



- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *H04L 67/289* (2022.01)
- (21) **International Application Number:**
PCT/US2023/069103
- (22) **International Filing Date:**
26 June 2023 (26.06.2023)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).
- (72) **Inventors:** CHEN, Yuexi; P.O. Box 8999, San Francisco, California 94128 (US). WANG, Quan; P.O. Box 8999, San Francisco, California 94128 (US).
- (74) **Agent:** JEWIK, Patrick et al.; 1100 Peachtree Street, NE Suite 2800, Atlanta, Georgia 30309 (US).
- (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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, 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,

(54) **Title:** TOKEN DATA DELIVERY TO EDGE COMPUTER

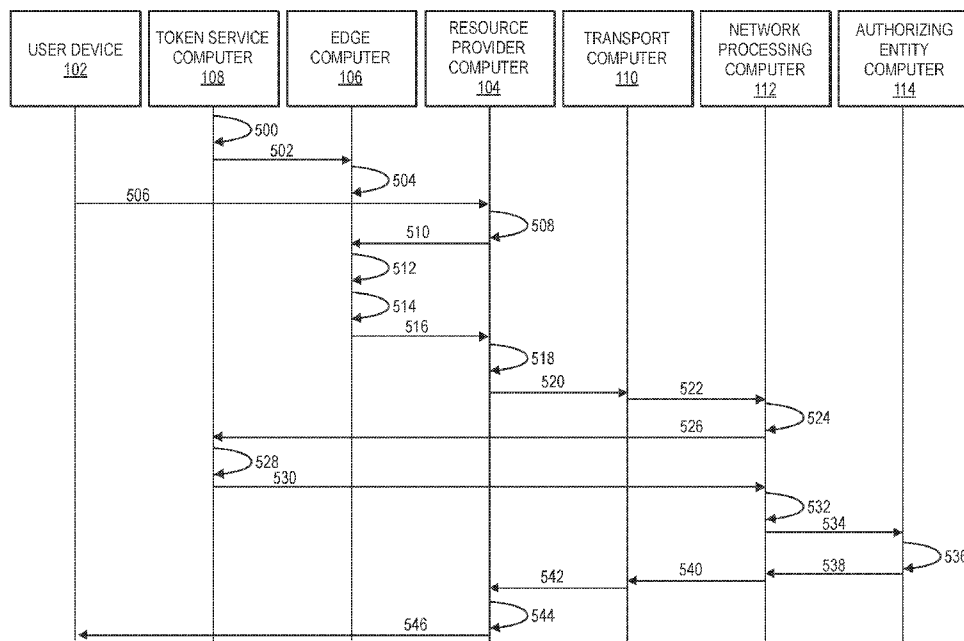


FIG. 5

(57) **Abstract:** A method includes an edge computer in a first region receiving a subset of token data corresponding to a subset of credentials from a token service computer in a second region. The first region and the second region are remotely located with respect to each other. The token service computer stores a set of token data where the subset of token data are selected from the set of token data based on data associated with users of credentials of the subset of credentials. The edge computer receives a token request message comprising a credential from a token requestor. The edge computer transmits a token response message comprising token data to the token requestor. The token requestor then uses the token data to perform an interaction for a user associated with the credential.

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).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

- *with international search report (Art. 21(3))*

TOKEN DATA DELIVERY TO EDGE COMPUTER

BACKGROUND

[0001] Cloud based tokens and token cryptograms are used in remote interactions by token requestors (e.g., merchants). To perform and complete an interaction, a token requestor requests a token and/or a token cryptogram from a token vault for the user involved in the interaction. Due to various technical requirements and regulation requirements (e.g., domestic data processing), the token and token cryptogram are generated in a home country or region of the user involved in the interaction. Further, due to technical complexity the token and token cryptogram can only be generated in a few data centers and server nodes.

[0002] However, some token requestors (e.g., e-commerce merchants) can operate internationally, where the token requestor requests tokens and token cryptograms for user devices issued in different countries.

[0003] Due to the limitations above, the token cryptogram request leads to higher latency and thus delays in the interaction process. For example, a global ecommerce merchant and token requestor can be US based, where its token requestor server is US based, and the endpoint of the token API call to the network is US based. For an interaction made by a US issued user device, the token cryptogram is generated in the US, thus the latency is minimal. However, for an interaction made by an EU (European Union) issued user device, the token cryptogram is generated in EU, where the latency is high, which degrades the interaction user experience and may cause the interaction to time out (e.g., terminate). As such, in this example, an interaction made by an EU user has two high latency calls. However, there is no existing solution to optimize this latency, since, unlike solutions used for web page and web media, token cryptograms are dynamic, require a key to generate, and the key is highly sensitive and has to be used in a particular region.

[0004] Embodiments of the disclosure address this problem and other problems individually and collectively.

SUMMARY

[0005] One embodiment is related to a method comprising: receiving, by an edge computer in a first region, a subset of token data corresponding to a subset of credentials from a token service computer in a second region, the first region and the second region being remotely located with respect to each other, wherein the token service computer stores a set of token data, the subset of token data being selected from the set of token data based on data associated with users of credentials of the subset of credentials; receiving, by the edge computer, a token request message comprising a credential from a token requestor; and transmitting, by the edge computer, a token response message comprising token data to the token requestor, wherein the token requestor uses the token data to perform an interaction for a user associated with the credential.

[0006] Another embodiment is related to an edge computer comprising: a processor; and a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising: receiving, by the edge computer in a first region, a subset of token data corresponding to a subset of credentials from a token service computer in a second region, the first region and the second region being remotely located with respect to each other, wherein the token service computer stores a set of token data, the subset of token data being selected from the set of token data based on data associated with users of credentials of the subset of credentials; receiving, by the edge computer, a token request message comprising a credential from a token requestor; and transmitting, by the edge computer, a token response message comprising token data to the token requestor, wherein the token requestor uses the token data to perform an interaction for a user associated with the credential.

[0007] Another embodiment is related to a system comprising: one or more token requestor computers; a token service computer; and an edge computer comprising: a processor; and a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising: receiving, by the edge computer in a first region, a subset of token data corresponding to a subset of credentials from a

token service computer in a second region, the first region and the second region being remotely located with respect to each other, wherein the token service computer stores a set of token data, the subset of token data being selected from the set of token data based on data associated with users of credentials of the subset of
5 credentials; receiving, by the edge computer, a token request message comprising a credential from a token requestor; and transmitting, by the edge computer, a token response message comprising token data to the token requestor, wherein the token requestor uses the token data to perform an interaction for a user associated with the credential.

10 **[0008]** Further details regarding embodiments of the disclosure can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 shows a block diagram of a token cryptogram delivery network system according to embodiments.

15 **[0010]** FIG. 2 shows a block diagram of components of an edge computer according to embodiments.

[0011] FIG. 3 shows a block diagram of components of a token service computer according to embodiments.

20 **[0012]** FIG. 4 shows a block diagram of two regions in a token cryptogram delivery network according to embodiments.

[0013] FIG. 5 shows a flow diagram illustrating a first token delivery method according to embodiments.

25 **[0014]** FIG. 6 shows a flow diagram illustrating delays that can occur when communications occur between token requestors and token service computers that are located in different regions, which may be geographically separated from each other by a large distance.

DETAILED DESCRIPTION

[0015] Prior to discussing embodiments of the disclosure, some terms can be described in further detail.

[0016] A “user device” may be a device that is operated by a user. Examples of user devices may include a mobile phone, a smart phone, a card, a personal digital assistant (PDA), a laptop computer, a desktop computer, a server computer, a vehicle such as an automobile, a thin-client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user input. The user device may also include one or more input sensors for receiving user input. There are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The user device may comprise any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network.

[0017] A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments. In some embodiments, a resource provider can be a user and may operate a user device.

[0018] An “interaction” may include a reciprocal action or influence. An interaction can include a communication, contact, or exchange between parties, devices, and/or entities. Example interactions include a transaction between two parties and a data exchange between two devices. In other embodiments, an interaction can include a payment transaction in which two devices can interact to facilitate a payment.

[0019] “Interaction data” can include data related to and/or recorded during an interaction. In some embodiments, interaction data can be transaction data of the network data. Transaction data can comprise a plurality of data elements with data values.

5 **[0020]** “Credentials” may comprise any evidence of authority, rights, or entitlement to privileges. For example, access credentials may comprise permissions to access certain tangible or intangible assets, such as a building or a file. Examples of credentials may include passwords, passcodes, or secret messages. In another example, payment credentials may include any suitable information associated with
10 and/or identifying an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include an “account identifier” such as a PAN (primary account number or “account number”), a token, a subtoken, a gift card number or code, a
15 prepaid card number or code, a username, an expiration date, a CVV (card verification value), a dCVV (dynamic card verification value), a CVV2 (card verification value 2), a CVC3 card verification value, etc. An example of a PAN is a 16-digit number, such as “4147 0900 0000 1234”. In some embodiments, credentials may be considered sensitive information.

20 **[0021]** A “token” may be a substitute value for a credential. A token may be a string of numbers, letters, or any other suitable characters. Examples of tokens include payment tokens, access tokens, personal identification tokens, etc.

[0022] A “payment token” may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN).
25 For example, a payment token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments, a payment token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing transaction
30 processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a payment token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other

systems where the original credential would typically be provided. In some embodiments, a payment token may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0023] “Tokenization” is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g., a token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization enhances transaction efficiency and security.

[0024] A “token issuer,” token provider,” “token service system,” or “token service computer” can include a system that services tokens. In some embodiments, a token service system can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g., token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may include or be in communication with a token vault where the generated tokens are stored. The token service system may support token processing of payment transactions submitted using tokens by de-tokenizing the tokens to obtain the actual PANs. In some embodiments, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer. Various entities of a tokenization ecosystem may assume the roles of the token service provider. For example, payment networks and issuers or their agents may become the token service provider by implementing the token services according to embodiments of the present invention.

[0025] A “token domain” may indicate an area and/or circumstance in which a token can be used. Examples of token domains may include, but are not limited to,

payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e., token domain restriction controls) may be established as part of token issuance by the token service provider that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the token with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0026] A “token cryptogram” may include a token authentication verification value (TAVV) associated with a token. A token cryptogram may be a string of numbers, letters, or any other suitable characters, of any suitable length. In some embodiments, a token cryptogram may include encrypted token data associated with a token (e.g., a token domain, a token expiry date, etc.). For example, a token cryptogram may be used to validate that the token is being used within a token domain and/or by a token expiry date associated with the token.

[0027] “Token data” can include information related to a token. Token data can include a token and/or a token cryptogram. In some embodiments, token data can include only a token. In other embodiments, token data can include only a token cryptogram. In yet other embodiments, token data can include a token and a token cryptogram that is related to the token. Token data can include additional data related to the token (e.g., a token expiry date, etc.).

[0028] A “token expiry date” can include an expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g., a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0029] A “token request message” may be an electronic message for requesting token data. A token request message can request token data including a token and/or a token cryptogram. A token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a payment token. For example, a token request message may include payment credentials, mobile device identification information (e.g., a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a token cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key).

[0030] A “token response message” may be a message that responds to a token request. A token response message may include an indication that a token request was approved or denied. A token response message may also include a payment token, mobile device identification information (e.g., a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a token cryptogram, and/or any other suitable information. Information included in a token response message can be encrypted (e.g., with an issuer-specific key).

[0031] A “token requestor identifier” may include any characters, numerals, or other identifiers associated with an entity associated with a network token system. For example, a token requestor identifier may be associated with an entity that is registered with the network token system. In some embodiments, a unique token requestor identifier may be assigned for each domain for a token request associated with the same token requestor. For example, a token requestor identifier can identify a pairing of a token requestor (e.g., a mobile device, a mobile wallet provider, etc.) with a token domain (e.g., e-commerce, contactless, etc.). A token requestor identifier may include any format or type of information. For example, in one embodiment, the token requestor identifier may include a numerical value such as a ten digit or an eleven digit number (e.g., 4678012345).

[0032] An “amount” can include a quantity of something. An amount can include a total of a thing or things in number, size, value, or extent.

[0033] A “resource provider” may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of resource providers includes merchants, data providers, transit agencies, governmental entities, venue and dwelling operators, etc.

5 **[0034]** The term “verification” and its derivatives may refer to a process that utilizes information to determine whether an underlying subject is valid under a given set of circumstances. Verification may include any comparison of information to ensure some data or information is correct, valid, accurate, legitimate, and/or in good standing.

10 **[0035]** The term “public/private key pair” may include a pair of linked cryptographic keys generated by an entity. The public key may be used for functions such as encrypting a message to send to the entity or for verifying a digital signature which was supposedly made by the entity. The private key may be used for functions such as decrypting a received message or applying a digital signature. The public
15 key can be authorized by a certificate authority, which can store the public key in a database and distribute it to any other entity which requests the public key. The private key can be kept in a secure storage medium and will usually only be known to the entity. However, the cryptographic systems described herein may feature key recovery mechanisms for recovering lost keys and avoiding data loss. Public and
20 private keys may be in any suitable format, including those based on Rivest-Shamir-Adleman (RSA) or elliptic curve cryptography (ECC).

[0036] A “zone encryption key” (ZEK) can include cryptographic keys used to encrypt data between two specific points. For example, zone encryption keys can be used to encrypt data transmitted between a first device and a second device.

25 **[0037]** An “authorization request message” may be an electronic message that requests authorization for a transaction. In some embodiments, it is sent to a payment processing network and/or an issuer of a payment account to request authorization for a payment transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for
30 systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or a payment account. An authorization request message may also comprise additional data elements

corresponding to “identification information” including, for example, a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc. An authorization request message may also comprise “transaction data,” such as any information associated with a current transaction (e.g., the transaction amount, merchant identifier, merchant location, etc.), as well as any other information that may be utilized in determining whether to identify and/or authorize a payment transaction.

[0038] An “authorization response message” may be reply to an authorization request message. In some embodiments, an authorization response message may be an electronic message reply to an authorization request message generated by an issuing financial institution (i.e., issuer) or a payment processing network. An authorization response message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or a payment account. The authorization response message may include an authorization code, which may be a code that an account issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to a merchant's access device (e.g., point of sale terminal) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate and/or forward the authorization response message to the merchant.

[0039] An “authorization computer” may include any system involved in authorization of a transaction. The authorization computer may determine whether a transaction can be authorized and may generate an authorization response message including an authorization status (also may be known as an authorization decision). In some embodiments, an authorization computer may be a payment account issuer computer. In some cases, the authorization computer may store contact information of one or more users. In other embodiments, the authorization computer may authorize non-financial transactions involving a user. For example, the authorization computer may make an authorization decision regarding whether the user can access a certain resource. In some cases, the authorization computer may be a

content provider server computer associated with a content providing entity, which manages one or more resources that may be accessed by the user. The authorization computer may be known as an authorizing entity computer. The authorization computer may include an “access control server” that may be
5 configured to authenticate a user.

[0040] A “network processing computer” may include a server computer used for interaction processing. In some embodiments, the network processing computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client
10 computers or user devices. The network processing computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers or user devices. In some embodiments, the network processing computer may operate multiple server computers. In such embodiments,
15 each server computer may be configured to process an interaction for a given region or handles transactions of a specific type based on interaction data.

[0041] The network processing computer may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary
20 network processing computer may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes an integrated payments system (Integrated Payments system) which processes authorization requests and a Base II system, which performs clearing and settlement
25 services. The network processing computer may use any suitable wired or wireless network including the Internet.

[0042] The network processing computer may process transaction-related messages (e.g., authorization request messages and authorization response messages) and determine the appropriate destination computer (e.g., issuer
30 computer/authorizing entity computer) for the interaction-related messages. In some embodiments, the network processing computer may authorize interactions on

behalf of an issuer. The network processing computer may also handle and/or facilitate the clearing and settlement of financial transactions.

[0043] An “interaction request message” may be an electronic message that indicates that the user has initiated an interaction with a resource provider. An
5 interaction request message may include transaction data associated with the interaction.

[0044] An “interaction response message” may be an electronic message that is used to respond to an interaction request message. In some embodiments, an interaction response message may indicate that the interaction associated with an
10 interaction request message was successful or unsuccessful.

[0045] A “processor” may include a device that processes something. In some embodiments, a processor can include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising at
15 least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0046] A “memory” may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more
20 memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0047] A “server computer” may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server
30 computer may comprise one or more computational apparatuses and may use any

of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0048] Embodiments provide for a system and method of using pre-generated token data (e.g., including a token and/or a token cryptogram) and storing them in an edge computer that can be close (e.g., in terms of network communication latency) to the token requestor. When the token requestor generates and provides a token request message to the edge computer to obtain token data (e.g., using an API call such as `getPaymentData()`), the edge computer can query a local secure database for pre-generated token data. The token request message can request token data including a token and/or a token cryptogram. The edge computer can then return the pre-generated token data, if available. Otherwise, the edge computer can forward the token request message call to token service computer.

[0049] The edge computer can be located in a first region and can receive a subset of token data from a token service computer that is located in a second region. The subset of token data can correspond to a subset of credentials. The first region and the second region can be remotely located from one another (e.g., in different countries). The token service computer can store a set of token data, where the subset of token data are selected from the set of token data based on data associated with users of the credentials (e.g., based on historical interaction data, etc.).

[0050] After receiving the subset of token data, the edge computer can receive a token request message comprising the credential from a token requestor. The edge computer can identify the token data that corresponds with the credential from the subset of token data. The edge computer can generate and transmit a token response message comprising the token data to the token requestor. The token requestor can use the token data to perform an interaction for a user associated with the credential.

[0051] FIG. 1 shows a system 100 according to embodiments of the disclosure. The system 100 comprises a user device 102, a resource provider computer 104, an edge computer 106, token service computer 108, a transport computer 110, a network processing computer 112, and an authorizing entity

computer 114. The user device 102, the resource provider computer 104, and the edge computer 106 can be in a first region 150.

[0052] The user device can be in operative communication with the resource provider computer 104. The resource provider computer 104 can be in operative communication with the edge computer 106 and the transport computer 110. The edge computer 106 can be in operative communication with the token service computer 108. The transport computer 110 can be in operative communication with the network processing computer 112. The network processing computer can be in operative communication with the authorizing entity computer 114.

[0053] For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1.

[0054] Messages between the device in the system 100 in FIG. 1 can be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), SSL, ISO (e.g., ISO 8583) and/or the like. The communications network include any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like. The communications network can use any suitable communications protocol to generate one or more secure communication channels. A communications channel may, in some instances, comprise a secure communication channel, which may be established in any known manner, such as through the use of mutual authentication and a session key, and establishment of a Secure Socket Layer (SSL) session.

[0055] The user device 102 can include one or more computers, portable computers, laptop computers, tablet computers, mobile devices, cellular phones, wearable devices (e.g., watches, glasses, lenses, clothing, etc.), personal digital assistants (PDAs), Internet of Things (IoT) devices, and/or the like. The user device

102 can initiate interactions (e.g., transactions) with resource provider computers such as the resource provider computer 104. For example, the user device 102 can access a website hosted and/or operated by the resource provider computer 104 to select one or more items for the interaction. For example, the user of the user device

5 102 can navigate to the resource provider website using an Internet browser installed on the user device 102, select one or more items provided by the resource provider computer 104, and submit the interaction (e.g., checkout) for approval.

[0056] The resource provider computer 104 can include any suitable computational apparatus operated by a resource provider (e.g., a merchant). In

10 some embodiments, the resource provider computer 104 may include one or more server computers that may host one or more websites associated with the resource provider (e.g., a merchant). In some embodiments, the resource provider computer 104 may be configured to send data to a network processing computer 112 via a transport computer 110 as part of a payment verification and/or authentication

15 process for a transaction between the user (e.g., consumer) and the resource provider. The resource provider computer 104 may also be configured to generate authorization request messages for transactions between the resource provider and the user 118, and route the authorization request messages to an authorizing entity computer 114 for transaction processing. The resource provider computer 104 can

20 be an example of a token requestor.

[0057] The edge computer 106 can include a computer, a server computer, or other computational apparatus. The edge computer 106 can store token data (e.g., tokens and/or token cryptograms) for users from regions located outside of the region in which the edge computer 106 resides. The edge computer 106 can be

25 close to the token requestor server (e.g., the resource provider computer 104), or co-reside with token requestor in the same data center, or deployed into the token requestor's network, such that communication latency between the edge computer 106 and the token requestor is low. The edge computer 106 can be operated by token service providers, by the network processing computer 112, and/or other

30 entity. The connection between the edge computer 106 and the token service computer(s) can be secured, for example, where data exchange is protected using zone keys.

[0058] In some embodiments, one token requestor can be served by multiple edge computers for active-active, fail-safe, and load balancing. In other embodiments, one edge computer can serve multiple token requestors in a region.

[0059] The edge computer 106 can maintain a list of token data which are provisioned to the token requestor(s) that the edge computer 106 communicates with. These token data, which can be a subset of token data of a set of token data in a different region, are associated with user devices issued in different regions, which are used by users when interacting with the token requestor(s).

[0060] In some embodiments, the edge computer 106 can obtain pre-generated token cryptogram(s) from the token service computer 108 in different regions prior to those token cryptograms being used in interactions. The edge computer 106 can maintain a number of pre-generated token cryptograms for each token stored by the edge computer 106. If the number of pre-generated token cryptograms for a token reaches a low threshold (e.g., 0, 1, 2, 3, etc.), the edge computer 106 can obtain new pre-generated token cryptogram(s) from the token service computer 108, from which the token originated. The edge computer 106 can utilize prediction and projections (e.g., transaction volume curve/trend, card issuance region distribution, upcoming sales season/festival) to fetch a number of token cryptograms for tokens stored by the edge computer 106.

[0061] Upon receiving a token request message comprising a credential from a token requestor computer (e.g., the resource provider computer 104), the edge computer 106 can search through the subset of token data stored by the edge computer 106 for token data (e.g., a token and/or token cryptogram) stored in association with the credential. If pre-generated token data is available (e.g., stored in the edge computer 106 in a local database), the edge computer 106 can utilize the token data and return the token data to the token requestor. In such a case, the token latency retrieval time is minimized. If the pre-generated token data is not available in the edge computer 106, then the edge computer 106 can redirect the token request message to the corresponding token service computer 108 (which can be located in a different region).

[0062] The token service computer 108 can include a computer programmed to facilitate requesting, determining (e.g., generating) and/or issuing token data, as

well as maintaining an established mapping of token data to credentials (e.g., primary account numbers) in a repository (e.g., token vault). The token service computer 108 may include or be in communication with a token vault where the generated tokens are stored. The token service computer 108 may support token processing of interactions submitted using tokens by de-tokenizing the tokens to obtain the actual credentials. In some embodiments, a token service computer 108 may include a tokenization computer alone, or in combination with other computers such as a network processing computer 112.

[0063] The token service computer 108 can store a set of token data. The token service computer 108 can select a subset of token data from the set of token data based on data associated with users of credentials (e.g., based on historic data, projects, etc.). The token service computer 108 can provide the subset of token data to the edge computer 106 upon determining that the token data of the subset of token data have a high probability of being used in interactions with the resource provider computer 104 in a region in which the edge computer 106 resides. Embodiments can reduce during interaction communication latency by pre-providing the subset of token data to the edge computer 106 prior to the token data being used in interactions with the resource provider computer 104.

[0064] The transport computer 110 can include a server computer. The transport computer 110 may be associated with an acquirer, which may be an entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers.

[0065] The network processing computer 112 may be disposed between the transport computer 110 and the authorizing entity computer 114. The network processing computer 112 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the network processing computer 112 may comprise a server coupled to a network interface (e.g., by an external communication interface), and databases of information. The network processing computer 112 may be representative of a transaction processing network. An exemplary transaction processing network may include VisaNet™.

Transaction processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The network processing computer 112 may use any suitable wired or wireless network, including the Internet.

[0066] The authorizing entity computer 114 can include a server computer operated by an authorizing entity. The authorizing entity computer 114 may be associated with an authorizing entity, which may be an entity that authorizes a request. An example of an authorizing entity may be an issuer, which may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue and manage an account associated with a user device.

[0067] The network processing computer 112, the transport computer 110, and the authorizing entity computer 114 may operate suitable routing tables to route authorization request messages and/or authorization response messages using credentials, token data, merchant identifiers, and/or other account identifiers.

[0068] FIG. 2 shows a block diagram of an edge computer 106 according to embodiments. The exemplary edge computer 106 may comprise a processor 204. The processor 204 may be coupled to a memory 202, a network interface 206, and a computer readable medium 208. The computer readable medium 208 can comprise a token module 208A and a communication module 208B.

[0069] The memory 202 can be used to store data and code. For example, the memory 202 can be a secure database which can store a subset of token data, a subset of token cryptograms, a subset of credentials, etc. The memory 202 may be coupled to the processor 204 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device.

[0070] The computer readable medium 208 may comprise code, executable by the processor 204, for performing a method comprising: receiving, by an edge computer in a first region, a subset of token data corresponding to a subset of credentials from a token service computer in a second region, the first region and the

second region being remotely located with respect to each other, wherein the token service computer stores a set of token data, the subset of token data being selected from the set of token data based on data associated with users of credentials of the subset of credentials; receiving, by the edge computer, a token request message
5 comprising the credential from a token requestor; and transmitting, by the edge computer, a token response message comprising token data to the token requestor, wherein the token requestor uses the token data to perform an interaction for a user associated with the credential.

[0071] The token module 208A include may comprise code or software,
10 executable by the processor 204, for obtaining and providing tokens. The token module 208A, in conjunction with the processor 204, can process tokens. The token module 208A, in conjunction with the processor 204, can receive a subset of token data corresponding to a subset of credentials from a token service computer. The token module 208A, in conjunction with the processor 204, can store the subset of
15 token data in the secure token database. Each token can be stored in association with the corresponding credential.

[0072] The token module 208A, in conjunction with the processor 204, can also process token cryptograms. The token module 208A, in conjunction with the processor 204, can receive a subset of token cryptograms from a token service
20 computer. The token module 208A, in conjunction with the processor 204, can store the subset of token cryptograms in the secure token database. Each token cryptogram can be stored in association with the corresponding token. In some embodiments, one or more token cryptograms can correspond to a token.

[0073] For example, the token module 208A, in conjunction with the processor
25 204, can receive a token request message from a resource provider computer. Upon receipt of the token request message, the token module 208A, in conjunction with the processor 204, can confirm that the credential (e.g., account identifier) included in the token request message is eligible for tokenization. For example, the token module 208A, in conjunction with the processor 204, can determine whether or not a
30 credential stored in a secure token database matches the received credential.

[0074] The communication module 208B include may comprise code or software, executable by the processor 204, for communicating with other devices.

The communication module 208B, in conjunction with the processor 204, can generate messages, receive messages, and parse messages. The communication module 208B, in conjunction with the processor 204, can receive token request messages, credential request messages, messages including a subset of token data, messages including a subset of token cryptograms, etc. The communication module 208B, in conjunction with the processor 204, can generate and transmit token response messages, credential request messages, messages requesting a subset of token data, messages requesting a subset of token cryptograms, etc.

[0075] For example, the communication module 208B, in conjunction with the processor 204, can receive a token request message from a token requestor computer (e.g., a resource provider computer). The token request message may include at least an account identifier (e.g., a primary account number (PAN)) of an account issued by an authorizing entity computer to a user of a user device.

[0076] The network interface 206 may include an interface that can allow edge computer 106 to communicate with external computers. The network interface 206 may enable the edge computer 106 to communicate data to and from another device (e.g., resource provider computers, token service computers, etc.). Some examples of the network interface 206 may include a modem, a physical network interface (such as an Ethernet card or other Network Interface Card (NIC)), a virtual network interface, a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. The wireless protocols enabled by the network interface 206 may include Wi-Fi™. Data transferred via the network interface 206 may be in the form of signals which may be electrical, electromagnetic, optical, or any other signal capable of being received by the external communications interface (collectively referred to as “electronic signals” or “electronic messages”). These electronic messages that may comprise data or instructions may be provided between the network interface 206 and other devices via a communications path or channel. As noted above, any suitable communication path or channel may be used such as, for instance, a wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, a WAN or LAN network, the Internet, or any other suitable medium.

[0077] FIG. 3 shows a block diagram of a token service computer 108 according to embodiments. The exemplary token service computer 108 may comprise a processor 304. The processor 304 may be coupled to a memory 302, a network interface 306, input elements 310, output elements 312, and a computer readable medium 308. The computer readable medium 308 can comprise a prediction module 308A, a token module 308B, and a communication module 308C.

[0078] The memory 302 can be used to store data and code and may be similar to the memory 202 as described herein. For example, the memory 302 can store tokens, token cryptograms, credentials, etc.

[0079] The prediction module 308A may comprise code or software, executable by the processor 304, for creating predictions. The prediction module 308A, in conjunction with the processor 304, can generate predictions for selecting a subset of token data from the set of token data based on data associated with users of credentials of the subset of credentials. The prediction module 308A, in conjunction with the processor 304, can generate a prediction of which tokens and/or token cryptograms may be utilized in a different region than the region in which the token service computer 108 resides.

[0080] For example, the prediction module 308A, can be located in a first region. The prediction module 308A, in conjunction with the processor 304, can determine whether or not a user (located in the first region) of a credential and token is likely to perform an interaction with a resource provider computer located in a second region. The prediction module 308A, in conjunction with the processor 304, can utilize data associated with the users of the credentials (e.g., utilize historic interaction data, upcoming event data, etc.). For example, the prediction module 308A, in conjunction with the processor 304, can determine that a user in the first region interacts with a resource provider computer in the second region once per month for the last year (e.g., as determined from historic interaction data). The prediction module 308A, in conjunction with the processor 304, can predict that the user will interact with the resource provider computer again.

[0081] The prediction module 308A, in conjunction with the processor 304, can select a subset of token data from the set of token data (e.g., the tokens and/or the token cryptograms stored by the token service computer 108) based on the

prediction that the user will interact with the resource provider computer in the second region again. The subset of token data can include token data of the user, and any other token data of other users that are also predicted to interact with resource provider computers in the second region.

- 5 **[0082]** The prediction module 308A, in conjunction with the processor 304, can provide the subset of token data as well as a subset of credentials, where each credential corresponds to a token, to an edge computer located in the second region for later use in interactions between the users of the credentials and resource provider computers located in the second region.
- 10 **[0083]** The token module 308B can include may comprise code or software, executable by the processor 204, for processing tokens. The token module 308B, in conjunction with the processor 304, can generate or obtain token data that correspond to credentials of users. The token module 308B, in conjunction with the processor 304, can generate the token data in any suitable manner. The token
- 15 module 308B, in conjunction with the processor 304, can generate a token that appears to be a string of random characters and does not relate to tokens created previously or subsequently. The token module 308B, in conjunction with the processor 304, can generate the token data based on random values, keys, user data, user device data, etc.
- 20 **[0084]** The communication module 308C can include may comprise code or software, executable by the processor 304, for communicating with other devices. The communication module 308C may be similar to the communication module 208B and the descriptions thereof are incorporated herein and need not be repeated here.
- 25 **[0085]** The network interface 306 may be similar to the network interface 206 and the descriptions thereof are incorporated herein and need not be repeated here.

[0086] FIG. 4 shows a block diagram of two regions in a token cryptogram delivery network according to embodiments. FIG. 4 includes a first region 410 comprising a first resource provider computer 412, a first edge computer 414, a first

30 user device 418, and a first token service computer 416. FIG. 4 also includes a second region 420 comprising a second resource provider computer 422, a second

edge computer 424, a second user device 428, and a second token service computer 426.

[0087] The first region 410 and the second region 420 can be remotely located with respect to each other. Each region can be a geographical region, a computing network region, political region, etc. For example, the first region 410 can be the United States, while the second region 420 is the European Union. As another example, the first region 410 is a first country and the second region 420 is a second country. In other embodiments, the first region 410 and the second region 420 can be within the same country, but can be far from each other (e.g., California and New York).

[0088] Each region can include a token service computer that stores tokens and token cryptograms for user devices that are issued in the region. For example, the first token service computer 416 can store tokens and token cryptograms for the first user device that was issued by a first authorizing entity computer (not shown) in the first region 410. The second token service computer 426 can store tokens and cryptograms for the second user device that was issued by a second authorizing entity computer (not shown) in the second region 420.

[0089] Since the regions are remotely located with respect to each other, there can be higher communication latency between devices in the different regions than between devices in the same region. For example, there can be higher communication latency between the first resource provider computer 412 and the second token service computer 426 than between the first resource provider computer 412 and the first edge computer 414. As such, by preemptively providing token data (e.g., tokens and/or token cryptograms) from the second token service computer 426 to the first edge computer 414, as described herein, the overall communication latency of the first resource provider computer 412 obtaining token data that was originally from the second token service computer 426 can be reduced.

[0090] In some embodiments, the communication time between a resource provider computer and an edge computer can be between 100 milliseconds and 300 milliseconds. Whereas an interaction between the second user device 428 and the first resource provider computer 412 that needs to obtain token data directly from the

second token service computer 426 without an edge computer can take a total time of approximately 5600 milliseconds.

[0091] FIG. 5 shows a flow diagram illustrating a first token delivery method according to embodiments. The method illustrated in FIG. 5 will be described in the context of the user device 102 interacting with the resource provider computer 104. It is understood, however, that the invention can be applied to other circumstances.

[0092] At step 500, the token service computer 108 can determine a subset of token data from a set of token data stored by the token service computer. The subset of token data can correspond to a subset of credentials. The token service computer 108 can store a set of tokens as well as a set of token cryptograms in a secure database, which can be referred to as a token vault. The token cryptograms can be used to confirm that their corresponding tokens are being used in their intended manner. For example, a token may only be used with a particular merchant and the cryptogram may include encrypted information such as a merchant identifier. If an authorization request message comprising the token originates from a merchant that does not correspond with the merchant identifier encoded in the cryptogram, then the authorization request message may be declined. Thus, the use of cryptograms with tokens improves data security.

[0093] The token service computer 108 can select the subset of token data from the set of token data based on data associated with users of the credentials. The selection of the subset of token data can be made based on historical user interaction data (e.g., the user has previously interacted with a resource provider computer in a different region once per month), event data (e.g., users from a first region typically interaction with resource provider computers in a second region during a holiday), and/or based on other data related to the user's interactions with resource provider computers in other regions.

[0094] At step 502, the token service computer 108 can provide the subset of token data to the edge computer 106. The edge computer 106 can be located in a first region and the token service computer 108 can be located in a second region. The first region and the second region are remotely located with respect to each other.

[0095] The token service computer 108 can also provide a subset of credentials that correspond to the subset of token data to the edge computer 106.

[0096] At step 504, after receiving the subset of token data from the token service computer 108, the edge computer 106 can store the subset of token data into a secure memory or database. The edge computer 106 can store each token data in association with the corresponding credential.

[0097] At a point later in time, at step 506, the user device 102 can initiate an interaction with the resource provider computer 104. For example, the user of the user device 102 can conduct an interaction (e.g., a transaction) with the resource provider computer 104 (e.g., a merchant). The interaction may be a payment transaction (e.g., for the purchase of a good or service), an access interaction (e.g., for access to a transit system), or any other suitable interaction. In some embodiments, the user device 102 can provide payment account information to the resource provider computer 104 electronically, such as in an online transaction. For example, the user device 102 can generate an interaction request message comprising a credential (e.g., a primary account number). The user device 102 can provide the interaction request message to the resource provider computer 104. The interaction request message can also include interaction data relating to the interaction or the devices involved in the interaction. For example, the interaction request message can include interaction data including an amount, one or more items selected by the user, a user identifier, a user device identifier, a user device certificate, a resource provider identifier, a time, a date, a location, etc.

[0098] At step 508, after receiving the interaction request message from the user device 102, the resource provider computer 104 can determine that the interaction request message includes a credential. The resource provider computer 104 can communicate with an edge computer 106 to obtain token data for the credential. The resource provider computer 104 can generate a token request message comprising the credential.

[0099] At step 510, after generating the interaction request message, the resource provider computer 104 can transmit the token request message to the edge computer 106. In some embodiments, communications between the resource provider computer 104 and the edge computer 106 can be encrypted using zone

keys. Zone keys can be symmetric cryptographic keys. The resource provider computer 104 can encrypt the token request message using a first zone key. The zone keys can be pre-established prior to the interaction.

[0100] At step 512, after receiving the token request message comprising the credential from the resource provider computer 104, the edge computer 106 can query a memory and/or database included in the edge computer 106 for token data that is stored in association with the credential.

[0101] In some embodiments, if the token request message is encrypted with a zone key, then the edge computer 106 can decrypt the token request message using a second zone key that corresponds to the first zone key.

[0102] At step 514, after obtaining the token data that corresponds to the credential, the edge computer 106 can generate a token response message. The token response message can include the token data. In some embodiments, the token response message can also include the credential.

[0103] At step 516, after generating the token response message, the edge computer 106 can provide the token response message to the resource provider computer 104. In some embodiments, the edge computer 106 can encrypt the token response message using the second zone key.

[0104] At step 518, after receiving the token data from the edge computer 106, the resource provider computer 104 can generate an authorization request message. The authorization request message can request authorization of the interaction. The authorization request message can comprise the token data and the interaction data. In some embodiments, the resource provider computer 104 can decrypt the token response message using the first zone key.

[0105] At step 520, the resource provider computer 104 can transmit the authorization request message to the transport computer 110.

[0106] At step 522, after receiving the authorization request message, the transport computer 110 can transmit the authorization request message to the network processing computer 112.

[0107] At step 524, after receiving the authorization request message from the transport computer 110, the network processing computer 112 can generate a credential request message that requests the credential that is associated with the token data. The credential request message includes the token data. The network processing computer 112 can communicate with the token service computer 108 or other token vault to validate the token data (e.g., the token and/or the token cryptogram) and obtain the credential. In some embodiments, the cryptogram can be decrypted to obtain information that can be used to determine if the token is being used in an intended manner (e.g., in a specific payment channel or with a specific merchant).

[0108] At step 526, the network processing computer 112 can transmit the credential request message to the token service computer 108.

[0109] At step 528, after receiving the credential request message comprising the token data, the token service computer 108 can identify a credential in a secure database that is stored in association with the token data. The token service computer 108 can obtain the credential. The token service computer 108 can generate a credential response message comprising the credential.

[0110] At step 530, after obtaining the credential, the token service computer 108 can provide credential response message to the network processing computer 112.

[0111] In other embodiments, instead of communicating with the token service computer 108 in steps 526 and 530, the network processing computer 112 can communicate with the edge computer 106 to retrieve the credential associated with the token data.

[0112] At step 532, after receiving the credential response message, the network processing computer 112 can modify the authorization request message to replace the token data with the credential. As such, the token data is removed from the authorization request message and the credential is added to the authorization request message.

[0113] At step 534, after modifying the authorization request message, the network processing computer can provide the authorization request message to the authorizing entity computer 114.

[0114] At step 536, the authorizing entity computer 114 can determine whether or not to authorize the interaction between the user device 102 and the resource provider computer 104. The authorizing entity computer 114 can determine whether or not to authorize the interaction based on any suitable data known to the authorizing entity computer 114 (e.g., the interaction data, the authorizing entity computer data, etc.). The authorizing entity computer 114 can generate an indication of whether or not the interaction is authorized. For example, if the authorizing entity computer 114 authorizes the interaction, then the authorizing entity computer 114 can generate an indication that the interaction is authorized. If the authorizing entity computer 114 determines not to authorize the interaction, then the authorizing entity computer 114 can generate an indication that the interaction is not authorized.

[0115] The authorizing entity computer can generate an authorization response message that comprises the indication of whether or not the interaction is authorized. The authorization response message can also include the interaction data from the authorization request message. The authorization response message can include the credential.

[0116] At step 538, the authorizing entity computer 114 can provide the authorization response message to the network processing computer 112.

[0117] After receiving the authorization response message, the network processing computer 112 can communicate with the token service computer 108 (or the edge computer 106 as described above) to obtain the token data the corresponds to the credential in the authorization response message (not shown). The token service computer 108 can identify the token data in a secure database using the credential. Upon obtaining the token data from the token service computer 108, the network processing computer 112 can modify the authorization response message to replace the credential with the token data.

[0118] At step 540, the network processing computer 112 can provide the authorization response message to the transport computer 110.

[0119] At step 542, the transport computer 110 can provide the authorization response message to the resource provider computer 104.

[0120] At step 544, after receiving the authorization response message from the transport computer 110, the resource provider computer 104 can evaluate the indication of whether or not the interaction is authorized. If the interaction is authorized, then the resource provider computer 104 can initiate providing the resources selected by the user of the user device 102 to the user.

[0121] At step 546, the resource provider computer 104 can provide the authorization response message or a derivation thereof to the user device 102. For example, the resource provider computer 104 can provide a web page or other indication of the authorization response message as a virtual receipt. The receipts may include the interaction data for the interaction.

[0122] At the end of the day, a normal clearing and settlement process can be conducted by the network processing computer 112. A clearing process is a process of exchanging financial details between an acquirer and an authorizing entity to facilitate posting to a user's payment account and reconciliation of the user's settlement position.

[0123] In some embodiments, during the interaction, the resource provider computer 104 can generate a cryptogram request message that requests a cryptogram. As an example, the token request message can be a cryptogram request message. The resource provider computer 104 can provide the cryptogram request message to the edge computer 106. In some embodiments, the cryptogram request message can be provided along with the token request message. The cryptogram request message can comprise the credential.

[0124] The edge computer 106 can receive the cryptogram request message comprising the credential from the resource provider computer 104. The edge computer 106 can determine a token cryptogram from a subset of token cryptograms using the credential. The subset of token cryptograms can be stored in a secure database by the edge computer 106. The edge computer 106 can previously receive the subset of token cryptograms from the token service computer 108 in a different region based on the token service computer's 108 prediction that the credentials

associated with the token cryptograms will be used in interactions in the region in which the edge computer 106 resides.

[0125] The edge computer 106 can retrieve the token cryptogram the database and generate a cryptogram response message comprising the token cryptogram. The edge computer 106 can provide the cryptogram response message in response to the cryptogram request message to the resource provider computer 104. The resource provider computer 104 can include the cryptogram into the authorization request message for authorization.

[0126] FIG. 6 shows a flow diagram illustrating delays that can occur when communications occur between token requestors and token service computers that are located in different regions, which may be geographically separated from each other by a large distance. FIG. 6 illustrates example network communication latency between various computers in region 1 and region 2. Region 1 includes a resource provider computer 602, a first token service computer 606, and a first authorizing entity computer 608. Region 2 includes a second token service computer 612 and a second authorizing entity computer 614. FIG. 6 also includes an internet connection 604 and a WAN (wide area network) connection 610. As an example, region 1 can be the United States and region 2 can be Turkey.

[0127] FIG. 6 includes two web domains including a token requestor website 620 domain and an issuer websites 630 domain. The resource provider computer 602 is included in the token requestor website 620 domain. The first authorizing entity computer 608 and the second authorizing entity computer 614 are included in the issuer websites 630 domain, where each issuer website of each authorizing entity computer can be hosted separately.

[0128] Communication times between computers in the same region can be smaller than communication times between computers in different regions. Currently the 98th percentile response time from the resource provider computer 602 to the first token service computer 606 is between 100 ms and 300 ms. If the resource provider computer 602 needs to obtain token data from the second token service computer 612, then the response time is approximately 2715 ms. Communicating with the token service computer in a different region can take 9 to 27 times longer than communicating with a token service computer in the same region. Further,

communication between the regions, which can be provided between the two token service computers, is routed through the WAN connection 610 which can take between 130 ms to 745 ms.

[0129] The 98th percentile total end-to-end provisioning response time between the resource provider computer 602 and the first authorizing entity computer 608 (all located in region 1) is approximately 2771 ms. Whereas the total end-to-end provisioning response time between the resource provider computer 602 in region 1 and the second authorizing entity computer 614 in region 2 is approximately 5624 ms. This means that the resource provider computer in a first region that needs to obtain token data in a second region and have an authorization be performed in the second region takes double the amount of time than if all processing takes place in the first region.

[0130] Embodiments of the disclosure have a number of advantages. Currently high communication latency leads to delays in the interaction process when obtaining token data from computers in a different region. For example, a global ecommerce merchant and token requestor can be US based, where its token requestor server is US based, and the endpoint of the token API call to the network is US based. For an interaction made by an EU issued user device operated by a user in the US, the token data is generated in EU, where the latency is high, which degrades the interaction user experience and may cause the interaction to time out (e.g., terminate).

[0131] Embodiments provide for an advantage of pre-provisioning the user's token data (e.g., token and/or token cryptogram) to an edge computer in the region in which the interaction is predicted to occur. During the interaction, the resource provider computer can request and receive the token data from the edge computer, without needing to communicate with a token service computer in a different region, thus eliminating the high communication delays between the regions.

[0132] Although the steps in the flowcharts and process flows described above are illustrated or described in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

[0133] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0134] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g., a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0135] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0136] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0137] As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, by an edge computer in a first region, a subset of token data
3 corresponding to a subset of credentials from a token service computer in a second
4 region, the first region and the second region being remotely located with respect to
5 each other, wherein the token service computer stores a set of token data, the
6 subset of token data being selected from the set of token data based on data
7 associated with users of credentials of the subset of credentials;
8 receiving, by the edge computer, a token request message comprising
9 a credential from a token requestor; and
10 transmitting, by the edge computer, a token response message
11 comprising token data to the token requestor, wherein the token requestor uses the
12 token data to perform an interaction for a user associated with the credential.
- 1 2. The method of claim 1 further comprising:
2 determining, by the edge computer, whether or not the credential in the
3 token request message matches the credential corresponding to token data.
- 1 3. The method of claim 2 further comprising:
2 if the credential in the token request message matches a credential
3 corresponding to token data that is stored in a memory, then obtaining, by the edge
4 computer, the token data from the memory.
- 1 4. The method of claim 1, wherein the credential is associated with
2 an authorizing entity computer in the second region.
- 1 5. The method of claim 1 wherein receiving the token data
2 comprises:
3 receiving, by the edge computer from the token service computer, a
4 plurality of token data corresponding to a plurality of credentials, wherein the plurality
5 of credentials are associated with the second region, and wherein the plurality of
6 credentials are associated with users that have interacted with resource providers in
7 the first region.

1 6. The method of claim 1 wherein the token requestor generates
2 an authorization request message comprising the token data and provides the
3 authorization request message to an authorizing entity computer associated with the
4 token data for authorization.

1 7. The method of claim 1, wherein the credential and the token are
2 in the same format.

1 8. The method of claim 1 further comprising:
2 storing, by the edge computer, the token data into a secure database.

1 9. The method of claim 8 further comprising:
2 retrieving, by the edge computer, the token data from the secure
3 database based on the credential.

1 10. The method of claim 1, wherein the token data includes a token
2 and/or a token cryptogram.

1 11. The method of claim 1 wherein the token data is a token
2 cryptogram.

1 12. The method of claim 1, wherein the first region is a first country
2 and the second region is a second country.

1 13. The method of claim 1, wherein the token requestor is a
2 resource provider computer, and wherein communication latency between the
3 resource provider computer and the edge computer is between 100 milliseconds and
4 300 milliseconds.

1 14. The method of claim 1, wherein the token request message is
2 encrypted with a first zone key, wherein the method further comprises:
3 decrypting, by the edge computer, the token request message using a
4 second zone key that corresponds to the first zone key, wherein the first zone key
5 and the second zone key are symmetric cryptographic keys;
6 generating, by the edge computer, the token response message
7 comprising the token data; and

8 encrypting, by the edge computer, the token response message using
9 the second zone key.

1 15. An edge computer comprising:
2 a processor; and
3 a computer-readable medium coupled to the processor, the computer-
4 readable medium comprising code executable by the processor for implementing a
5 method comprising:

6 receiving, by the edge computer in a first region, a subset of
7 token data corresponding to a subset of credentials from a token service
8 computer in a second region, the first region and the second region being
9 remotely located with respect to each other, wherein the token service
10 computer stores a set of token data, the subset of token data being selected
11 from the set of token data based on data associated with users of credentials
12 of the subset of credentials;

13 receiving, by the edge computer, a token request message
14 comprising a credential from a token requestor; and

15 transmitting, by the edge computer, a token response message
16 comprising token data to the token requestor, wherein the token requestor
17 uses the token data to perform an interaction for a user associated with the
18 credential.

1 16. The edge computer of claim 15, wherein the token requestor is a
2 resource provider computer communicating with a user device associated with an
3 authorizing entity computer in the second region.

1 17. The edge computer of claim 15 further comprising:
2 a token module; and
3 and a communication module.

1 18. A system comprising:
2 one or more token requestor computers;
3 a token service computer; and
4 an edge computer comprising:
5 a processor; and

6 a computer-readable medium coupled to the processor, the
7 computer-readable medium comprising code executable by the processor for
8 implementing a method comprising:

9 receiving, by the edge computer in a first region, a subset
10 of token data corresponding to a subset of credentials from the token
11 service computer in a second region, the first region and the second
12 region being remotely located with respect to each other, wherein the
13 token service computer stores a set of token data, the subset of token
14 data being selected from the set of token data based on data
15 associated with users of credentials of the subset of credentials;

16 receiving, by the edge computer, a token request
17 message comprising a credential from a token requestor; and

18 transmitting, by the edge computer, a token response
19 message comprising token data to the token requestor, wherein the
20 token requestor uses the token data to perform an interaction for a user
21 associated with the credential.

1 19. The system of claim 18, wherein receiving the token data
2 comprises:

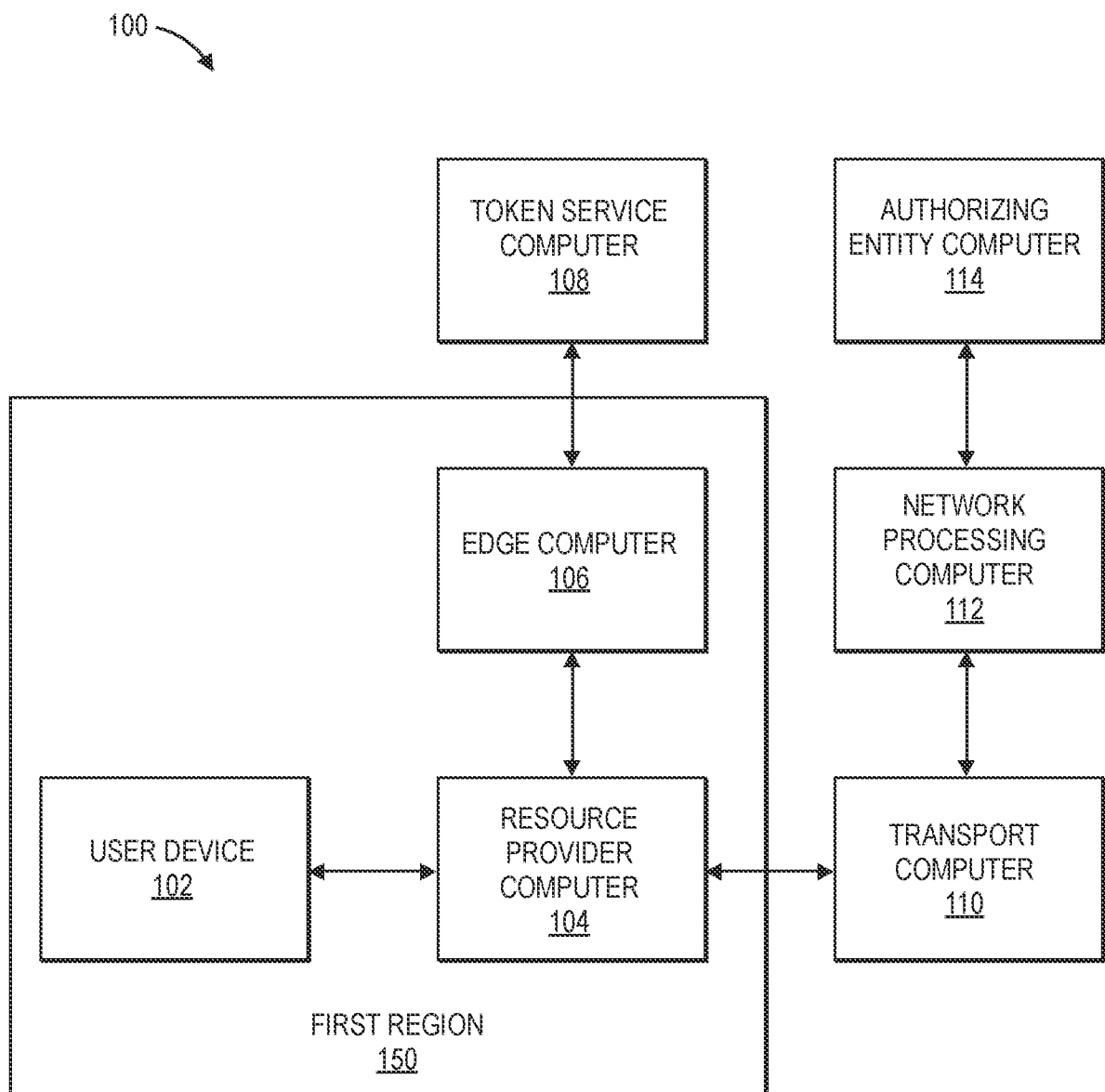
3 receiving, by the edge computer from the token service computer, a
4 plurality of token data corresponding to a plurality of credentials, wherein the plurality
5 of credentials are associated with the second region, and wherein the plurality of
6 credentials are associated with users that have interacted with resource providers in
7 the first region.

1 20. The system of claim 18, wherein the token data includes a token
2 and/or a token cryptogram, wherein the credential is associated with an authorizing
3 entity computer in the second region, and wherein the method further comprises:

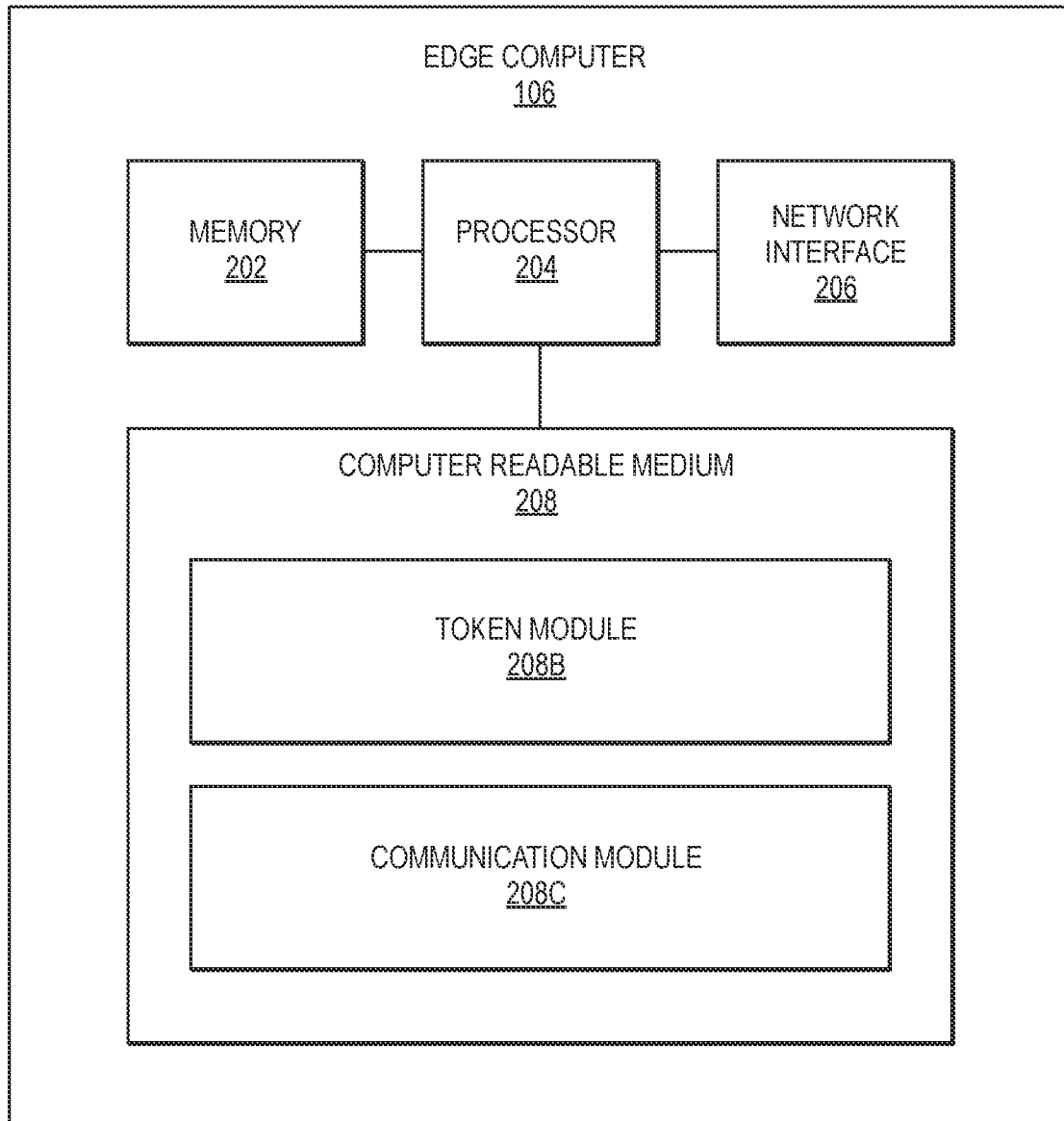
4 determining, by the edge computer, whether or not the
5 credential in the token request message matches the credential
6 corresponding to the token data; and

7 if the credential in the token request message matches the
8 credential corresponding to the token data, obtaining, by the edge computer,
9 the token data from memory.

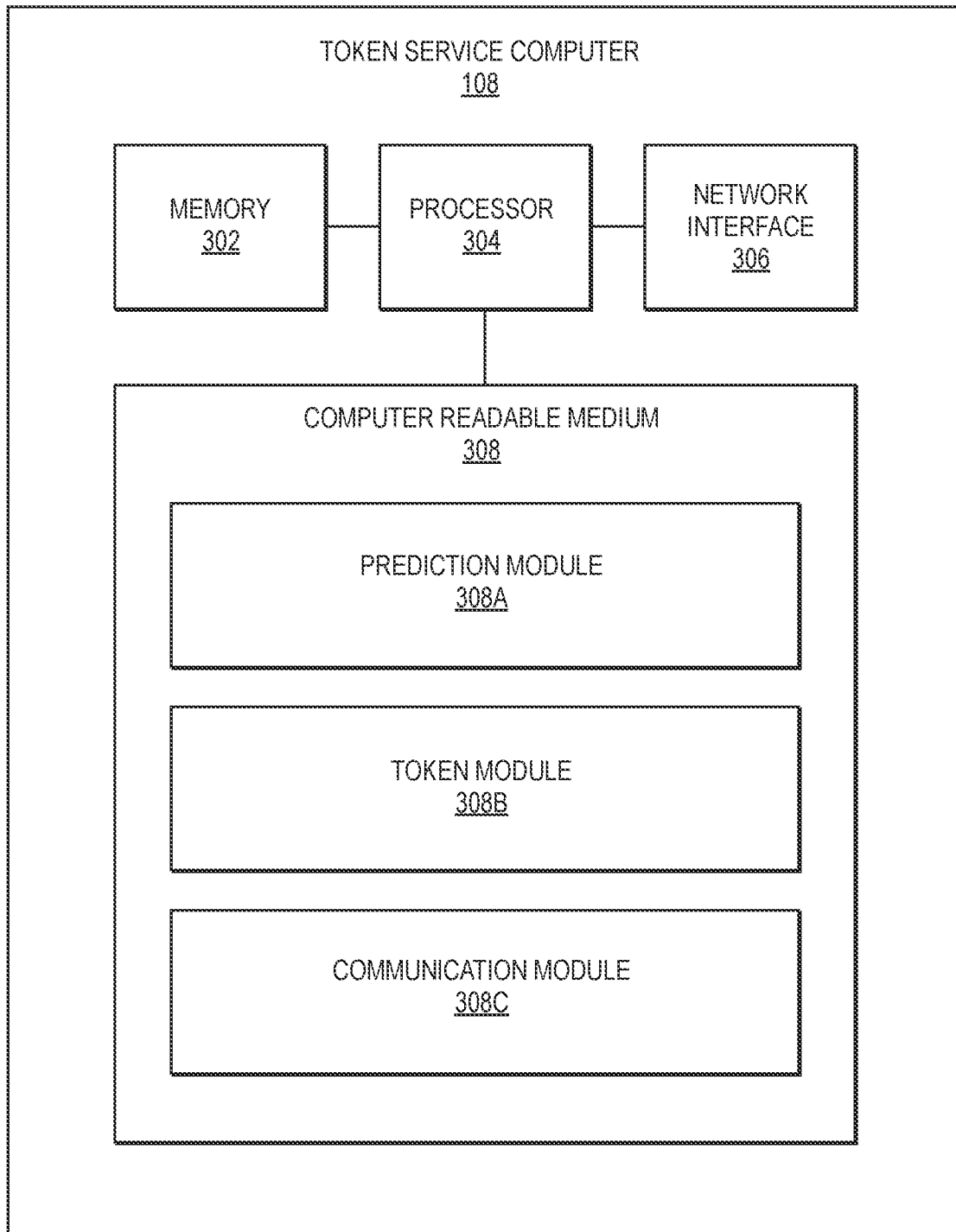
1/6

**FIG. 1**

2/6

**FIG. 2**

3/6

**FIG. 3**

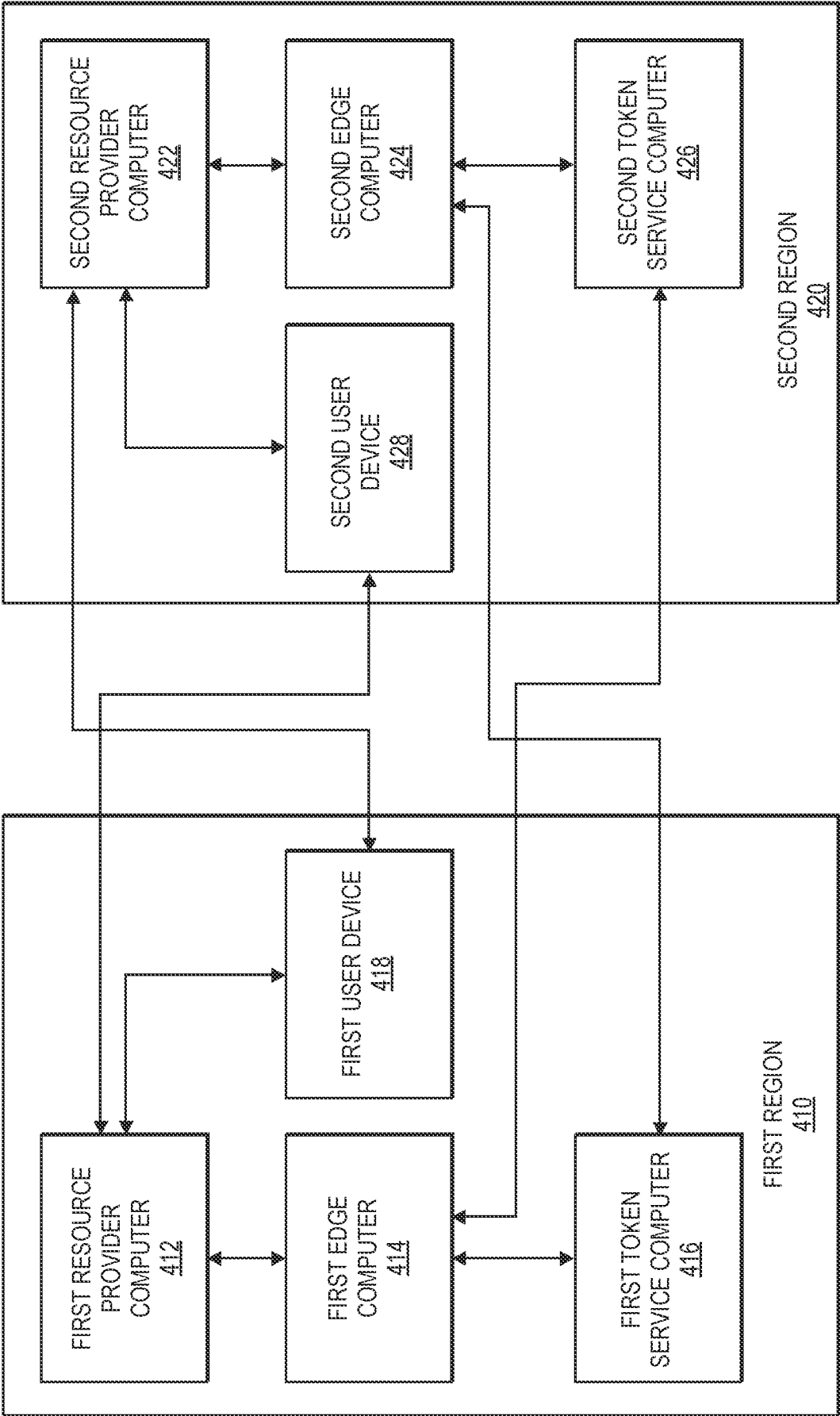


FIG. 4

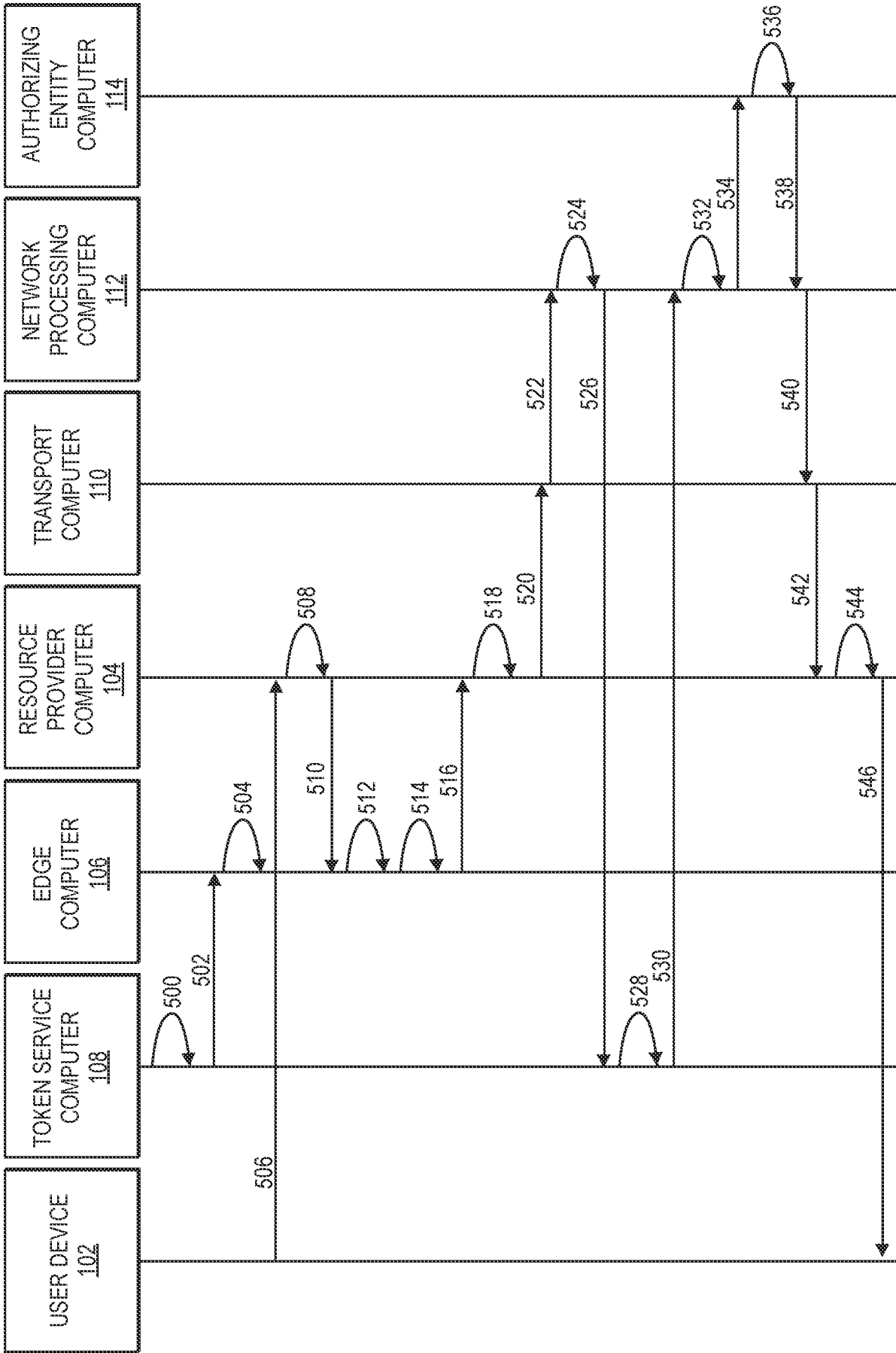


FIG. 5

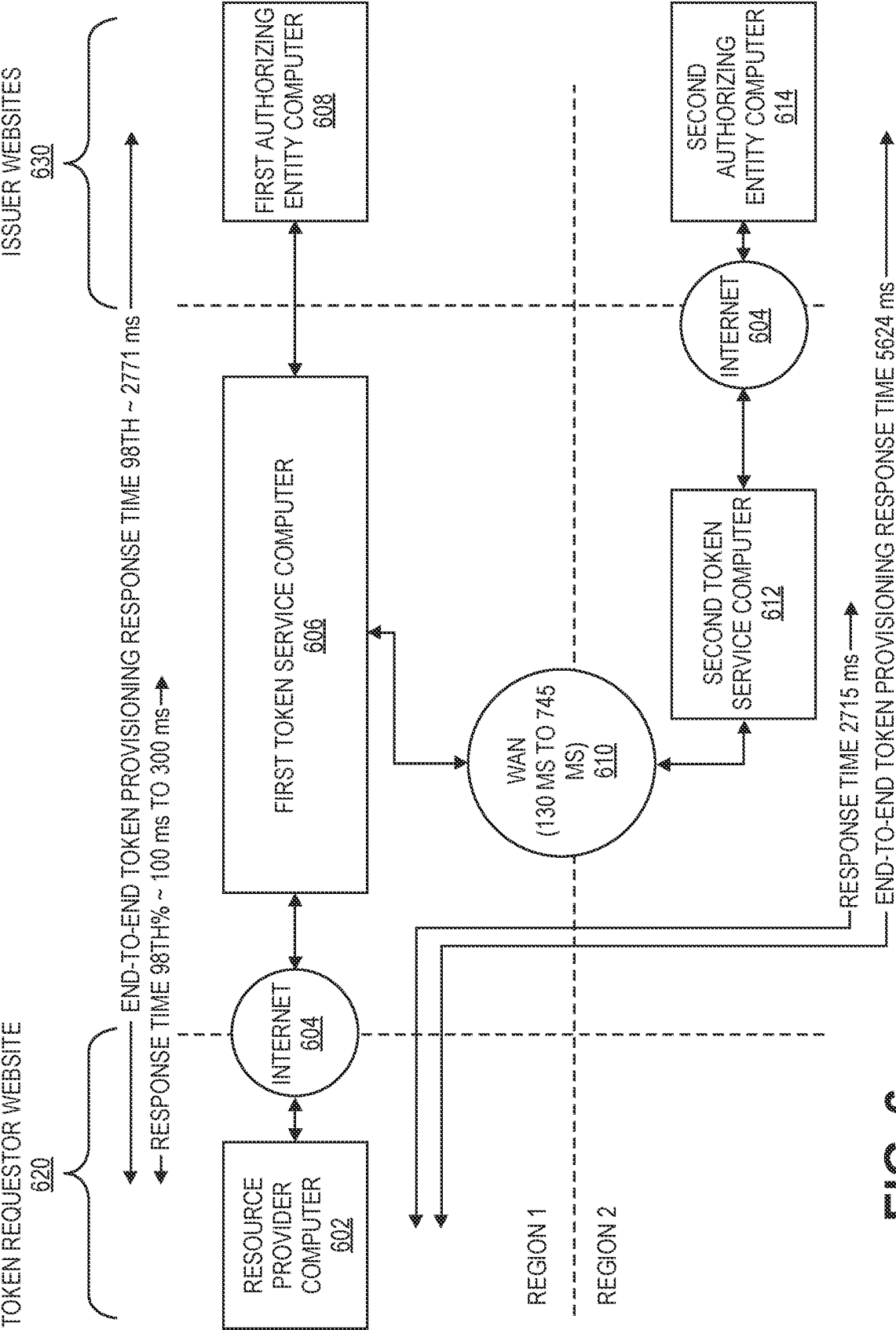


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2023/069103

A. CLASSIFICATION OF SUBJECT MATTER**H04L 9/32**(2006.01)i; **H04L 67/289**(2022.01)i

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)

H04L 9/32(2006.01); H04L 12/721(2013.01); H04L 12/741(2013.01); H04L 29/06(2006.01); H04L 29/08(2006.01);
H04L 9/08(2006.01); H04L 9/40(2022.01); H04W 12/06(2009.01); H04W 12/084(2021.01)

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: edge computer, token, resource provider, interact, credential

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2019-0007306 A1 (FUJITSU LIMITED) 03 January 2019 (2019-01-03) paragraphs [0046], [0049], [0059], [0138]; and figures 2-5, 19A	1-20
Y	US 2020-0084202 A1 (NED M. SMITH et al.) 12 March 2020 (2020-03-12) paragraphs [0144], [0153], [0215]-[0216]; and figures 3, 8-9, 14	1-20
Y	US 2022-0329414 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 13 October 2022 (2022-10-13) paragraphs [0026]-[0027], [0030], [0043], [0057], [0073]-[0074], [0082], [0096], [0115], [0120]-[0121], [0127]-[0129]; and figures 1, 3, 7-10	4-13,16-17,19-20
Y	US 2019-0373016 A1 (CLOUDFLARE, INC.) 05 December 2019 (2019-12-05) paragraphs [0033], [0036], [0042]	14
A	WO 2023-031037 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 09 March 2023 (2023-03-09) pages 7-17	1-20

☐ 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

25 March 2024

Date of mailing of the international search report

25 March 2024

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon
35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

KIM, Sung Hee

Telephone No. +82-42-481-3516

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/US2023/069103

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2019-0007306	A1	03 January 2019	JP	2019-012982	A	24 January 2019
				JP	6926734	B2	25 August 2021
				US	10785147	B2	22 September 2020
US	2020-0084202	A1	12 March 2020	US	11425111	B2	23 August 2022
US	2022-0329414	A1	13 October 2022	CN	114270780	A	01 April 2022
				EP	4022871	A1	06 July 2022
				EP	4022871	A4	02 November 2022
				WO	2021-040784	A1	04 March 2021
US	2019-0373016	A1	05 December 2019	US	10911485	B2	02 February 2021
WO	2023-031037	A1	09 March 2023	None			