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

(11) EP 3 010 177 A1

(12) DEMANDE DE BREVET EUROPEEN

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

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

(21) Numéro de dépôt: **15189617.2**

(22) Date de dépôt: **13.10.2015**

(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
Etats d'extension désignés:
BA ME
Etats de validation désignés:
MA

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

(71) Demandeur: **Morpho**
92130 Issy-les-Moulineaux (FR)

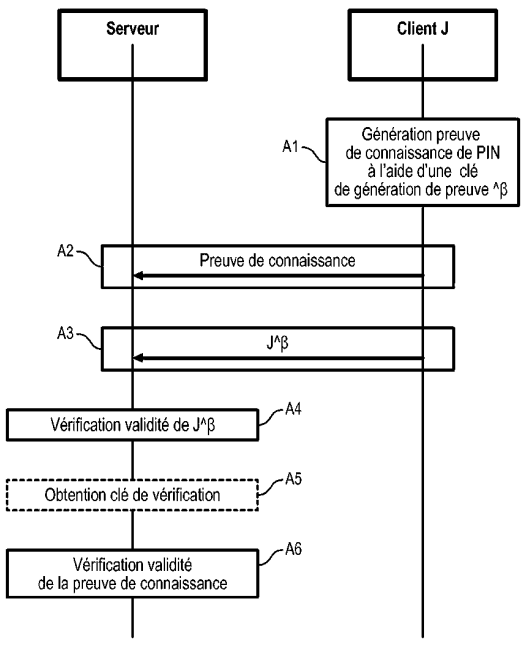
(72) Inventeurs:
- **BRINGER, Julien**
  92130 ISSY LES MOULINEAUX (FR)
- **CHABANNE, Hervé**
  92130 ISSY LES MOULINEAUX (FR)
- **CIPIERE, Olivier**
  92130 ISSY-LES-MOULINEAUX (FR)
- **HUGEL, Rodolphe**
  92130 ISSY LES MOULINEAUX (FR)
- **LESCUYER, Roch**
  92130 ISSY-LES-MOULINEAUX (FR)

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

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

(57) L'invention concerne un procédé d'authentification d'un dispositif client détenant un jeton d'authentification généré à l'aide d'une fonction pseudo-homomorphique et à partir d'un élément secret (PIN) connu uniquement du dispositif client, auprès d'un serveur, comprenant :
- la génération (A1), par le dispositif client, d'une preuve de connaissance de l'élément secret à partir d'une clé de génération de preuve masquée avec une donnée de masque, ladite clé de génération de preuve masquée étant fonction dudit élément secret,
- transmission, au serveur, par le dispositif client de ladite preuve de connaissance de l'élément secret générée (A2) et du jeton d'authentification (J) masqué à l'aide de la donnée de masque (A3),
- vérification de la validité du jeton d'authentification masqué (A4), et de la validité de la preuve de connaissance par le serveur (A6) par une preuve à divulgation nulle de connaissance prouvant la connaissance dudit élément secret par le dispositif client sans le divulguer.

FIG. 2



EP 3 010 177 A1