-CSCF forward this message to the S-CSCF.

SM7:
REGISTER(Failure = *AuthenticationFailure*, IMPI)

Upon receiving SM9, which includes the cause of authentication failure, the S-CSCF shall set the registration-flag in the HSS ~~*tounregistered*~~ to *unregistered* or *Not registered*, if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF does not update the registration flag.

CM3:
Cx-AV-Put(IMPI, Clear S-CSCF name)

The HSS responds to CM3 with a Cx-Put-Resp in CM4.

In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed, no security parameters shall be included in this message.

SM10:
SIP/2.0 4xx Auth_Failure

For SIP Digest, the flow is identical as for the successful registration in 6.1.1 up to SM12. After receipt of the 2xx Auth_OK, the UE will attempt to validate the response digest. If the response digest authentication fails, the UE shall not send any further SIP messages.

• • •

6.1.3 Synchronization failure

In this clause the case of an authenticated registration with synchronization failure is described.

After re-synchronization, authentication may be successfully completed, but it may also happen that in subsequent attempts other failure conditions (i.e., user authentication failure, network authentication failure) occur. In below only the case of synchronization failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions.

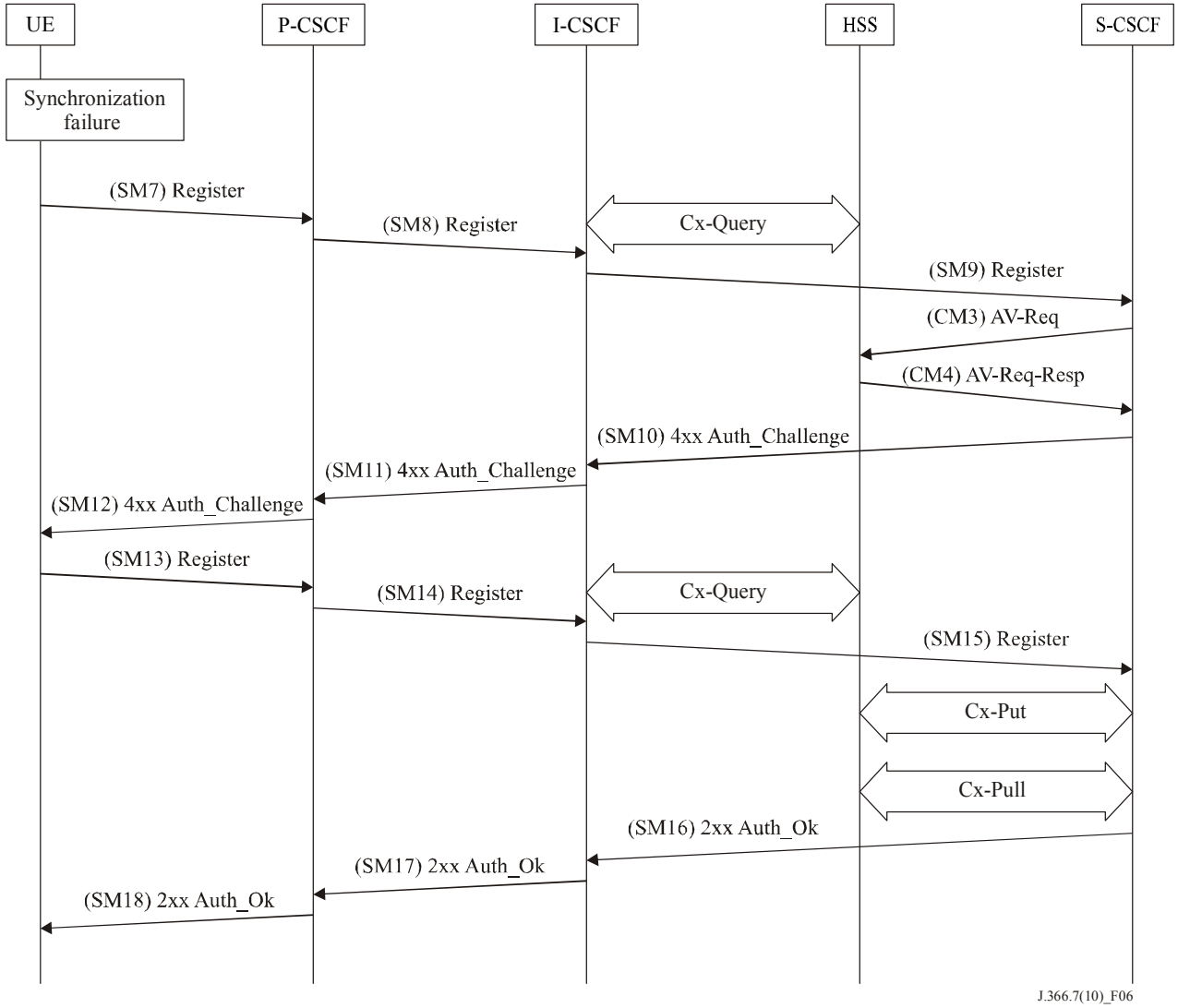

Figure 6

The flow equals the flow in 6.1.1 up to SM6. For IMS AKA based authentication, w~~W~~hen the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7. RFC 3310 [17] describes the fields to populate corresponding parameters of synchronization failure.

SM7:
REGISTER(Failure = *Synchronization Failure,* AUTS, IMPI*)*

Upon receiving the *Synchronization Failure* and the AUTS the S-CSCF sends an Av-Req to the HSS in CM3 including the RAND stored by the S-CSCF and the required number of Avs, m.

CM3:
Cx-AV-Req(IMPI, RAND,AUTS, m)

The HSS checks the AUTS as in clause 6.3.5 of TS 33.102 [1]. After potentially updating the SQN, the HSS sends new AVs to the S-CSCF in CM4.

CM4:
Cx-AV-Req-Resp(IMPI, n,$RAND_1$||$AUTN_1$||$XRES_1$||CK_1||IK_1,….,$RAND_n$||$AUTN_n$||$XRES_n$||CK_n||IK_n)

When the S-CSCF receives the new batch of authentication vectors from the HSS it deletes the old ones for that user in the S-CSCF.

The rest of the messages i.e., SM10-SM18 including the Cx messages are exactly the same as SM4-SM12 and the corresponding Cx messages in 6.1.1.

For SIP Digest-based authentication, the UE cannot detect synchronization failures when processing SM6 but the S-CSCF can check if the nonce value in SM9 is invalid with a valid digest for that nonce (indicating that the client knows the correct username/password) to determine that a synchronization failure has occurred. In this situation, the S-CSCF shall reject the request and send out the challenge (i.e., SM4) again using a new nonce. The stale parameter in the www-Authenticate header is set to TRUE (case-insensitive) in this message.

When the UE receives the challenge with the stale parameter in the www-Authenticate header set to TRUE, it shall retry the REGISTER request with a new encrypted response (i.e., starting from SM7 in figure 6), without re-prompting the user for a new username and password.

6.1.4 Network Initiated authentications

In order to authenticate an already registered user, the S-CSCF shall send a request to the UE to initiate a re-registration procedure. When received at the S-CSCF, the re-registration shall trigger a new IMS AKA procedure or SIP Digest procedure that will allow the S-CSCF to re-authenticate the user.

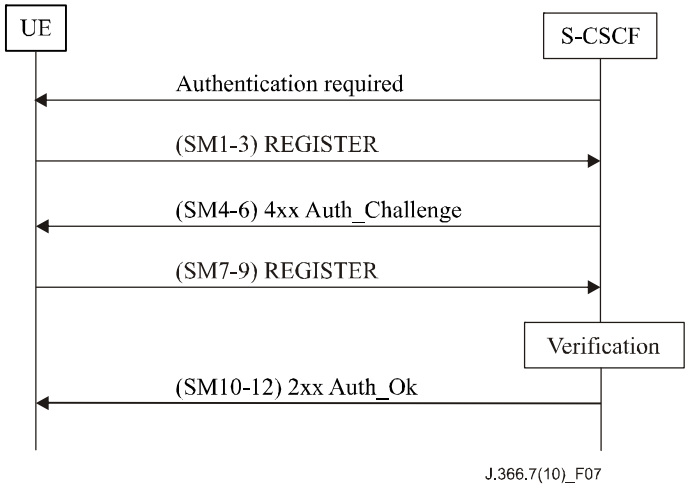

Figure 7

The UE shall initiate the re-registration on the reception of the Authentication Required indication. In the event that the UE does not initiate the re-registration procedure after the request from the S-CSCF, the S-CSCF may decide to de-register the subscriber or re-issue an Authentication-Required.

6.1.5 Integrity protection indicator

In the context of integrity protection, an SA is a secure channel for exchanging messages. For IPSec-based access security, an IPSec SA is an integrity protection SA. For TLS-based access security, a mutually authenticated TLS channel is considered an integrity protection SA.

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if:

– the P-CSCF receives a REGISTER containing an authentication response and the message is protected with an SA created during this authentication procedure; or

– the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with an SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

6.2 Confidentiality mechanisms

Add the following at the end of the clause:

The encryption key expansion on the user side is done in the UE. The encryption key expansion on the network side is done in the P-CSCF.

TLS-based protection mechanisms are specified in clause 7.1.2.

6.3 Integrity mechanisms

Add the following at the end of the clause:

The integrity key expansion on the user side is done in the UE. The integrity key expansion on the network side is done in the P-CSCF.

The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.

TLS-based protection mechanisms are specified in clause 7.1.2.

6.4 Hiding mechanisms

No Change.

6.5 CSCF interoperating with proxy located in a non-IMS network

No Change.

7 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services to apply and when the security services start. In the IMS authentication of users is performed during registration as specified in clause 6.1. Subsequent signalling communications in this session will be integrity protected based on the security association that was established ~~keys derived~~ during the authentication process.

7.1 Security association parameters

The existing text becomes clause 7.1.1 and a new clause 7.1.2 is created.

7.1.1 IPsec-based access security

For protecting IMS signalling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication and confidentiality, in accordance with the provisions in clauses 5.1.3 and 6.2.

…

7) For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE_protected_port, P-CSCF_protected_port) in the "SA table".

NOTE – If the integrity check of a received packet fails then IPsec will automatically discard the packet.

7.1.2 TLS profile for TLS-based access security

The UE and the P-CSCF shall support the TLS version as specified in RFC 2246 [31], WAP-219-TLS [30], RFC 3268 [29], or higher. Earlier versions are not allowed.

– **Protection mechanisms**

- The UE and P-CSCF shall support the CipherSuite TLS_RSA_WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [31] and RFC 3268 [29] are optional for implementation.
- Cipher Suites with NULL encryption shall not be used. During the TLS handshake phase the UE should offer the TLS Cipher Suites that it supports and is willing to use for encryption.
- Cipher Suites with NULL integrity protection (or HASH) shall not be allowed.
- RFC 2246 [31] supports the negotiation and use of compression methods. However, since these methods are not specified within RFC 2246 [31], compression shall not be used.

– **Authentication of the P-CSCF**

- The P-CSCF shall be authenticated by the UE as specified in RFC 2246 [31] by presenting a valid server certificate.
- The P-CSCF may be authenticated by the UE as specified in WAP-219-TLS [30].
- If the P-CSCF is authenticated by use as specified in WAP-219-TLS [30], the P-CSCF certificate profile shall be based on WAP Certificate as defined in WAP-211-WAPCert [27]. If a PKI is used, additional CRL profile should be as defined in WAP-211-WAP-Cert [27].

– **Authentication of the UE**

- The P-CSCF shall not request a certificate in a Server Hello Message from the UE. The S-CSCF shall authenticate the UE as specified in clause 6.1.1.

– **Verification of the TLS tunnel endpoints**

- In order for the UE to be able to trust the TLS tunnel endpoint, the P-CSCF certificate shall be used during the authentication procedure.

– **TLS session parameters**

- The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The UE and the P-CSCF shall allow for resuming a session. The lifetime of a Session ID is subject to local policies of the UE and the P-CSCF. A recommended lifetime is one hour (or at least more than the re-REGISTRATION time out). The maximum lifetime specified in RFC 2246 [31] is 24 hours.

– **Ports**

- The P-CSCF shall be prepared to accept TLS session requests on port 5061.
- The procedures in <sip-outbound> [26] shall apply when managing TLS connections.

7.2 Set-up of security associations (successful case)

The existing text becomes clause 7.2.1 and a new clause 7.2.2 is created.

7.2.1 IPsec-based access security

The set-up of security associations is based on RFC 3329 [21]. Annex H of this specification shows how to use RFC 3329 [21] for the set-up of security associations.

•••

An example of how to make use of two pairs of unidirectional SAs is illustrated in the figure below with a set of example message exchanges protected by the respective IPsec SAs where the INVITE and following messages are assumed to be carried over TCP.

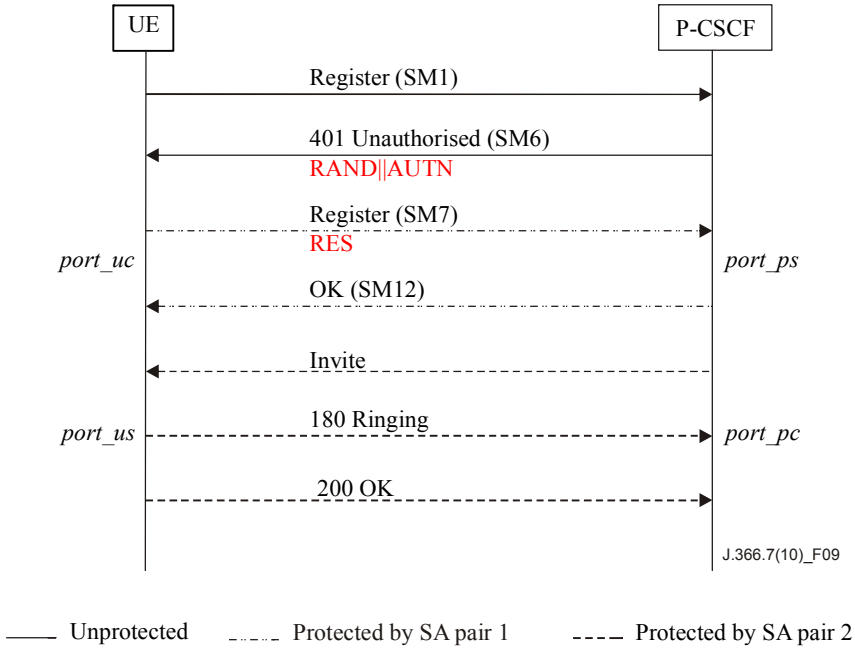

Figure 9

7.2.2 TLS-based access security

The set-up of the TLS tunnel between the UE and the P-CSCF is based on the TLS profile specified in clause 7.1.2. The sip-sec-agree negotiation according to RFC 3329 [21] is performed during the registration procedure to confirm the choice of the security mechanism. Annex H of this specification explains how to use RFC 3329 [21] for the set-up of security associations.

If the UE supports TLS, the UE and the P-CSCF may set up a server authenticated TLS tunnel prior to the registration procedure, where the P-CSCF uses a server certificate for authentication. If the TLS tunnel is negotiated prior to the register, all the messages between the UE and the P-CSCF shall be sent through this TLS tunnel.

7.3 Error cases in the set-up of security associations

7.3.1 Error cases related to IMS AKA and TLS-based access security

Errors related to IMS AKA failures are specified in clause 6.1. However, this clause additionally describes how these shall be treated, related to security association setup.

7.3.1.1 User authentication failure

For IPsec-based access security the following applies:

In this case, SM7 fails integrity check by IPsec at the P-CSCF if the IK_{IM} derived from RAND at UE is wrong. The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily stored SA parameters associated with this registration after a time-out.

In case IK_{IM} was derived correctly, but the response was wrong the authentication of the user fails at the S-CSCF due to an incorrect response. The S-CSCF shall send a 4xx Auth_Failure message to the UE, via the P-CSCF, which may pass through an already established SA. Afterwards, both, the UE and the P-CSCF shall delete the new SAs.

For TLS-based access security the following applies:

If the UE response does not match with the response calculated by the S-CSCF, the authentication of the user fails at the S-CSCF. The S-CSCF shall send a 4xx Auth_Failure message to the UE, via the P-CSCF. Afterwards, both the UE and the P-CSCF shall delete the TLS tunnel if one was established.

7.3.1.2 Network authentication failure

For IPsec-based access security the following applies:

If the UE is not able to successfully authenticate the network, the UE shall send a REGISTER message which may pass through an already established SA, indicating a network authentication failure, to the P-CSCF. The P-CSCF deletes the new SAs after receiving this message.

For TLS-based access security the following applies:

If the UE is not able to successfully authenticate the network due to failed validation of the P-CSCF certificate, the UE shall send an alert message to the P-CSCF, which includes the failure information as specified in RFC 2246 [31].

7.3.1.3 Synchronisation failure

For IPsec-based access security the following applies:

In this situation, the UE observes that the AUTN sent by the network in SM6 contains an out-of-range sequence number. The UE shall send a REGISTER message to the P-CSCF, which may pass through an already established SA, indicating the synchronization failure. The P-CSCF deletes the new SAs after receiving this message.

For TLS-based access security the following applies:

When the UE receives the challenge with the stale parameter in the www-Authenticate header set to TRUE, the UE shall retry the REGISTER request with a new encrypted response, without re-prompting the user for a new username and password. The existing TLS session shall be used for the retry.

7.3.1.4 Incomplete authentication

For IPsec-based access security the following applies:

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

When the P-CSCF receives a challenge from the S-CSCF and creates the corresponding SAs during a registration procedure, it shall delete any information relating to any previous registration procedure (including the SAs created during the previous registration procedure).

If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to the registration procedure that created the SA.

For TLS-based access security the following applies:

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services.

7.3.2 Error cases related to the Security-Set-up

7.3.2.1 Proposal unacceptable to P-CSCF

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command of SM1. The P-CSCF shall respond to SM1 indicating a failure, by sending an error response to the UE.

7.3.2.2 Proposal unacceptable to UE

If the P-CSCF sends in the security-setup line of SM6 a proposal that is not acceptable for the UE, the UE shall abandon the registration procedure.

7.3.2.3 Failed consistency check of Security-Set-up lines at the P-CSCF

For IPsec-based access security the following applies:

The P-CSCF shall check whether authentication and encryption algorithms list received in SM7 is identical with the authentication and encryption algorithms list sent in SM6. If this is not the case the registration procedure is aborted. (Cf. clause 7.2).

7.4 Authenticated re-registration

For IPsec-based access security the following applies:

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P-CSCF handle this replacement and which SAs to apply to which message.

When security associations are changed in an authenticated re-registration then the protected server ports at the UE (*port_us*) and the P-CSCF (*port_ps*) shall remain unchanged, while the protected client ports at the UE (*port_uc*) and the P-CSCF (*port_pc*) shall change. For the definition of these ports see clause 7.1.

If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case,

the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE considers the SAs no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message.

Security associations may be unidirectional or bi-directional. This clause assumes that security associations are unidirectional, as this is the general case. For IP layer SAs, the lifetime mentioned in the following clauses is the lifetime held at the application layer. Furthermore deleting an SA means deleting the SA from both the application and IPsec layer. The message numbers, e.g., SM1, used in the following clauses relate to the message flow given in clause 6.1.1.

For TLS-based access security the following applies:

If established, the lifetime of the TLS session negotiated between the UE and the P-CSCF is subject to local policies. Either party can force a full handshake as specified in RFC 2246 [31]. All the registration messages must be protected by an active TLS session.

7.4.1 Void

7.4.1a Management of security associations in the UE

For IPsec-based access security the following applies:

The UE shall be involved in only one registration procedure at a time, i.e., the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with two existing pairs of SAs. These will be referred to as the old SAs. The authentication produces two pairs of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

– The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.

– The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.

– If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to clause 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. Meanwhile, if SM1 was protected, the UE shall use the old SAs for messages other than those in the authentication, until a successful message of new authentication is received (SM12); if SM1 was unprotected, the UE is not allowed to use IMS service until it receives an authentication successful message (SM12).

– The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.

– After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life. For further SIP messages sent from UE, the new outbound SAs are used, with the following exception: when a SIP message is part of a pending SIP transaction it may still be sent over the old SA. A SIP transaction is called pending if it was started using an old SA. When a further SIP message protected with a new inbound SA is successfully received from the P-CSCF, then the old SAs shall be deleted as soon as either

all pending SIP transactions have been completed, or have timed out. The old SAs shall be always deleted when the lifetime is expired. This completes the SA handling procedure for the UE.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the UE shall delete the new SAs.

The UE shall monitor the expiry time of registrations without an authentication and if necessary increase the lifetime of the SAs created by the last successful authentication such that it will expire shortly after the registration timer in the message.

NOTE – In particular this means that the lifetime of a SA is never decreased.

The UE shall delete any SA whose lifetime is exceeded. The UE shall delete all SAs it holds once all the IMPUs are de-registered.

For TLS-based access security the following applies:

The UE shall be involved in only one registration procedure at a time, i.e., the UE shall remove any data relating to any previous incomplete registrations or authentications, including any TLS tunnel created by an incomplete authentication.

7.4.2 Void

7.4.2a Management of security associations in the P-CSCF

For IPsec-based access security the following applies:

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain existing SAs from previously completed authentications. It may also contain two existing pairs of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces two pairs of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI to an SA.

A successful authentication proceeds in the following steps:

– The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA.

– The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA, if SM1 was protected and unprotected otherwise.

– The P-CSCF then creates the new SAs, which are derived according to clause 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.

– The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. If SM1 was protected, the old SAs are used to protect messages other than those in the authentication.

– The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs such that they either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the

message, depending which gives the SAs the longer life.

– After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:
  – If there are old SAs, but SM1 belonging to the same registration procedure was received unprotected, the P-CSCF considers error cases happened, and assumes UE does not have those old SAs for use. In this case the P-CSCF shall remove the old SAs.
  – If SM1 belonging to the same registration procedure was protected with an old valid SA, the P-CSCF keeps this inbound SA and the corresponding three SAs created during the same registration with the UE active, and continues to use them. Any other old SAs are deleted. When the old SAs have only a short time left before expiring or a further SIP message protected with a new inbound SA is successfully received from the UE, the P-CSCF starts to use the new SAs for outbound messages with the following exception: when a SIP message is part of a pending SIP transaction it may still be sent over the old SA. A SIP transaction is called pending if it was started using an old SA. The old SAs are then deleted as soon as all pending SIP transactions have been completed, or have timed out. The old SAs are always deleted when the old SAs lifetime are expired. When the old SAs expire without a further SIP message protected by the new SAs, the new SAs are taken into use for outbound messages. This completes the SA handling procedure for the P-CSCF.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SAs. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the P-CSCF shall delete the new SAs.

The P-CSCF shall monitor the expiry time of registrations without an authentication and if necessary increase the lifetime of SAs created by the last successful authentication such that it will expire shortly after the registration timer in the message.

The P-CSCF shall delete any SA whose lifetime is exceeded. The P-CSCF shall delete all SAs it holds that are associated with a particular IMPI once all the associated IMPUs are de-registered.

For TLS-based access security the following applies:

A server side authenticated TLS session may be established before the UE is authenticated.

When the S-CSCF initiates authentication by sending a challenge to the UE, the P-CSCF may use the existing TLS tunnel to protect all authentication traffic. In this case if the authentication is successful including verification of authorization tokens, the P-CSCF may continue to use the existing TLS tunnel, but if the authentication is unsuccessful, the P-CSCF shall release the existing TLS tunnel.

The P-CSCF associates UE's IP address given in the registration procedure with the IMPI and all the successfully registered IMPUs related to that IMPI to a TLS tunnel.

7.5 Rules for security association handling when the UE changes IP address

…

7.6 Interoperability cases between IPsec and TLS-based access security

7.6.1 Requirements for interoperability

When a UE (or P-CSCF) is upgraded to support TLS, it may be possible that the peer P-CSCF (or UE) has not been upgraded, but supports only IPsec-based access security. To ensure interoperability, UEs and P-CSCFs supporting TLS-based access security may support IPsec-based access security. The UE should always initiate the communication with TLS if the UE supports it.

Starting with TLS handshake has the benefit that the negotiation is protected from message SM1.

If the UE does not support TLS and IPSec, the UE can be authenticated by SIP Digest but the security association cannot be setup.

The following clauses describe the cases where either of the nodes supports TLS and both support IPsec-based access security to ensure backwards compatibility:

– TLS security set up initiated by UE;

– IPsec security set up due to P-CSCF not supporting TLS;

– IPsec security set up due to UE not supporting TLS.

NOTE – The flows in the following clauses illustrate only the parameters that are relevant for selecting the access security method.

7.6.2 TLS security set up initiated by UE

In this case UE and P-CSCF both support IPsec- and TLS-based access security. The UE may start with TLS handshake before SM1. The Sec-agree negotiation according to RFC 3329 [21] is run in the messages to confirm the choice of the security mechanism i.e., TLS-based access security is set-up. Figure 10 depicts an example flow.

NOTE – If the UE does not support IPsec, it does not add the ipsec-3gpp mechanism name to the Sec-agree header.

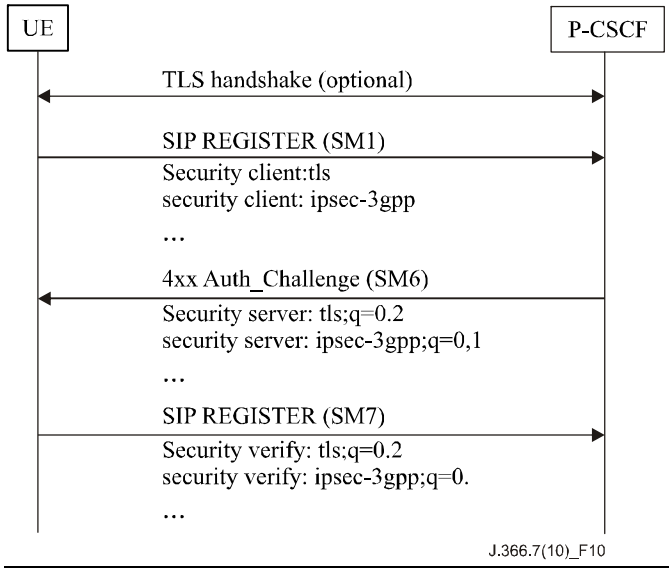

Figure 10

7.6.3 IPsec security set up due to P-CSCF not supporting TLS

In this case the P-CSCF supports IPsec and the UE supports at least IPsec and it may support also TLS. The UE may start with TLS handshake, which is rejected by the P-CSCF e.g., with an ICMP message, since the P-CSCF does not support TLS handshake. When receiving the error message the UE falls back to Sec-agree. Then the UE and P-CSCF negotiate the use of IPsec-based access security. Figure 11 depicts an example flow.

NOTE – It should be noted that since the error message from the P-CSCF cannot be authenticated by the UE, i.e., it could be sent by an attacker, the following Sec-agree negotiation may still lead to establishment of TLS (e.g., due to that the P-CSCF is not using a standard port for TLS, but a private port). This is possible if both UE and P-CSCF support TLS.

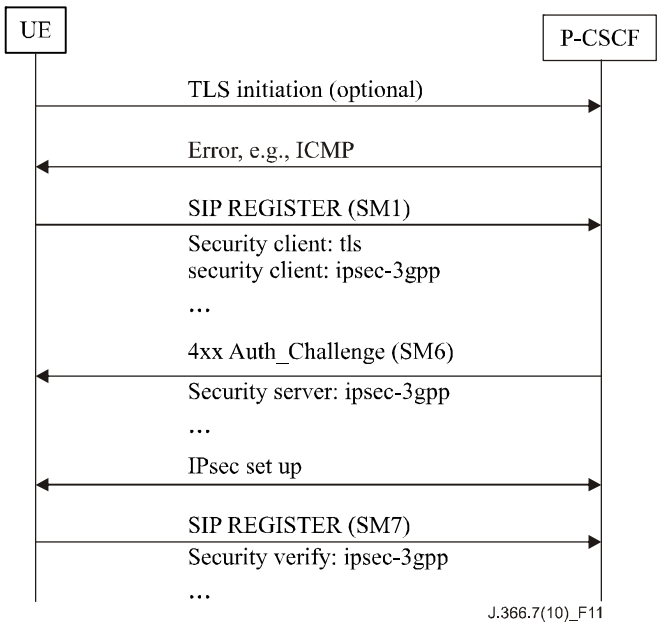

Figure 11

7.6.4 IPsec security set up due to UE only supporting IPsec

In this case the UE supports IPsec and P-CSCF supports both IPsec- and TLS-based access security. The UE starts with the Sec-agree negotiation according to RFC 3329 [21]. IPsec-based access security is set-up. Figure 12 depicts an example flow.

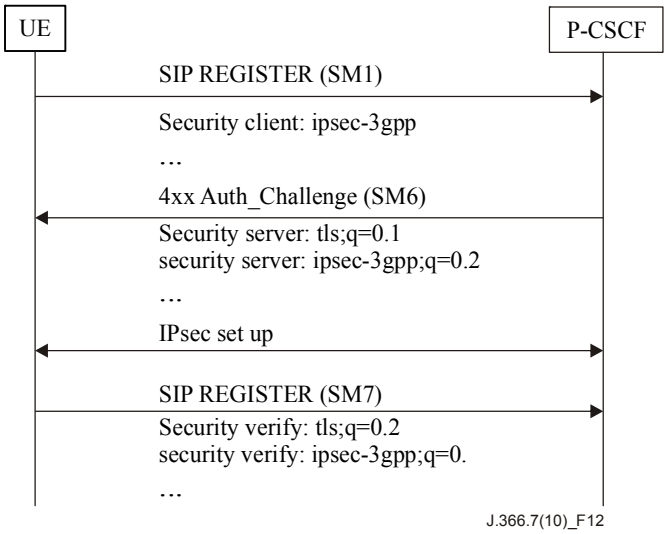

Figure 12

8 ISIM

…

Annex H
(normative)

The use of "Security Mechanism Agreement for SIP Sessions" [21] for security mode set-up

The BNF syntax of RFC 3329 [21], with the addition of the "aes-cbc" value for the "ealg" parameter, is defined for negotiating security associations for semi-manually keyed IPsec in the following way:

security-client	= "Security-Client" HCOLON sec-mechanism *(COMMA sec-mechanism)
security-server	= "Security-Server" HCOLON sec-mechanism *(COMMA sec-mechanism)
security-verify	= "Security-Verify" HCOLON sec-mechanism *(COMMA sec-mechanism)
sec-mechanism	= mechanism-name *(SEMI mech-parameters)
mechanism-name	= "ipsec- 3gpp" / "tls"
mech-parameters	= (preference / algorithm / protocol / mode / encrypt-algorithm / spi-c / spi-s / port-c / port-s)
preference	= "q" EQUAL qvalue
qvalue	= ("0" ["." 0*3DIGIT]) / ("1" ["." 0*3("0")])
algorithm	= "alg" EQUAL ("hmac-md5-96" / "hmac-sha-1-96")
protocol	= "prot" EQUAL ("ah" / "esp")
mode	= "mod" EQUAL ("trans" / "tun")
encrypt-algorithm	= "ealg" EQUAL ("des-ede3-cbc" /"aes-cbc" / "null")
spi-c	= "spi-c" EQUAL spivalue
spi-s	= "spi-s" EQUAL spivalue
spivalue	= 10DIGIT; 0 to 4294967295
port-c	= "port-c" EQUAL port
port-s	= "port-s" EQUAL port
port	= 1*DIGIT

The parameters described by the BNF above have the following semantics:

Mechanism-name: For TLS as defined in RFC 3329 [21]. For manually keyed IPsec, this field includes the value "ipsec-3gpp". "ipsec-3gpp" mechanism extends the general negotiation procedure of RFC 3329 [21] in the following way:

1 The server shall store the Security-Client header received in the request before sending the response with the Security-Server header.

2 The client shall include the Security-Client header in the first protected request. In other words, the first protected request shall include both Security-Verify and Security-Client header fields.

3 The server shall check that the content of Security-Client headers received in previous steps (1 and 2) are the same.

Preference: As defined in RFC 3329 [21].

The rest of the parameters in this annex are applicable to IPsec only.

Algorithm: Defines the authentication algorithm. May have a value "hmac-md5-96" for algorithm defined in RFC 2403 [15], or "hmac-sha-1-96" for algorithm defined in RFC 2404 [16]. The algorithm parameter is mandatory.

Protocol: Defines the IPsec protocol. May have a value "ah" for RFC 2402 [19] and "esp" for RFC 2406 [13]. If no Protocol parameter is present, the value will be "esp".

NOTE – According to clause 6 only "esp" is allowed for use in IMS.

Mode: Defines the mode in which the IPsec protocol is used. May have a value "trans" for transport mode, and value "tun" for tunneling mode. If no Mode parameter is present, the value will be "trans".

NOTE – According to clause 6.3 ESP integrity shall be applied in transport mode i.e., only "trans" is allowed for use in IMS.

Encrypt-algorithm: If present, defines the encryption algorithm. May have a value "des-ede3-cbc" for algorithm defined in RFC 2451 [20] or "aes-cbc" for the algorithm defined in IETF RFC 3602 [22] or "null" if encryption is not used. If no Encrypt-algorithm parameter is present, the algorithm will be "null".

Spi-c: Defines the SPI number of the inbound SA at the protected client port.

Spi-s: Defines the SPI number of the inbound SA at the protected server port.

Port-c: Defines the protected client port.

Port-s: Defines the protected server port.

It is assumed that the underlying IPsec implementation supports selectors that allow all transport protocols supported by SIP to be protected with a single SA.

…

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011