(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 October 2025 (30.10.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/226204 A1

(51) International Patent Classification:
G06Q 20/08 (2012.01) *H04L 9/00* (2022.01)

(21) International Application Number:
PCT/SE2025/050378

(22) International Filing Date:
23 April 2025 (23.04.2025)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2450442-5 23 April 2024 (23.04.2024) SE

(71) Applicant: **CRUNCHFISH DIGITAL CASH AB** [SE/SE]; c/o Crunchfish AB, Stora Varvsgatan 6A 4TR, 211 19 MALMÖ (SE).

(72) Inventors: **SAMUELSSON, Joachim**; Drottninggatan 77, lgh 1602, 254 33 HELSINGBORG (SE). **PERPETUA, Jerson**; Dalbyvägen 38, 232 33 ARLÖV (SE).

(74) Agent: **STRÖM & GULLIKSSON AB**; P.O. Box 4188, 203 13 MALMÖ (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,

(54) **Title:** DIGITAL PAYMENTS WITH PAYER PRIVACY

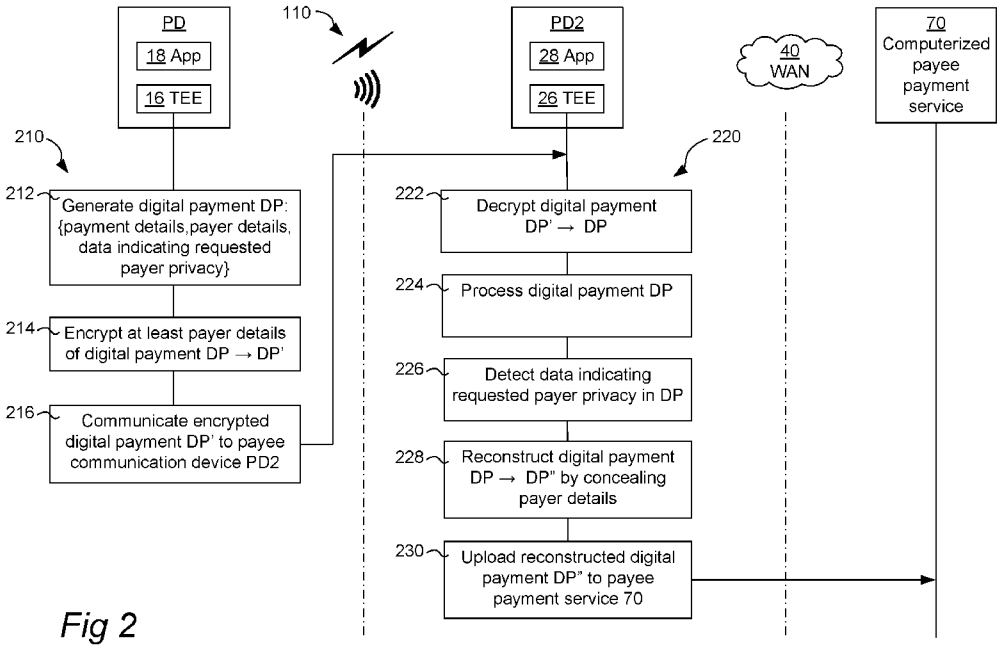

Fig 2

(57) **Abstract:** A computerized method of providing payer privacy in digital payments is disclosed. In a trusted execution environment (16) of a payer communication device (PD), the following takes place: generating (212) a digital payment, the digital payment comprising payment details, payer details and data indicating requested payer privacy; encrypting (214) at least the payer details of the digital payment; and communicating (114; 216) the encrypted digital payment to a payee communication device (PD2). In a trusted execution environment (26) of the payee communication device (PD2), the following takes place: decrypting (222) the digital payment; processing (224) the digital payment; and upon detecting (226) said data indicating requested payer privacy in the digital payment received from the payer communication device (PD): reconstructing (228) the digital payment by concealing the payer details thereof; and uploading (122'; 230) the reconstructed digital payment to a payee payment service (70).

WO 2025/226204 A1

[Continued on next page]

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UY, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

DIGITAL PAYMENTS WITH PAYER PRIVACY

TECHNICAL FIELD

The present invention generally relates to digital payments. More particularly, the present invention relates to technical improvements to enable privacy for the payer. Even more particularly, the present invention relates to a computerized method of providing payer privacy in digital payments, and an associated digital payment system as well as associated communication devices, computer program products and non-volatile computer readable media.

BACKGROUND

The technical field of digital communication has seen an overwhelming market penetration during the last decades. Digital communication is typically enabled between one or more mobile communication devices over wide-area networks, WAN, for instance via cellular radio systems like 5G, UMTS or GSM, or over wireless local area networks, WLAN. Alternatively or additionally, digital communication may be enabled over various short-range wireless data communication standards, such as Bluetooth or WiFi. As used in this document, the term "communication device" includes a mobile communication device, a mobile phone, a smart phone, a tablet computer, a personal digital assistant, a portable computer, smart glasses, a smart wearable (e.g. smart watch or smart bracelet), a smart card, a payment terminal, a service terminal, a point-of-sales terminal, a checkout counter, a delivery pickup point, a vending machine, a ticket machine, a dispensing machine and an access control system, without limitation.

A common application of digital communication is digital payments between users of communication devices. While digital payments surely are a very convenient tool for transfer of value between users, often in exchange of other performance (e.g. goods or services) in the opposite direction between said users, the present inventors have realized that payers of digital payments may benefit from privacy in some situations. By way of comparison, conventional cash ("paper money") offers true payer anonymity, at the expense of a lack of regulatory or governmental traceability of cash transactions.

SUMMARY

The present inventors have made valuable technical insights when it comes to the enabling of privacy for payers of digital payments. These insights will be presented

as inventive aspects below as well as in the detailed description section, the claims and the drawings. The list of inventive aspects is not to be seen as exhaustive but rather a summary of particularly beneficial inventive aspects.

A first inventive aspect is computerized method of providing payer privacy in digital payments. The method comprises, in a trusted execution environment of a payer communication device:

generating a digital payment, the digital payment comprising payment details, payer details and data indicating requested payer privacy;

encrypting at least the payer details of the digital payment;

communicating the encrypted digital payment to a payee communication device.

The method further comprises, in a trusted execution environment of the payee communication device:

decrypting the digital payment;

processing the digital payment; and

upon detecting said data indicating requested payer privacy in the digital payment received from the payer communication device:

reconstructing the digital payment by concealing the payer details thereof; and

uploading the reconstructed digital payment to a payee payment service.

This method will allow a payer to request and benefit from payer privacy, while still allowing a secure local processing of the digital payment at the payee side, without revealing payer details outside of this secure local processing. Embodiments of the computerized method will be disclosed in remaining parts of this document, including the appended claims, as well as in the attached drawings.

A second inventive aspect is a digital payment system that comprises a payer communication device and a payee communication device, each having a short-range data communication interface, a wide-area data communication interface and a trusted execution environment. The digital payment system further comprises a computerized payer payment service being a cloud-based computing resource capable of wide-area data communication, and a computerized payee payment service being a cloud-based computing resource capable of wide-area data communication.

The trusted execution environment of the payer communication device is configured for:

generating a digital payment, the digital payment comprising payment details, payer details and data indicating requested payer privacy,

encrypting at least the payer details of the digital payment, and

communicating the encrypted digital payment to the payee communication device.

The trusted execution environment of the payee communication device is configured for:

decrypting the digital payment,

processing the digital payment, and

upon detecting said data indicating requested payer privacy in the digital payment received from the payer communication device:

reconstructing the digital payment by concealing the payer details thereof, and

uploading the reconstructed digital payment to the payee payment service.

The trusted execution environment of the payer communication device may be configured for performing the functionality of the payer communication device in the computerized method as defined for the first inventive aspect or any of its embodiments as disclosed in this document, and the trusted execution environment of the payee communication device may be configured for performing the functionality of the payee communication device in the computerized method as defined for the first inventive aspect or any of its embodiments as disclosed in this document.

A third inventive aspect is a communication device for use in a digital payment system, the communication device comprising a short-range data communication interface, a wide-area data communication interface, and a trusted execution environment configured for performing the functionality of the payer communication device in the computerized method as defined for the first inventive aspect or any of its embodiments as disclosed in this document.

A fourth inventive aspect is a communication device for use in a digital payment system, the communication device comprising a short-range data communication interface, a wide-area data communication interface, and a trusted execution environment configured for performing the functionality of the payee communication device in the computerized method as defined for the first inventive aspect or any of its embodiments as disclosed in this document.

A fifth inventive aspect is a computer program product comprising computer program code for performing the functionality of the payer communication device in the computerized method defined for the first inventive aspect or any of its embodiments as

disclosed in this document when the computer program code is executed by a processing device.

A sixth inventive aspect is a computer program product comprising computer program code for performing the functionality of the payee communication device in the computerized method defined for the first inventive aspect or any of its embodiments as disclosed in this document when the computer program code is executed by a processing device.

A seventh inventive aspect is a non-volatile computer readable medium having stored thereon a computer program comprising computer program code for performing the functionality of the payer communication device in the computerized method defined for the first inventive aspect or any of its embodiments as disclosed in this document when the computer program code is executed by a processing device.

An eighth inventive aspect is a non-volatile computer readable medium having stored thereon a computer program comprising computer program code for performing the functionality of the payee communication device in the computerized method defined for the first inventive aspect or any of its embodiments as disclosed in this document when the computer program code is executed by a processing device.

As used in this document, the term "short-range data communication" includes any form of proximity-based device-to-device communication, unidirectional or bidirectional. This includes radio-based short-range wireless data communication such as, for instance, Bluetooth, BLE (Bluetooth Low Energy), RFID, WLAN, WiFi, mesh communication or LTE Direct, without limitation. It also includes non-radio-based short-range wireless data communication such as, for instance, magnetic communication (such as NFC), audio communication, ultrasound communication, or optical communication (such as QR, barcode, IrDA).

As used in this document, the term "wide area network communication" (abbreviated as "WAN communication") includes any form of data network communication with a party which may be remote (e.g. cloud-based), including cellular radio communication like W-CDMA, GSM, UTRAN, HSPA, LTE, LTE Advanced or 5G, possibly communicated as TCP/IP traffic, or via a WLAN (WiFi) access point, without limitation. Moreover, the terms "wide area data communication", "long-range data communication" and "broadband data communication" are considered as synonyms of "wide-area network communication".

It should be emphasized that the term "comprises/comprising" when used in this specification is taken to specify the presence of stated features, integers, steps, or

components, but does not preclude the presence or addition of one or more other features, integers, steps, components, or groups thereof. All terms used herein are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the [element, device, component, means, step, etc.]" are to be interpreted openly as referring to at least one instance of the element, device, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

Expressions like "[entity] is configured for… [performing activity]" or "[entity] is configured to … [perform activity]" will include typical cases where a computerized entity (having one or more controllers, processing units, programmable circuitry, etc.) executes software or firmware installed in the computerized entity, wherein the execution occurs in order to perform the activity in question.

Other aspects, objectives, features and advantages of the inventive aspects will appear from the following detailed disclosure as well as from the claims and the drawings. Generally, all terms used herein are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein.

All references to "a/an/the [element, device, component, means, step, etc.]" are to be interpreted openly as referring to at least one instance of the element, device, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic block diagram of a digital payment system in an exemplary embodiment.

Figure 2 is a schematic flowchart diagram of a computerized method of providing payer privacy in digital payments in an exemplary embodiment.

Figure 3 is a schematic illustration of a computer-readable medium in an exemplary embodiment, capable of storing a computer program product.

DETAILED DESCRIPTION OF EMBODIMENTS

Embodiments of the invention will now be described with reference to the accompanying drawings. The invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein;

rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. The terminology used in the detailed description of the particular embodiments illustrated in the accompanying drawings is not intended to be limiting of the invention. In the drawings, like reference signs refer to like elements.

Figure 1 illustrates an exemplary embodiment of a digital payment system 1 The digital payment system 1 is capable of handling digital payments that relate to exchange of monetary value between a payer PA and a payee PA2 using a payer communication device PD and a payee communication device PD2, respectively. Such digital payments may be referred to as proximity digital payments or offline digital payments. The payer PA and the payee PA2 may typically be human users. However, it is also envisaged that one or both of the payer PA and payee PA2 may be automated machines or incarnations of artificial intelligence.

The digital payment system 1 may execute a computerized method of providing payer privacy in digital payments. Embodiments of this method will be described in detail with reference to Figure 2 and onwards. First, however, the digital payment system 1 in Figure 1 will be described in some detail.

Generally, a private or non-private digital payment from the payer PA to the payee PA2 may start with the payee communication device PD2 sending a payment request 112 to the payer communication device PD over a proximity link 110 established between the devices PD, PD2. The proximity link 110 uses short-range data communication, as generally defined in a previous section of this document. The payer communication device PD generates the digital payment and communicates it at 114 to the payee communication device PD2 over the proximity link 110. The payee communication device PD2 uploads the digital payment at 122' for online reconciliation 120 via, for instance, a wide area network 40. In some embodiments, the payer communication device PD, too, uploads the digital payment at 122 for online reconciliation 120 via, for instance, the wide area network 40.

The digital payment system 1 comprises a computerized payer payment service 60. Such a computerized payer payment may be referred to as an *Issuer* in the terminology of contemporary payments schemes. The digital payment system 1 also comprises a computerized payee payment service 70, which may be referred to as an *Acquirer* in the terminology of contemporary payments schemes. The computerized payer payment service 60 and the computerized payee payment service 70 are preferably cloud-based computing resources, for instance operated by respective banks

or similar financial institutions. Each one of the computerized payer payment service 60 and the computerized payee payment service 70 is capable of (i.e., enabled or configured for) wide area data communication, as enabled by, for instance, the wide-area network 40.

In some embodiments, the computerized payer payment service 60 and the computerized payee payment service 70 are the same account provider, i.e. a common account provider for the payer PA and payee PA2.

The digital payment system 1 further comprises a payment switch 80 and a central bank 90. The payment switch 80 and the central bank 90 are, in conjunction with the computerized payer payment service 60 and the computerized payee payment service 70, responsible for handling online reconciliation (settlement) 120 of digital payments. The payment switch 80 is invoked by either one of the computerized payer or payee payment services 60, 70 for initiating the online reconciliation 120. For an ordinary (non-private) digital payment, the online reconciliation 120 then transfers monetary value from a payer account 62 maintained by the computerized payer payment service 60, to a payee account 72 maintained by the computerized payee payment service 70. When payer privacy has been invoked for the digital payment as described in this document, the online reconciliation 120 may instead involve transferring monetary value to and from a private payment pool 95, as the skilled reader will understand.

The central bank 90 may also be involved in the online reconciliation 120, for instance by carrying out monetary policies or controlling monetary supplies.

As seen in Figure 1, each one of the payer communication device PD and the payee communication device PD2 comprises a plurality of computerized/digital/-electronic units. The skilled person appreciates that the components of the payer communication device PD and the payee communication device PD2 sharing the same name are configured to operate similarly, i.e. broadband data communication interfaces (WAN I/F) 11; 21, short-range data communication interfaces (SRDC I/F) 12; 22, controllers (Ctrl) 13; 23, local storages including memories (Mem) 14; 24 and user interfaces (UI) 15; 25.

Of course, the skilled person realizes that the components illustrated in Figure 1 merely constitute one potential embodiment of the payer communication device PD and the payee communication device PD2. The scope of the present disclosure is not limited to these particular components and/or configurations. Alternative embodiments may thus be realized for either one of them, provided that they are suitable for handling

digital payments in the manner described in this document. The payer communication device PD and/or the payee communication device PD2 may be implemented in the form of, for instance, a mobile communication device, a mobile phone, a smart phone, a tablet computer, a personal digital assistant, a portable computer, smart glasses, a smart wearable (e.g. smart watch or smart bracelet), a smart card, a payment terminal, a service terminal, a point-of-sales terminal, a checkout counter, a delivery pickup point, a vending machine, a ticket machine, a dispensing machine and an access control system, without limitation. Moreover, offline (proximity) digital payments may be effected in both peer-to-peer cases, where the mobile transaction is done straight to an app on the payee's mobile communication device, and in business-to-consumer, B2C, cases, where the mobile transaction goes from a customer via, for instance, a payment terminal to a physical cash register operated by a merchant in store.

The WAN I/Fs 11; 21 may be configured for wide area network communication compliant with, for instance, one or more of W-CDMA, GSM, UTRAN, HSPA, LTE, LTE Advanced or 5G, and TCP/IP, and/or WLAN (WiFi), without limitation.

The SRDC I/Fs 12; 22 may be configured for Bluetooth communication, or any other radio-based short-range wireless data communication such as, for instance, Bluetooth Low Energy, RFID, WLAN, WiFi, mesh communication or LTE Direct, without limitation, or any non-radio-based short-range wireless data communication such as, for instance, magnetic communication (such as NFC), (ultra)sound communication, or optical communication (such as IrDA) without limitation. In some embodiments, at least one of the SRDC I/Fs 12; 22 comprise equipment and functionality for presenting or scanning a QR code.

The controllers 13; 23 comprise one or more processing units. The controllers 13; 23 may be implemented in any known controller technology, including but not limited to microcontroller, processor (e.g. PLC, CPU, DSP), FPGA, ASIC or any other suitable digital and/or analog circuitry capable of performing the intended functionality.

The memories 14; 24 may be implemented in any known memory technology, including but not limited to ROM, RAM, SRAM, DRAM, CMOS, FLASH, DDR, SDRAM or some other memory technology. In some embodiments, the memories 14; 24 or parts thereof may be integrated with or internal to the controllers 13; 23, and more specifically the processing units thereof. The memories 14; 24 may store program instruction for execution by the controllers 13; 23, and more specifically the processing units thereof, as well as temporary and permanent data.

The user interfaces 15; 25 may comprise an input device and a presentation device, as is generally known *per se*. In some embodiments, the input device and the presentation device are constituted by one common physical device, such as for instance a touch screen (touch-sensitive display screen), implemented in for instance resistive touch technology, surface capacitive technology, projected capacitive technology, surface acoustic wave technology or infrared technology.

The payer communication device PD and the payee communication device PD2 further comprise a respective trusted execution environment (TEE) 16; 26, such as a secure element, i.e. a tamper-resistant hardware or virtual platform. The TEEs 16; 26 are configured to securely host applications, i.e. trusted applications, and to store confidential and cryptographic data and therefore provide a trusted environment for execution of such applications. This is commonly referred to as secure runtime. Advantageously, some of the data and functionality in embodiments of the invention may be stored in and performed by the TEEs 16; 26 of the devices PD, PD2. As can be seen in Figure 1, such data and functionality may include a payer private cryptographic key *payer_priv_key* kept strictly within the TEE 16 of the payer communication device PD, as well as private payment functionality 30 executable within the TEE 16. Correspondingly, a payee private cryptographic key *payee_priv_key* may be kept strictly within the TEE 26 of the payee communication device PD2, and private payment functionality 30' is executable within the TEE 26.

Not seen in Figure 1 but shown in Figure 2, the payer communication device PD and the payee communication device PD2 may execute a digital payment app 18 and 28, respectively, in a normal (rich, non-secure) execution environment. The digital payment app 18; 28 will interact with the private payment functionality 30; 30' in the TEE 16; 26, with the payer PD/payee PD2 via the user interface 15; 25, with the other device PD2; PD via the SRDC I/F 12; 22, and with the payer payment service 60/payee payment service 70 via the WAN I/F 11; 21.

The TEEs 16; 26 furthermore accommodate a local digital wallet LDW and LDW2 of the payer PA and payee PA2, respectively. In the disclosed embodiment of Figure 1, each local digital wallet LDW; LDW2 stores data, *balance*, that represents a monetary value available for proximity digital payments. Such monetary value may, for instance, be in the form of tokens or variable values and may have been downloaded in advance to the LDW; LDW2 from the payer payment service 60 and payee payment service 70, typically withdrawn from the payer account 62 and payee account 72,

respectively. Furthermore, such monetary value may have been received in one or more previous digital payments in the digital payment system 1.

The TEEs 16; 26 may be configured according to any hardware-based computer architecture schemes known in the art, including but not limited to Samsung TEEGRIS, Qualcomm TEE, Huawei iTrustee, Trustonic Kinibi, Google Open Source Trusty, Open Portable TEE, Nvidia's Trusted Little Kernel for Tegra, Sierra TEE, ProvenCore TEE, Trusty TEE for Android, or TrustKernel T6. Moreover, the TEEs 16; 26 may be adapted to protect hardware resource of the devices PD, PD2 by implementing any hardware support technologies known in the art, including but not limited to Arm's TrustZone, MultiZone Security, AMD Platform Security Processor, Intel Software Guard Extensions, Apple's Secure Enclave Processor, or Google's Titan M. In some embodiments, the TEEs 16; 26 are implemented by Secure Elements (SE).

The TEEs 16; 26 may alternatively be configured according to any software-based computer architecture schemes known in the art, such as the virtual execution environment provided by V-key, Inc., disclosed for instance in the European patent EP 2 795 829 B1. In this case, the TEEs 16; 26 may be implemented in software and may reside in the local storage of the devices PD, PD2 or even the memories 14; 24. Software-based implementations of the TEEs may be beneficial over hardware-based implementations when it comes to scalability and distribution to users of mobile communication devices.

Reference is now made to Figure 2, illustrating an embodiment of a computerized method of providing payer privacy, which may be executed in the digital payment system 1 of Figure 1. The computerized method of providing payer privacy in digital payments generally comprises two part, a first part 210 that comprises steps executed in the trusted execution environment 16 of the payer communication device PD (cf. private payment functionality 30 for TEE 16 in Figure 1), and a second part 220 that comprises steps executed in the trusted execution environment 26 of the payee communication device PD2 (cf. private payment functionality 30' for TEE 26 in Figure 1).

The first part 210, executed in the TEE 16 of the payer communication device PD, comprises the following functionality.

A step 212 involves generating a private digital payment, which is referred to as DP in the following. The digital payment DP comprises payment details, payer details, and data indicating requested payer privacy. The payment details may, for instance, include a transaction identifier, a payment amount, a payment currency, etc.,

which in turn may have been defined in the payment request 112 of Figure 1. The payer details may, for instance, include a payer identifier, *payer_address*, stored in the TEE 16 or non-secure memory 14 of the payer communication device PD. The payer identifier *payer_address* may be indicative of an account 62 or other depository held by the payer PA at the payer payment service 60. Examples of data indicating requested payer privacy will be given later in this document. In some embodiments, to prevent fraudulent double-spending, the TEE 16 of the payer communication device PD may determine the transaction identifier by monotonically increasing a local counter function in the TEE 16.

A step 214 involves encrypting at least the payer details of the digital payment DP, resulting in an encrypted digital payment DP'.

A step 216 involves communicating (cf. 114 in Figure 1) the encrypted digital payment DP' to the payee communication device PD2.

The second part 220, executed in the TEE 26 of the payee communication device PD2, comprises the following functionality.

A step 222 involves decrypting the digital payment, such that the encrypted digital payment DP' as received from the payer communication device PD results in a decrypted digital payment DP.

A step 224 involves processing the digital payment DP. The processing may include measures such as verifying that the payment details match what is expected by the payee PA2 (for instance, corresponds to payment data stated in the payment request 112 of Figure 1 in terms of transaction ID, payment amount, currency, etc.). Since the processing occurs strictly within the TEE 26, the payer details will be open for any check or verification that may be called for by the payee side, for instance screening the payer PA (as represented by the payer details) against a blacklist of payers not trusted by the digital payment system 1, or verifying that the payer PA is known to the payee PA2, as non-limiting examples.

A step 226 involves detecting said data indicating requested payer privacy in the encrypted digital payment DP' received from the payer communication device PD and decrypted to digital payment DP in step 222.

As a result of detecting the data that indicates requested payer privacy in step 226, a step 228 follows in which the digital payment DP is reconstructed into a reconstructed digital payment DP" by concealing the payer details thereof.

In a subsequent step 230, the reconstructed digital payment DP" is uploaded to the payee payment service 70 (cf. 122' in Figure 1). Since the payer details have been

concealed in the preceding step 228, payer privacy is assured. Still, processing of the payer details has been possible in the TEE 26 of the payee communication device PD2 in the preceding step 224.

The encrypting of at least the payer details of the digital payment DP by the TEE 16 of the payer communication device PD in step 214 (i.e., for the purpose of secure local communication over the proximity link 110) may be done in different customary ways, as the skilled person will understand. In one embodiment, the encryption in step 214 involves an asymmetric encryption method (public-key cryptography) using a public cryptographic key of the payee communication device PD2, for instance corresponding to the aforementioned payee private cryptographic key *payee_priv_key* kept strictly within the TEE 26 of the payee communication device PD2. An example of such a public cryptographic key of the payee communication device PD2 is seen as *payee_pub_key* in Figure 1; it may be part of a digital certificate *payee_cert* stored in the TEE 26 or non-secure memory 24 of the payee communication device PD2. The *payee_pub_key* or the *payee_cert* may be communicated from the payee communication device PD2 to the payer communication device PD in the payment request 112. The TEE 26 of the payee communication device PD2 will then use the payee private cryptographic key *payee_priv_key* in step 222 to decrypt the encrypted digital payment as communicated from the payer communication device PD in step 216.

In another embodiment, the TEEs 16; 26 of the payer and payee communication devices PD; PD2 employ a key agreement protocol such as ECDH (Elliptic-Curve Diffie–Hellman) to securely generate a shared secret using elliptic curve cryptography (ECC). This shared secret is then used in steps 214 and 222 by the TEEs 16; 26 to derive, by means of a key derivation function (KDF), a symmetric key for encryption/decryption of at least the payer details of the digital payment. The symmetric key may, for instance, be an AES (Advanced Encryption Standard) key.

Some preferred but non-limiting examples of how the payer details may be concealed in the reconstructed digital payment DP" will now be given.

In some embodiments, the step 228 of reconstructing the digital payment DP by concealing the payer details thereof in the TEE 26 of the payee communication device PD2 involves encrypting at least the payer details of the digital payment DP by one or more cryptographic operations which are based on a payee public/private cryptographic key pair, with the payee private cryptographic key of the pair being kept strictly within the TEE 26 of the payee communication device PD2. The payee public

cryptographic key of the pair may be included in a digital certificate which may be stored in the TEE 26 or in the non-secure memory 24 of the payee communication device PD2. In such a case, the payee public/private cryptographic key pair may have been provisioned in advance to the TEE 26 of the payee communication device PD2 from, for instance, the payee payment service 70. Alternatively, the payee public/private cryptographic key pair may be ephemeral, i.e. generated on the fly by the TEE 26. The actual encryption may be done in different ways, using a cryptographic scheme known *per se*, such as asymmetric encryption (public-key cryptography) or a key agreement protocol such as ECDH to securely generate a shared secret using ECC and a key derivation function to derive a symmetric encryption/decryption key. In one way or the other, the cryptographic scheme will use the payee public cryptographic key for encryption and require, in one way or the other, access to the payee private cryptographic key in order to perform decryption of the concealed payer details in the digital payment.

In other embodiments, the step 228 of reconstructing the digital payment DP by concealing the payer details thereof in the TEE 26 of the payee communication device PD2 involves encrypting at least the payer details of the digital payment by one or more cryptographic operations being based on a payer public cryptographic key provided in or with the encrypted digital payment DP' communicated from the payer communication device PD to the payee communication device PD2 in step 216, wherein the payer public cryptographic key corresponds to a payer private cryptographic key kept strictly within the trusted execution environment 16 of the payer communication device PD. Any of the cryptographic schemes referred to above may, for instance, be used.

In still other embodiments, the step 228 of reconstructing the digital payment DP by concealing the payer details thereof in the TEE 26 of the payee communication device PD2 involves deleting the payer details after processing of the digital payment, such that the reconstructed digital payment DP" uploaded to the payee payment service 70 will not contain the payer details.

Common to all these embodiments is the following. While the payer details of the digital payment DP have been made available for scrutinization by the private payment functionality 30' of the TEE 26 in the payee communication device PD2, they are effectively concealed to entities outside of the TEE 26, including the payee payment service 70 that receives the uploaded reconstructed digital payment DP". Accordingly, payer privacy is obtained, as requested by the payer PA.

In one embodiment, upon detecting in step 226 said data indicating requested payer privacy in the digital payment DP received from the payer communication device PD, the TEE 26 of the payee communication device PD2 constructs an anonymous payment report including the decrypted payment details but without the payer details. The TEE 26 provides the constructed anonymous payment report to the digital payment app 28 that executes in the normal or rich execution environment on the payee communication device PD2. Accordingly, the payer PA represented by the payer details is kept anonymous even to the payee PA2 being the user of the payee communication device PD2. This further enhances the payer privacy. At the same time, the anonymous payment report provides important information to the payee PA2 in the digital payment app 28 regarding the payment details, for instance allowing the payee PA2 to verify that the payment amount is correct.

In one embodiment, the TEE 26 of the payee communication device PD2 is configured for receiving a request originating from an external entity to provide information about an encrypted digital payment previously received 216, processed 224 and uploaded 230 by the payee communication device PD2. The external entity may, for instance, be the payee payment service 70 or the payer payment service 60 in Figure 1, without limitation. The previously uploaded encrypted digital payment that is the subject of the request may be stored locally in the memory 24 of the payee communication device PD2 (and thus be readily available to the TEE 26), or provided with the request from the external entity, depending on implementation details and the time lapsed between uploading and requesting information (the memory 24 of the payee communication device PD2 may not have unlimited capacity to store historic digital payments “forever” but may have to prune them after some time). In some embodiment, digital payments are deleted from the payee communication device PD2 already upon uploading to the payee payment service 70.

Upon receiving the request to provide information about such a previously uploaded encrypted digital payment from the external entity, the TEE 26 of the payee communication device PD2 will decrypt the encrypted digital payment in question and detect, in the decrypted digital payment, presence of said data indicating requested payer privacy. As a result, the TEE 26 constructs an anonymous payment report that includes the decrypted payment details but without the payer details. The constructed anonymous payment report is provided to the requesting external entity. Accordingly, the payer PA represented by the payer details is kept anonymous to the requesting external entity.

In some embodiments, proximity digital payments are uploaded not only from the payee communication device PD2 to the payee payment service 70 (cf. 122' in Figure 1 and 230 in Figure 2), but also from the payer communication device PD to the payer payment service 60 (cf. 122 in Figure 1). In such embodiments, the TEE 16 of the payer communication device PD may be configured for encrypting at least the payer details of a digital payment DP for which payer privacy is requested by one or more cryptographic operations being based on a payer private cryptographic key kept strictly within the trusted execution environment 16 of the payer communication device PD (for instance, *payer_priv_key* in Figure 1), and for uploading 122 the encrypted digital payment to the payer payment service 60.

In such embodiments, the TEE 16 of the payer communication device PD may be configured for receiving a request originating from an external entity to provide information about an encrypted digital payment previously made by the payer communication device PD. The external entity may, for instance, be the payee payment service 70 or the payer payment service 60 in Figure 1, or the central bank 90, or generally any governmental or regulatory body that may have a wish to examine the particulars of an encrypted digital payment.

The TEE 16 of the payer communication device PD may be further configured for waiving the privacy of the payer PA represented by the payer details of the encrypted digital payment at the payer's own discretion by:

a) decrypting the encrypted digital payment using said payer private cryptographic key;
b) constructing a non-anonymous payment report including the decrypted payment details as well as the payer details; and
c) providing the non-anonymous payment report to the requesting external entity.

Alternatively, the TEE 16 of the payer communication device PD may be further configured for waiving the privacy of the payer PA represented by the payer details of the encrypted digital payment at the payer's own discretion by:

d) providing the payer private cryptographic key to the requesting external entity.

Accordingly, the payer PA is given the possibility to comply with the external entity's request and waive his or her privacy, at the discretion of the payer PA himself or herself. In one embodiment, the payer's PA discretion is exercised by the TEE 16 of the payer communication device PD being configured for retrieving an approval by the

user of the payer communication device PD (i.e., the payer PA) as a requisite for providing the non-anonymous payment report in step c) or the payer private cryptographic key in step d) to the requesting external entity. The approval may be given in the digital payment app 18 that executes in the normal or rich execution environment on the payer communication device PD.

In some embodiments, sanctions may be imposed onto the payer PA if not obeying a request from an external entity to provide information about an encrypted digital payment previously made by the payer communication device PD. Accordingly, the TEE 16 of the payer communication device PD may be configured for detecting that the user of the payer communication device PD denies or fails to provide said approval, and in response updating a state of the local digital wallet LDW hosted by the TEE 16 in any of the following ways:

- restricting use of the local digital wallet LDW for subsequent digital payments with respect to payer privacy and/or payment amount; or
- disabling the local digital wallet LDW such that subsequent digital payments are prohibited.

As will be understood, the payer PA will still be in control of his or her privacy, at the risk of sanctions if not cooperating with the requesting external entity. This introduces a balance between individual needs for payment privacy (like with conventional cash), and society needs for prevention of proximity digital payments used for illegal activities.

Some beneficial embodiments introduce escrow possibilities to the digital payment system 1. Accordingly, prior to uploading 122, 122' the encrypted digital payment to the payer payment service 60 or the payee payment service 70, the TEE 16 or the TEE 26, respectively, may be configured for encrypting at least the payer details of the digital payment based on an escrow public cryptographic key, thereby allowing decryption of the uploaded encrypted digital payment by an external entity having a corresponding escrow private cryptographic key.

Some beneficial embodiments introduce payer privacy at multiple levels. Accordingly, the TEE 16 of the payer communication device PD may be configured in step 212 of Figure 2 for assigning said data indicating requested payer privacy as a particular privacy level among at least two privacy levels. A first privacy level indicates full payer privacy, with decryption of an uploaded encrypted digital payment requiring use of a payer private cryptographic key (for instance, *payer_priv_key*) kept strictly within the trusted execution environment 16 of the payer communication device PD. A

second privacy level indicates less than full payer privacy, with decryption of an uploaded encrypted digital payment being possible also by using a different cryptographic key than said payer private cryptographic key. In some embodiments, said different cryptographic key for the second privacy level is an escrow private cryptographic corresponding to the escrow public cryptographic key referred to above.

There may also be a third privacy level to indicate that no payer privacy is requested by the payer PA for the particular digital payment to be made.

Beneficially, the first privacy level may be available for selection by the payer PA only when the digital payment to be made is in an amount less than a threshold value. From the society's point of view, this may be an acceptable trade-off between personal integrity and prevention of illegal activities.

In some embodiments, upon detecting in step 226 of Figure 2 that the data indicating requested payer privacy is set to the first privacy level in the digital payment DP received from the payer communication device PD, the TEE 26 of the payee communication device PD2 conceals the payer details in step 228 by performing the encryption thereof as described above.

In those embodiments described above, where use of the local digital wallet LDW is restricted for subsequent digital payments when the payer PA does not approve to a request from an external entity to provide information about an encrypted digital payment, the TEE 16 of the payer communication device PD may update the state of the local digital wallet LDW by reducing a maximum privacy level permitted. Reducing the maximum privacy level permitted may involve one of: changing the maximum privacy level permitted from the first privacy level to the second privacy level, changing the maximum privacy level permitted from the second privacy level to the third privacy level, and changing the maximum privacy level permitted from the first privacy level to the third privacy level.

Some beneficial embodiments introduce recovery password possibilities to the digital payment system 1. Accordingly, prior to uploading 122, 122' the encrypted digital payment to the payer payment service 60 or the payee payment service 70, the TEE 16 or the TEE 26, respectively, may be configured for encrypting at least the payer details of the digital payment based on a recovery password, thereby allowing decryption of an uploaded encrypted digital payment by providing the recovery password.

A potential additional issue identified by the present inventors is that payer privacy may be compromised if the payee payment service 70 and the payer payment

service 60 cooperate to match private digital payments as uploaded at 122'/230 and 122, by spotting identical payment amounts in one digital payment uploaded from the payer side and one digital payment uploaded from the payee side, and concluding that they in fact represent the same digital payment. Such matching may be prevented by uploading 122 the encrypted digital payment to the payer payment service 60 from the TEE 16 in a batch of a plurality of encrypted digital payments having been made by the payer communication device PD, wherein the batch includes an aggregate payment amount for all encrypted digital payments in the batch but not individual payment amounts of each encrypted digital payment. In a refined embodiment, the uploaded batch includes encrypted digital payments having been made by the payer communication device PD as well as encrypted digital payments having been received by the payer communication device PD, wherein the aggregate payment amount is for all encrypted digital payments made and received.

Some beneficial embodiments introduce payer signature possibilities to the digital payment system 1. In such embodiments, the payer details of the digital payment DP generated in the TEE 16 of the payer communication device PD in step 212 of Figure 2 will include a payer certificate (cf. *payer_cert* in Figure 1) comprising a payer public cryptographic key (cf. *payer_pub_key* in Figure 1). The generated digital payment DP is signed in the TEE 16 of the payer communication PD using a payer private cryptographic key (cf. *payer_priv_key* in Figure 1) corresponding to the payer public cryptographic key. At the payee side, processing of the decrypted digital payment in the TEE 26 of the payee communication device PD2 in step 222 of Figure 2 will involve verifying the payer's signature using the payer public cryptographic key *payer_pub_key* in the payer certificate *payer_cert*.

The step 224 of processing the digital payment DP in the TEE 26 of the payee communication device PD2 may further involve checking the payment amount against a payment amount requested by the payee PA2, for instance in the payment request 112. Alternatively or additionally, step 224 may involve checking that the digital payment DP matches the payment request 112 from the payee communication device PD2 to the payer communication device PD, for instance in terms of a matching transaction identifier. Alternatively or additionally, step 224 may involve checking that the payer address *payer_address* is not on a list of non-legitimate payer addresses. Alternatively or additionally, step 224 may involve checking the payer certificate *payer_cert* against a root certificate issued by a certificate authority 50 (see Figure 1).

In view of the above description, the skilled reader will immediately note that the digital payment system 1 in Figure 1 comprises a payer communication device PD and a payee communication device PD2, each having a short-range data communication interface 12, 22, a wide-area data communication interface 11, 21 and a trusted execution environment 16, 26. The digital payment system 1 further comprises a computerized payer payment service 60 being a cloud-based computing resource capable of wide-area data communication, and a computerized payee payment service 70 being a cloud-based computing resource capable of wide-area data communication.

The trusted execution environment 16 of the payer communication device PD is configured for:

generating a digital payment, the digital payment comprising payment details, payer details and data indicating requested payer privacy,

encrypting at least the payer details of the digital payment,

communicating the encrypted digital payment to the payee communication device PD2.

The trusted execution environment 26 of the payee communication device PD2 is configured for:

decrypting the digital payment;

processing the digital payment; and

upon detecting said data indicating requested payer privacy in the digital payment received from the payer communication device:

reconstructing the digital payment by concealing the payer details thereof; and

uploading the reconstructed digital payment to the payee payment service 70.

Furthermore, the skilled reader will immediately note that the trusted execution environment 16 of the payer communication device PD is configured for performing the functionality of the payer communication device PD in the computerized method according one or more of the embodiments described above, and that the trusted execution environment 26 of the payee communication device PD2 is configured for performing the functionality of the payee communication device PD2 in the computerized method according one or more of the embodiments described above.

Additionally, in view of the above description, the skilled reader will immediately note that the description includes a communication device PD for use in a digital payment system 1, the communication device comprising a short-range data communication interface 12, a wide-area data communication interface 11, and a trusted execution environment 16 configured for performing the functionality of the payer

communication device in the computerized method according one or more of the embodiments described above. Likewise, the above description includes a communication device PD2 for use in a digital payment system 1, the communication device comprising a short-range data communication interface 22, a wide-area data communication interface 21, and a trusted execution environment 26 configured for performing the functionality of the payee communication device in the computerized method according one or more of the embodiments described above.

Figure 3 is a schematic illustration of a computer-readable medium 300 in one exemplary embodiment, capable of storing a computer program product 310. The computer-readable medium 300 in the disclosed embodiment is a portable memory device, such as a Universal Serial Bus (USB) stick. The computer-readable medium 300 may however be embodied in various other ways instead, as is well-known *per se* to the skilled person. The portable memory device 300 comprises a housing 330 having an interface, such as a connector 340, and a memory chip 320. In the disclosed embodiment, the memory chip 320 is a flash memory, i.e. a non-volatile data storage that can be electrically erased and re-programmed. The memory chip 320 stores the computer program product 310 which is programmed with computer program code (instructions) that when loaded into a processing device, such as a CPU, will perform any of the functionalities listed in the next paragraph. The processing device may, for instance, be the aforementioned processing unit(s) of the controllers 13; 23 as described with reference to Figure 1. The portable memory device 300 is arranged to be connected to and read by a reading device for loading the instructions into the processing device. It should be noted that a computer-readable medium can also be other media such as compact discs, digital video discs, hard drives or other memory technologies commonly used. The computer program code (instructions) can also be downloaded from the computer-readable medium via a wireless interface to be loaded into the processing device.

In one embodiment, therefore, the computer-readable medium 300/computer program product 310 comprises computer program code for performing the functionality of the payer communication device PD in the computerized method according to one or more of the embodiments described above when the computer program code is executed by the processing device. In another embodiment, the computer-readable medium 300/computer program product 310 comprises computer program code for performing the functionality of the payee communication device PD2

in the computerized method according to one or more of the embodiments described above when the computer program code is executed by the processing device.

As will be understood from the above, the invention and the embodiments thereof will make it possible to balance regulatory requirements for transactional traceability of digital payments with true payer privacy through encryption of transactional information, typically for amounts below defined thresholds, defined by the issuer and the regulator, using wallet keys.

The invention has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims.

CLAIMS

1. A computerized method of providing payer privacy in digital payments, comprising:

in a trusted execution environment (16) of a payer communication device (PD):

generating (212) a digital payment, the digital payment comprising payment details, payer details and data indicating requested payer privacy;

encrypting (214) at least the payer details of the digital payment;

communicating (114; 216) the encrypted digital payment to a payee communication device (PD2); and

in a trusted execution environment (26) of the payee communication device (PD2):

decrypting (222) the digital payment;

processing (224) the digital payment; and

upon detecting (226) said data indicating requested payer privacy in the digital payment received from the payer communication device (PD):

reconstructing (228) the digital payment by concealing the payer details thereof; and

uploading (122'; 230) the reconstructed digital payment to a payee payment service (70).

2. The computerized method as defined in claim 1, wherein reconstructing the digital payment by concealing the payer details thereof in the trusted execution environment (26) of the payee communication device (PD2) involves:

encrypting at least the payer details of the digital payment by one or more cryptographic operations being based on a payee public/private cryptographic key pair, the payee private cryptographic key being kept strictly within the trusted execution environment (26) of the payee communication device (PD2).

3. The computerized method as defined in claim 1, wherein reconstructing the digital payment by concealing the payer details thereof involves, in the trusted execution environment (26) of the payee communication device (PD2):

encrypting at least the payer details of the digital payment by one or more cryptographic operations being based on a payer public cryptographic key provided in or with the encrypted digital payment communicated from the payer communication

device (PD) to the payee communication device (PD2), wherein the payer public cryptographic key (*payer_pub_key*) corresponds to a payer private cryptographic key (*payer_priv_key*) kept strictly within the trusted execution environment (16) of the payer communication device (PD).

4. The computerized method as defined in claim 1, wherein reconstructing the digital payment by concealing the payer details thereof involves, in the trusted execution environment (26) of the payee communication device (PD2):

deleting the payer details after processing of the digital payment, such that the reconstructed digital payment uploaded to the payee payment service (70) will not contain the payer details.

5. The computerized method as defined in any preceding claim, further comprising, in the trusted execution environment (26) of the payee communication device (PD2), upon detecting said data indicating requested payer privacy in the digital payment received from the payer communication device (PD):

constructing an anonymous payment report including the decrypted payment details but without the payer details; and

providing the constructed anonymous payment report to a digital payment app (28) executing in a normal or rich execution environment on the payee communication device (PD2), wherein a payer (PA) represented by the payer details is thus kept anonymous to a payee (PA2) being a user of the payee communication device (PD2).

6. The computerized method as defined in any preceding claim, further comprising, in the trusted execution environment (26) of the payee communication device (PD2):

receiving a request originating from an external entity to provide information about an encrypted digital payment previously received, processed and uploaded by the payee communication device (PD2);

decrypting the encrypted digital payment;

detecting, in the decrypted digital payment, presence of said data indicating requested payer privacy;

constructing an anonymous payment report including the decrypted payment details but without the payer details; and

providing the constructed anonymous payment report to the requesting external entity, wherein a payer (PA) represented by the payer details is thus kept anonymous to the requesting external entity.

7. The computerized method as defined in any preceding claim, further comprising, in the trusted execution environment (16) of the payer communication device (PD):

encrypting at least the payer details of a digital payment for which payer privacy is requested by one or more cryptographic operations being based on a payer private cryptographic key (*payer_priv_key*) kept strictly within the trusted execution environment (16) of the payer communication device (PD); and

uploading (122) the encrypted digital payment to a payer payment service (60).

8. The computerized method as defined in claim 7, further comprising, in the trusted execution environment (16) of the payer communication device (PD):

receiving a request originating from an external entity to provide information about an encrypted digital payment previously made by the payer communication device (PD); and

waiving the privacy of a payer (PA) represented by the payer details of the encrypted digital payment at the payer's own discretion by either:

a) decrypting the encrypted digital payment using said payer private cryptographic key (*payer_priv_key*);
b) constructing a non-anonymous payment report including the decrypted payment details as well as the payer details; and
c) providing the non-anonymous payment report to the requesting external entity,

or:

d) providing the payer private cryptographic key (*payer_priv_key*) to the requesting external entity.

9. The computerized method as defined in claim 8, further comprising, in the trusted execution environment (TEE) of the payer communication device (PD):

retrieving an approval by a user (PA) of the payer communication device (PD) as a requisite for providing the non-anonymous payment report in step c) or the payer private cryptographic key (*payer_priv_key*) in step d) to the requesting external entity.

10. The computerized method as defined in claim 9, further comprising, in the trusted execution environment (16) of the payer communication device (PD):

upon detecting that the user denies or fails to provide said approval, updating a state of a local digital wallet (LDW) hosted within the trusted execution environment (16), wherein the updated state is one of the following:

- restricting use of the local digital wallet (LDW) for subsequent digital payments with respect to payer privacy and/or payment amount; and
- disabling the local digital wallet (LDW) such that subsequent digital payments are prohibited.

11. The computerized method as defined in any of claims 2, 3 or 7, or any claim dependent thereon, further comprising, prior to uploading (122, 122') the encrypted digital payment to the payee payment service (70) or payer payment service (60), respectively:

encrypting at least the payer details of the digital payment based on an escrow public cryptographic key, thereby allowing decryption of the uploaded encrypted digital payment by an external entity having a corresponding escrow private cryptographic key.

12. The computerized method as defined in any preceding claim, further comprising, in the trusted execution environment (16) of the payer communication device (PD), assigning said data indicating requested payer privacy as a particular privacy level, wherein

a first privacy level indicates full payer privacy, with decryption of an uploaded encrypted digital payment requiring use of a payer private cryptographic key (*payer_priv_key*) kept strictly within the trusted execution environment (16) of the payer communication device (PD); and

a second privacy level indicates less than full payer privacy, with decryption of an uploaded encrypted digital payment being possible also by using a different cryptographic key than said payer private cryptographic key (*payer_priv_key*).

13. The computerized method as defined in claim 12, wherein a third privacy level indicates no payer privacy.

14. The computerized method as defined in claim 12 or 13, wherein the first privacy level is available only when the digital payment is in an amount less than a threshold value.

15. The computerized method as defined in any of claims 12-14 when dependent on claim 11, wherein for the second privacy level, said different cryptographic key is said corresponding escrow private cryptographic key.

16. The computerized method as defined in claim 15, wherein the trusted execution environment (26) of the payee communication device (PD2), upon detecting said data indicating requested payer privacy being set to the first privacy level in the digital payment received from the payer communication device (PD), performs the encrypting step defined in claim 3.

17. The computerized method as defined in claims 10 and 12, wherein restricting use of the local digital wallet (LDW) for subsequent digital payments involves updating the state of the local digital wallet (LDW) by reducing a maximum privacy level permitted.

18. The computerized method as defined in claim 17, wherein reducing the maximum privacy level permitted involves one of:

changing the maximum privacy level permitted from the first privacy level to the second privacy level;

changing the maximum privacy level permitted from the second privacy level to the third privacy level; and

changing the maximum privacy level permitted from the first privacy level to the third privacy level.

19. The computerized method as defined in any of claims 2, 3 or 7, or any claim dependent thereon, further comprising, prior to uploading (122', 122) the encrypted digital payment to the payee payment service (70) or payer payment service (60), respectively:

encrypting at least the payer details of the digital payment based on a recovery password, thereby allowing decryption of an uploaded encrypted digital payment by providing the recovery password.

20. The computerized method as defined in any of the preceding claims when dependent on claim 7, wherein uploading (122) the encrypted digital payment to the payer payment service (60) is made in a batch of a plurality of encrypted digital payments having been made by the payer communication device (PD), wherein the batch includes an aggregate payment amount for all encrypted digital payments in the batch but not individual payment amounts of each encrypted digital payment.

21. The computerized method as defined in claim 20, wherein the uploaded batch includes encrypted digital payments having been made by the payer communication device (PD) as well as encrypted digital payments having been received by the payer communication device (PD), wherein the aggregate payment amount is for all encrypted digital payments made and received.

22. The computerized method as defined in any of the preceding claims, wherein the digital payment generated in the trusted execution environment (16) of the payer communication device (PD) comprises:

said payment details, including a payment amount and optionally a payment currency;

said payer details, including a payer address (*payer_address*) indicative of an account (62) or depository held by the payer (PA) at a payer payment service (60);

said data indicating requested payer privacy; and

payee details, including a payee address (*payee_address*) indicative of an account (72) or depository held by the payee (PA2) at the payee payment service (70).

23. The computerized method as defined in claim 22, wherein the digital payment generated in the trusted execution environment (16) of the payer communication device (PD) furthermore comprises:

a transaction identifier determined by monotonically increasing a local counter function in the trusted execution environment (16) of the payer communication device (PD).

24. The computerized method as defined in claim 22 or 23,

wherein said payer details includes a payer certificate (*payer_cert*) comprising a payer public cryptographic key (*payer_pub_key*),

wherein the generated digital payment is signed in the trusted execution environment (16) of the payer communication (PD) using a payer private cryptographic key (*payer_priv_key*) corresponding to the payer public cryptographic key (*payer_pub_key*), and

wherein processing of the decrypted digital payment in the trusted execution environment (26) of the payee communication device (PD2) involves verifying the payer's signature using the payer public cryptographic key (*payer_pub_key*) in the payer certificate (*payer_cert*).

25. The computerized method as defined in any of claims 22-24, wherein the step of processing the digital payment in the trusted execution environment (26) of the payee communication device (PD2) involves one or more of:

checking the payment amount against a payment amount requested by the payee (PA2);

checking that the digital payment matches a payment request (112) from the payee communication device (PD2) to the payer communication device (PD);

checking that the payer address (*payer_address*) is not on a list of non-legitimate payer addresses; and

checking the payer certificate (*payer_cert*) against a root certificate issued by a certificate authority (50).

26. A digital payment system (1), comprising:

a payer communication device (PD) and a payee communication device (PD2), each having a short-range data communication interface (12, 22), a wide-area data communication interface (11, 21) and a trusted execution environment (16, 26);

a computerized payer payment service (60) being a cloud-based computing resource capable of wide-area data communication; and

a computerized payee payment service (70) being a cloud-based computing resource capable of wide-area data communication,

wherein the trusted execution environment (16) of the payer communication device (PD) is configured for:

generating a digital payment, the digital payment comprising payment details, payer details and data indicating requested payer privacy,

encrypting at least the payer details of the digital payment,

communicating the encrypted digital payment to the payee communication device (PD2), and

wherein the trusted execution environment (26) of the payee communication device (PD2) is configured for:

decrypting the digital payment;

processing the digital payment; and

upon detecting said data indicating requested payer privacy in the digital payment received from the payer communication device:

reconstructing the digital payment by concealing the payer details thereof; and

uploading the reconstructed digital payment to the payee payment service (70).

27. The digital payment system (1) as defined in claim 26,

wherein the trusted execution environment (16) of the payer communication device (PD) is configured for performing the functionality of the payer communication device (PD) in the computerized method as defined by any of claims 1-25, and

wherein the trusted execution environment (26) of the payee communication device (PD2) is configured for performing the functionality of the payee communication device (PD2) in the computerized method as defined by any of claims 1-25.

28. A communication device (PD) for use in a digital payment system (1), the communication device comprising:

a short-range data communication interface (12);

a wide-area data communication interface (11); and

a trusted execution environment (16) configured for performing the functionality of the payer communication device in the computerized method as defined by any of claims 1-25.

29. A communication device (PD2) for use in a digital payment system (1), the communication device comprising:

a short-range data communication interface (22);

a wide-area data communication interface (21); and

a trusted execution environment (26) configured for performing the functionality of the payee communication device in the computerized method as defined by any of claims 1-25.

30. A computer program product comprising computer program code for performing the functionality of the payer communication device (PD) in the computerized method as defined by any of claims 1-25 when the computer program code is executed by a processing device.

31. A computer program product comprising computer program code for performing the functionality of the payee communication device (PD2) in the computerized method as defined by any of claims 1-25 when the computer program code is executed by a processing device.

32. A non-volatile computer readable medium having stored thereon a computer program comprising computer program code for performing the functionality of the payer communication device (PD) in the computerized method as defined by any of claims 1-25 when the computer program code is executed by a processing device.

33. A non-volatile computer readable medium having stored thereon a computer program comprising computer program code for performing the functionality of the payee communication device (PD2) in the computerized method as defined by any of claims 1-25 when the computer program code is executed by a processing device.

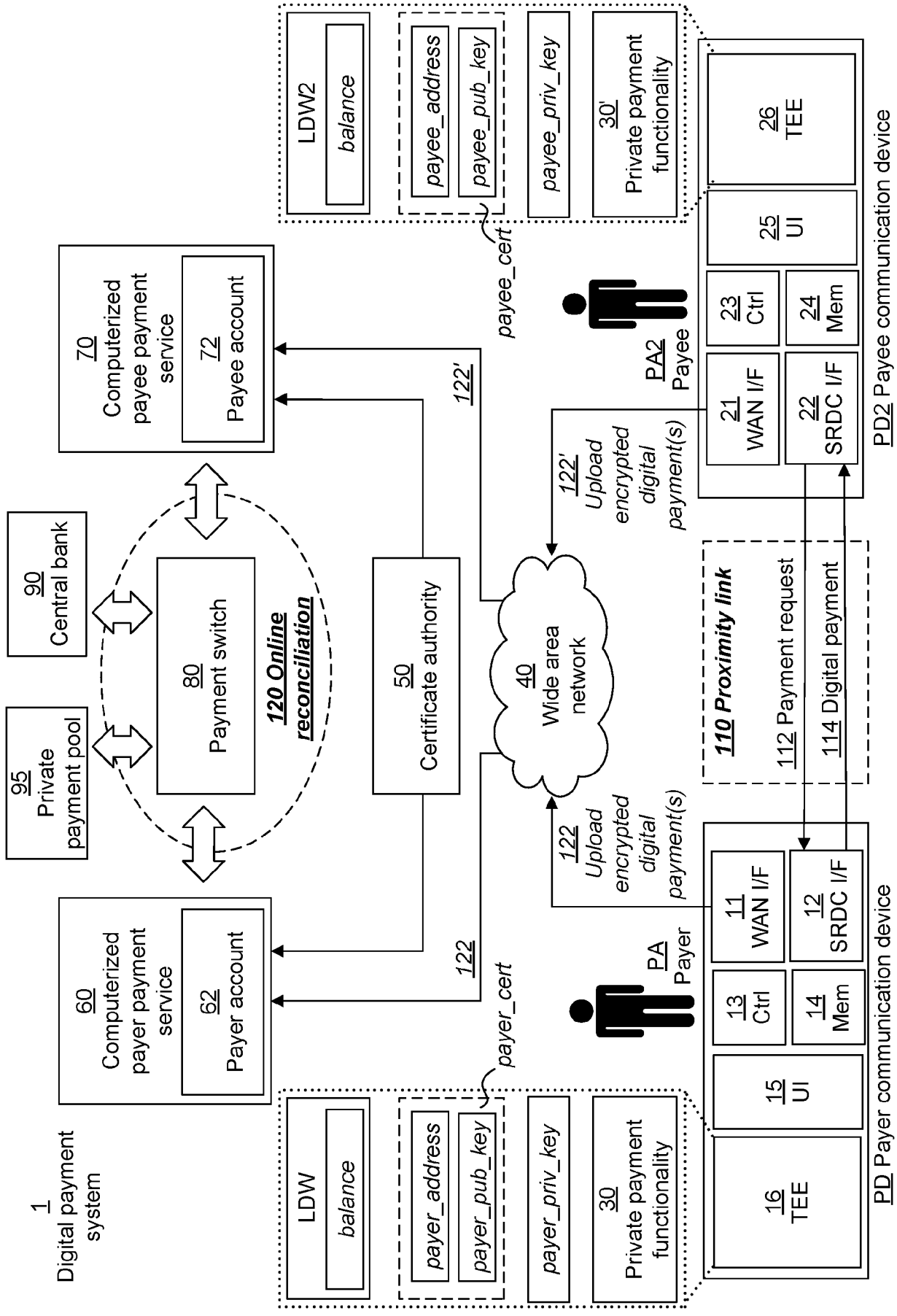
1
Digital payment system
LDW
balance
payer_address
payer_pub_key
payer_priv_key
30
Private payment functionality
payer_cert
60
Computerized payer payment service
62
Payer account
PA
Payer
PD Payer communication device
16
TEE
15
UI
13
Ctrl
14
Mem
11
WAN I/F
12
SRDC I/F
122
Upload encrypted digital payment(s)
122
payer_cert
50
Certificate authority
40
Wide area network
110 Proximity link
112 Payment request
114 Digital payment
122'
Upload encrypted digital payment(s)
PA2
Payee
PD2 Payee communication device
21
WAN I/F
22
SRDC I/F
23
Ctrl
24
Mem
25
UI
26
TEE
30'
Private payment functionality
payee_priv_key
payee_address
payee_pub_key
LDW2
balance
payee_cert
122'
70
Computerized payee payment service
72
Payee account
90
Central bank
95
Private payment pool
80
Payment switch
120 Online reconciliation

Fig 1

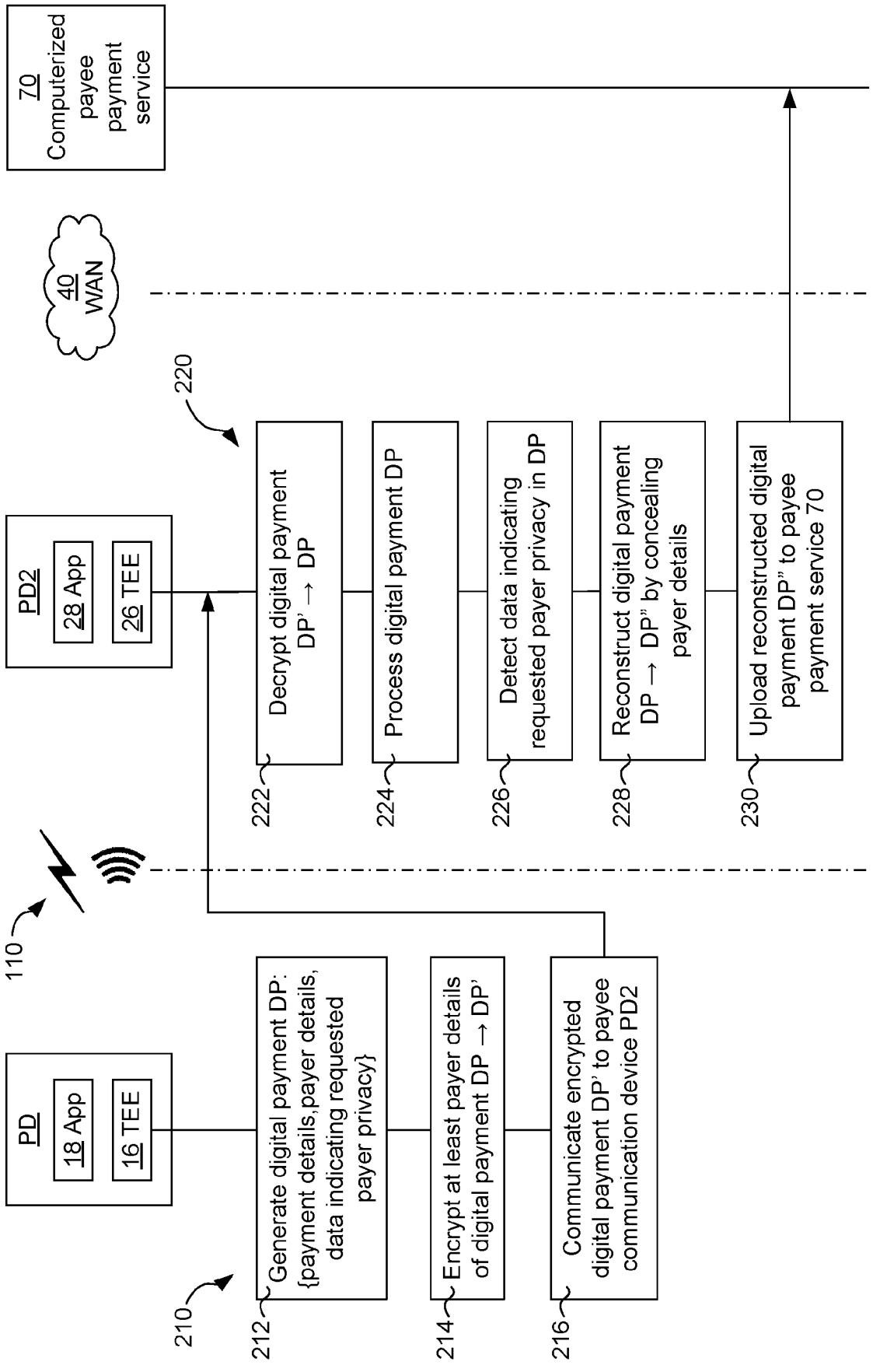
70 Computerized payee payment service
40 WAN
220
PD2
28 App
26 TEE
Decrypt digital payment DP' → DP
Process digital payment DP
Detect data indicating requested payer privacy in DP
Reconstruct digital payment DP → DP" by concealing payer details
Upload reconstructed digital payment DP" to payee payment service 70
222
224
226
228
230
110
PD
18 App
16 TEE
Generate digital payment DP: {payment details,payer details, data indicating requested payer privacy}
Encrypt at least payer details of digital payment DP → DP'
Communicate encrypted digital payment DP' to payee communication device PD2
210
212
214
216

Fig 2

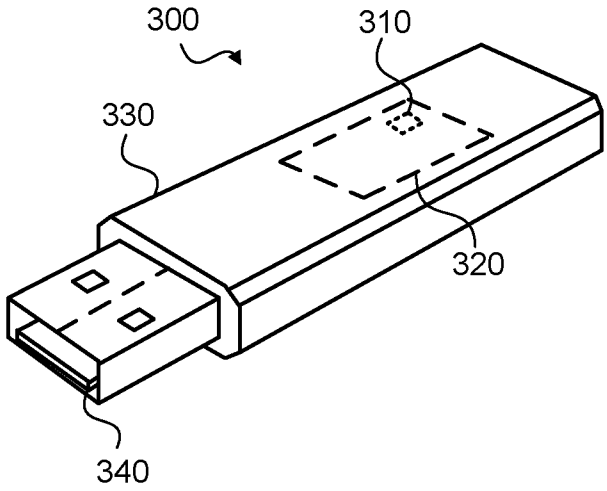

Fig 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2025/050378

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

KIME

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20180089660 A1 (ELLIOTT THOMAS ET AL), 29 March 2018 (2018-03-29); abstract; paragraphs [0021]-[0028], [0035]-[0038]; figures 1-6	1-33
	--	
A	US 20160117680 A1 (PRIEL TOMER ET AL), 28 April 2016 (2016-04-28); abstract	1-33
	--	
A	US 20120143767 A1 (ABADIR ESSAM ERNEST), 7 June 2012 (2012-06-07); abstract	1-33
	--	
A	US 11935020 B1 (FAKHRAIE LILA ET AL), 19 March 2024 (2024-03-19); abstract	1-33
	--	

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12-05-2025	12-05-2025

Name and mailing address of the ISA/SE	Authorized officer
Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Oskar Pihlgren Telephone No. + 46 8 782 28 00

International application No.
PCT/SE2025/050378

Continuation of: second sheet

International Patent Classification (IPC)

G06Q 20/08 (2012.01)
H04L 9/00 (2022.01)

US	20180089660	A1	29/03/2018	WO	2018057284	A1	29/03/2018
US	20160117680	A1	28/04/2016	CN	105393269	A	09/03/2016
				EP	3014544	A4	15/02/2017
				WO	2014209314	A1	31/12/2014
US	20120143767	A1	07/06/2012	US	9141945	B2	22/09/2015
				US	20120143772	A1	07/06/2012
				US	20150356554	A1	10/12/2015
				US	9779393	B2	03/10/2017
				US	20220101282	A1	31/03/2022
US	11935020	B1	19/03/2024	US	20240220954	A1	04/07/2024