(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 549 021 A8

(12) **CORRECTED EUROPEAN PATENT APPLICATION**
Note: Bibliography reflects the latest situation

(15) Correction information:
Corrected version no 1 (W1 A1)
INID code(s) 54

(48) Corrigendum issued on:
12.07.2006 Bulletin 2006/28

(43) Date of publication:
29.06.2005 Bulletin 2005/26

(21) Application number: **04293092.5**

(22) Date of filing: **22.12.2004**

(51) Int Cl.:
H04L 29/06 *(1990.01)* ***G06F 1/00*** *(1968.09)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR

(30) Priority: **23.12.2003 US 743323**

(71) Applicant: **Activcard Inc.**
Fremont, CA 94555 (US)

(72) Inventors:
- **Fedronic, Dominique Louis Joseph**
  Belmont, CA 94002 (US)
- **Le Saint, Eric F.**
  Los Altos, CA 94024 (US)

(74) Representative: **Colas, Jean-Pierre**
Cabinet JP Colas,
37, avenue Franklin D. Roosevelt
75008 Paris (FR)

(54) **Access to a security token mediated by a server**

(57) A method, system and computer program product for accessing one or more security token resources (75) using an authentication server (110) as an intermediary before access is permitted to the security token resources. The server intermediary performs an initial authentication based on a user supplied critical security parameter. To ensure confidentiality of transported critical security parameters, a secure messaging session is established which provides end-to-end security between the authentication server (110) and the security token (75). A second critical security parameter is then sent to the security token. The security token authenticates the second critical security parameter and allows access token resources. Alternate secure communications mechanisms and an invalid entry counter reset capability are also described.

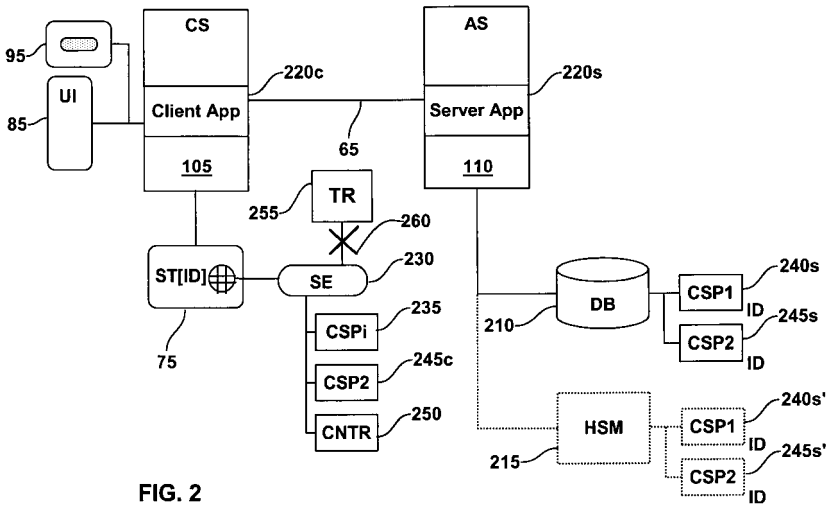

FIG. 2

EP 1 549 021 A8