Title: METHOD AND COMMUNICATION SYSTEM FOR CONTROLLING SECURITY ASSOCIATION LIFETIME

Abstract: A method for selecting a time length of a security association (SA) between user equipment (UE) which transmits and receives communications and a control entity in a communication system in accordance with the invention, includes transmitting a registration message (SM1) from the user equipment to the control entity (P-CSCF) requesting registration of the user equipment with the control entity; after transmission of the registration message, setting the time length of the security association between the user equipment and the control entity to be equal to a registration time length set between the user equipment and the control entity during which registration of the user equipment with the control entity is valid; and transmitting the set time length of the security association to the user equipment as part of an acknowledgment message (SM10 or SM12) to the registration message to cause the security association to have a time equal to the registration timer length.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
METHOD AND COMMUNICATION SYSTEM FOR CONTROLLING SECURITY ASSOCIATION LIFETIME

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

[0001] This invention relates to selecting a Security Association (SA) timer between user equipment (UE) and a control entity in a communication system and in a preferred application selecting a SA timer for IPSec SA between the UE and a proxy call state control function (P-CSCF) in a 3G communications environment.

BACKGROUND ART

[0002] Fig. 1 illustrates a block diagram of a successful set up of SAs as set forth in Section 7.2 of 3GPP TS 33.203 V5.3.0 (2002-03) which is incorporated herein by reference in its entirety.

[0003] In the packet switched domain, service is not provided until a SA is established between the UE and the communication system 10 such as the P-CSCF. An IP Multimedia Core Network Subsystem (IMS) is essentially an overlay to the packet switched domain and has a low dependency on the packet switched domain. Consequently, a separate SA is required between a multimedia UE (client) and the IMS before access is granted to multimedia services.

[0004] The SA set up procedure is necessary in order to decide what security services to apply and when the security services are to start in the IMS. In the IMS, authentication of users is performed during registration as specified in section 6.1 of the aforementioned 3GPP publication. Subsequent signalling

CONFIRMATION COPY
communications in a session are integrity protected based on keys derived during the authentication process.

[0005] For protecting IMS signalling between the UE and the P-CSCF, it is necessary to agree on shared keys that are provided by the IMS Authentication and Key Agreement (AKA) protocol and a set of parameters specific to a protection method. The security mode set up as described below with reference to Fig. 1 is used to negotiate the SA parameters required for authentication, but without confidentiality. Section 7.1 of the aforementioned 3GPP publication describes the SA parameters.

[0006] Fig. 1 illustrates the normal case of setup of SAs using SIP protocol messages when failure does not occur. Some of the nodes and messages in a typical SIP architecture, which are not directly related to the set up of a SA, have been omitted. Accordingly, there are gaps in the numbering of messages and the Interrogating Call State Control Function (I-CSCF) has been omitted. The UE sends a SM1 REGISTER message to the P-CSCF and towards the Serving Call State Control Function (S-CSCF) to register the location of the UE and to set up the security mode. In order to start the security mode set-up procedure, the UE includes a security set-up line in the SM1 REGISTER message. The security set-up line in SM1 contains the Service Provisioning Infrastructure (SPI) numbers, the protected port selected by the UE and a list of identifiers for the integrity algorithms which the UE supports. Upon receipt of the SM1 REGISTER message by the P-CSCF, the P-CSCF temporarily stores the parameters received in the security set-up line together with the UE's IP address from the source IP address
of the IP packet header, the IP multimedia IM Private Identity (IMPI) and the IM Public Identity (IMPU). The P-CSCF sends a SM2 REGISTER message to the S-CSCF. Upon receipt by the P-CSCF of a SM4 4xx Auth_Challenge message originated from the S-CSCF in response to the SM2 REGISTER message, the P-CSCF adds the key IKIM received from the S-CSCF to the temporary stored parameters. The P-CSCF then selects the SPI for the inbound SA. The P-CSCF defines the SPIs such that they are unique and different from any SPIs received in the security-set-up line of the UE. This role is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic. In order to determine the integrity of the algorithm, the P-CSCF proceeds such that the P-CSCF has a list of integrity algorithms that the P-CSCF supports, ordered by priority. The P-CSCF selects the first integrity algorithm on its own which is also supported by the UE. The P-CSCF then establishes another pair of SAs in the local security association data base. The security set-up line in the SM6 message contains the SPI assigned by the P-CSCF and a fixed number of the protected port at the P-CSCF. The SM6 message also contains a list of identifiers for the integrity algorithms which the P-CSCF supports. Upon receipt of the SM6 message, the UE determines the integrity algorithm so that UE selects the first integrity algorithm on the list received from the P-CSCF in the SM6 message which is also supported by the UE. The UE then proceeds to establish another pair of SAs. The UE integrity protects the SM7 message and all the following SIP messages. The list of integrity algorithms received in SM6 message are included. After receiving the SM7 message from the UE, the P-CSCF checks whether the
integrity algorithm list received in the SM7 message is identical with the integrity algorithms list in the SM6 message. If this is not the case, the registration procedure is aborted. The P-CSCF includes in the SM8 message information for the S-CSCF that the received message from the UE was integrity protected. The P-CSCF adds this information to all subsequent registration messages received from the UE that have successfully passed the integrity check in the P-CSCF. The S-CSCF sends a SM10 2xx Auth_OK message to the P-CSCF. The P-CSCF sends a SM12 2xx Auth_OK message to the UE. The SM12 message does not contain information specific to security mode setup (i.e., a security-set-up line). However, when the SM12 message does not indicate any error, the P-CSCF confirms that security mode setup has been successful. After receiving the SM12 message not indicating any error, the UE assumes successful completion of the security-mode set-up.

[0007] Every registration message that includes a user authentication attempt produces new SAs. If the authentication attempt is successful, then these new SAs replace previous ones. If the UE has an already active SA, then the UE uses this to protect the registration message. If the S-CSCF is notified by the P-CSCF that the registration message from the UE was integrity protected, the S-CSCF may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected registration messages at any time. In this case, the S-CSCF authenticates the user by means of the AKA protocol. In particular, if the UE has an indication that the SA is no longer active at P-CSCF side, the UE sends an unprotected registration message. SAs may be unidirectional or
bidirectional. For IP layer SAs, the lifetime is held at the application layer.

Furthermore, deleting a SA means deleting the SA from both the application and the IPsec layer.

[0008] A UE is involved in only one registration procedure at a time. The UE removes any data relating to any previous incomplete registrations or authentications, including SAs created by an incomplete authentication. The UE may start a registration procedure with an existing pair of SAs. These SAs are referred to as an old SAs. The authentication produces a pair of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication of flow. In the same way, certain message in the authentication are protected with a particular SA. If the UE receives a message protected with incorrect SA, it shall discard the message.

[0009] RFC 3261, which is incorporated herein by reference in its entirety, describes the SIP protocol. As described in Section 10.3 therein, when a UE sends a REGISTER message, a registrant, which may be the P-CSCF, processes the request. The REGISTER message has a Contact address and Contact header field for each address.

[0010] The determination of the expiration time of registration of a UE is as follows:

(1) if the field value has an expires parameter, that value must be used.

(2) If there is no such parameter, but the request has an Expires header field, that value must be used.
(3) If there is neither, a locally configured default value must be used. The registrant may shorten the expiration interval.

[0012] With the SIP protocol, the so-called "non-INVITE transaction timeout timer" is 32 seconds. This timer is used as a temporary timer when sending the SM4 and SM6 messages as described above. The UE has 30 seconds to send the SM7 REGISTER message, containing the response to the SM6 4xx Auth_Challenge message by the network. When the authentication challenge in the SM6 message is answered in time with SM7 and SM8 REGISTER messages and the result is verified by the network, a SIP 200 Ok response is sent to the UE with messages SM10 and SM12 described above. The 200 Ok message contains an Expires header or a Contact field described above that indicates the time length of the registration of the UE with the control entity.

[0013] In the prior art, the SA timer can be set rather long, which results in network inefficiency in database management and the chance for UE to flood attack the P-CSCF with messages that require an appropriate response. If the UE does not have a SA with the network, such messages do not reach the P-CSCF which is preferred by the network operators because of more efficient use of resources.

[0014] In 3G communication systems, the UE has to register and re-register from time to time. When a re-registration is not requested within a specified time, subscriber data is deleted from the network elements responsible for handling the communications to and from the UE, such as the P-CSCF. Therefore, a
registration timer is maintained in the UE to determine when re-registration is appropriate.

**DISCLOSURE OF INVENTION**

[0015] The present invention is a method for selecting a time length of a SA(s) between a UE which transmits and receives communications and a control entity in a communication system and a communication system in which the lifetime of a SA(s) is set with sufficient time to allow completion of the registration. This goal is accomplished with the invention by the UE setting the lifetime of each new SA(s) equal to the time duration of the registration timer which determines the time limit a registration of a UE is invalid. The SA(s) are set for bidirectional communications between the UE and the control entity of the communication system. In a preferred embodiment, the control entity is the P-CSCF. Also, in accordance with the invention, an old SA as is continued for one more interval than when deletion should occur when a new SA is set with a time duration equal to the registration times.

[0016] In accordance with a preferred embodiment of the invention using the SIP protocol, the SM1 REGISTER message is sent by the UE to register the UE with the IMS at the P-CSCF. If the SM1 message is protected, it is protected with an old outbound SA. The UE receives an authentication challenge in a SM6 message from the P-CSCF which is protected with the old outbound SA if the SM1 message was protected and is unprotected otherwise. If the SM6 message can be successfully processed by the UE, the UE creates at least one new SA,
which is derived in accordance with the security association parameters of Section 7.1 of the 3GPP TS 33.203 V. 5.3.0 (2002-09). The lifetime of each new SA(s) created at this time is set to allow enough time to complete the registration procedure. The UE sends a SM7 message before expiration of a temporary timer value sent in the SM4 and SM6 messages to the P-CSCF which is protected with the new outbound SA. The P-CSCF sends a SM8 message to the S-CSCF. If the SM1 message was protected, the new SAs can now be used to protect messages other than those in the authentication. Furthermore, for outbound traffic, the new SA is used. The S-CSCF sends a SM10 message to the P-CSCF which uses the registration timer value contained in the Expires or Contact header to set the time duration of the new SA in the P-CSCF. The UE receives the SM12 message from the P-CSCF indicating successful authentication from the P-CSCF which is protected with the new outbound SA. The UE uses the registration time value contained in the Expires or Contact header to set the time duration of the new SA therein. After the successful processing of the message by the UE, registration is complete. The old SAs are now deleted or optionally may be retained for one more interval and the new SAs are used to protect all messages and have a time duration equal to a time length of the registration timer value contained in the SM10 and SM12 messages.

[0017] The present invention eliminates the problems of the prior art by eliminating the flooding of the P-CSCF with messages when the time duration of new SA(s), was not set to have any particular time length with respect to the registration timer and had a time duration longer than the registration timer for the
UE to register with the control entity of the communication system. As a result of the invention, the efficiency of the communication system is enhanced in accordance with the present invention.

[0018] A method for selecting a time length of a security association between user equipment which transmits and receives communications and a control entity in a communication system in accordance with the invention includes transmitting a registration message from the user equipment to the control entity requesting registration of the user equipment with the control entity; after transmission of the registration message, setting the time length of the security association between the user equipment and the control entity to be equal to a registration timer length set between the user equipment and the control entity during which registration of the user equipment with the control entity is valid; and transmitting the set time length of the security association to the user equipment as part of an acknowledgment message to the registration message to cause the security association to have a time equal to the registration timer. The control entity may perform a call state control function in the communication system. Communications between the user equipment and the communication system may use the Session Initiated Protocol (SIP) and the registration message may be a SIP REGISTER request message and the acknowledgment message may be a SIP 2xx response message. An authentication challenge may be sent including a temporary timer to the user equipment, preceding the acknowledgment, which sets a time duration for the user equipment to respond to the authentication challenge. A registration message may be sent from the user
equipment to the control entity in a response message to the authentication challenge within the set time duration for the user equipment to respond to the authentication challenge. The time duration may be contained in one of an Expires or Contact header of the SIP protocol. The temporary timer may be a non-INVITE transaction timeout timer of the SIP protocol.

[0019] A communication system in accordance with the invention including a user equipment which transmits and receives communications and a control entity which provides control functions in the communication system, and wherein a registration message is transmitted from the user equipment to the control entity requesting registration of the user equipment with the control entity; after transmission of the registration message, the time length of the security association between the user equipment and the control entity is set to be equal to a time length of a registration timer set between the user equipment and the control entity during which registration of the user equipment with the control entity is valid; and the set time length of the security association is transmitted from the control entity to the user equipment as an acknowledgment message to the registration message to cause the security association to have a time duration equal to the registration timer. The control entity may perform a call state control function in the communication system. Communications between the user equipment and the communication system may use the Session Initiated Protocol (SIP) and the registration message may be a SIP REGISTER request message and the acknowledgment message may be a SIP 2xx response message. An authentication challenge may be sent including a temporary timer to the user
equipment, preceding the acknowledgment, which sets a time duration for the user equipment to respond to the authentication challenge. A registration message may be sent from the user equipment to the control entity in a response message to the authentication challenge within the set time duration for the user equipment to respond to the authentication challenge. The time duration may be contained in one of an Expires or Contact header of the SIP protocol. The temporary timer may be a non-INVITE transaction timeout timer of the SIP protocol.

**BRIEF DESCRIPTION OF THE DRAWINGS**

**[0020]** Fig. 1 illustrates the prior art registration of a UE in a communication system using the SIP protocol including P-CSCF and S-CSCF control entities therein.

**[0021]** Fig. 2 illustrates a method of setting the time duration of a new SA(s) to be equal to the registration timer controlling registration of a UE as in the prior art system of Fig. 1.

**[0022]** Like parts are identified identically in Figs. 1 and 2.

**BEST MODE FOR CARRYING OUT THE INVENTION**

**[0023]** A communication system and a method which sets the SA(s) to have a timer duration equal to the registration timer defining when registration of a UE is valid in accordance with the invention is described in conjunction with Fig. 2.
While the invention has been described with reference to the SIP protocol, it should be understood that the invention is not limited thereto.

[0024] The first step in Fig. 2 is that the UE sends a registration message to a communication system control entity requesting registration of the UE. The control entity in a preferred embodiment is a P-CSCF and the registration message is the SM1 SIP REGISTER message transmitted to the P-CSCF in accordance with the prior art. The P-CSCF forwards the registration message, which preferably is the SM2 SIP REGISTER message, to the S-CSCF. The S-CSCF sends an authentication challenge message which preferably is the SIP SM4 message 4xx AUTH_Challenge message to the P-CSCF. The P-CSCF sends an authentication challenge message, which is preferably the SIP protocol SM6 4xx AUTH_Challenge, to the UE. The SM4 and SM6 authentication challenge messages include a temporary timer setting a time limit for the UE to transmit registration message, which preferably is the SM7 REGISTER message of the SIP protocol, in response to the authentication challenge message SM6. In one embodiment of the invention, the temporary timer value is set equal to 32 seconds, which is the non-INVITE transaction timeout timer of the SIP protocol. The P-CSCF determines by processing the SM7 message if the UE has responded within the temporary timer value. If the temporary timer expires, the registration process and the setting of SA is aborted. The P-CSCF then sends a register message, which is preferably the SIP protocol SM8 REGISTER message, to the S-CSCF. The S-CSCF sets the time length of its SA for the P_CSCF equal to the registration timer limit contained in the SM8 message. The set time limit for
the SA, which is equal to the registration timer, is sent as part of the SM10 message to the P-CSCF and then from the P-CSCF as the SM12 message to the UE. When the invention is practiced with the SIP protocol, the Expires or Contact Fields may be used to contains the set timer limit for the new SA(s). The P-CSCF also sets its SA time interval to be equal to the registration timer interval. The P-CSCF forwards the set value of its SA timer, which is equal to the registration timer, to the UE. The UE sets the time limit for its SA for communications with the P-CSCF to be equal to a registration timer length set by the UE defining when registration of the UE with the control entity is valid. The time length of the SAs is for bidirectionally communications between the P-CSCF and the UE. The invention is not limited to the SA time limit being sent by the SM10 and SM12 messages and is not limited to using the Expires and Contact headers to transmit the SA time limit to the P-CSCF and the UE. The time limit is preferably transmitted as part of the acknowledgment message which, in a preferred embodiment, is the SM10 and SM12 messages of the SIP protocol, which are responsive to the SM8 registration message received by the S-CSCF. Setting of the one or more SAs equal to the time length of the registration timer between the UE and the P-CSCF ensures that the problem of the prior art of flooding the P-CSCF with messages is eliminated as described above.

[0025] While the present invention has been described in terms of its preferred embodiments, it should be understood that numerous modifications may be made thereto without departing from the spirit and scope of the present invention. It is intended that all such modifications fall within the scope of the appended claims.
**CLAIMS**

What is claimed is:

1. A method for selecting a time length of a security association between user equipment which transmits and receives communications and a control entity in a communication system comprising:

   transmitting a registration message from the user equipment to the control entity requesting registration of the user equipment with the control entity;

   after transmission of the registration message, setting the time length of the security association between the user equipment and the control entity to be equal to a registration time length set between the user equipment and the control entity during which registration of the user equipment with the control entity is valid; and

   transmitting the set time length of the security association to the user equipment as part of an acknowledgment message to the registration message to cause the security association to have a time equal to the registration timer.

2. A method in accordance with claim 1 wherein:

   the control entity performs a call state control function in the communication system.
3. A method in accordance with claims 1 and 2 wherein:
communications between the user equipment and the
communication system use the Session Initiated Protocol (SIP) and the
registration message is a SIP REGISTER request message and the
acknowledgment message is a SIP 2xx response message.

4. A method in accordance with claim 3 wherein:
the SIP 2xx response is a 200 Auth_OK message.

5. A method in accordance with claims 1-4 comprising:
sending an authentication challenge including a temporary timer to
the user equipment, preceding the acknowledgment, which sets a time duration
for the user equipment to respond to the authentication challenge.

6. A method in accordance with claim 5 comprising:
sending a registration message from the user equipment to the
control entity in a response message to the authentication challenge within the set
time duration for the user equipment to respond to the authentication challenge.

7. A method in accordance with claim 5 wherein:
the timer length is contained in one of an Expires or Contact
header of the SIP protocol.
8. A method in accordance with claim 7 wherein:

the temporary timer is a non-INVITE transaction timeout timer of
the SIP protocol.

9. A communication system comprising:

a user equipment which transmits and receives communications
and a control entity which provides control functions in the communication system,
and wherein

a registration message is transmitted from the user equipment to the
control entity requesting registration of the user equipment with the control entity;

after transmission of the registration message, the time length of the
security association between the user equipment and the control entity is set to be
equal to a time length of a registration timer set between the user equipment and
the control entity during which registration of the user equipment with the control
entity is valid; and

the set time length of the security association is transmitted to the
user equipment as an acknowledgment message to the registration message to
cause the security association to have a time duration equal to the registration
timer.

10. A communication system in accordance with claim 9 wherein:

the control entity performs a call state control function in the
communication system.
11. A communication system in accordance with claims 9 and 10 wherein:
communications between the user equipment and the communication system use the Session Initiated Protocol (SIP) and the registration message is a SIP REGISTER request and the acknowledgment message is a SIP 2xx response message.

12. A communication system in accordance with claim 11 wherein:
the SIP 2xx response message is a 200 Auth_OK message.

13. A communication system in accordance with claims 9-12 wherein:
an authentication challenge including a temporary timer is sent to the user equipment, preceding the acknowledgment, which sets a time duration for the user equipment to respond to the authentication challenge.

14. A communication system in accordance with claims 9-13 comprising:
sending a registration message from the user equipment to the control entity in a response message to the authentication challenge within the set time duration set for the user equipment to respond to the authentication challenge.
15. A communication system in accordance with claim 13 wherein:
the timer length is contained in one of an Expires or Contact
header of the SIP protocol.

16. A communication system in accordance with claim 13 wherein:
the temporary timer is a non-INVITE transaction timeout timer of
the SIP protocol.
**FIG. 1 (PRIOR ART)**

- UE
- P-CSCF
- S-CSCF

- (SM1) Register
- (SM2) Register
- (SM6) 4xx Auth_Challenge
- (SM4) 4xx Auth_Challenge
- (SM7) Register
- (SM8) Register
- (SM10) 2xx Auth_Ok
- (SM12) 2xx Auth_Ok

**FIG. 2**

- UE
- P-CSCF
- S-CSCF

- (SM1) Register
- (SM2) Register
- (SM6) 4xx Auth_Challenge
- (SM4) 4xx Auth_Challenge
- (SM7) Register
- (SM8) Register
- (SM10) 2xx Auth_Ok
- (SM12) 2xx Auth_Ok

- (temporary timer)
- (SA(s) timer equal to registration timer)
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
   IPC(7) : HO4L 9/00
   US CL : 713/176
   According to International Patent Classification (IPC) or to both national classification and IPC

B. MINIMUM DOCUMENTATION SEARCHED
   U.S. : 713/176; 705/52, 80
   Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

   Electronic database consulted during the international search (name of database and, where practicable, search terms used)
   Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5,642,398 A (TIEDEMANN, JR. et al) 24 June 1997 (24.06.1997), figure 2; column 9, lines 28-56; column 11, lines 8-55.</td>
<td>1, 2, 9, 10</td>
</tr>
<tr>
<td>A</td>
<td>Voss, J. M. Limited Software Warranties Reliable Software Technologies. April 1999 pages 1-6</td>
<td>1-16</td>
</tr>
<tr>
<td>A</td>
<td>Anonymous ARI's PartSmart Provides Electronic Price File Updates Over the Internet; Secure Website to Maintain Manufacturer Price Updates for Electronic Delivery to Dealers Business Wire, February 2002 pages 1-2</td>
<td>1-16</td>
</tr>
<tr>
<td>A, P</td>
<td>Anonymous Metris Adds Identity Theft Protection Plan to Fraud Alert Services Business Wire, May 2002 pages 1-3</td>
<td>1-16</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

Date of the actual completion of the international search
14 August 2003 (14.08.2003)

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Date of mailing of the international search report
16 SEP 2003

Authorized Officer

Telephone No. 703-305-1373

Form PCT/ISA/210 (second sheet) (July 1998)
Continuation of B. FIELDS SEARCHED Item 3:
EAST, IEE, PROQUEST, GOOGLE
search terms: registration, reply message, warranty, warranty registering, reply message, acknowledgement message
INTERNATIONAL SEARCH REPORT

Box I: Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claim Nos.: because they relate to subject matter not required to be searched by this Authority, namely: Claims 3-8 and 11-16 were not searched due to improper dependent claims.

2. No Claim Nos.: 3-8 and 11-16 because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. No Claim Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II: Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☑ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant’s protest.
☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1)) (July 1998)