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

(11) EP 3 340 531 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
27.06.2018 Bulletin 2018/26

(51) Int Cl.:
H04L 9/08 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(21) Numéro de dépôt: **18156896.5**

(22) Date de dépôt: **17.07.2015**

(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 de validation désignés:
MA

(30) Priorité: **21.07.2014 FR 1457016**

(62) Numéro(s) de document de la (des) demande(s) initiale(s) en application de l'article 76 CBE:
15177194.6 / 2 978 161

(71) Demandeur: **Ercom**
78457 Velizy Villacoublay (FR)

(72) Inventeurs:
- **BALC'H, Martin**
  75014 Paris (FR)
- **KOWALSKI, Julien**
  89290 Egriselles VENOY (FR)
- **LAUBACHER, Eric**
  78390 BOIS D'ARCY (FR)
- **LEHOUX, Renaud**
  78210 SAINT-CYR L'ECOLE (FR)

(74) Mandataire: **Ipside**
7-9 Allées Haussmann
33300 Bordeaux Cedex (FR)

Remarques:
Cette demande a été déposée le 15-02-2018 comme demande divisionnaire de la demande mentionnée sous le code INID 62.

(54) PROCÉDÉ DE RESTAURATION D'UN SECRET D'UN UTILISATEUR

(57) La présente invention concerne un procédé de restauration d'un secret d'un utilisateur qui comporte:
- établissement d'un canal sécurisé entre l'utilisateur et au moins une valeur limite prédéterminée de dépositaires d'une partition du secret, ladite valeur limite prédéterminée correspondant à un nombre de partitions du secret nécessaires pour restaurer le secret, l'utilisateur authentifiant chaque dépositaire et chaque dépositaire authentifiant l'utilisateur,
- demande de restauration du secret par l'utilisateur à un serveur,
- déchiffrement d'au moins la valeur limite prédéterminée de partitions, chaque partition étant déchiffrée au moyen d'une clef privée dudit dépositaire correspondant,
- transmission à l'utilisateur par chaque dépositaire correspondant audit dépositaire déchiffrée, au moyen du canal sécurisé établi et
- reconstruction par l'utilisateur du secret à partir de chaque partition déchiffrée.

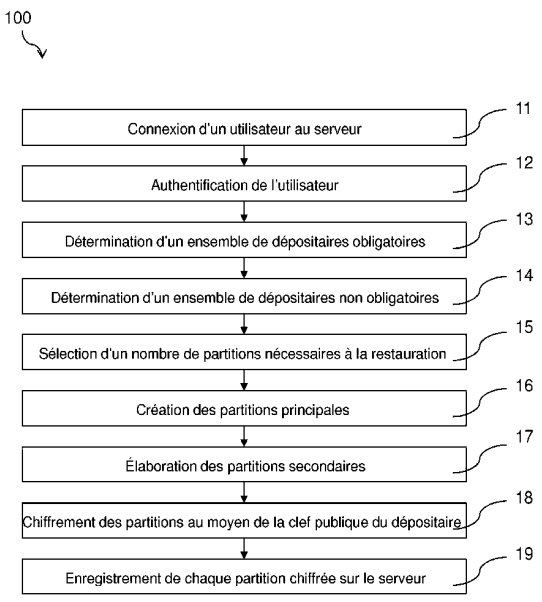

Figure 1

EP 3 340 531 A1