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

(11) **EP 4 016 339 A8**

(12) **KORRIGIERTE EUROPÄISCHE PATENTANMELDUNG**

(15) Korrekturinformation:
Korrigierte Fassung Nr. 1 (W1 A1)
Korrekturen, siehe
Bibliographie
Bemerkungen

(48) Corrigendum ausgegeben am:
27.07.2022 Patentblatt 2022/30

(43) Veröffentlichungstag:
22.06.2022 Patentblatt 2022/25

(21) Anmeldenummer: **21213780.6**

(22) Anmeldetag: **10.12.2021**

(51) Internationale Patentklassifikation (IPC):
G06F 21/30 *(2013.01)* ***G06F 21/57*** *(2013.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G06F 21/57; G06F 21/30

(84) Benannte Vertragsstaaten:
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
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
KH MA MD TN

(30) Priorität: **21.12.2020 DE 102020007809**
21.04.2021 DE 102021110144

(71) Anmelder:
- **Bundesdruckerei GmbH**
  10969 Berlin (DE)
- **Deutsche Telekom AG**
  53113 Bonn (DE)
- **Freie Universität Berlin**
  14195 Berlin (DE)

(72) Erfinder:
- **DIETRICH, Frank**
  12437 Berlin (DE)
- **Dr. SCHWAN, Matthias**
  13086 Berlin (DE)
- **ZASTRAU, Robert**
  13089 Berlin (DE)
- **KALL, Steven**
  57078 Siegen (DE)
- **OHLENDORF, Tim**
  12163 Berlin (DE)
- **PROF. DR. MARGRAF, Marian**
  14542 Werder (DE)

(74) Vertreter: **Richardt Patentanwälte PartG mbB**
Wilhelmstraße 7
65185 Wiesbaden (DE)

Bemerkungen:
Die Patentansprüche wurden nach dem Anmeldetag eingereicht (R. 68(4) EPÜ).

(54) PROVISIONIEREN EINES SICHERHEITSAPPLETS AUF EINEM MOBILEN ENDGERÄT

(57) Die Erfindung betrifft ein Verfahren zum Provisionieren eines auf einem mobilen Endgerät (100) installierten ID-Anwendungsprogramms (108) mit kryptographischen Schlüsseln und einem Sicherheitsapplet (114). Das mobile Endgerät (100) umfasst ein erstes Sicherheitselement (112) und ein zweites Sicherheitselement (110). Das Verfahren umfasst:

• auf ein Senden einer ersten Schlüsselerzeugungsanfrage einer Provisionierungskomponente des ID-Anwendungsprogramms (108) an das zweite Sicherheitselement (110) hin, Erzeugen eines dem ID-Anwendungsprogramm (108) zugeordneten ersten asymmetrischen Schlüsselpaars durch das zweite Sicherheitselement (110),

• auf ein Senden einer ersten Anfrage der Provisionierungskomponente über ein Netzwerk (150) an einen Provisionierungsserver (280) zum Einbringen des Sicherheitsapplets (114) für das ID-Anwendungsprogramm (108) hin, Einbringen des Sicherheitsapplets (114) für das ID-Anwendungsprogramm (108) in das erste Sicherheitselement (112) durch den Provisionierungsserver (280) über das Netzwerk (150).

EP 4 016 339 A8

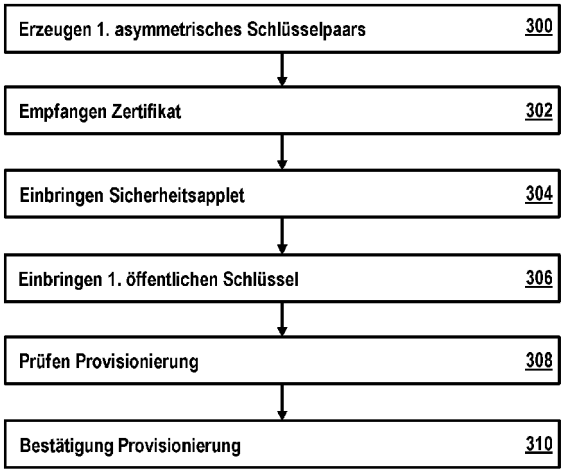
Erzeugen 1. asymmetrisches Schlüsselpaars
300
Empfangen Zertifikat
302
Einbringen Sicherheitsapplet
304
Einbringen 1. öffentlichen Schlüssel
306
Prüfen Provisionierung
308
Bestätigung Provisionierung
310

Fig. 4