(19) Deutsches
Patent- und Markenamt

(10) **DE 603 38 312 C5 2024.08.29**

(12) # Geänderte Patentschrift

Europäische Veröffentlichungsnummer
(97) **EP 1 973 297 B1**
(21) Deutsches Aktenzeichen: **603 38 312.2**
(96) Europäisches Aktenzeichen: **08 16 0321.9**
(96) Europäischer Anmeldetag: **27.06.2003**
(97) Erstveröffentlichung durch das EPA: **24.09.2008**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **31.08.2011**
(45) Veröffentlichungstag
des geänderten Patents im Patentblatt: **29.08.2024**

(51) Int Cl.: ***H04L 65/00*** (2022.01)
G06F 21/00 (2013.01)
H04L 67/00 (2022.01)
H04L 69/00 (2022.01)
H04L 9/40 (2022.01)

Patent nach Nichtigkeitsverfahren beschränkt aufrechterhalten

(30) Unionspriorität:
02078076 **26.07.2002** **EP**

(73) Patentinhaber:
Koninklijke Philips N.V., Eindhoven, NL

(74) Vertreter:
Eisenführ Speiser Patentanwälte Rechtsanwälte PartGmbB, 20355 Hamburg, DE

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR

(72) Erfinder:
Kamperman, Franciscus L. A. J., 5600 AE Eindhoven, NL

(54) Bezeichnung: **Sichere authentifizierte Abstandmessung**

(57) Hauptanspruch: A method of determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203), the method comprising the step of performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval, characterized in that the distance measurement is an authenticated distance measurement and in that the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and wherein the first device (201) authenticates the second device (203) and then the first device (201) securely shares the common secret with the second device (203) according to a key management protocol, and wherein the common secret is shared before performing the distance measurement.

Beschreibung

[0001] Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 23. Januar 2024 für Recht erkannt:

> Auf die Anschlussberufung der Beklagten und unter Zurückweisung der Berufung der Klägerinnen wird das Urteil des 5. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 20. Oktober 2021 abgeändert.
>
> Das europäische Patent 1 973 297 wird mit Wirkung für die Bundesrepublik Deutschland dadurch teilweise für nichtig erklärt, dass die Patentansprüche 1 und 16 die nachfolgende Fassung erhalten und sich die übrigen Ansprüche auf diese Fassung beziehen.

Patentansprüche

1. A method of determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203), the method comprising the step of performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval, characterized in that the distance measurement is an authenticated distance measurement and in that the first and the second communication device share a common secret and said common secret is used for performing the distance measurement and wherein the first device (201) authenticates the second device (203) and then the first device (201) securely shares the common secret with the second device (203) according to a key management protocol, and wherein the common secret is shared before performing the distance measurement.

2. A method according to claim 1, wherein the common secret is securely shared with the second device by encrypting the common secret using a public key of a private/public key-pair.

3. A method according to claim 1, wherein the distance measurement comprises a round trip time measurement to determine the measured distance.

4. A method according to claim 3, wherein the round trip time measurement is performed according to the following steps,
- transmitting (305) a first signal from the first communication device (201) to the second communication device (203) at a first time t1, said second communication device being adapted for receiving (311) said first signal, generating (313) a second signal by modifying the received first signal according to the common secret and transmitting (315) the second signal to the first device,
- receiving (317) the second signal at a second time t2,
- checking (319) if the second signal has been modified according to the common secret,
- determining (323) a time difference between the first time t1 and the second time t2.

5. A method according to claim 4, wherein the first signal is a spread spectrum signal.

6. A method according to claim 5, wherein the step of checking if the second signal has been modified according to the common secret is performed by the steps of,
- generating a third signal by modifying the first signal according to the common secret,
- comparing the third signal with the received second signal.

7. A method according to claim 4, wherein the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bitwords.

8. A method according to claim 1, wherein the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,
- performing an authentication check (205) from the first communication device (201) on the second communication device (203), by checking whether said second communication device (203) is compliant with a set of predefined compliance rules,
- if the second communication device is compliant, sharing (207) said common secret by transmitting said secret to the second communication device (203).

9. A method according to claim 8, wherein the authentication check further comprises checking if the identification of the second device (203) is compliantwith an expected identification.

10. Amethod according toclaim 1, wherein the protected content stored on the first device (201) are sent to the second device (203) if it is determined that the protected content stored on the first device (201) are to be accessed by the second device (203).

11. A method as in claim 10, wherein the protected content can be sent between the first and the second device after the distance has been measured in a secure authenticated way.

12. A method according to claim 1, wherein authenticating of the second device (203) by the first device (201) comprises the steps of checking

whether the second device (203) is a compliant device.

13. A method according to claim 1, wherein authenticating of the second device (203) by the first device (201) comprises the step of checking whether the second device (203) really is the device identified to the first device (201).

14. A method according to claim 1, wherein securely sharing the secret with the second device (203) by the first device (201) comprises transmitting a random generated bit word to the second device (203).

15. A method according to claim 1, wherein the shared common secret is afterwards used for generating a secure authenticated channel between the first (201) and the second communication device (203).

16. A first communication device (201) configured for determining whether protected content stored on the first communication device (201) are to be accessed by a second communication device (203), the first device comprising means for performing a distance measurement between the first (201) and the second communication device (203) and checking whether said measured distance is within a predefined distance interval, characterized in that the distance measurement is an authenticated distance measurement and that the first device comprises a memory storing a common secret also stored on the second communication device, which common secret is used for performing the distance measurement, the first device being configured (411, 413, 417) for authenticating the second device (203) and then securely sharing the secret with the second device before performing the distance measurement.

Es folgen keine Zeichnungen