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

(11) **EP 3 010 177 B8**

(12) **FASCICULE DE BREVET EUROPEEN CORRIGE**

(15) Information de correction:
Version corrigée no 1 (W1 B1)
Corrections, voir
Bibliographie code(s) INID 73

(48) Corrigendum publié le:
12.09.2018 Bulletin 2018/37

(45) Date de publication et mention de la délivrance du brevet:
25.07.2018 Bulletin 2018/30

(21) Numéro de dépôt: **15189617.2**

(22) Date de dépôt: **13.10.2015**

(51) Int Cl.:
H04L 9/32 *(2006.01)* ***H04L 9/00*** *(2006.01)*
H04L 29/06 *(2006.01)*

(54) **PROCÉDÉ D'AUTHENTIFICATION D'UN DISPOSITIF CLIENT AUPRÈS D'UN SERVEUR À L'AIDE D'UN ÉLÉMENT SECRET**

AUTHENTIFIZIERUNGSVERFAHREN EINES CLIENT-GERÄTS BEI EINEM SERVER MITHILFE EINES GEHEIMEN ELEMENTS

METHOD FOR AUTHENTICATING A CLIENT DEVICE WITH A SERVER USING A SECRET ELEMENT

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priorité: **13.10.2014 FR 1459804**

(43) Date de publication de la demande:
20.04.2016 Bulletin 2016/16

(73) Titulaire: **Idemia Identity & Security France**
92130 Issy-les-Moulineaux (FR)

(72) Inventeurs:
- **BRINGER, Julien**
  92130 ISSY LES MOULINEAUX (FR)
- **CHABANNE, Hervé**
  92130 ISSY LES MOULINEAUX (FR)
- **CIPIERE, Olivier**
  92130 ISSY-LES-MOULINEAUX (FR)
- **HUGEL, Rodolphe**
  92130 ISSY LES MOULINEAUX (FR)
- **LESCUYER, Roch**
  92130 ISSY-LES-MOULINEAUX (FR)

(74) Mandataire: **Regimbeau**
20, rue de Chazelles
75847 Paris Cedex 17 (FR)

(56) Documents cités:
- **YANJIANG YANG ET AL: "A New Approach for Anonymous Password Authentication", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2009. ACSAC '09. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 7 décembre 2009 (2009-12-07), pages 199-208, XP031610110, DOI: 10.1109/ACSAC.2009.26 ISBN: 978-0-7695-3919-5**
- **CHRISTOPH HERBST ET AL: "An AES Smart Card Implementation Resistant to Power Analysis Attacks", 1 janvier 2006 (2006-01-01), APPLIED CRYPTOGRAPHY AND NETWORK SECURITY LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 239 - 252, XP019034418, ISBN: 978-3-540-34703-3 * le document en entier ***

EP 3 010 177 B8