



(12) **DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION**

(13) **A1**

(86) **Date de dépôt PCT/PCT Filing Date:** 2022/03/23
(87) **Date publication PCT/PCT Publication Date:** 2022/09/29
(85) **Entrée phase nationale/National Entry:** 2023/09/22
(86) **N° demande PCT/PCT Application No.:** CA 2022/050438
(87) **N° publication PCT/PCT Publication No.:** 2022/198323
(30) **Priorité/Priority:** 2021/03/23 (US63/165,116)

(51) **Cl.Int./Int.Cl. H04L 9/40** (2022.01),
G06Q 20/38 (2012.01), **G16Y 10/45** (2020.01)
(71) **Demandeur/Applicant:**
ROYAL BANK OF CANADA, CA
(72) **Inventeurs/Inventors:**
ORTIZ, EDISON U., CA;
BADAL-BADALIAN, ARNOLD, CA;
LIU, MING LI, CA;
KHANDAVILLI, RAVI, CA
(74) **Agent:** NORTON ROSE FULBRIGHT CANADA
LLP/S.E.N.C.R.L., S.R.L.

(54) **Titre : PROTOCOLE ET PORTAIL POUR COMMUNIQUER DES DONNEES DE TRANSACTION SECURISEE**
(54) **Title: PROTOCOL AND GATEWAY FOR COMMUNICATING SECURE TRANSACTION DATA**

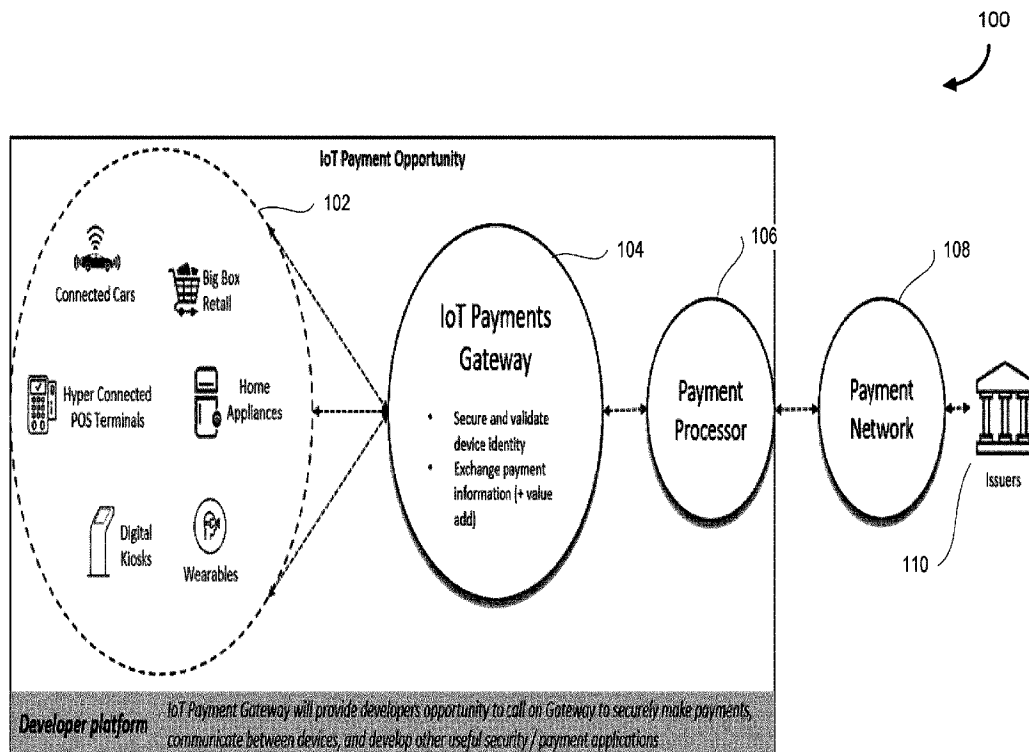


FIG. 1

(57) **Abrégé/Abstract:**

Systems and methods for secure communication of data packets are described using a communications gateway and protocol. One or more payment generator devices utilize trusted execution environments to store identity attestation parameters which are then utilized during registration and/or validation of device identity at the gateway for secure transmission of secure data, including, for example, payment data.

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

(19) World Intellectual Property

Organization

International Bureau

(43) International Publication Date

29 September 2022 (29.09.2022)



(10) International Publication Number

WO 2022/198323 A1

(51) International Patent Classification:

H04L 9/40 (2022.01)

G16Y 10/45 (2020.01)

G06Q 20/38 (2012.01)

(21) International Application Number:

PCT/CA2022/050438

(22) International Filing Date:

23 March 2022 (23.03.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/165,116

23 March 2021 (23.03.2021)

US

(71) Applicant: **ROYAL BANK OF CANADA** [CA/CA]; 6th Floor, South Tower, Royal Bank Plaza, 200 Bay Street, Toronto, Ontario M5J 2J5 (CA).

(72) Inventors: **ORTIZ, Edison U.**; c/o Royal Bank of Canada, 6th Floor, South Tower, Royal Bank Plaza, 200 Bay Street, Toronto, Ontario M5J 2J5 (CA). **BADAL-BADALIAN, Arnold**; c/o Royal Bank of Canada, 6th Floor, South Tower, Royal Bank Plaza, 200 Bay Street, Toronto, Ontario M5J

2J5 (CA). **LIU, Ming Li**; c/o Royal Bank of Canada, 6th Floor, South Tower, Royal Bank Plaza, 200 Bay Street, Toronto, Ontario M5J 2J5 (CA). **KHANDAVILLI, Ravi**; c/o Royal Bank of Canada, 6th Floor, South Tower, Royal Bank Plaza, 200 Bay Street, Toronto, Ontario M5J 2J5 (CA).

(74) Agent: **NORTON ROSE FULBRIGHT CANADA LLP**; 1 PLACE VILLE MARIE, SUITE 2500, MONTREAL, Québec H3B 1R1 (CA).

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: PROTOCOL AND GATEWAY FOR COMMUNICATING SECURE TRANSACTION DATA

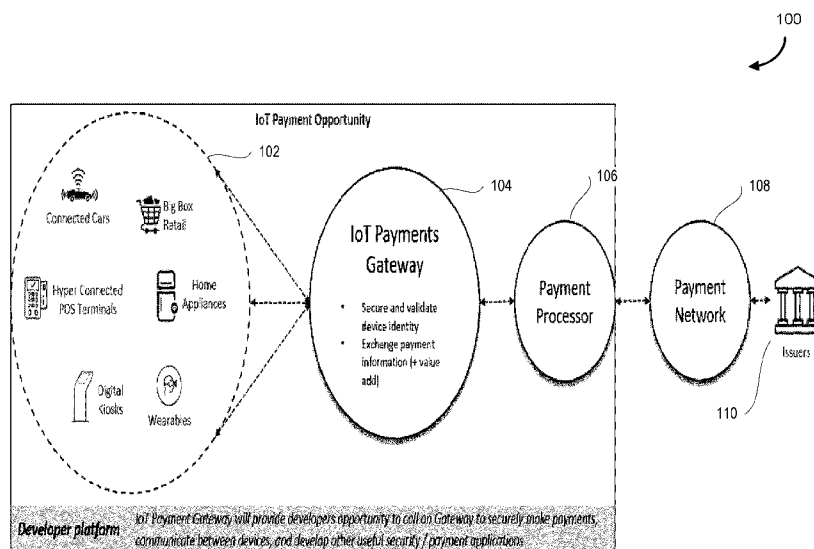


FIG. 1

(57) Abstract: Systems and methods for secure communication of data packets are described using a communications gateway and protocol. One or more payment generator devices utilize trusted execution environments to store identity attestation parameters which are then utilized during registration and/or validation of device identity at the gateway for secure transmission of secure data, including, for example, payment data.



WO 2022/198323 A1

WO 2022/198323 A1

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))*

PROTOCOL AND GATEWAY FOR COMMUNICATING SECURE TRANSACTION DATA

CROSS REFERENCE

[0001] This application is a non-provisional application, claiming all benefit, including
5 priority to US Application No. 63/165116, entitled PROTOCOL AND GATEWAY FOR COMMUNICATING SECURE TRANSACTION DATA, filed 23-Mar-2021, incorporated herein by reference.

[0002] This application is related to US Application No. 63/077,443, entitled SYSTEM
AND METHOD FOR ELECTRONIC CREDENTIAL TOKENIZATION, filed 11-Sep-2020, and
10 US Application No. 14/056,440, filed October 17, 2013 and entitled VIRTUALIZATION AND SECURE PROCESSING OF DATA which claimed priority to US Provisional Application No. 61/715,142 filed October 17, 2012; US Provisional Application No. 61/811,783 filed April 14, 2013; US Provisional Application No. 61/825,865 filed May 21, 2013; US Provisional Application No. 61/833,188 filed June 10, 2013; and US Provisional Application No.
15 61/863,593 filed August 8, 2013; of which all priority applications entitled SECURE PROCESSING AND STORAGE OF PAYMENT DATA.

[0003] This application is also related to US Application No. 15/201,428, filed July 2, 2016 which claimed priority to US Provisional Application No. 61/188,067 filed July 2, 2015; US Provisional Application No. 62/200,859 filed August 4, 2015; US Patent Application No.
20 15/000,685 filed January 19, 2016; all of which are entitled SECURE PROCESSING OF ELECTRONIC PAYMENTS.

[0004] This application is also related to US Application No. 16/424,242, filed May 28, 2019 which claimed priority to US Provisional Application No. 62/677,133 filed May 28, 2018; US Provisional Application No. 62/691,406 filed June 28, 2018; US Provisional Application
25 No. 62/697,140 filed July 12, 2018; US Provisional Application No. 62/806,394 filed February 15, 2019; and US Provisional Application No. 62/824,697 filed March 27, 2019; all of which are entitled SYSTEM AND METHOD FOR SECURE ELECTRONIC TRANSACTION PLATFORM.

FIELD

[0005] Embodiments of the present disclosure generally relate to the field of data communications, and more specifically, embodiments relate to devices, systems and methods for communicating secure transaction data between a plurality of network
5 connected devices.

INTRODUCTION

[0006] Internet of Things implementations provide a network of physical objects that are coupled with connectivity components for transferring power and/or data. The physical objects themselves are often low-power, low capability devices that are adapted to
10 economically provide, in concert, a connected, "smart" solution, such as an electronically enabled home having temperature sensors, water leak sensors, among others. Because these objects have low-power and low capability, there are limitations on the complexity of operations that can be performed on them, including limitations relating to communication distances, security, and encryption. There are further limitations due to size and cost.

[0007] An increase in 5G adoption and decrease in cost of ownership of IoT devices will lead to a surge in adoption IoT devices, and each machine will need its own identity and ability to act independently (e.g. to pay for things). Furthermore, the payment data may provide visibility and value in real-time insights / decision-making, and encourage
15 investments in infrastructure to support adoption. Establishing machine identity is a core
20 challenge as a potential threat vector comes from devices masquerading as other devices.

[0008] Each of the devices need to communicate with other devices, and different protocols have been introduced for doing so. In particular, these protocols are adapted for creating networks out of the Internet of Things devices, and in some cases, the devices are required to connect through a hub for more robust communications.

[0009] A deficiency of these approaches is that the architecture is not secure, and malicious devices are able to engage in malicious communications across the network.

[0010] NFC based payments are utilized for EMV contactless payments and has seen wide adoption in Canada over the previous decade and slowly gaining adoption in the US.

[0011] The standard was built on the foundation of chip and pin also know as "dip" which issuers, acquires and merchant partners are familiar with. The need for proximity also made it a good fit and provided the foundation for mobile contactless payments.

[0012] A hindrance to the adoption of NFC payments was the need for hardware upgrades in brick and mortar stores. Being built upon old and familiar standards also has its shortcomings, adding additional data fields for value add services such as loyalty proved to be a hassle and was not worth the investment for many retailers.

[0013] Bluetooth, as a protocol, does not provide additional security guarantees and performance improvements over NFC payments, but can be used to enhance the user experience and provide other value added services.

SUMMARY

[0014] A surge in IoT devices will lead to an increase in end-points that are able to initiate payments, and accordingly, a system and corresponding methods and computer readable media are proposed that are adapted to secure communications for making payments, for example, between connected devices. IoT devices can be utilized as an alternative for consumers to traditional payments in a store where customers have to wait in line to pay at a limited number of cashier terminals. The IoT devices can provide proximity payments using communication technologies (e.g., Bluetooth Low Energy, ultra-wideband communications), and can be adapted, for example, to provide a flexible set of payment receiver devices that each act as remote checkout terminals that can be deployed throughout a physical location.

[0015] Proposed approaches are described in various embodiments herein directed to mechanisms for mutual authentication approaches that can be used, for example, when introducing new devices into a trusted ecosystem, or periodically authenticating devices in the trusted ecosystem. Mutual authentication is useful in situations where it is important for devices to be able to trust the identity of devices that are being added and to reduce a technical threat vector associated with either fake devices or devices masquerading as other devices (e.g., "device spoof" by a malicious device). The mutual authentication can be conducted between a plurality of device devices, such as between a pair of devices having a first device (e.g., a payment generator device) and a second device (e.g., a payment

receiver device), and the mutual authentication can be implemented a series of communication steps between the devices using key certificates and keys for securing the communications. The mutual authentication can be adapted for use over less secure short range communications, such as Bluetooth Low Energy. The mutual authentication steps are provided so that even if intercepted (e.g., in a man in the middle attack), the communications may not be useful for the malicious party. The mutual authentication steps can be implemented through controlled communications by mobile applications residing on, operating on, or otherwise present on either or both of the IoT devices.

[0016] The IoT devices operate and communicate with one another to secure communications, and management of the devices can be conducted by a secure payment gateway that communicates with various IoT devices, managing a certificate authority operating alongside backend servers, such as financial payment processing backends and inventory management servers (e.g., for tracking sold inventory or services, and updating stock).

[0017] A specific, non-limiting example use case for IoT communications using the proposed mutual authentication approach includes using a first set of IoT devices that operate as IoT payment receiver devices. These IoT payment receiver devices can be strategically located throughout a store, such as a supermarket, and configured to operate each as mobile checkout devices. A number of different IoT payment receiver devices can be flexibility connected to the financial backend through the gateway, for example, based on store demand or busyness level (e.g., increasing the number of devices during a holiday period or major shopping dates, such as Black Friday).

[0018] The IoT payment receiver devices, for example, can be provided in a specific “checkout” area, for example, that can be geo-fenced or simply the area within range of the broadcast from their communications interfaces (e.g., Bluetooth Low Energy). In each checkout area, for example, a pillar can be provided having many embedded IoT payment receiver devices disposed therein.

[0019] Each of the IoT payment receiver devices then acts as a connectable “checkout” terminal, awaiting connections from customers, who may be walking around the store and

scanning items from their physical shopping cart into an application into their device. When the customer is finished and seeking to purchase, instead of standing in line, the customer then simply enters a “checkout” zone, and connects to an available IoT payment receiver device.

5 [0020] A consumer, for example, can then utilize a smartphone that is adapted as a payment generator device that connects to the IoT payment receiver device. The smartphone, for example, could have a Bluetooth Low Energy communications modem controllable by the mobile application for communication with the IoT payment receiver device. Bluetooth Low Energy can be used for limited range communications, but other
10 protocols are considered as well.

[0021] One or both of the IoT payment receiver device and the payment generator device, in various embodiments, are coupled to a payment gateway that coordinates and orchestrates communications for processing payment and checkout data flows in accordance with a specialized secure message protocol. The secure message protocol is
15 adapted for utilizing encryption keys and/or device attestations to automatically improve a security level between inter-device communications to reduce a system vulnerabilities (e.g., malicious payment receiver or payment generator devices).

[0022] In particular, the payment gateway that is proposed in some embodiments for the IoT ecosystem, enabling secure exchange of payment data between devices, as there are
20 no existing standardized and widely accepted method for two IoT devices to securely make payments, and the IoT payments gateway provides necessary security to attest device identities, as well, ensure secure payments.

[0023] The gateway acts as a exchange layer between IoT end-points and existing payment rails, helping secure payment data and also enabling value-add services such as
25 loyalty The gateway mechanism improves the security of data packets for communications between IoT devices when the data packets are used, for example, for handling payment information.

[0024] Communicating devices are secured using a trusted execution environment that may be on-board that holds a set of public key / private key encryption key pairs that are established during manufacturing. The trusted execution environment stores the private key securely and the private key is used to attest (sign) or verify communications originating from the trusted device to conduct a secure transaction. Because the public key can be held at the gateway, the gateway can verify that the message was indeed signed by the trusted device.

[0025] Example use cases include in-aisle IoT devices where a number of IoT devices located in a grocery store that each become mini point of sale devices so someone doesn't have to check out at a cashier, and a smart parking lot where each parking spot has a smart IoT device that each acts as a secure transaction initiating device.

DESCRIPTION OF THE FIGURES

[0026] In the figures, embodiments are illustrated by way of example. It is to be expressly understood that the description and figures are only for the purpose of illustration and as an aid to understanding.

[0027] Embodiments will now be described, by way of example only, with reference to the attached figures, wherein in the figures:

[0028] **FIG. 1** is an example ecosystem diagram illustrating an IoT payment ecosystem along with a number of potential connected IoT devices and backend payment processing networks, according to some embodiments.

[0029] **FIGS. 2A-2J** show example user interface screenshots of an example user experience flow for the first use case, according to some embodiments.

[0030] **FIG. 3** is an example block schematic of the ecosystem diagram of **FIG. 1**, according to some embodiments.

[0031] **FIG. 4** is an example schematic of the system of **FIG. 1**, showing a set of mechanisms utilized for secure token generation, payment receipt and processing, device integrity verification, and device attestation, among others.

[0032] FIG. 5 is a process flow diagram illustrating steps of a transaction, beginning with the sending of a checkout notification to a payment receiver device, from a cloud based payments gateway service.

5 [0033] FIG. 6 is a listing of components of an example IoT Payment Gateway, according to some embodiments.

[0034] FIG. 7 is an example process flow for IoT device registration, according to some embodiments. This step may run on device setup or on a pre-determined interval to validate that the device is in good health and provision with a token attesting the device and a set of certificates for authentication and data encryption.

10 [0035] FIG. 8 is an example payment transaction flow, according to some embodiments.

[0036] FIG. 9 is an example process flow for registering a device to obtain a signed certificate, according to some embodiments.

15 [0037] FIG. 10 is an example process flow for registering a payment generator device where a signed device certificate is obtained from the certificate authority, according to some embodiments.

[0038] FIG. 11 is an example process flow for generating a shared secret between a payment generator device and a payment receiver application, according to some embodiments.

20 [0039] FIG. 12 is an example process flow for PKI initialization, according to some embodiments.

[0040] FIG. 13 is an example process flow for payment generator device personalization, according to some embodiments.

[0041] FIG. 14 is an example process flow for payment receiver device personalization, according to some embodiments.

[0042] FIG. 15A is an example process flow for device mutual authentication and secure messaging establishment, according to some embodiments.

[0043] FIG. 15B is an example process flow showing sample timings for steps from FIG. 15A.

5 [0044] FIG. 16 is an example customer profile for a potential user of the system, according to some embodiments.

[0045] FIG. 17 is an example method for an asynchronous payment, according to some embodiments.

10 [0046] FIG. 18 is an example method for a synchronous payment, according to some embodiments.

[0047] FIG. 19 is an example block schematic diagram showing an example computational device for near range communications, according to some embodiments.

[0048] FIG. 20 is an example method for a payment using a first vendor's computational platform, according to some embodiments.

15 [0049] FIG. 21 is an example method for a payment using a second vendor's computational platform, according to some embodiments.

[0050] FIG. 22 is a schematic diagram of a computing device such as a computer server for providing a gateway for IoT communications.

DETAILED DESCRIPTION

20 [0051] As described herein, a proposed gateway (or communication protocol) will act as a exchange layer between IoT end-points and existing payment rails, helping secure payment data and also enabling value-add services such as loyalty.

[0052] The gateway is adapted to control and route communications to improve the security of data packets for communications between IoT devices when the data packets are
25 used, for example, for handling payment information.

[0053] FIG. 1 is an example ecosystem diagram illustrating an IoT payment ecosystem along with a number of potential connected IoT devices and backend payment processing networks, according to some embodiments.

[0054] In the diagram 100, the connected IoT devices 102 can include devices such as connected cars, communication devices present at various retail stores (e.g., supermarkets), connected point-of-sale terminals, home appliances, digital kiosks, and wearables, among others, which are coupled, either directly (e.g., connected by WiFi or Bluetooth) or indirectly (e.g., using an ad-hoc connection or sending packets through another IoT devices) to the IoT payments gateway 104, which is adapted to securely validate a device's identity and allow it to exchange payment information to a payment processor engine 106, which can be coupled to a backend payment network 108 and ultimately issuers 110. In some embodiments, the issuers 110 provision a certificate to the IoT device which will be further used for mutual authentication and secure communication to the server, for example, through a secure network connection from the issuer 110 to should be able to establish secure communication from the application on the IoT device to the issuer 110's servers, and logs may be collected for diagnostic and troubleshooting purposes.

[0055] In a first use case, the connected IoT devices 102 may be configured to communicate using Bluetooth Low Energy (BLE), and utilize BLE communications to conduct payments between two or more devices. In this example, in-aisle payments can be conducted at a supermarket using a retailer's Scan & Go application. See, for example, FIG. 2A to FIG. 2J.

[0056] The connected IoT devices 102 are utilized to further 'technify' checkouts by providing multiple end-points for check-out that will shift a larger portions of payments to in-store touchless transactions such as in-aisle payments, using automation to help save costs (reducing dependency on slower, traditional checkout) and to provide an improved user experience. Mutual authentication approaches are used between a plurality (e.g., a pair) of connected IoT devices 102.

[0057] Mutual authentication is the process by which two applications that need to communicate validate are legitimate. In the context of the IoT payment, mutual

authentication refers to the authentication between the two device exchanging payment data. An example mutual authentication approach is shown in more detail at **FIG. 15A** and **FIG. 15B**.

5 [0058] In a traditional point of sale transaction, there is no mutual authentication between the card and the point of sale terminal, whether physical or loaded digitally onto a mobile device. Offline data authentication is an approach in EMV that is used for validating whether the card which is used for payments is a valid card through a hierarchy of Issuer and Payment scheme PKI. Physical cards do have support for this, but most POS terminals do not require this flow to be supported as most transactions are now online (i.e., the
10 cryptogram verification requester goes to the issuer or someone that the issuer delegated the process to).

[0059] This is true in the case for BLE where the issuer accepts the payments to be authorized online. In the current point of sale setting, the user performing the transaction is at a proximity with the terminal to either tap, swipe, dip or scan (in the case of QR code
15 payments) their card and credentials at the point of sale terminal.

[0060] BLE (and other similar technologies that may be utilized for IoT devices) however, does not require proximity, hence there is the additional need for establishing mutual authentication before the exchange of sensitive data.

[0061] **FIGS. 2A-2J** show example user interface screenshots of an example user
20 experience flow for the first use case, according to some embodiments. This experience flow may be provided, for example, by a mobile application on the customer's device that is capable of controlling communications using a modem (e.g., a Bluetooth Low Energy modem) on the device. The customer has loaded the mobile application, and in some embodiments, the customer already has an account with the merchant, or is using a guest
25 account. The customer's mobile application effectively turns the customer's mobile device into a IoT payment generator device.

[0062] The customer enters the premises of the store, and begins walking around and adding items into a physical shopping cart, for example.

[0063] The customer also loads the application and uses during the shopping process. In **FIGS. 2A-2C**, at example interface screens **202**, **204**, **206**, a customer may be able to scan various QR codes or bar codes to add items to a cart. At **FIG. 2D**, the customer scans the code on the food item, and it is added to the cart. At **FIG. 2E**, the item is added to the cart, and other offers may be surfaced, for example, based on what as added to the cart presently, in the past, or estimated to be added in the future.

[0064] During this process, the customer's virtual cart has records of all the items that have been scanned, and for example, a tally of cost and/or pricing can be maintained so that the customer is able to see a running subtotal.

[0065] When the customer is ready to finalize the transaction, the customer can head over to a "checkout zone" where IoT devices are residing. This zone could be a geofenced region, or a demarcated physical region where the IoT devices act as virtual "checkout staff". A benefit of this approach is that the physical security threat footprint is minimized to the small area of the checkout zone, while the number of virtual "check out staff" can be dynamically adjusted simply by adding or removing IoT payment receiver devices from each zone.

[0066] Each IoT payment receiver device may handle a number of transactions serially or in parallel, and when the number of communication pathways are saturated or the device is at a pre-defined limit, a communications queue can be established where payment generator devices are queued for payment. In some embodiments, where there are active payment generator devices queued for payment, a signal may be sent to a backend system to activate more IoT payment receiver devices, or to send a request to bring more IoT payment receiver devices to service the specific "checkout zone".

[0067] At **FIG. 2F**, a checkout screen is shown. At **FIG. 2G** and **FIG. 2H**, the customer's smartphone connects to the IoT checkout station (in this case, Station #3), which initiates an IoT payment process whereby a payment is processed at **FIG. 2I**. At **FIG. 2J**, a purchase completion confirmation page is shown to the customer.

[0068] FIG. 3 is an example block schematic of the ecosystem diagram of FIG. 1, according to some embodiments.

[0069] In FIG. 3, IoT devices 302 and 304 can include groups of devices that each have their own trusted execution environment (TEE), and are secured using a trusted execution
5 environment that may be on-board that hold encryption keys, such as a set of public key / private key encryption key pairs that are established during manufacturing.

[0070] The TEE can utilize isolation properties of a hardware module or circuit to provide a secure processing environment. Any sensitive data including payment related data or potential PII data will need to be processed inside this isolated environment and
10 communicated to the server in a secure manner.

[0071] The server will need to be able to validate with cryptographic proofs from the root of trust that the transaction has been sent from a genuine processing device with security properties intact.

[0072] The TEE may have the following properties: secure random number generation, generation of non-exportable asymmetric private keys (preferably NIST approved elliptic
15 curve based public and private key pairs), code isolation and secure processing of logic that is protected from the host operating system and any peer applications running on the host operating systems, and a global platform TEE certification mechanism to validate the above.

[0073] In some embodiments, the IoT device 304 may also connect through a hub 306
20 which may optionally also have its own TEE. Encryption can include using a RSA secret generation mechanism, or other approaches such as ECDH, among others. The keys can be directly embedded, for example, at a chipset, system on a chip, or printed circuit board level. The data being transferred should be protected at transport and at the message layer, in some embodiments, and for example, data is protected at the application level via shared
25 key between mobile device and server, and transport level encryption can be provided through a communications protocol specification (e.g., using Bluetooth capabilities).

[0074] The trusted execution environment stores the private key securely and the private key is used to attest (sign) or verify communications originating from the trusted device (or

hub **306**) to conduct a secure transaction. Because the public key can be held at the gateway, the gateway can verify that the message was indeed signed by the trusted device. In some embodiments, trusted devices without TEE can also connect through hub **306**, and be secured by the hub **306**'s TEE.

- 5 [0075] In a further embodiment, the devices may be configured to mutually authenticate each other at the application layer before exchange of sensitive data, where the mobile device is able to authenticate the IoT gateway, and vice-versa. In an alternate embodiment, the data is protected from the mobile device to the payment processing server end to end so there is no hard requirement to authenticate these two devices.
- 10 [0076] The devices **302**, **304**, or hub **306** may communicate secure payment information through secure data communications with an IoT secure payment gateway **310**, and in some embodiments, the TEEs are utilized to encrypt and/or attest information such that the keys stored onboard can be utilized as certificates to be validated at a certificate authority **314**, which may be configured to manage certificates.
- 15 [0077] In some embodiments, the IoT devices **302** are coupled to one another (e.g., in an adhoc network) where one device **302** has another device **304** relay a message to the gateway **310**. In some embodiments, as each TEE has a secret key or a parameter that cannot be changed established during manufacturing, and the certificate authority can utilize a known aspect of the secret key or parameter (or in some instances, a copy of the secret
- 20 key or parameter) to determine that the data communication did indeed come from the device associated with the TEE. To reduce the likelihood of replay attacks, in some embodiments, the messages are encrypted or encapsulated with a time-varying aspect such that the encryption or signing is only valid for a short duration of time. Other security countermeasures are possible.
- 25 [0078] The IoT secure payment gateway **310** may be coupled with a financial backend server **312** adapted for processing payments, which may be further coupled to an inventory management server **316** to update inventory and/or stock levels.

[0079] A malicious IoT device **308** may be connected to the IoT gateway **310** that attempts to send a malicious message. Because the malicious device **308** does not have a TEE, the IoT gateway **310** may flag the payment transaction message as suspicious and/or fraudulent as it cannot look up or validate the identity of the malicious IoT device **308**. The
5 malicious device **308** may also be missing the requisite information and cannot conduct a mutual authentication.

[0080] This is a cybersecurity improvement relative to other protocols, such as simply connecting to wireless networks using known SSIDs and passwords to join a common network, or connecting to any available Bluetooth device that is broadcasting a pairing
10 single. The mutual authentication provides an improved handshaking mechanism that can be used for secure communications.

[0081] **FIG. 4** is an example schematic of the system of **FIG. 1**, showing a set of mechanisms utilized for secure token generation, payment receipt and processing, device integrity verification, and device attestation, among others.

15 [0082] **FIG. 5** is a process flow diagram **500** illustrating steps of a transaction, beginning with the sending of a checkout notification to a payment receiver device, from a cloud based payments gateway service.

[0083] The illustrated process flow is adapted as an alternative to traditional approaches where one has to queue in line to conduct a payment at the terminal in store. For example,
20 in typical payment situations, an individual would queue in line at one of many checkout terminals to await a turn to pay, and such approach is limited by a number of cashiers or checkout lanes as each of the checkout terminals pays using a particular point of sale device that is sequentially approached and utilized.

[0084] Instead, the proposed approach shown in **FIG. 5** illustrates a proximity
25 communications based payment, where a number of IoT payment receiver devices are strategically located and/or positioned throughout a facility to facilitate payments. The communications technology shown in many examples herein is based on Bluetooth Low Energy (BLE) technologies, but other technologies are possible, such as ultra wide-band

communications, among others. The payment receiver device, in some embodiments, can be portable and moved around to establish payment zones from which the payment receivers can be connected. As store layouts change, the payment receiver devices can be repositioned accordingly.

5 [0085] The payment generator device in this example is a customer's smartphone or mobile device, and the payment generator device is coupled with a mobile application or on-board functionality which is adapted for conducting an electronic payment transaction as described in various embodiments herein. The payment generator device, for example, can include a device that is adapted for scanning items, or encoding representing items (e.g.,
10 barcodes, QR codes) or loading pushed indications of services provided, among others. These items requiring payment can be digitally represented, and stored on a digital shopping cart.

[0086] At Step 1 in **FIG. 5**, the customer is ready for payment, and, in some embodiments, can move to enter a geofenced "payment zone" where the payment generator device is
15 capable of engaging in a proximity communication channel with the payment receiver device, which in this example, is the strategically located IoT device that acts as an improved checkout terminal that can handle many transactions in parallel, thus obviating the need for checkout lines).

[0087] At Step 2, the payment generator device then initiates the proximity communication
20 channel (e.g., BLE connection), and payment data objects can be provided along with linked payment card tokens and/or credentials to be sent to the payment receiver device.

[0088] At Step 3, the payment receiver device is adapted to verify the credentials of the payment generator device, and an attestation report is requested from an edge services engine. The attestation report can be utilized even, in some embodiments, for two devices
25 that are operating peer to peer, without specific secure element processors on-board.

[0089] At Step 4, transaction information can be returned to the payment generator device to indicate that the payment amount and currency.

[0090] At Step 5, a transaction request is transmitted to a cloud-based backend processing engine, represented as a data object containing data values and fields corresponding to transaction amount, currency, payment receiver device ID, payment generator device ID, payment card issue token, and the attestation report, for example.

- 5 [0091] At Step 6, a request to verify the attestation report is sent to the edge services engine, and on a successful verification, at Step 7, the transaction request is verified and transmitted to a payment processing engine.

- [0092] At Step 8, a transaction result can be provided to the payment generator device, which, for example, can be represented as a QR code or a digital data object (e.g., signed
10 using an encryption key) that can be used by the customer for presentation to show that the items have been successfully purchased.

- [0093] The digital data object can be used in place of receipt checks during exit, and in some embodiments, a graphical display element is rendered on a display of the smartphone or portable device with the receipt, and an attendant can conduct a manual check of the
15 information provided on the screen. In another embodiment, the digital data object can be transmitted or otherwise provided at a non-attended exit, such as a mantrap or a turnstile, which requires a payment data object corresponding to the purchased items to be validated prior to unlocking a latch for an exit. An individual, for example, could tap a smartphone or use another proximity device to communicate the digital data object.

- 20 [0094] As the proposed solution can handle multiple requests from payment generator devices simultaneously, the proximity technology-based payments approach is a useful mechanism that can be adapted to fit within current infrastructure, and can be deployed with minimal deployment changes. In view of investment in existing payment processing rails and associated regulations and standard protocols, the processing messages can be
25 adapted to align with existing message flows during a systems retrofit, operating as an adapter or interface that operates between the merchant and issuer computing devices.

[0095] The system can be interacted with, for example, through an API as an interface, for example, through a disseminated software development kit, or in another embodiment, as a

mobile application for provisioning on either or both of the payment generator and the payment receiver devices.

[0096] A technical challenge that arises with proximity payment messaging is that security across electronic communication channels needs to be addressed, as there is an increased potential attack surface relative to approaches that require very close physical proximity or reading of data directly from a payment card, such as a tap, a swipe, a card insertion, etc. There are different approaches for addressing security, and the proposed approaches of some embodiments herein is adapted from a payment perspective, adapted to maintaining industry standard data protection and cybersecurity policies and protecting communication channels using encryption and attestations.

[0097] **FIG. 6** is a schematic **600** showing a listing of components of an example IoT Payment Gateway, according to some embodiments.

[0098] The payment receiver device, for example, can be an IoT device having software, such as a mobile application, that is adapted for secure payments / checkouts.

[0099] The consumer, through the consumer's mobile device (payment generator device), initiates a BLE connection that writes payments data containing the payment generator device identifier and a linked payment card issue token to the payment receiver device. The payment generator device then verifies the payment generator device ID, and calls an edge processing API to generate an attestation report.

[00100] Transaction data containing an amount and currency, for example, encapsulated, as a data packet, can be read by the payment generator device if a payment data process completes successfully.

[00101] The payment receiver device then sends a transaction request data message containing a transaction amount / currency, payment receiver device ID, payment generator device ID, a payment card issue token, and the attestation report to the payment processor engine, which then sends a request to verify the attestation report from an edge processing server.

[00102] Upon successful verification, the transaction request data is validated and a payment card authorization token is retrieved, to be sent to a financial payments processor backend using the authorization token. The transaction result can be sent to the payment generator device (e.g., your payment was completed successfully).

- 5 [00103] **FIG. 7** is an example process flow **700** for IoT device registration, according to some embodiments. This step, for example, may be configured to run on device setup or on a pre-determined interval to validate that the device is in good health and provision with a token attesting the device and a set of certificates for authentication and data encryption.

- 10 [00104] **FIG. 8** is an example payment transaction flow **800**, according to some embodiments. An approach is shown that is an example approach where there is a proximity channel that is established prior to a data exchange (Bluetooth channel set up prior to the data exchange).

- 15 [00105] A communication channel is established between the payment generator device (e.g., customer's smartphone) and the payment receiver device (e.g., IoT device for handling purchase transactions), and in this example flow, it is important that from a security perspective that the payment generator can identify the payment receiver before exchanging any sensitive data.

- 20 [00106] A trusted execution environment, in some embodiments, is a protected file system or file storage operated by a special high security processor that may be segregated from other computing functionality, and the trusted execution environment may be present on the payment receiver device for securely generating and communicating attestation tokens so that a payment processing server is able to validate and/or verify the identity of the payment receiver device prior to processing any payments.

- 25 [00107] This is particularly important in view of potential issues related to attempts at "spoofing" or otherwise conducting malicious activities (e.g., false purchases, returns) through the provisioning of a falsified payment receiver device by a malicious third party.

[00108] A transaction is initiated, and confirmation details are confirmed. The payment receiver device provides identity and data protection certificates for payment, and these

certificates are validated by the payment generator device. Keypairs are generated, and transaction data along with public keys are transmitted to the payment generator. The payment generator uses a coupled trusted execution environment to prepare and transmit an attestation token with encrypted payment data to a payment processing data, which then
5 validates the token, creates a shared key using the payment generator's public key, and processes the transaction.

[00109] **FIG. 9** is an example process flow **900** for registering a device to obtain a signed certificate, according to some embodiments.

[00110] A process flow is shown whereby the payment receiver device can interoperate
10 with a certificate authority for conducting device registration. In this example, a registration processes is used between the payment receiver device for registration, and in the registration process, communications are made with certificate authorities for certificate generation through communications between edge services servers and clients.

[00111] **FIG. 10** is an example process flow **1000** for registering a payment generator
15 device where a signed device certificate is obtained from the certificate authority, according to some embodiments. A hardware backed keystore can be used for secure keypair generation.

[00112] A process flow is shown whereby the payment generator device can interoperate with a digital card facilitator and a certificate authority for conducting device registration.

[00113] This process flow can be utilized to establish a card token object (e.g., credit card,
20 debit card) which can then be utilized in the future for supporting a payment transaction initiated by the payment generator device.

[00114] An asymmetric keypair is generated, and the public key is used for a registration of the device. A digital card facilitator device is used to create a public key certificate, which is
25 then signed by a certificate authority server and returned to the payment generator application.

[00115] **FIG. 11** is an example process flow **1100** for generating a shared secret between a payment generator device and a payment receiver application, according to some embodiments.

5 [00116] In this process flow, a series of steps are shown for establishing a secure communication channel between the payment generator device and the payment receiver device. As shown in this example, a shared secret and a nonce, among other aspects, can be utilized to establish a shared channel as between the two devices.

10 [00117] The secure channel is used to validate certificates sent by the payment generator device, and the payment receiver generates a first nonce, which is sent back to the payment generator device, who generates a second nonce and a shared secret generated from both the certificate, as well as the two nonces). Each side is able to generate the shared certificate using the nonces and the certificates, and a secure channel can be thus set up.

15 [00118] **FIG. 12** is an example process flow **1200** for PKI initialization, according to some embodiments. This approach is utilized to utilize key certificates to establish payment generator and payment receiver public / private keypairs and corresponding certificates, which can be issued, generated, and/or revoked by a certificate authority server.

[00119] **FIG. 13** is an example process flow **1300** for payment generator device personalization, according to some embodiments.

20 [00120] In this process flow, the payment generator device initiates a request for generation of certificates, the request including a device payment generator public key, and the backend responds with a corresponding set of data objects that will be utilized during a payment process, including a certificate authority public key, an issuer payment generator public key certificate, a payment generator device public / private key pair, and a device payment generator device public key certificate.

25 [00121] After the personalization, the payment generator device is populated with a certificate authority public key, an issuer payment generator public key certificate, a keypair for the payment generator device, and a corresponding certificate.

[00122] **FIG. 14** is an example process flow **1400** for payment receiver device personalization, according to some embodiments.

[00123] In this process flow, the payment receiver device similarly initiates a request for generation of certificates, the request including a payment receiver device public key, and the backend responds with a corresponding set of data objects that will be utilized during a payment process, including a certificate authority public key, a manager payment receiver public key certificate, a payment receiver device public / private key pair, and a device payment receiver device public key certificate.

[00124] As noted, after the personalization process, the payment receiver device is populated with the certificate authority public key, a manager payment receiver public key certificate, a keypair for the payment receiver device, and a corresponding certificate..

[00125] **FIG. 15A** is an example process flow **1500A** for device mutual authentication and secure messaging establishment, according to some embodiments. The mutual authentication process uses the certificates generated during the personalization processes of **FIG. 13** and **FIG. 14**.

[00126] A problem that arises with traditional approaches is that while traditional payment cards include electronics or other identifiers for use in verifying that the card is indeed a trusted card, there are no existing mechanisms that can be used by the card to verify that a terminal is a trusted terminal. For this reason, there can be fraud, for example, in traditional approaches when a valid card is inserted into a fraudulent terminal. However, the potential for fraud is mitigated in traditional payment scenarios as there is often an attendant or a limited number of payment terminals provided in secure locations. This problem is more challenging when the terminal is capable of connecting through proximity communications, and deployed, for example, by a trusted terminal manager, which could be adapted for provisioning, verifying, and revoking credentials of one or more payment receiver devices disposed throughout a facility. A communication flow is shown between the payment generator device and the payment receiver device, and in this example process flow, the two devices conduct a mutual authentication process for establishing a secure messaging channel. The mutual authentication is particularly important as proximity communications

are vulnerable to cyberattacks and/or interception, and validated trust can be established through the exchange of keys established during the generation processes. Mutual authentication can be utilized to mitigate potential risks whereby, for example, a malicious user obtains an un-provisioned payment receiver terminal and attempts to skim card information from payment generator devices, and, for example, utilizes this for fraudulent transactions into their own bank accounts.

[00127] **FIG. 15A** is described from the perspective of the payment generator device, which is adapted to communicate to with the payment receiver device through transmitting data messages and receiving response data messages. While some of the example blocks have AES encryption shown, it is to be noted that other types of encryption are possible as well, such as other types of block ciphers, such as Blowfish, RC5, IDEA, DES, or other variations of Rijndael type ciphers, among others.

[00128] Referring to the step numbering shown in **FIG. 15B**:

[00129] At Step 1, data is written to the payment receiver device with the identifying information of the payment generator device. This message is BLE0.

[00130] The written data is a first message containing the payment generator device identifier, the issuer payment generator public key certificate, and the device payment generator public key certificate.

[00131] At Step 2, the payment receiver device verifies the issuer payment generator public key and then utilizes the verified issuer payment generator public key to verify the device payment generator public key certificate.

[00132] The certificate authority public key is used to verify the issuer payment generator public key certificate, and that is then used to extract the issuer payment generator public key. The issuer payment generator public key is used to verify the device payment generator public key certificate, and to extract the device payment generator public key.

[00133] At Step 3, the payment receiver device provides to the payment generator device (in a message noted as BLE1), a set of data elements identifying the identity and validating the identity of the payment receiver device.

5 [00134] The payment generator device reads this information, and the message contains the payment receiver device identifier, the manager payment receiver public key certificate, and the device payment receiver public key certificate.

[00135] At Step 4, the payment receiver device can be verified, and a set of encrypted AES key blocks can be generated, and corresponding private keys can be utilized to recover the underlying key blocks.

10 [00136] The payment generator device uses the certificate authority public key to verify the manager payment receiver public key certificate and extracts the manager payment receiver public key. The manager payment receiver public key is then used to verify the device payment receiver public key certificate, and to extract the device payment receiver public key. A generator key block can now be generated.

15 [00137] At step 5, the payment generator device writes a message (denoted for example, as BLE2) to the payment receiver device, which contains the payment generator device identifier, and the generator key block encrypted using the device payment receiver public key.

20 [00138] At Step 6, the payment receiver device receives the message BLE2, and uses the device payment receiver private key to recover the Generator key block (e.g., decrypts it). A receiver key block is generated. A secure message key is derived by conducting an XOR operation between the receiver key block and the generator key block. A message, BLE3, is prepared for transmission to the payment generator device.

25 [00139] At Step 7, the payment generator device receives BLE3, and obtains the payment receiver device identifier, as well as the receiver key block, encrypted using the device payment generator public key.

[00140] At Step 8, the payment generator device uses the device payment generator private key to recover the receiver key block, and generates the generator key block, and is able to then derive the secure message key based on a XOR operation between the receiver key block and the generator key block.

- 5 [00141] At Step 9, a message, BLE4, is then provided for transmission to the payment generator device having the payment receiver device identifier, and the payment data encrypted using the secure message key that was derived earlier using the receiver key block and the generator key block.

- 10 [00142] Accordingly, the payment data is secured using a shared secret key that was generated as part of the mutual authentication process.

[00143] At Step 10, BLE4 is received by the payment receiver device, and the payment data is decrypted using the secure message key block that was derived earlier.

- 15 [00144] When the payment data is decrypted, the payment receiver device can interoperate with a backend process to initiate processing of the transaction. Further steps can include the payment generator device transmitting receipts or other indications that the payment was successful. For example, a receipt could include a transaction number, a transaction confirmation code or message (e.g., message 200 for success, 400 for error). The transaction number may be obtained from the backend transaction processing, etc.

- 20 [00145] When the customer has successfully completed payment, the mobile application operating as the payment generator device can then render a success screen, such as a green checkmark screen with an itemized receipt shown on it, or a corresponding QR code indicating a successful transaction. The QR code, for example, may be adapted to be scanned by a gate device, and the gate device may coordinate with the backend server to confirm that a transaction having a particular transaction identifier was conducted by a
25 corresponding mobile application having a specific mobile application identifier or customer identifier. When the gate device has confirmed success, the customer may activate a turnstile or a door may open, and the customer leaves with the purchased goods.

[00146] In another embodiment, the QR code may be scanned by a human attendant carrying a portable scanning device, and a list of all or some of the items purchased can be shown on a screen for a light visual validation or verification by the human attendant. High value, or sensitive items (e.g., jewelry, pharmaceuticals), can be provided in a different color, or otherwise highlighted for particular attention etc.

[00147] **FIG. 15B** is a message flow diagram **1500B** that also shows example timing for messages sent back and forth for establishing the mutual authentication channel, according to some embodiments. The mutual authentication process shows the five (BLE0-BLE5) messages being sent back and forth to securely transmit payment data from the payment generator device to the payment receiver device. While five messages are shown, variations are possible, and more, less, or modified versions of the messages are possible.

[00148] The messages are designed to be computationally fast for use on low-speed and/or low capability devices.

[00149] As shown in the example timing from an experimental set up, the message flows are adequately fast between a test payment generator device and a payment receiver device such that the channel can be established expeditiously for message exchange.

[00150] In **FIG. 15B**, Bluetooth Low Energy (BLE) messages are utilized to represent the data messages, and these were denoted as BLE0, BLE1, BLE2, BLE3, and BLE4 in the diagram. In this specific example, the payment and acceptance devices authenticate each other) and secure messaging (messages between payment and acceptance devices are encrypted after mutual authentication).

[00151] The diagram illustrates a minimum time BLE connection needs to be established for the transaction to be completed between devices and then for the acceptance device to send transaction request for online approval. iPhone XS is used as the payment device. Kona is the chip used in IoT board as acceptance device.

[00152] As shown in the example diagram, the message timing for each of the messaging steps is acceptable on limited hardware (e.g., maximum of 600 ms), which indicates that the transaction was able to be completed in a few seconds, despite the enhanced security

measures implemented in the mutual authentication process flow. The total amount of storage space utilized is in the hundreds of bytes, which also indicates that the message flow can operate without requiring a large amount of storage space on the limited capability devices.

- 5 [00153] The amount of data for each read/write operation is described. Sample data captured from a transaction is provided below:

[00154] BLE0 packetData[467]=

424c453033303631363030432d394533312d343743432d393043462d45454245453735413
84342457cf81006a7438432dc37802a70ad0fa57135404c3849f772ef63da998c1db192319fd
10 af0f041911f22151676efa75ddfd29dc1877d0c5de02241d525ed43bb62fea17ed8200d254d8
08523860bf8f456e65b28b75b75815ec8ee8d5bbdc32cefa582fd56dfc7d436f05c00b11d6d2d
e9f72d1dfef2e0753904808cc50e6e43a280cbc6dfa18f78847014a0000f39b8f5c1576f4ab272
17feb5b6808c73ef87e58d782971ede99c7169e4462e8a5393683df28b7c2021819154cf0246
1aed7e478d0a0dc0e7ea7e0600de608cee09ccde2610931884b20a707545ff7a6614e39c345
15 8d97d3fa900e80929dd981eda2cb7f816fa501b6e4c344e31b05de49bb64577a0e6822d87c0
a39d2e12ace4b0d15d824baf27f19442dfb64d8563c09c220418d8b0911c311919304b42a27
50660e886202b4eac5c3bd2d077deb6311cb19f374c6c4c0ecf4601ac940f08afe8535a77ad4
064995980f079b2e31e5784ba7239d809ba803cda68b7c4f0dcd0dc368f8ec827047bb78857
953ce78cc7532fce06233fed5ecee4572caf032605e3410ddd83f0340a935e9d3e4afa2c2ca25
20 ba1282d5d43e01b41f5936023

[00155] BLE1 packetData[447]=

424c4531343335333136306532646539633939377cf866401ef6a261363b15de34aa9552ed
045217e2eb9ddf1d1835a5abf0d492e992381dd5f6b26d9b070f537e1ff1db8565e6832d6e83
ec7da572c47c03469b6d397a8304d724c26ba4ac3fd708d09d6395fcfa8d7a5dbfff928ff571f1
25 a83fb5806c6c50efc0b5aef72760f0b14c1759282937a3749755e4e5970517a2b88105903d04
064ba5d8b7fbfc9c7d61997b74a95fa83302ddda05f3520e714e34c86a5ba784d7b398b91e8c
d37313b6a51540d0e2b6cc2759df43e40ee79b216b3058817f055be3437fbf8634277b5840e
47e8c2fe1e491c5b102c24fef42cc3e6bfb553ecd150e5ee647bffe03828e6aa8e31c43ffc984
99e544b06d0070a4abf3bc13855f427756740572cf051b6614e6406aa6e24513043da765fb5
30 513bebb4f07a92d51125f44be413dc85b107a7a0cf29511c045e42b39e942204a656a3ceeff2

82fd1651e3f67baf0bf98e74faa561c1bdb043d55088d2de0c205dd66ae5f6f8e18d73ed7f715c
173d69cc4e753b200af068e492685f6365fb7ecf354dee2777c695fdd9ac9a059aa12ab345b3
50a2b2ddd261c204a0fe3a7f204a28100b93590551d3a1c5688bbfb

[00156] BLE2 packetData[170]=

5 424c453233303631363030432d394533312d343743432d393043462d45454245453735413
84342457c80627fd2d798a1071128d01094022c8e3bd2d564aefa2fa0a7eca1765e6157fb16d
cecf420c3ec73857f5a7e736c0d4b406a90ac06ae57428f70d36b503a9b5dddb8ee2e339d8cd
46a479b275adc0e8fdf60cfab7c8a9babe316f127dc964b4df0c6780627bc860d8b29895c2d95
b11401a6bf205b23380559b38a602c0d368968

10 [00157] BLE3 packetData[150]=

424c4533343335333136306532646539633939377c8047605cb2666d0d76987c6f979d4ddd
45437c5f278d6a71eedb54dc480bb350f1be1e5e768f77f577a2bb0a199908202052baa9c988
2903a0033f7a6490ca4e7d819ed562cad9c1f3efa90f41086f6f48c872c5364cef11f77ddbd3d1
5b42681f1133dd19943ffbf64092c03147d96521a281038afe883e28caa0f52c5bd6565b

15 [00158] BLE4 packetData[90]=

424c453433303631363030432d394533312d343743432d393043462d45454245453735413
84342457c3041d6c431934dba84f5684e341772b0582f0237adf473a4c4b2c217691ee8b28a
badb904750e256fdece637f677bf76b

[00159] The actual size of data packets is dependent on key sizes. In an example
20 embodiment, the system uses 1948 RSA for CA, 1408 RSA for Payment Issuer / Device
Manager, and 1024 RSA for all devices.

[00160] As shown above, the timing of the entire flow required about 600 ms, even with
the maximum size keys.

[00161] **FIG. 16** is an example customer profile for a potential customer of the system,
25 according to some embodiments. In this customer profile, the customer is Jill, a health
conscious shopper. As described in her profile, she is interested in ways to reduce human-
interactions, especially in view of the pandemic climate.

[00162] She is frustrated with the shopping experience and would appreciate technology whereby she is able to check out in a more seamless manner. The system as described in some embodiments can be used by Jill through her mobile device operating, for example, using a low-energy communications protocol to communicate in a secure manner with a distributed IoT device (that can be placed at strategic locations, or consolidated into a payment zone) that acts as a pseudo-mobile checkout terminal that she can interact with.

[00163] Steps as described above, etc., can be utilized for ensuring that secure communication channels are utilized to ensure that there is mutual authentication and exchange of certificates. The mutual authentication process needs to be robust, yet computationally “fast” enough to avoid inconveniencing Jill, so there are technical constraints imposed on the solution.

[00164] **FIG. 17** is an example method **1700** for an asynchronous payment, according to some embodiments. In this example, a number of steps are shown whereby the transaction data can be conducted without waiting for an online processing result. This is particularly useful in situations where there is either no online connection, the connection is not operating temporarily, or where there is a backlog in processing.

[00165] **FIG. 18** is an example method **1800** for a synchronous payment, according to some embodiments. In this example, the synchronous payment requires a waiting for an online processing result. This approach improves security at the cost of processing speed, especially if there is a backend processing backlog or constrained resources. In some embodiments, the approach can include toggling between synchronous and asynchronous flows based on detected network conditions, system load, or connection availability. In some embodiments, certain IoT devices operate in a synchronous mode, while others can operate in an asynchronous mode. For example, IoT devices that reside within a basement of a shopping center may not have available connections to obtain online processing results.

[00166] **FIG. 19** is an example block schematic diagram **1900** showing an example computational device for near range communications, according to some embodiments. As shown here, there are a number of systems that interoperate with one another using communication mechanisms such as Bluetooth, near field communications, among others.

[00167] FIG. 20 is an example method 2000 for a payment using a first vendor's computational platform, according to some embodiments.

[00168] FIG. 21 is an example method 2100 for a payment using a second vendor's computational platform, according to some embodiments.

5 [00169] These two flows show two different practical approaches that can be used in the context of differing technology platforms and stacks.

[00170] FIG. 22 is a schematic diagram of a computing device 2200 such as a computer server for providing a gateway for IoT communications. As depicted, the computing device includes at least one processor 2202, memory 2204, at least one I/O interface 2206, and at
10 least one network interface 2208.

[00171] Processor 2202 may be an Intel or AMD x86 or x64, PowerPC, ARM processor, or the like. Memory 2204 may include a suitable combination of computer memory that is located either internally or externally such as, for example, random-access memory (RAM), read-only memory (ROM), compact disc read-only memory (CDROM).

15 [00172] Each I/O interface 2206 enables computing device 2200 to interconnect with one or more input devices, such as a keyboard, mouse, camera, touch screen and a microphone, or with one or more output devices such as a display screen and a speaker.

[00173] Each network interface 2208 enables computing device 2200 to communicate with other components, for example, through API 118 to exchange data with other components,
20 to access and connect to network resources, to serve applications, and perform other computing applications by connecting to a network (or multiple networks) capable of carrying data including the Internet, Ethernet, plain old telephone service (POTS) line, public switch telephone network (PSTN), integrated services digital network (ISDN), digital subscriber line (DSL), coaxial cable, fiber optics, satellite, mobile, wireless (e.g., Wi-Fi, WiMAX), SS7
25 signaling network, fixed line, local area network, wide area network, and others.

[00174] Applicant notes that the described embodiments and examples are illustrative and non-limiting. Practical implementation of the features may incorporate a combination of

some or all of the aspects, and features described herein should not be taken as indications of future or existing product plans. Applicant partakes in both foundational and applied research, and in some cases, the features described are developed on an exploratory basis.

5 [00175] The term "connected" or "coupled to" may include both direct coupling (in which two elements that are coupled to each other contact each other) and indirect coupling (in which at least one additional element is located between the two elements).

10 [00176] Although the embodiments have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the scope. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification.

15 [00177] As one of ordinary skill in the art will readily appreciate from the disclosure, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized. Accordingly, the embodiments are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

[00178] As can be understood, the examples described above and illustrated are intended to be exemplary only.

WHAT IS CLAIMED IS:

1. A data communications gateway for secure communication of data packets, the data communications gateway comprising:

a processor operating in conjunction with computer memory and data storage, the processor configured to:

register one or more payment receiver devices using one or more encryption keys stored on one or more trusted execution element each corresponding to a corresponding one or more payment receiver devices;

upon receiving a data communication packet representing a request for payment, processing the data communication packet and validating a device identity by confirming that the data communication packet corresponds to at least one of the one or more registered payment receiver devices; and

processing a payment transaction based at least on the data communication packet.
2. The data communications gateway of claim 1, wherein the one or more encryption keys are utilized to attest one or more properties of the one or more trusted execution elements.
3. The data communications gateway of claim 2, wherein the attestation of the one or more properties is conducted both during registration of the one or more payment receiver devices and the validation of the identity of the one or more payment receiver devices.
4. The data communications gateway of claim 1, wherein the one or more payment receiver devices interoperate with one or more payment generator devices to generate the data communication packet representing the request for payment.
5. The data communications gateway of claim 4, wherein the one or more payment generator devices and the one or more payment receiver devices are configured for conducting a mutual authentication process to provide secure communications between a first payment generator device and a first payment receiver device.
6. The data communications gateway of claim 5, wherein both of the first payment generator device and the first payment receiver device are initialized with a certificate authority public key.

7. The data communications gateway of claim 6, wherein the first payment generator device, after a payment generator device personalization process, stores the certificate authority public key, a issuer payment generator public key certificate, a device payment generator private key, a device payment generator public key, and a device payment generator public key certificate.
8. The data communications gateway of claim 7, wherein the first payment receiver device, after a payment receiver device personalization process, stores the certificate authority public key, a manager payment receiver public key certificate, a device payment receiver private key, a device payment receiver public key, and a device payment receiver public key certificate.
9. The data communications gateway of claim 8, wherein the mutual authentication process includes a series of messages transmitted the first payment generator device and the first payment receiver device, the series of messages adapted to generate a shared key block between the first payment generator device and the first payment receiver device, the shared key block used to encrypt payment data for transfer from the payment generator device to the first payment receiver device.
10. The data communications gateway of claim 9, wherein the series of messages include:
 - a first message transmitted from the first payment generator device to the first payment receiver device, the first message including the issuer payment generator public key certificate and the device payment generator public key certificate, wherein the first payment receiver device is configured for using the certificate authority public key to verify the issuer payment generator public key certificate, using the issuer payment generator public key to verify the device payment generator public key certificate, and extracting the device payment generator public key;
 - a second message transmitted from the first payment receiver device to the first payment generator device, the second message including the manager payment receiver device public certificate, and the device payment receiver public key certificate, wherein the first payment generator device is configured for using the certificate authority public key to verify the manager payment receiver public key certificate and extract the manager payment receiver public key, and using the manager payment receiver public key to verify the device payment receiver public key certificate and extract the device payment receiver public key, and generating a generator key block;

a third message transmitted from the first payment generator device to the first payment receiver device, the third message including the generator key block encrypted using the device payment receiver public key, wherein the first payment receiver device is configured for using the device payment receiver private key to recover the generator key block, generating a receiver key block, and deriving the shared key block using a combination of the receiver key block and the generator key block;

a fourth message transmitted from the first payment receiver device to the first payment generator device, the fourth message including the receiver key block encrypted using the device payment generator public key, wherein the first payment generator device is configured for using the device payment generator private key to recover the receiver key block, and deriving the shared key block using the combination of the receiver key block and the generator key block; and

a fifth message transmitted from the first payment generator device to the first payment receiver device including the payment data encrypted using the shared key block.

11. A data communications method for secure communication of data packets, the data communications method comprising:

registering one or more payment receiver devices using one or more encryption keys stored on one or more trusted execution element each corresponding to a corresponding one or more payment receiver devices;

upon receiving a data communication packet representing a request for payment, processing the data communication packet and validating a device identity by confirming that the data communication packet corresponds to at least one of the one or more registered payment receiver devices; and

processing a payment transaction based at least on the data communication packet.

12. The data communications method of claim 11, wherein the one or more encryption keys are utilized to attest one or more properties of the one or more trusted execution elements, and the attestation of the one or more properties is conducted both during registration of the one or more payment receiver devices and the validation of the identity of the one or more payment receiver devices.

13. The data communications method of claim 11, wherein the one or more payment receiver devices interoperate with one or more payment generator devices to generate the data communication packet representing the request for payment.
14. The data communications method of claim 13, wherein the one or more payment generator devices and the one or more payment receiver devices are configured for conducting a mutual authentication process to provide secure communications between a first payment generator device and a first payment receiver device.
15. The data communications method of claim 14, wherein both of the first payment generator device and the first payment receiver device are initialized with a certificate authority public key.
16. The data communications method of claim 15, wherein the first payment generator device, after a payment generator device personalization process, stores the certificate authority public key, a issuer payment generator public key certificate, a device payment generator private key, a device payment generator public key, and a device payment generator public key certificate.
17. The data communications method of claim 16, wherein the first payment receiver device, after a payment receiver device personalization process, stores the certificate authority public key, a manager payment receiver public key certificate, a device payment receiver private key, a device payment receiver public key, and a device payment receiver public key certificate.
18. The data communications method of claim 17, wherein the mutual authentication process includes a series of messages transmitted the first payment generator device and the first payment receiver device, the series of messages adapted to generate a shared key block between the first payment generator device and the first payment receiver device, the shared key block used to encrypt payment data for transfer from the payment generator device to the first payment receiver device.
19. The data communications method of claim 18, wherein the series of messages include:
a first message transmitted from the first payment generator device to the first payment receiver device, the first message including the issuer payment generator public key certificate and the device payment generator public key certificate, wherein the first payment receiver device is configured for using the certificate authority public key to verify the issuer payment generator public key certificate, using the issuer payment

generator public key to verify the device payment generator public key certificate, and extracting the device payment generator public key;

a second message transmitted from the first payment receiver device to the first payment generator device, the second message including the manager payment receiver device public certificate, and the device payment receiver public key certificate, wherein the first payment generator device is configured for using the certificate authority public key to verify the manager payment receiver public key certificate and extract the manager payment receiver public key, and using the manager payment receiver public key to verify the device payment receiver public key certificate and extract the device payment receiver public key, and generating a generator key block;

a third message transmitted from the first payment generator device to the first payment receiver device, the third message including the generator key block encrypted using the device payment receiver public key, wherein the first payment receiver device is configured for using the device payment receiver private key to recover the generator key block, generating a receiver key block, and deriving the shared key block using a combination of the receiver key block and the generator key block;

a fourth message transmitted from the first payment receiver device to the first payment generator device, the fourth message including the receiver key block encrypted using the device payment generator public key, wherein the first payment generator device is configured for using the device payment generator private key to recover the receiver key block, and deriving the shared key block using the combination of the receiver key block and the generator key block; and

a fifth message transmitted from the first payment generator device to the first payment receiver device including the payment data encrypted using the shared key block.

20. A non-transitory computer readable medium storing machine interpretable instructions, which when executed by a processor, cause the processor to perform a method for secure communication of data packets, the method comprising:

registering one or more payment receiver devices using one or more encryption keys stored on one or more trusted execution element each corresponding to a corresponding one or more payment receiver devices;

upon receiving a data communication packet representing a request for payment, processing the data communication packet and validating a device identity by confirming that the data communication packet corresponds to at least one of the one or more registered payment receiver devices; and processing a payment transaction based at least on the data communication packet.

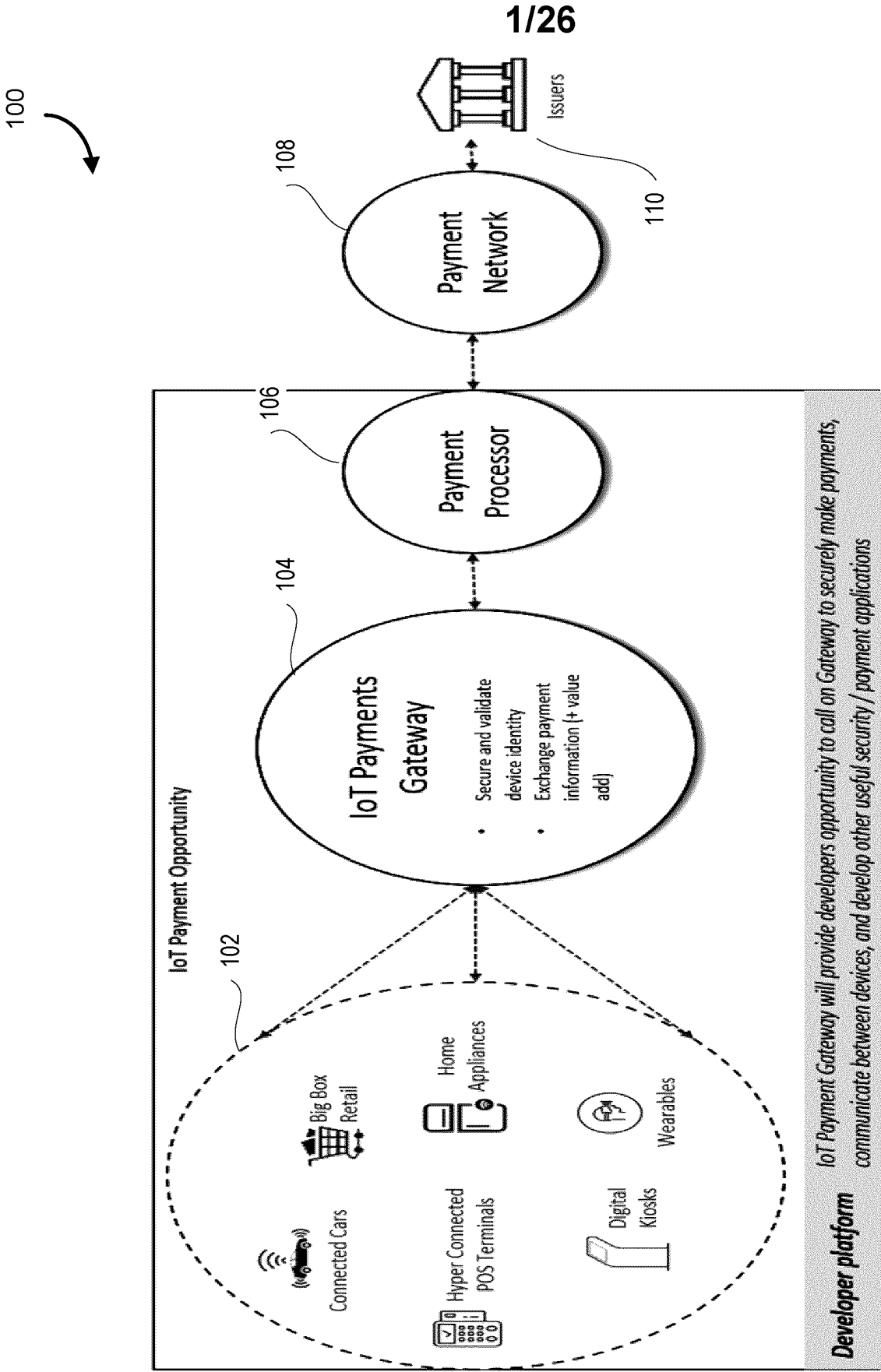


FIG. 1

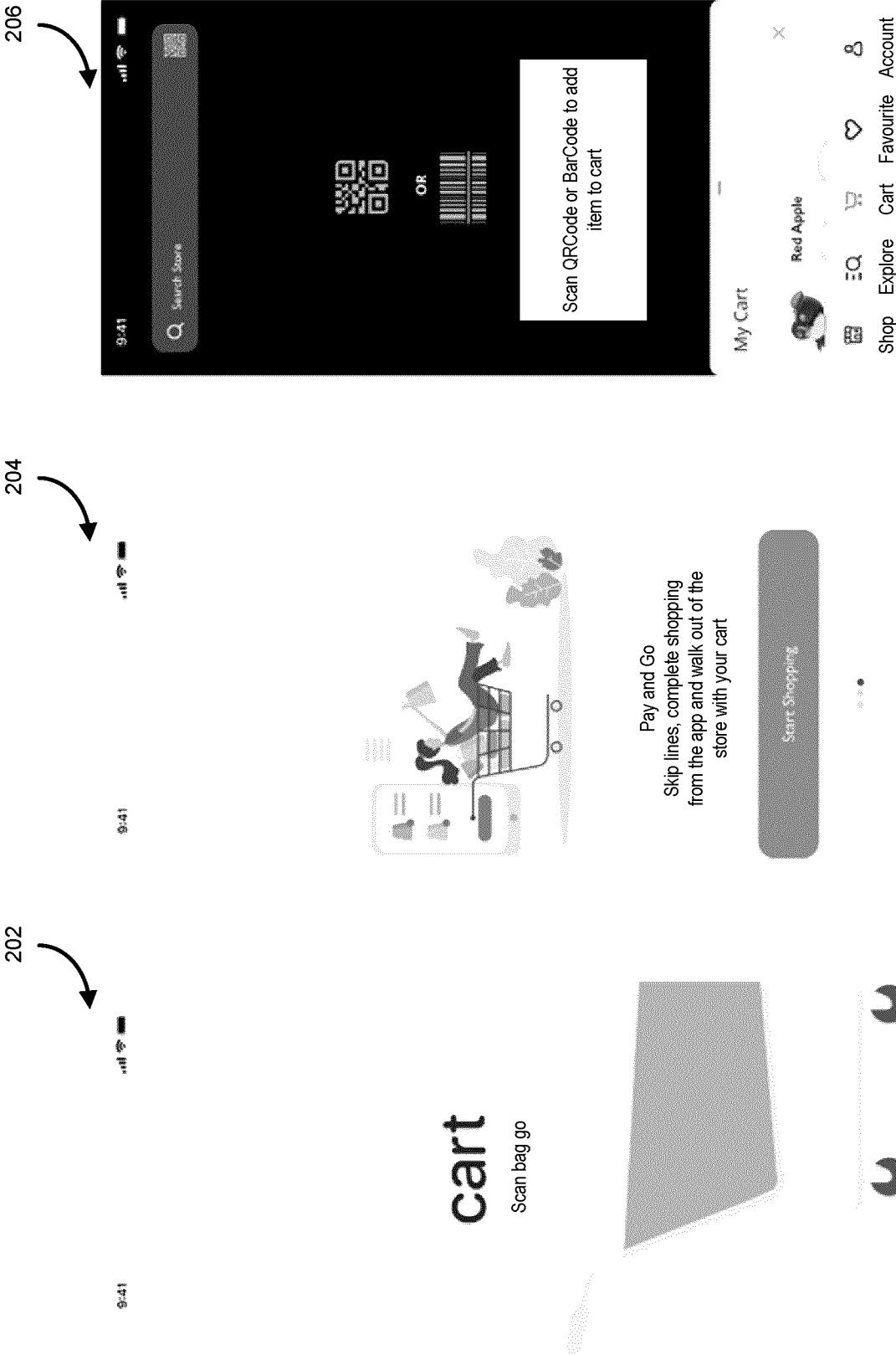


FIG. 2A

FIG. 2B

FIG. 2C

3/26

212

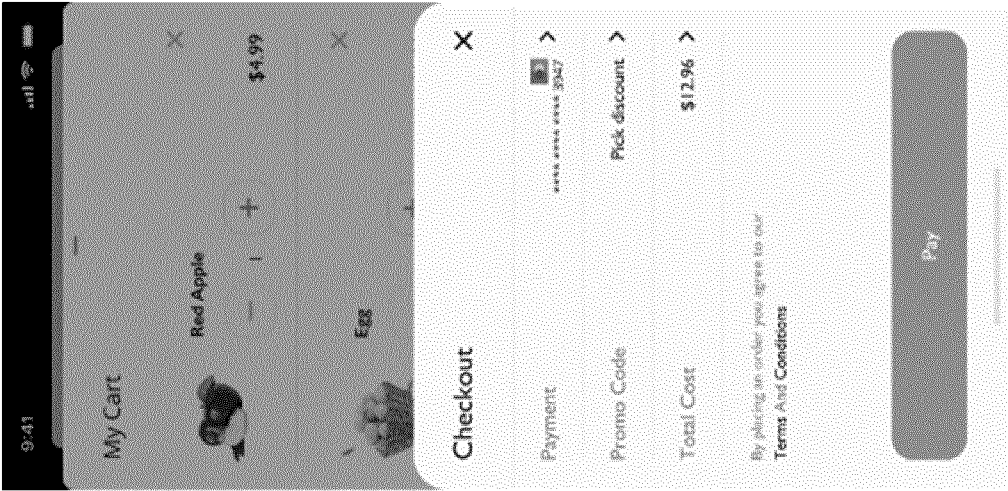


FIG. 2F

210

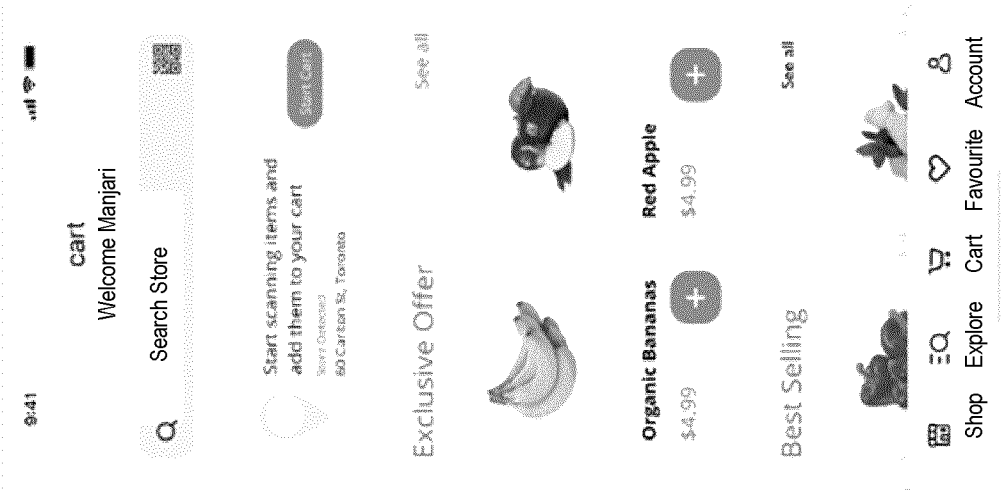


FIG. 2E

208

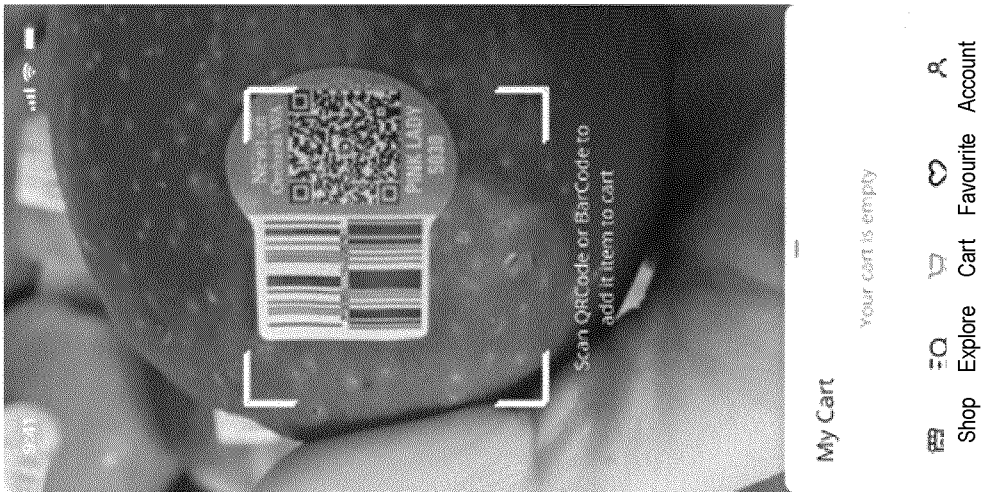


FIG. 2D

4/26

218

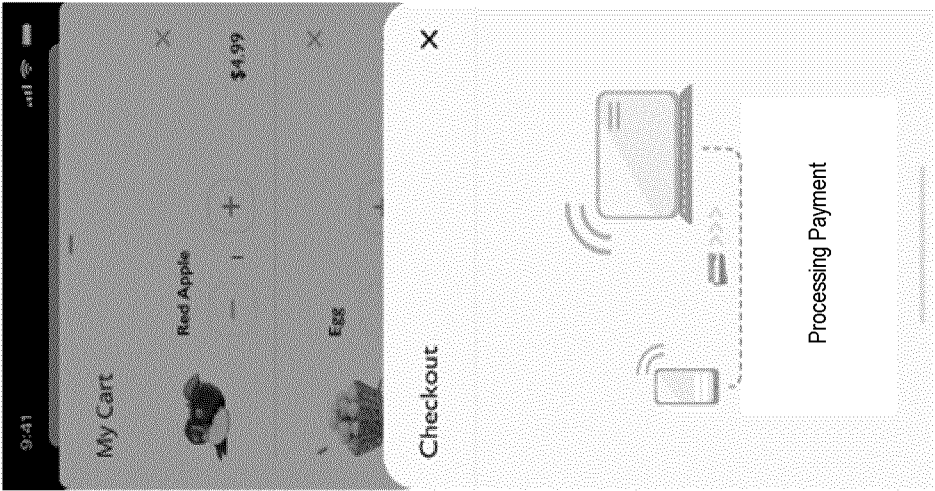


FIG. 2I

216

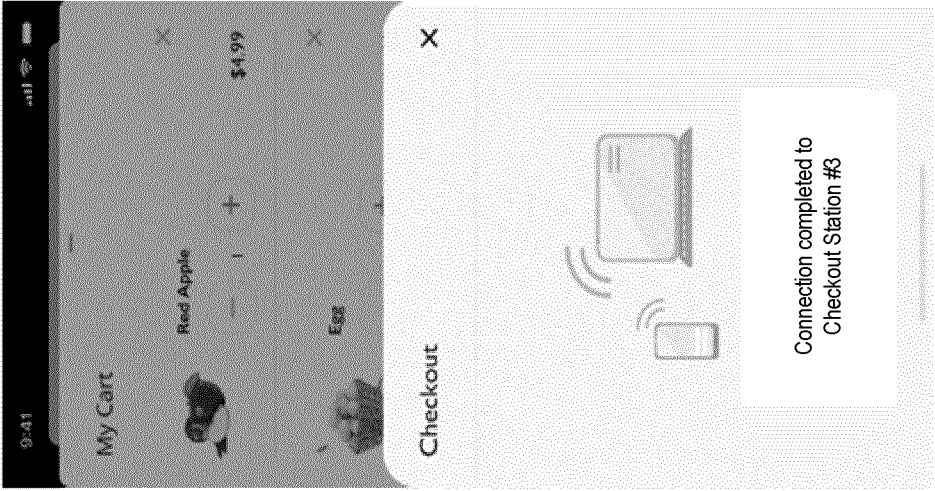


FIG. 2H

214

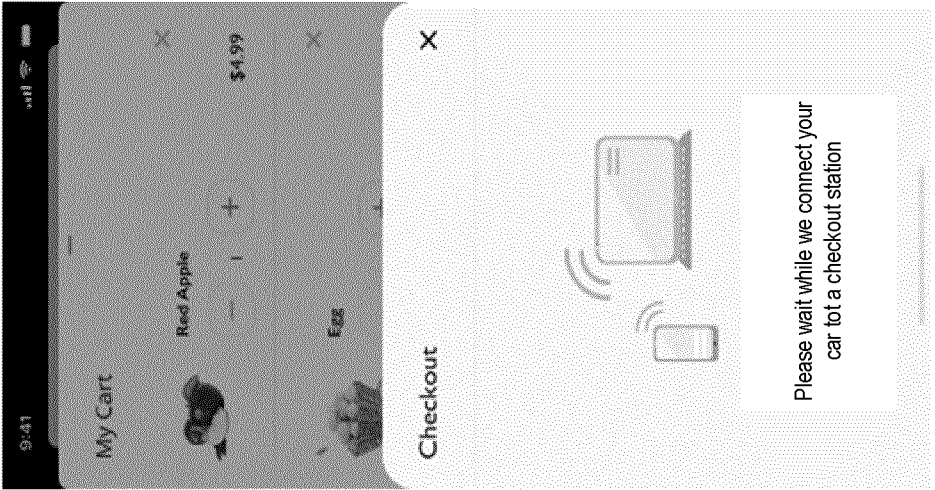


FIG. 2G

5/26



FIG. 2J

6/26

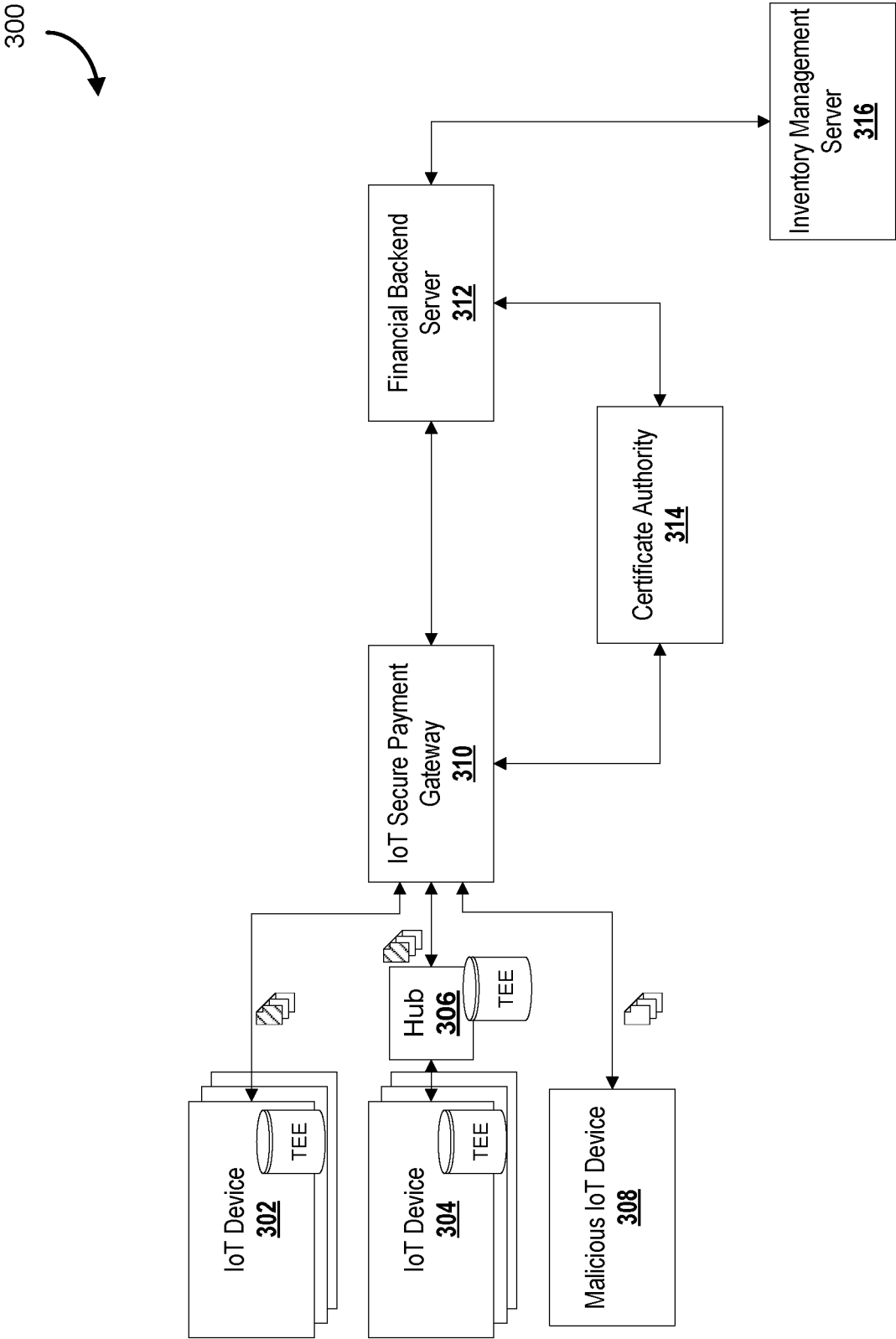


FIG. 3

7/26

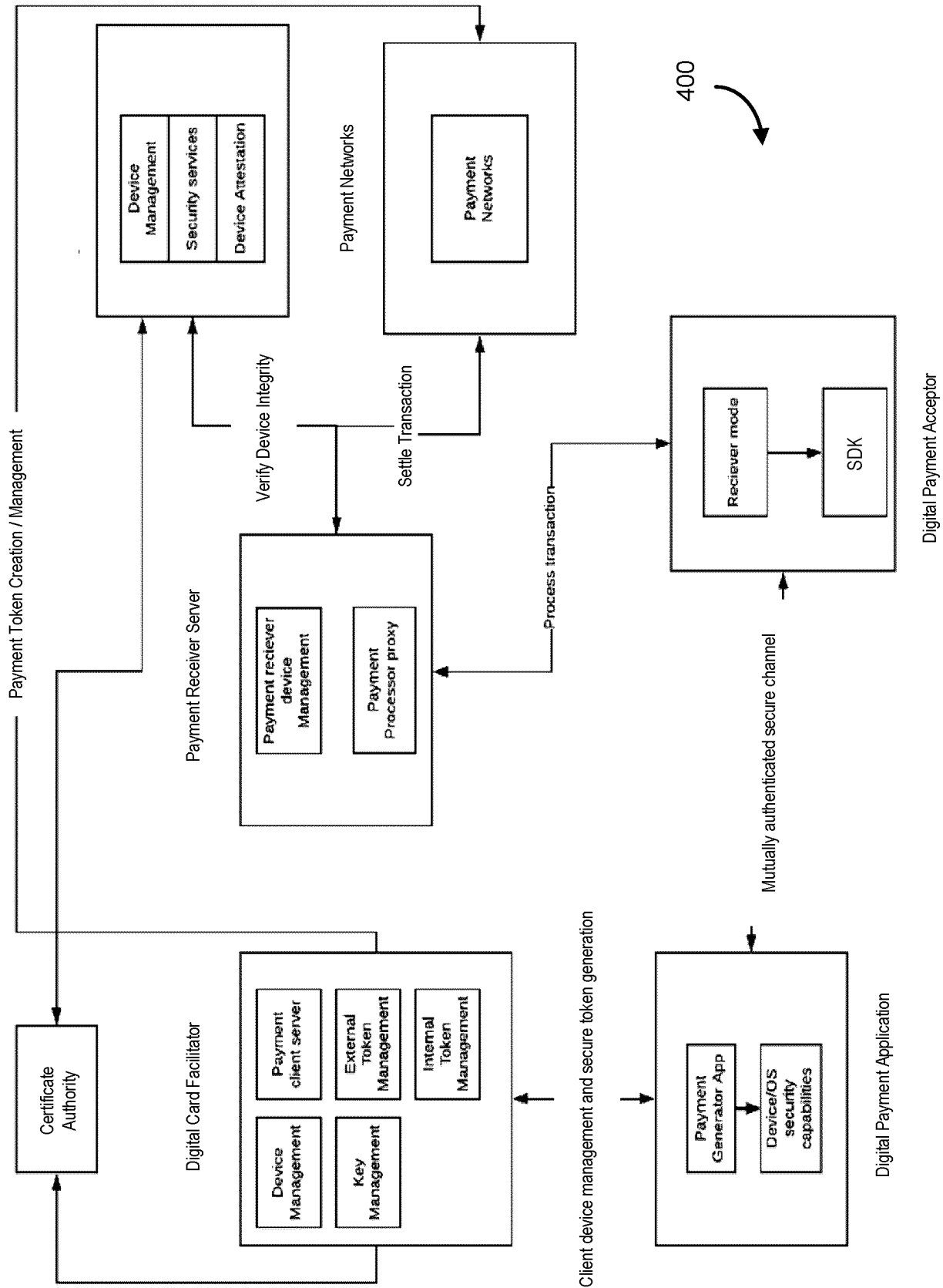


FIG. 4

8/26

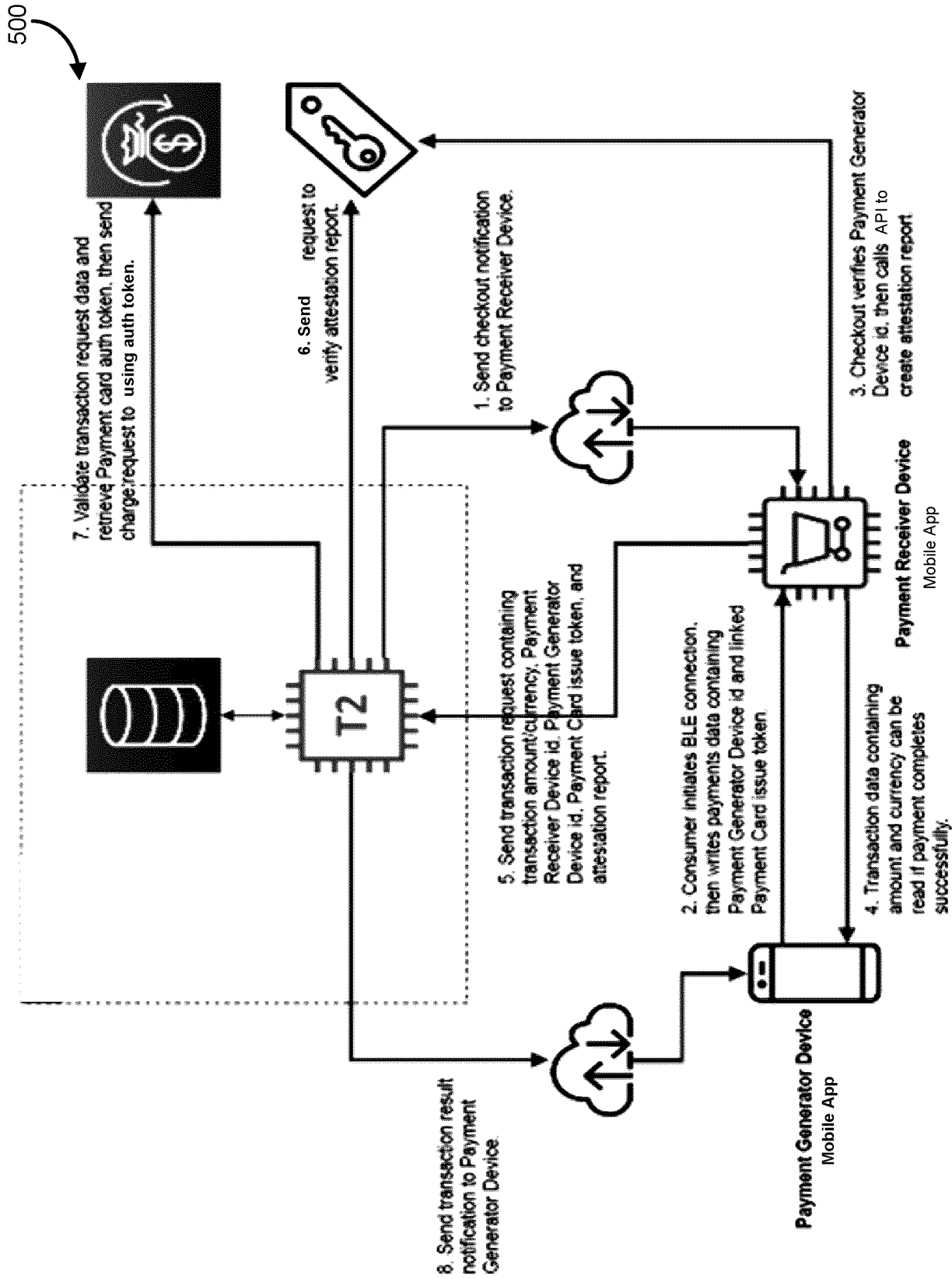


FIG. 5

9/26

600

IoT Payment Gateway & Protocol				
Consumer	Merchant Operator		Financial Institution	Payment Network
Customer Device	PoS Device Security TEEs	IoT Payment Processor, Security PoS Identity	Payment Gateway / Identity Verification	Aggregators, Gift Card Networks
		Certificate Authority		

FIG. 6

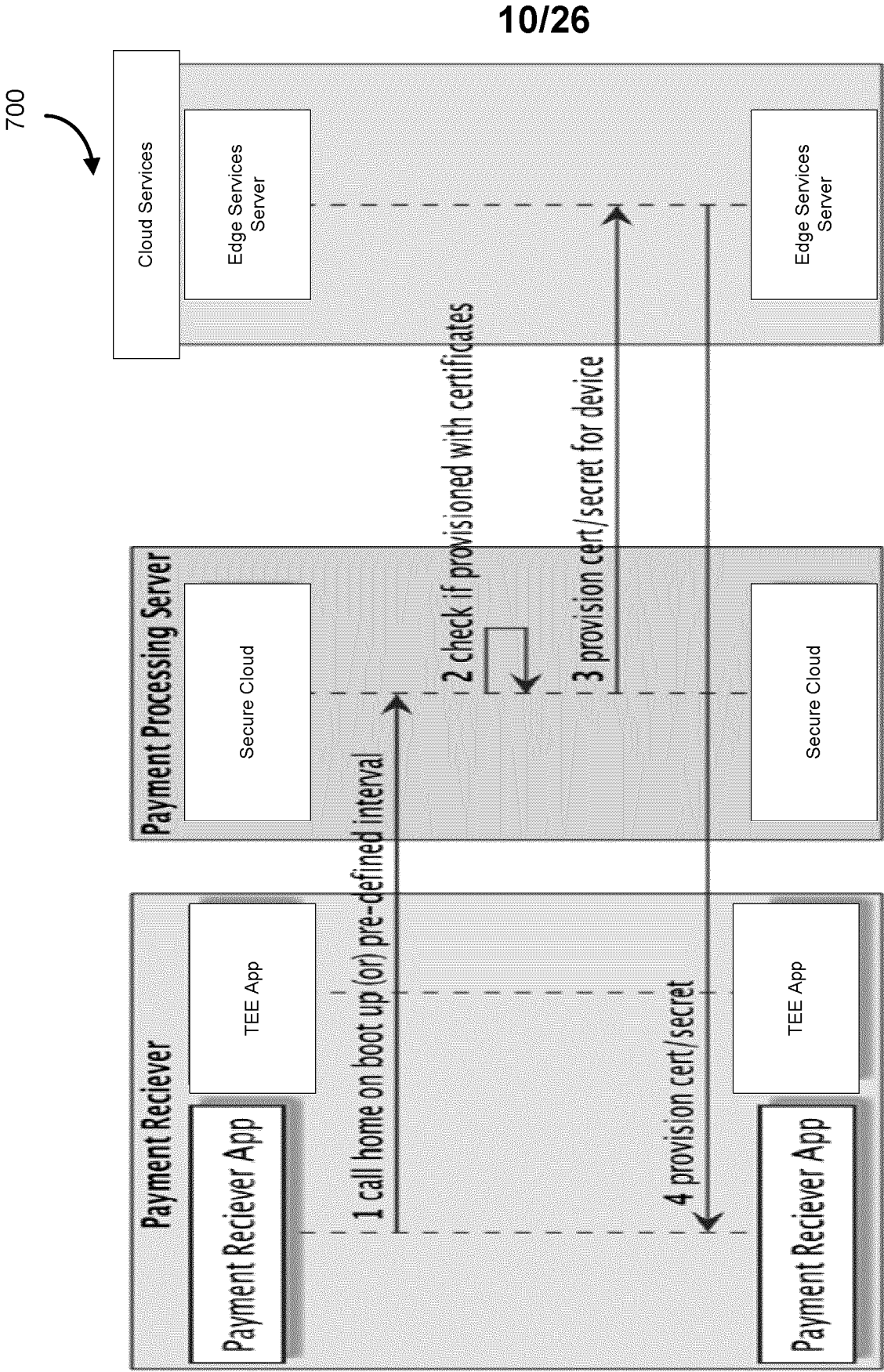


FIG. 7

11/26

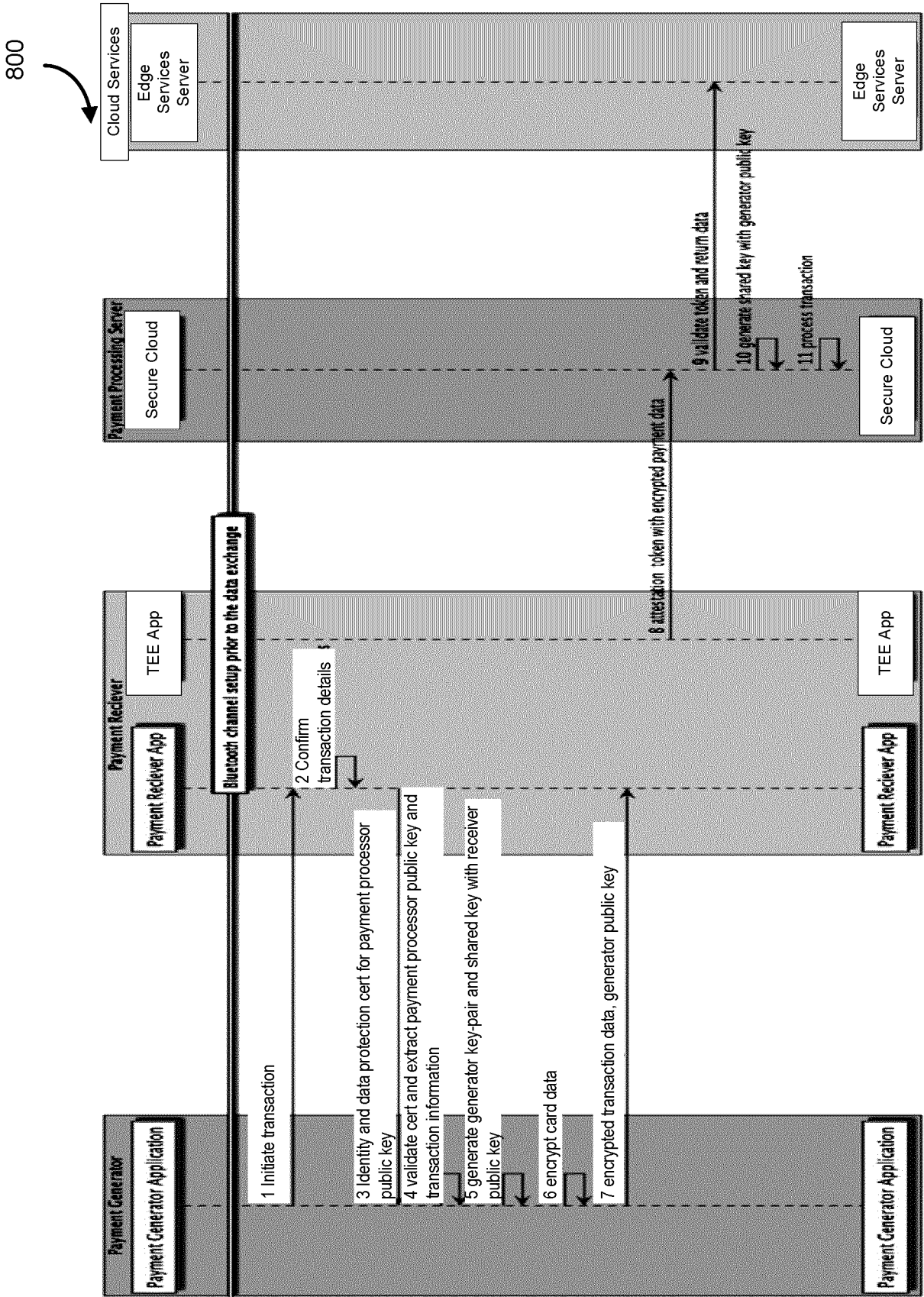


FIG. 8

12/26

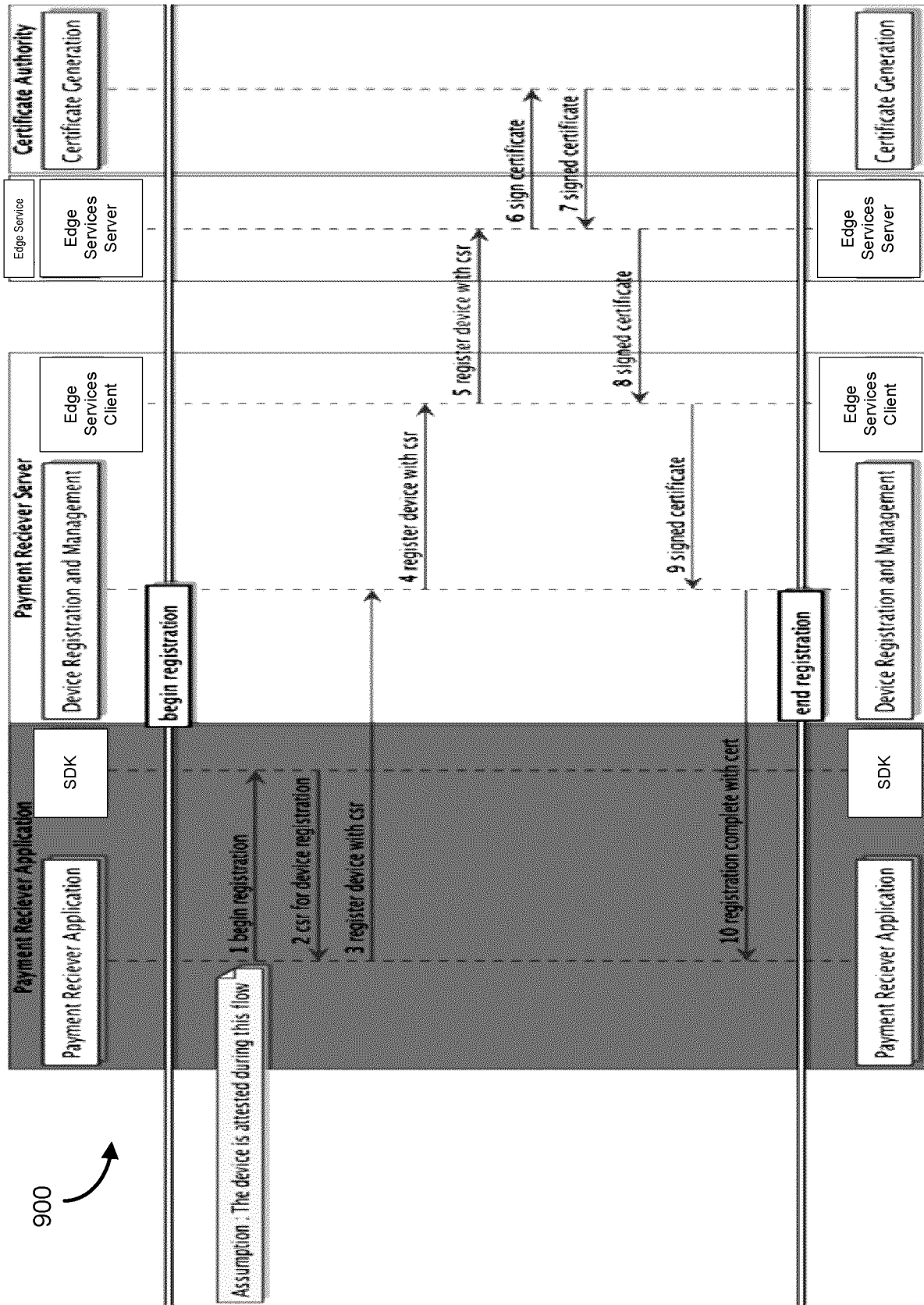


FIG. 9

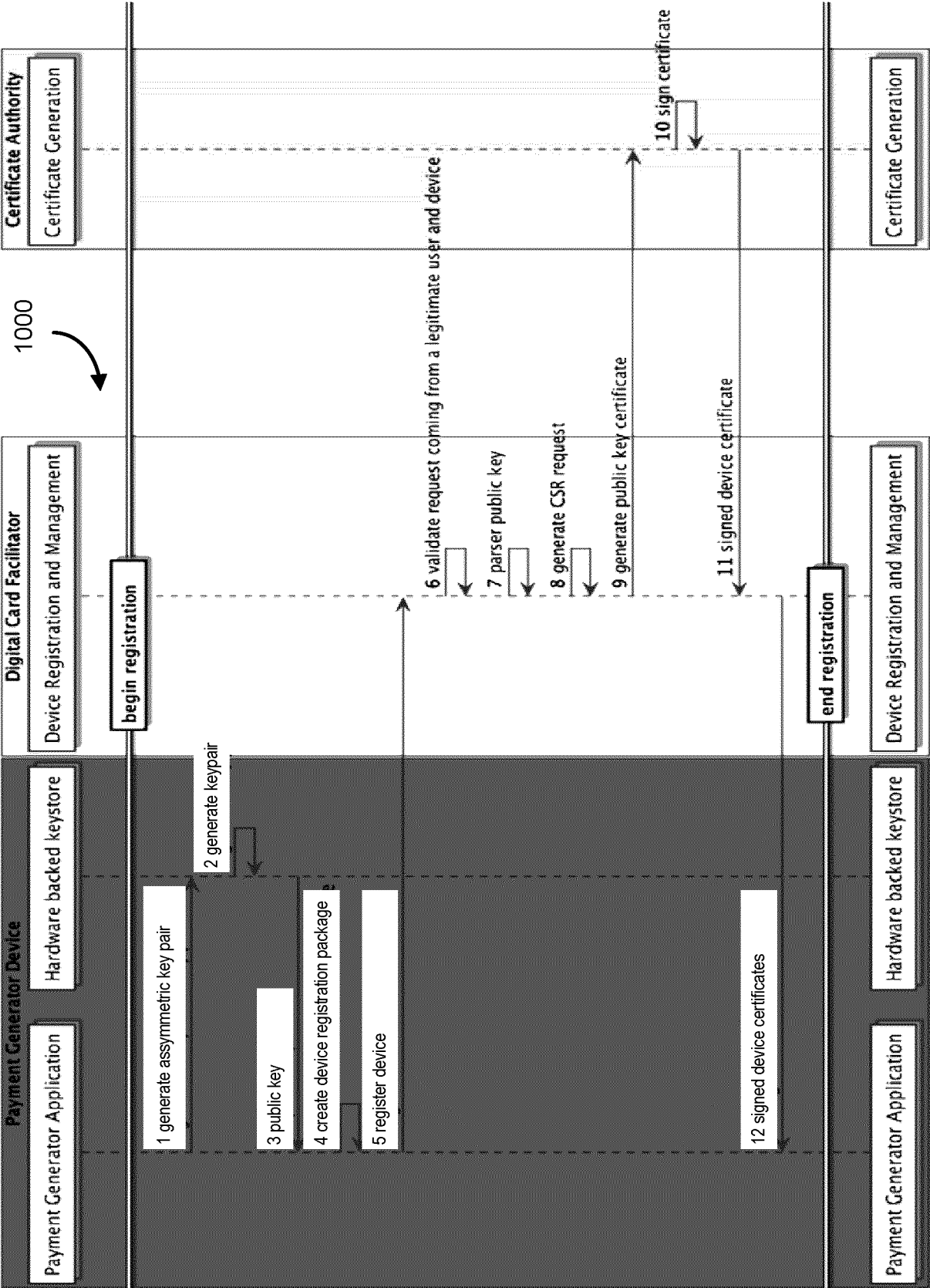


FIG. 10

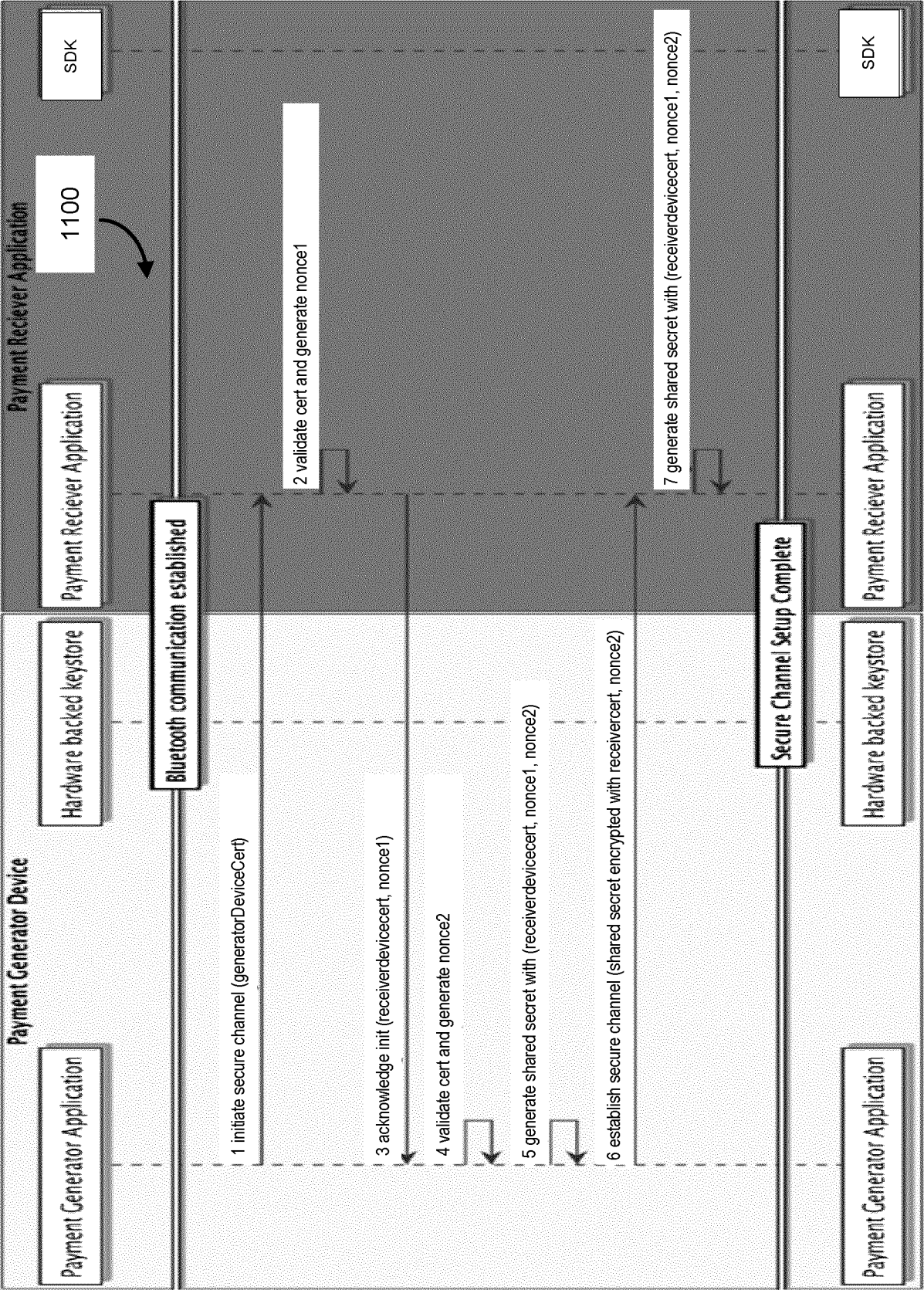


FIG. 11

PKI Initialization

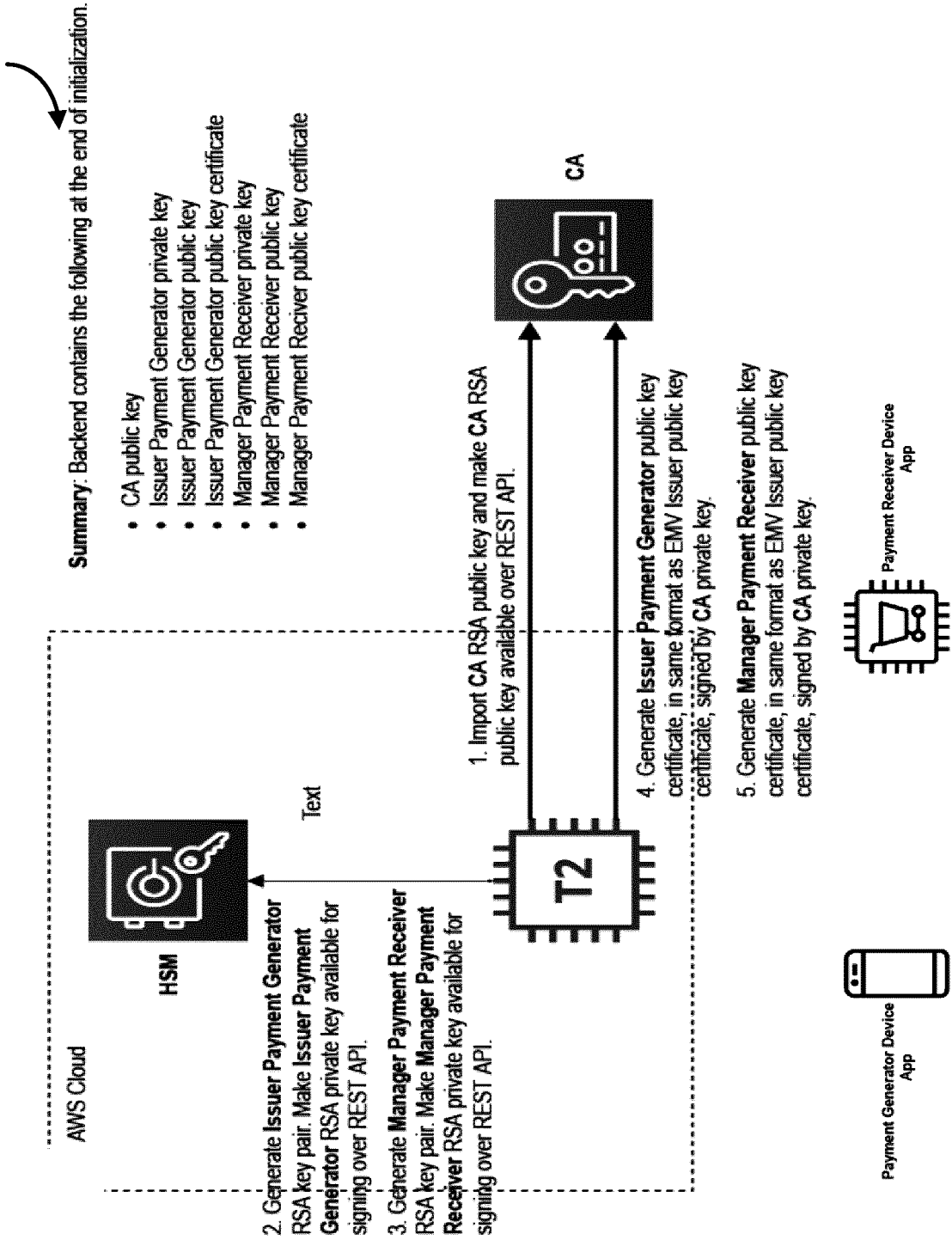
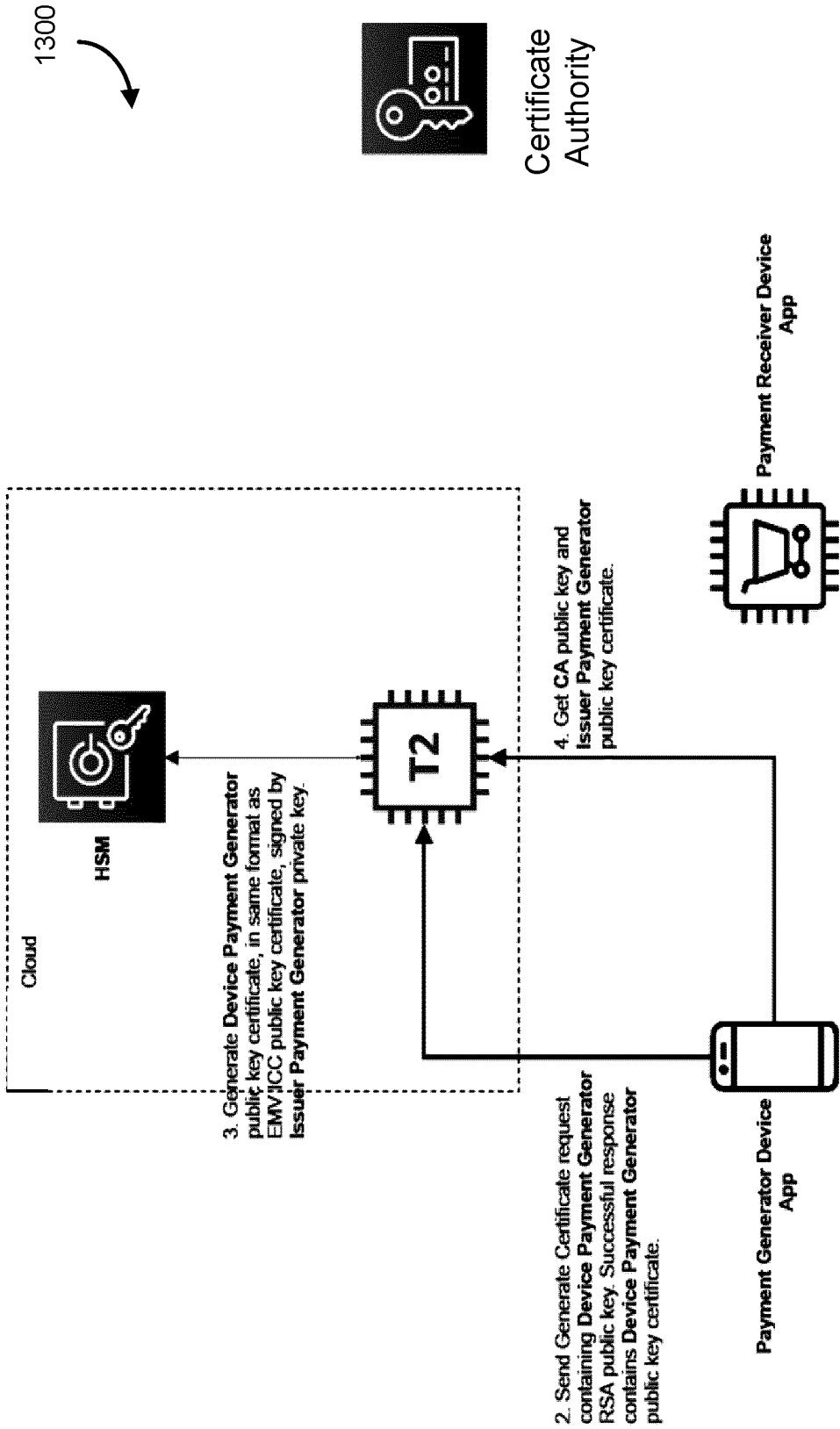


FIG. 12

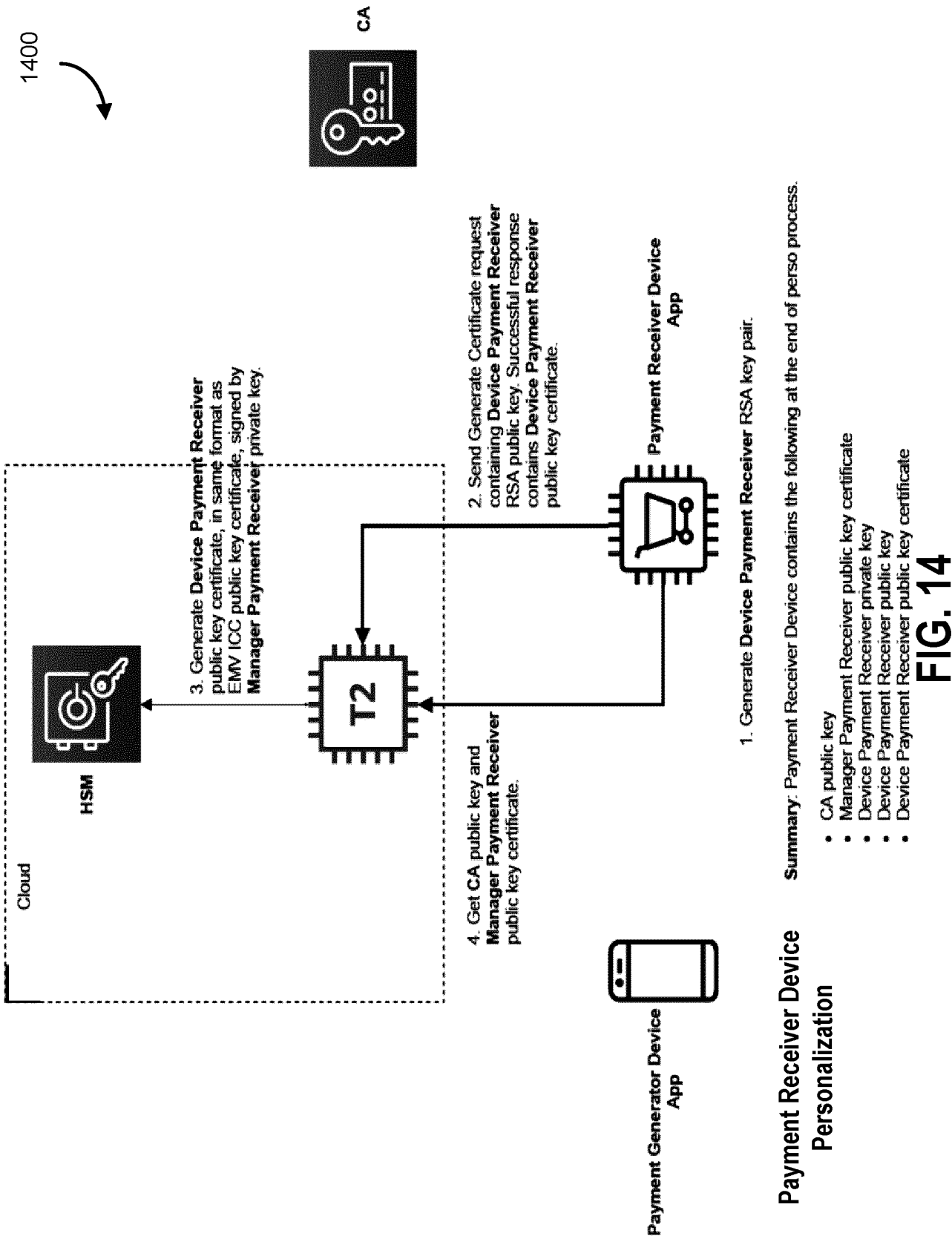


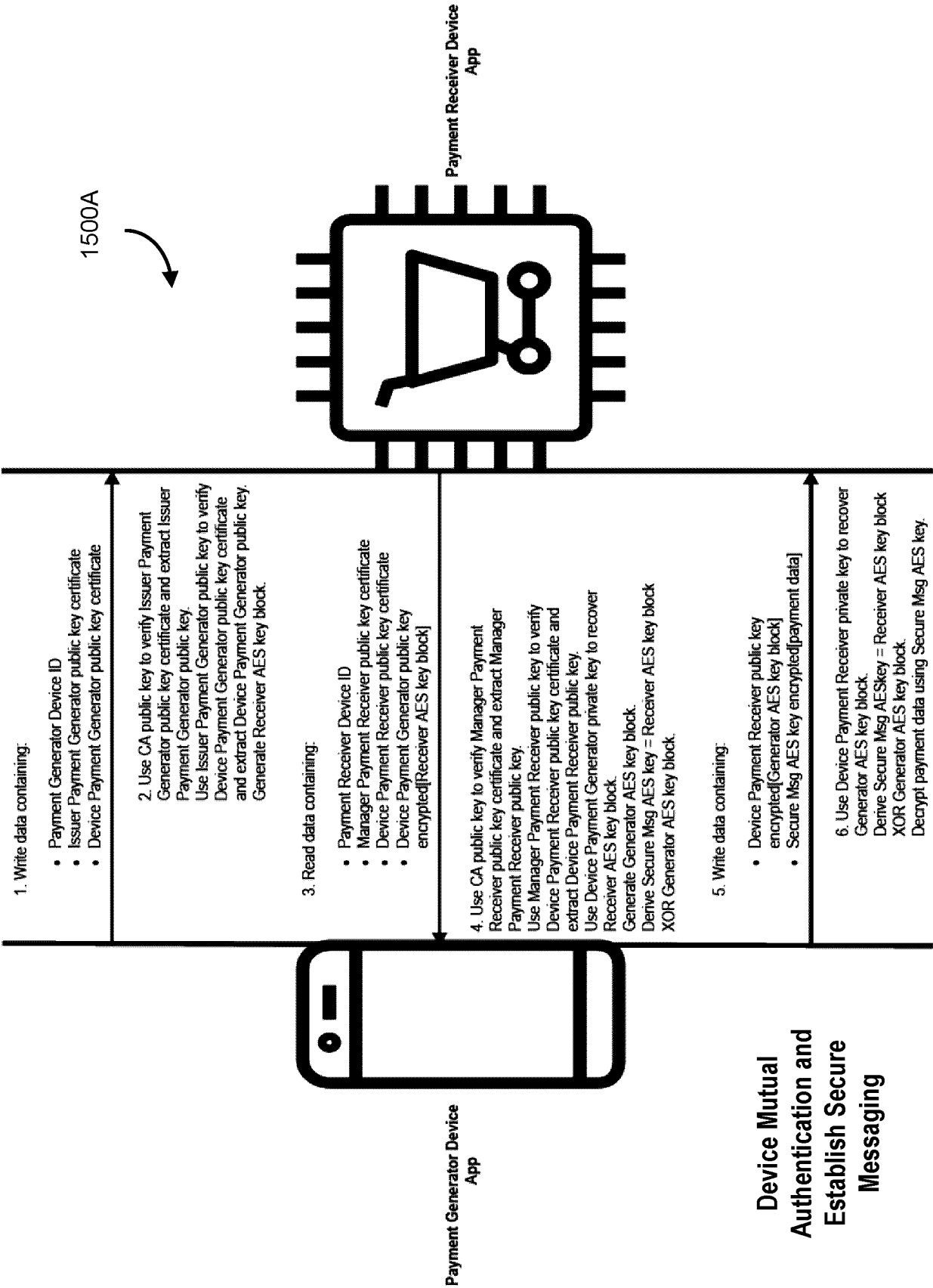
Payment Generator Device Personalization

Summary: Payment Generator Device contains the following at the end of perso process.

- CA public key
- Issuer Payment Generator public key certificate
- Device Payment Generator private key
- Device Payment Generator public key
- Device Payment Generator public key certificate

FIG. 13





19/26

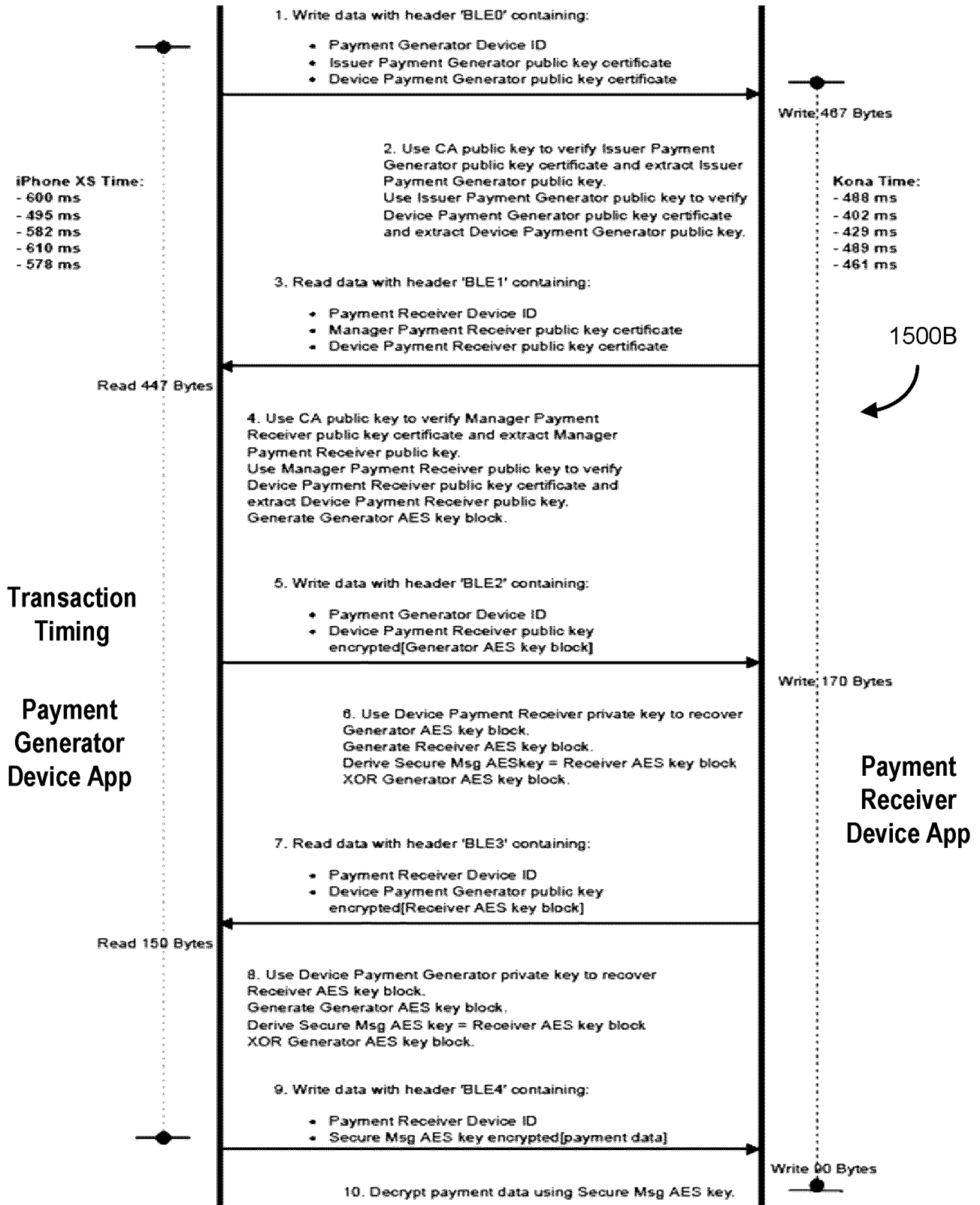


FIG. 15B

20/26

Jill Anderson – The Health Conscious Shopper



"I'm looking for safer ways to shop and get better discounts from the big retailers I usually shop with."

AGE: 35
WORK: Regional Director
FAMILY: Married, 1 Child
LOCATION: Toronto, Canada
ARCHETYPE: The Conscious Shopper

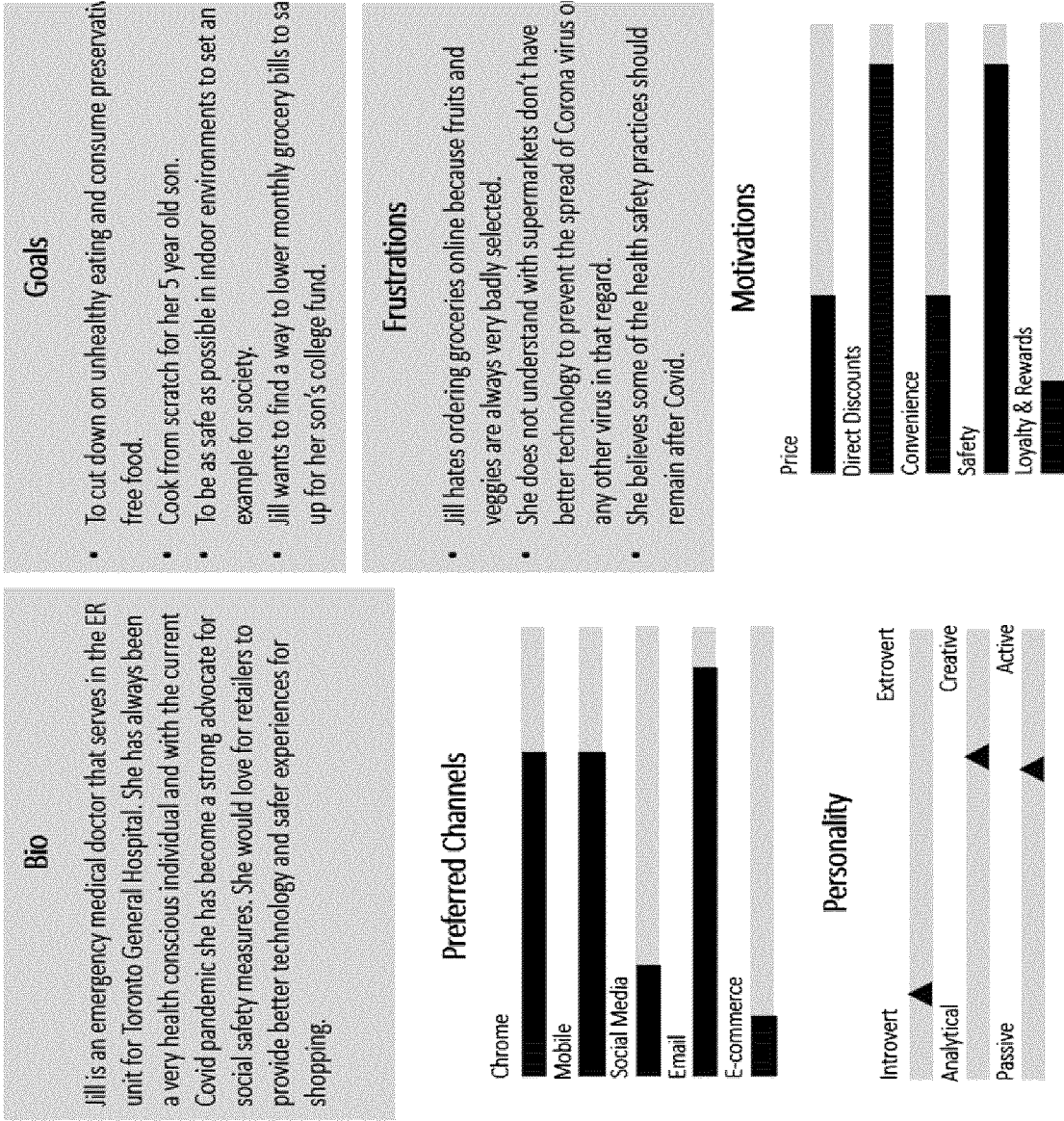


FIG. 16

21/26

IoT Payment Async Flow

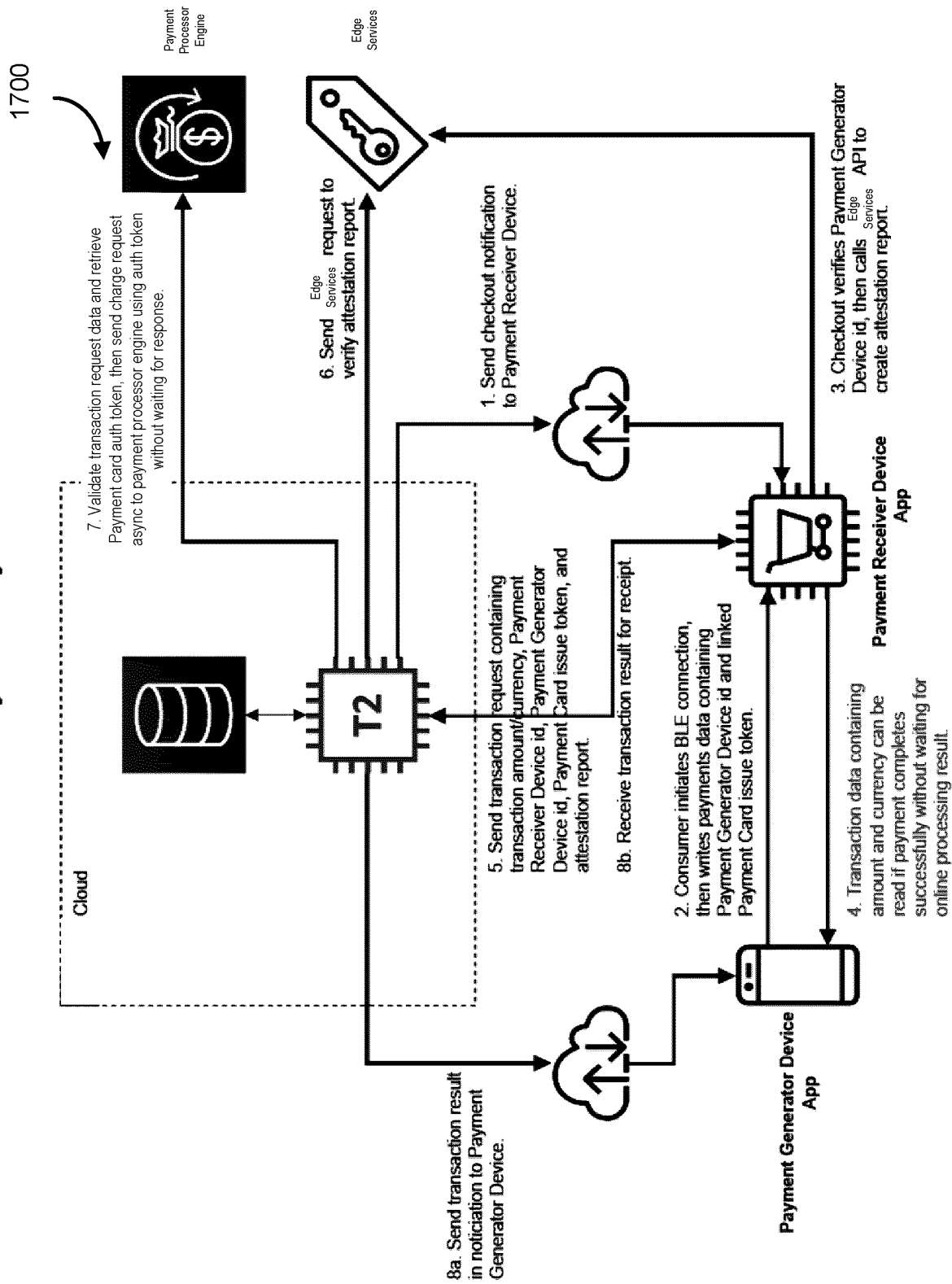


FIG. 17

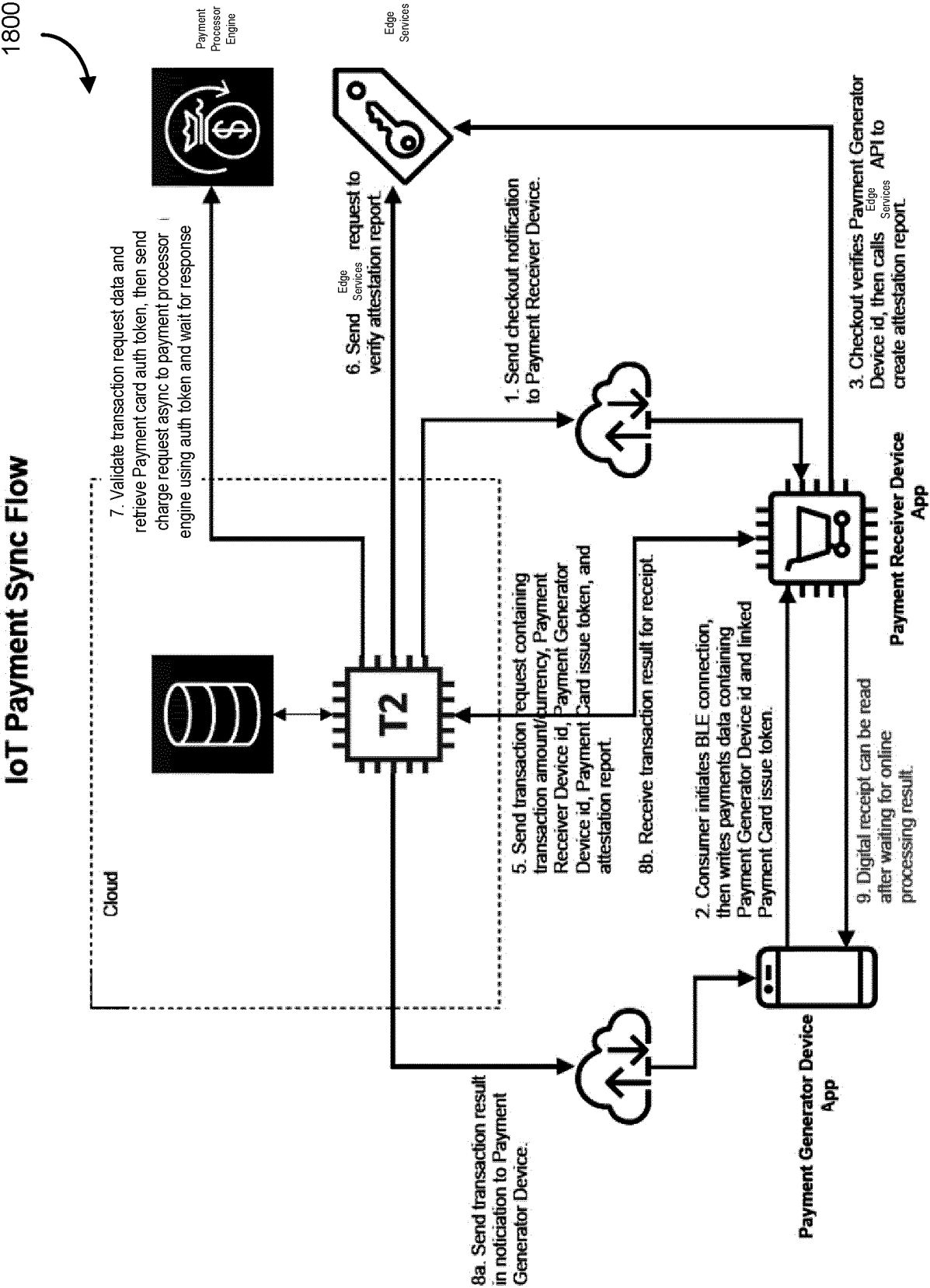


FIG. 18

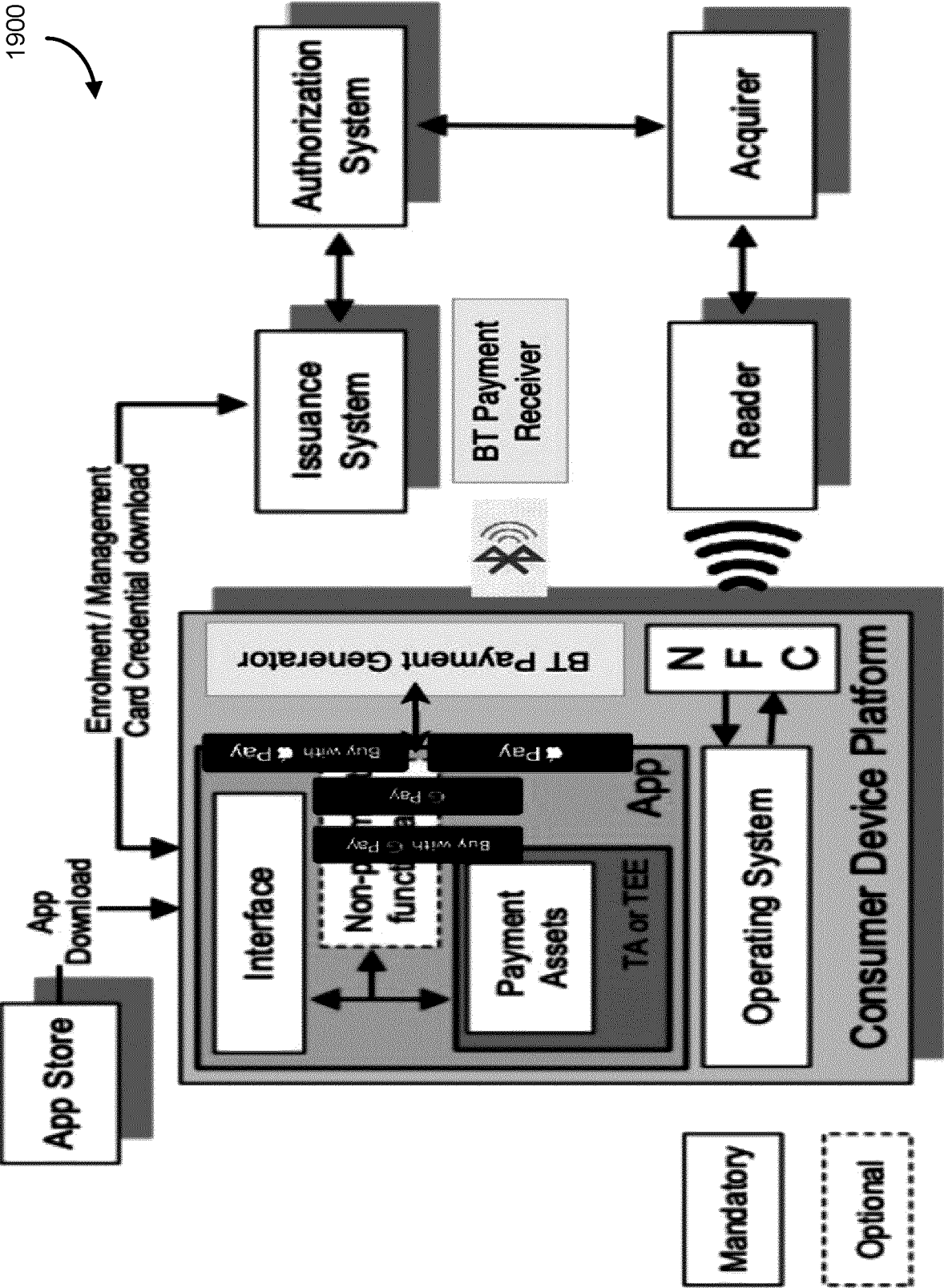


FIG. 19

24/26

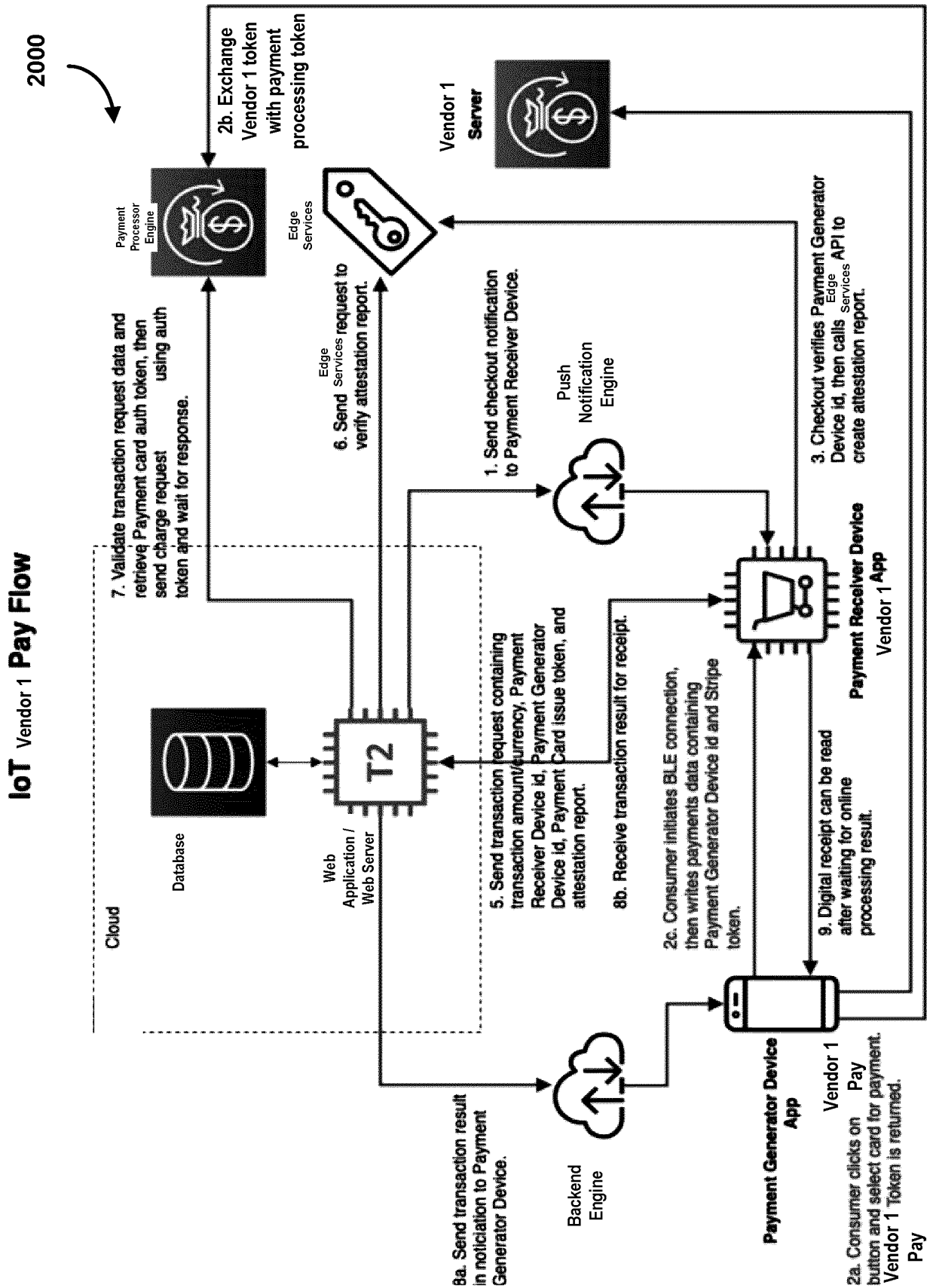


FIG. 20

25/26

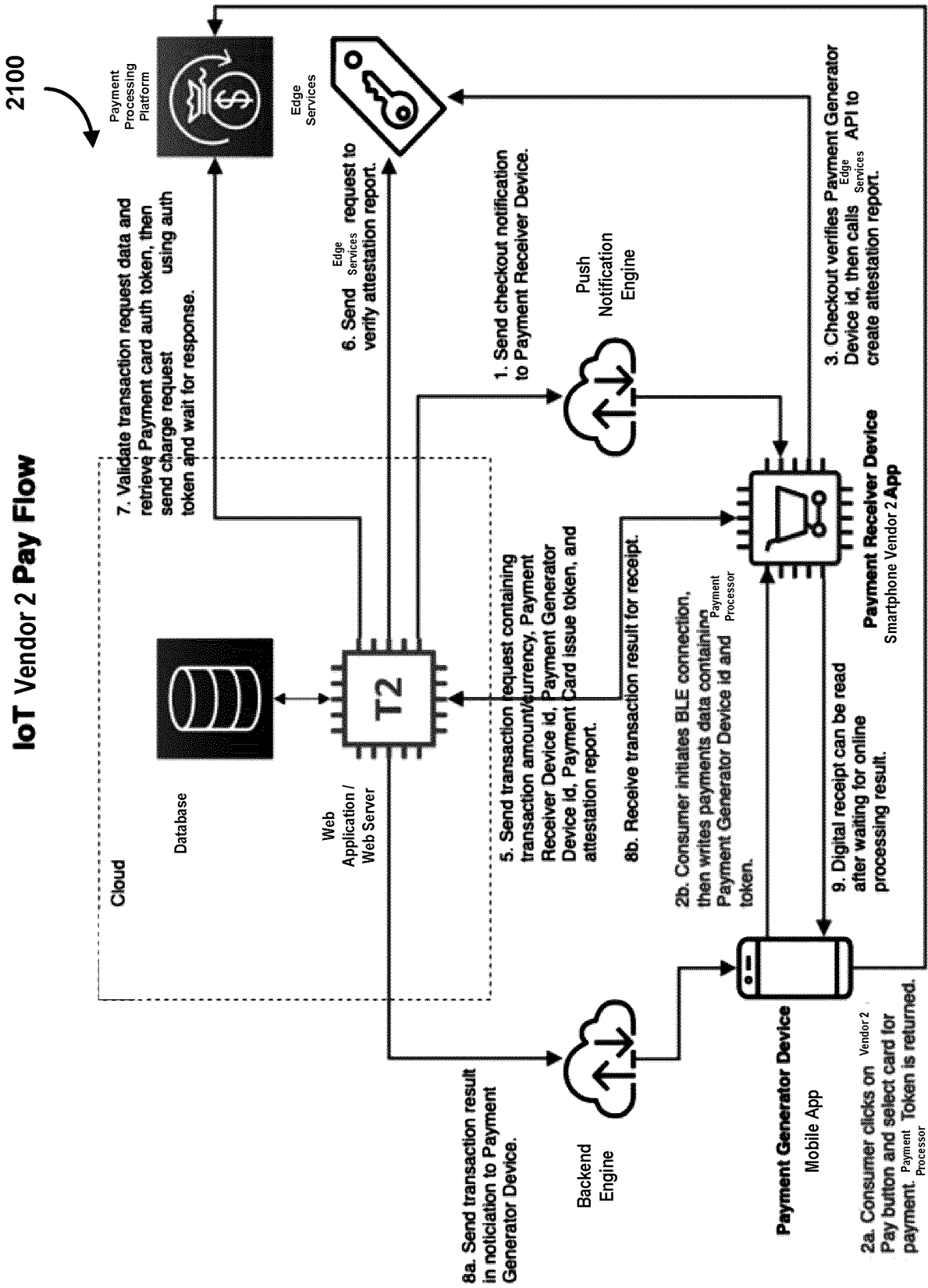


FIG. 21

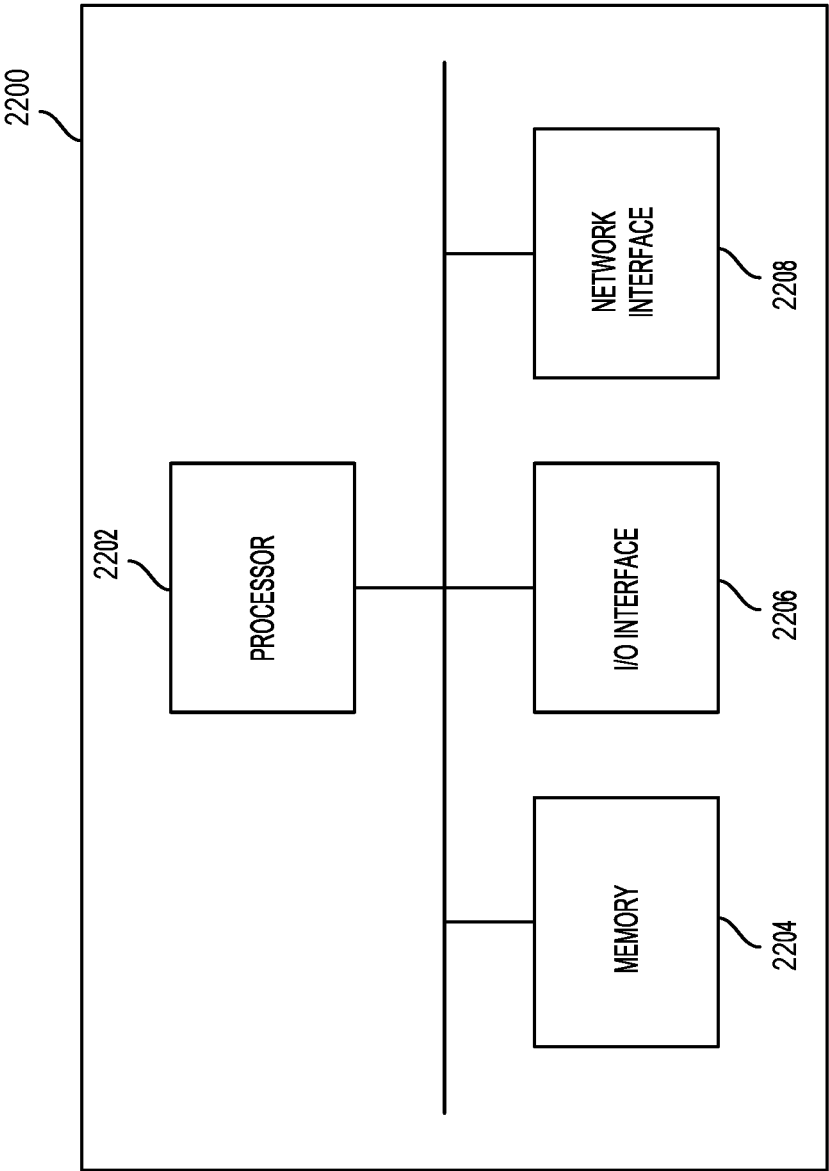


FIG. 22

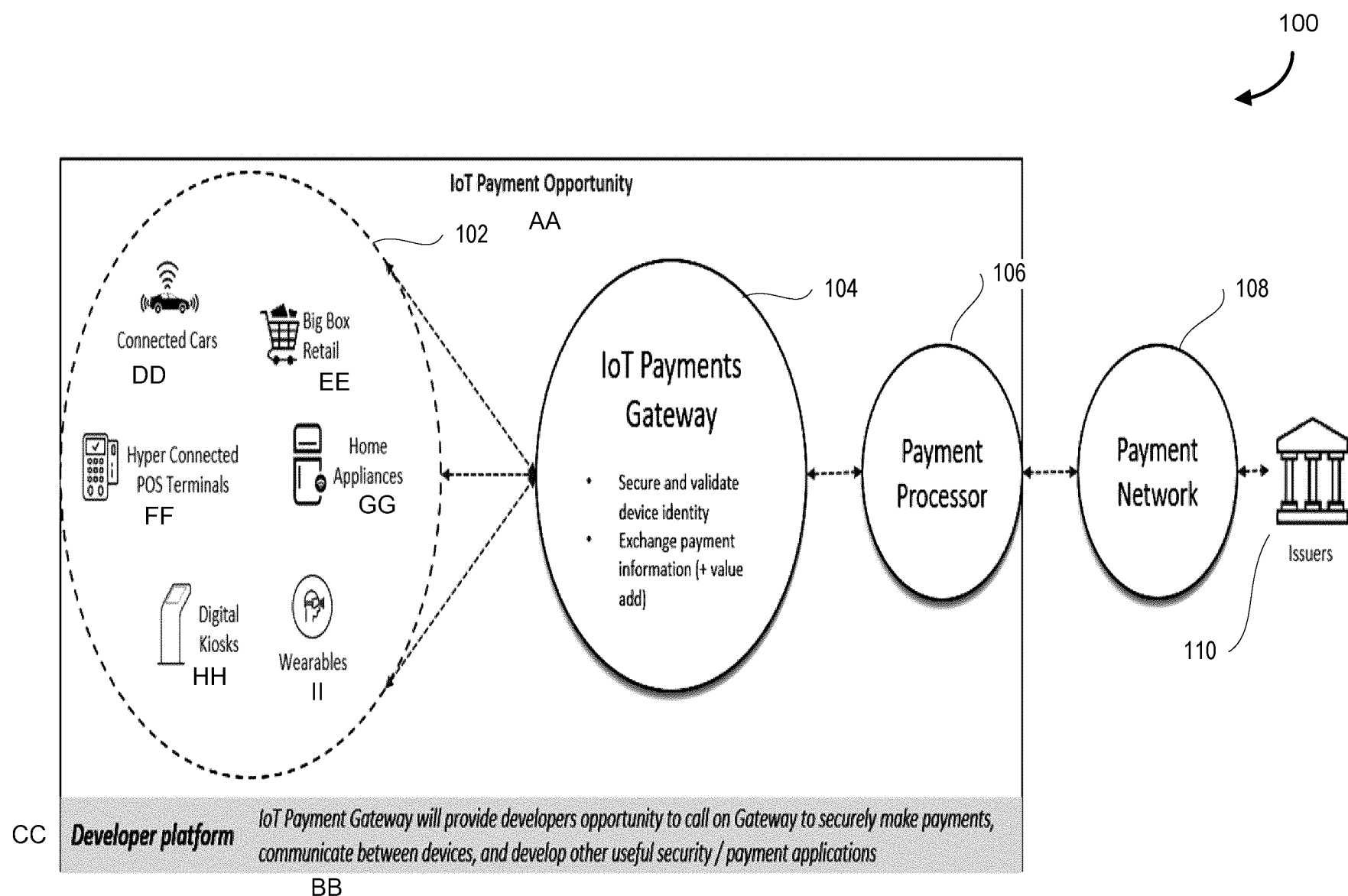


FIG. 1

- AA Opportunité de paiement IdO
- BB Le portail de paiement IdO fournira aux développeurs l'opportunité de faire appel au portail pour réaliser de manière sécurisée des paiements, pour communiquer entre des dispositifs et développer d'autres applications de paiement/de sécurité utiles
- CC Plateforme de développement
- DD Voitures connectées
- EE Grande boîte de vente
- FF Terminaux par point de vente hyper connectés
- GG Appareils électroménagers
- HH Kiosques numériques
- II Pouvant être portés
- 104 Portails de paiement IdO
Sécuriser et valider l'identité du dispositif
Échanger les informations de paiement (+ ajout de valeur)
- 106 Processeur de paiement
- 108 Réseau de paiement
- 110 Émetteurs