Title: KERBERIZED HANDOVER KEYING

Abstract: A media-independent handover key management architecture is disclosed that uses Kerberos for secure key distribution among a server, an authenticator, and a mobile node. In the preferred embodiments, signaling for key distribution is based on re-keying and is decoupled from re-authentication that requires EAP (Extensible Authentication Protocol) and AAA (Authorization, Authentication and Accounting) signaling similar to initial network access authentication. In this framework, the mobile node is able to obtain master session keys required for dynamically establishing the security associations with a set of authenticators without communicating with them before handover. By separating re-key operation from re-authentication, the proposed architecture is more optimized for a proactive mode of operation. It can also be optimized for reactive mode of operation by reversing the key distribution roles between the mobile node and the target access node.
## A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC.

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

## 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>BERNARD ABOBA DAN SIMON MICROSOFT: &quot;EAP GSS Authentication Protocol; draft-aboba-pppext-eapgss-12.txt&quot; IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 12, 6 April 2002 (2002-04-06), XP015000004 ISSN: 0000-0004 sections 5.4, 5.5 appendix A</td>
<td>1-21</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C

D See patent family annex

### Special categories of cited documents

- **X** document defining the general state of the art which is not considered to be of particular relevance
- **E** earlier document published on or after the international filing date
- **L** document which may throw doubts on the patentability (daims) or which is cited to establish the publication date of another citation or other special reason (as specified)
- **O** document referring to an oral disclosure, use, exhibition or other means
- **P** document published prior to the international filing date but later than the priority date claimed

### Date of the actual completion of the international search

22 July 2008

### Date of mailing of the international search report

30/07/2008

Name and mailing address of the ISA/

European Patent Office, P B 5818 Patentlaan 2 NL - 2280 HV RIJWIJK Tel (+31-70) 340-2040, Tx 31 651 epo nl, Fax (+31-70) 340-3016

Authorized officer

Bengi, Kemal
<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>MOHAMMED ALI KA'AFAR ET AL: &quot;A Kerberos-Based Authentication Architecture for Wireless LANs&quot; NETWORKING 2004, NETWORKING TECHNOLOGIES, SERVICES, AND PROTOCOLS; PERFORMANCE OF COMPUTER AND COMMUNICATION NETWORKS; MOBILE AND WIRELESS COMMUNICATIONS; [LECTURE NOTES IN COMPUTER SCIENCE; ;LNCS], SPRINGER-VERLAG, BERLIN/HEIDELBERG, vol. 3042, 8 April 2004 (2004-04-08), pages 1344-1353, XP019005538 ISBN: 978-3-540-21959-0 section 4 figures 1,3-5</td>
<td>1-21</td>
</tr>
</tbody>
</table>