Abstract: A method and apparatus for initiating secure operations in a microprocessor is described. In one embodiment, one initiating logical processor initiates the process by halting the execution of the other logical processors, and then loading initialization and secure virtual machine monitor software into memory. The initiating processor then loads the initialization software into secure memory for authentication and execution. The initialization software then authenticates and registers the secure virtual machine monitor software prior to secure system operations.

Published: with international search report (Art. 21(3))

Date of publication of the international search report: 11 September 2009
A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F12/14 G06F9/455

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)
IPC 7 G06F

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 practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

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>WO 01 75565 A (THAKKAR SHREEKANT S ; LIN DERRICK C (US) ; RENERIS KEN (US) ; ELLISON) 11 October 2001 (2001-10-11) page 3 - page 11 figure 1C abstract</td>
<td>1,3-5, 10, 14-16, 18,20,21</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents:
  *"A" document defining the general state of the art which is not considered to be of particular relevance
  *"E" earlier document but published on or after the international filing date
  *"L" document which may throw doubts on priority claim(s) 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

*"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
*"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
*"Z" document member of the same patent family

Date of the actual completion of the international search: 17 July 2003

Data of mailing of the international search report: 12. 08. 2003

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
B-2280 IV Rijswijk
Tel. (31-70) 340-2040, Te. 51 65 1 sec al
Fax: (31-70) 340-3116

Authorized officer
JENNY FORSS/MN

Form PCT/ISA/210 (second sheet) (July 1992)
<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>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 4939501 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1423765 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 10196005 T0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2377795 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0175565 A2</td>
</tr>
</tbody>
</table>