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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 January 2024 (04.01.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/005898 A1

(51) International Patent Classification:
*G06Q 20/34* (2012.01) *G06Q 20/40* (2012.01)
*G06Q 20/38* (2012.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2023/019576

(22) International Filing Date:
24 April 2023 (24.04.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2209451.0 28 June 2022 (28.06.2022) GB

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors: **NOE, James, Christian**; 50 Wickham Chase, West Wickham, Kent BR4 0BL (GB). **DELCROIX, Thierry**; Flat 303, Bluewater, House Smugglers Way, London SW18 1EB (GB). **TIERNEY, John**; 7 Highfields Heswall, Wirral, Merseyside CH60 7TF (GB).

(74) Agent: **KLOCINSKI, Steven**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (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,

(54) Title: SECURELY AND EFFICIENTLY USING TOKENISED VCNS ON ELECTRONIC DEVICES, AND IN E-COMMERCE PLATFORMS

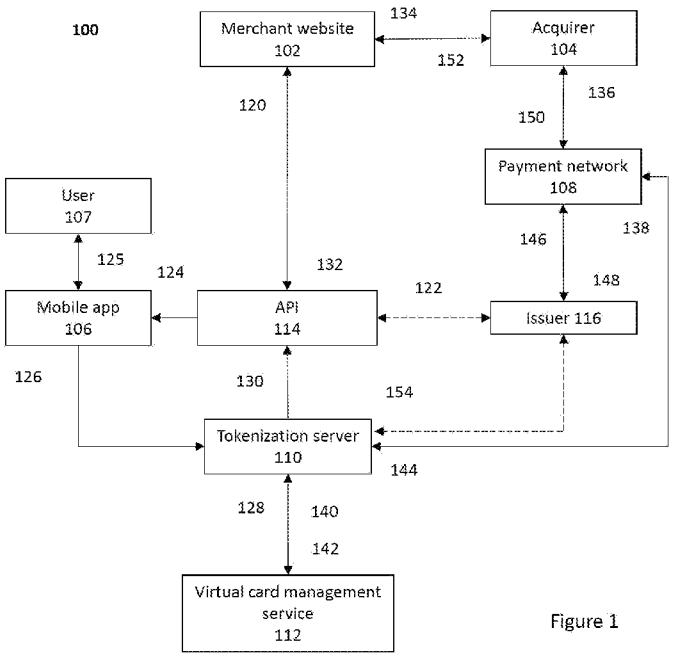


Figure 1

(57) Abstract: Broadly speaking, the present invention provides a technical solution by which virtual cards can be leveraged to become tokens generated by the payment platform and coupled with dynamic cryptography to enhance security, reliability, performances, user experience and reduce latency during the transactional flow. This technical solution advantageously ensures that transactions are simplified for implementation, while being efficient in terms of BIN and PAN usages, and having minimal latency, resulting in simpler integration and faster transactions. Additionally, the present invention requires relatively little change to the configuration of the computing devices that collectively function to enable the transaction to take place (e.g. payment network computing devices, merchant computing devices). Furthermore, the invention can improve the security around use of virtual cards as it enables a dynamic cryptogram to be used rather than a relatively insecure static cryptogram.

WO 2024/005898 A1

*[Continued on next page]*

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, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Published:**

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

# SECURELY AND EFFICIENTLY USING TOKENISED VCNS ON ELECTRONIC DEVICES, AND IN E-COMMERCE PLATFORMS

## CROSS REFERENCE TO RELATED APPLICATION

This application claims the benefit of United Kingdom Patent Application No. 2209451.0, which was filed on June 28, 2022, the entire contents of which are hereby incorporated by reference for all purposes.

## FIELD OF INVENTION

This invention relates generally to the use of virtual cards and virtual card numbers on electronic devices and more particularly on an electronic commerce platform.

## BACKGROUND

Virtual card numbers are a convenient way to make debit/credit card purchases online. They allow you to shop online without giving merchant your actual card number. Thanks to virtual card numbers, the consumer can shop online faster and more securely. The virtual numbers are still linked to a debit/credit/prepaid card account, but they allow consumers to use a different number to fill out payment information when they shop online.

Security is increased while using a Virtual Card, because the actual debit/credit card is never provided to any websites wherever the consumer shops. If a risk of fraud has been found on any of these websites, the debit/credit card will never be compromised. For this type of card, consumers may opt to create them for a specific transaction, for a single use, for a specific time period, or keep the virtual card indefinitely, until such time as they wish to delete it.

Virtual cards can also be used by corporations. For example, a manager may want to send one of their team on a business trip, and provide them with a specific budget. The manager may issue a virtual card to the employee that has limited use (e.g. limited to travel merchants and hotels only), limited budget, and a limited timespan.

However, in certain payment platforms it is currently only possible to use virtual cards for certain types of e-commerce transactions (a.k.a. card not present transactions). It is not always viewed as technologically efficient to tokenize a Virtual Card Number, VCN, since this creates multiple representations of the underlying card

number, and there may be challenges in ensuring the correct acceptance of the VCN's token in all of the relevant acceptance environments. As a result, dynamic cryptograms cannot be used for contactless and e-commerce transactions involving virtual cards.

Tokens, issued and maintained by a payment network service such as the 'Mastercard Digital Enablement Service' (MDES) provided by the assignee, are card numbers that mobile devices use in place of the card number printed on the physical card. As used herein, references to the Mastercard Digital Enablement Service (MDES), an example of a payment platform, are understood to refer to a collection of computer-implemented services that transform any connected device into a commerce device to make and receive payments. These tokens are not exposed to the end-users (only the last 4 digits are displayed on the graphic representation of the cards into the mobile payment wallet). Therefore, if an issuer wanted to utilise a service such as MDES with virtual cards, the consumer would potentially have multiple identifiers for different transaction types and a complex back-end solution would be needed. It would result in three different identifiers being used for a transaction: the token; the virtual card number; and the funding primary account number. This is complex to implement and adds significant latency to the transaction. It is furthermore inefficient, particularly in terms of bank identification number (BIN) and primary account number (PAN) usages, as well as cryptographic keys. Having three different identifiers in a transaction would have double mapping, which would require a large number of different PANs, BINs, and account ranges. Double mapping causes complications from an issuing and maintenance perspective and also adds significant latency to transactions. Particularly, the increased latency may be more visible during the processing phase of the transaction, when the data would have to be re-mapped twice – from the token to a virtual card number, and then from this virtual card number to the corresponding funding payment account number that is the entity actually funding the transaction. Alternatively, the MDES token would have to be exposed to the user in order to be entered for e-commerce on a merchant site, unless the merchant site has in-application transaction support. This is an issue because the back end MDES tokens should never been seen by the consumer for security reasons.

There is thus a need for techniques to implement virtual cards while using payment network services such as MDES.

SUMMARY OF THE INVENTION

In a first aspect, the invention provides a computer-implemented method for enabling use of virtual cards in e-commerce transactions, the method performed by a tokenization server. The method comprising receiving, from a user device, a transaction request corresponding to a transaction with a merchant, generating a virtual card number, VCN, which corresponds to a virtual card, generating and storing a cryptogram specific to the transaction with the merchant, providing the VCN to the merchant, obtaining an underlying funding primary account number, FPAN, of the virtual card, retrieving the cryptogram, checking the validity of the cryptogram, and providing an indication to the merchant if the cryptogram is valid or not valid.

In one embodiment of the first aspect, providing the VCN to the merchant further comprises transmitting the VCN to an API which transmits the VCN to the merchant.

In one embodiment of the first aspect, providing the VCN to the merchant further comprises providing the VCN to the user device for display to a user who manually transfers the VCN to the merchant.

In one embodiment of the first aspect, obtaining an underlying funding primary account number, FPAN, of the virtual card further comprises receiving the FPAN of the virtual card from a virtual card management service.

In one embodiment of the first aspect, the virtual card management service retrieves the FPAN by querying a database with the VCN to return the FPAN.

In one embodiment of the first aspect, when the cryptogram is not valid, a response declining authorisation is provided to the merchant via an acquirer.

In one embodiment of the first aspect, when the cryptogram is valid, the cryptogram is provided to the merchant with a virtual card management service which performs further checks.

In one embodiment of the first aspect, the further checks comprise one or more of determining whether the transaction is within a pre-configured timeframe, the transaction is at an allowed merchant and/or merchant category, the transaction amount is within a specified range, the transaction is for a specific amount, the aggregate of spend with the virtual card is less than or equal to a specified amount, the aggregate spend with the virtual card by merchant and/or merchant category is within a specified amount, the spend and/or aggregate spend with the virtual card at a

merchant/merchant category is within a specified amount and within a specified time period.

In one embodiment of the first aspect, it is determined whether the further checks result in the transaction being declined or allowed with an alert.

In one embodiment of the first aspect, the VCN is an alphanumeric string.

In one embodiment of the first aspect, checking the validity of the cryptogram further comprises one or more of, checking that a time of the cryptogram is valid, checking that a transaction amount and currency matches the amount and currency at the merchant, and checking a channel the cryptogram is being used for is correct.

In a second aspect, the invention provides a tokenization server configured to perform the method of the first aspect.

In a third aspect, the invention provides a computer-readable medium comprising instructions which, when executed by a processor, cause the processor to perform the method of the first aspect.

Broadly speaking, the present invention provides a technical solution by which virtual cards can act as tokens. Also the invention would allow the consumer to generate cryptograms for a given transaction by using their consumer facing application while using a service such as MDES. Consumer facing applications may be applications that directly interact with consumers and may be used by consumers to connect and engage with businesses (e.g., mobile applications or customer portals). This technical solution advantageously ensures that transactions are simplified for implementation, while being efficient in terms of BIN and PAN usages, and having minimal latency, resulting in simpler integration and faster transactions. Additionally, the present invention requires relatively little change to the configuration of the computing devices that collectively function to enable the transaction to take place (e.g. payment network computing devices, merchant computing devices). Furthermore, the invention can improve the security around use of virtual cards as it enables a dynamic cryptogram to be used rather than a relatively insecure static cryptogram. The present invention can also improve the user experience of the consumers using virtual card numbers (VCNs), if the merchants have integrated to a new API provided by MDES. The token and cryptogram, generated by MDES, could be directly passed on to the merchants for each transaction, minimizing efforts to

consumers and eliminating errors caused by mis-keying, incorrect copying, or other such user input errors.

## BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention are described below, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 illustrates in schematic form a system suitable for implementing aspects of the invention;

Figure 2 illustrates in schematic form a system suitable for implementing aspects of the invention; and

Figures 3 is a flow diagram setting out the method performed by a tokenization server according to an embodiment.

## DETAILED DESCRIPTION

In the following description aspects of the invention are at times described in the context of electronic payments. It will be appreciated however that the invention has application in any context outside of electronic payments where the use of virtual cards is required. The invention thus should not be limited in this regard.

As used herein, the term "Virtual Card Number" (VCN) is an alphanumeric (typically a 13-19 digit card number) identifier which has a format which is identifiable by a card network such as those networks implemented by Mastercard for the purpose of switching and otherwise processing transactions that rely on such numbers to identify the party making (or receiving) a payment, but which is never associated with a specific physical payment instrument (such as by appearing on the face of a payment card or being encoded on a chip or magnetic stripe of such a card). For example, a virtual card number may be a primary account number (PAN) in which some of the digits are a bank identification number (BIN) (also called an issuer identification number, IIN) used by the card network to identify and route a transaction authorisation request to the issuer of the virtual card number.

VCN details may include any one or more of, for example, the card number, an expiry date, a Card Verification Code (CVC), cardholder name and address details, a purchase type, a transaction amount, a transaction type (Single or Multi use), currency, supplier details, email instructions and validity period details.

Further details such as a sort-code number may be provided, or indeed fewer details may be provided.

Virtual card numbers are often used in situations in which a consumer may not trust a merchant, and wants a VCN that is only valid for one single transaction. Alternatively, the user of the VCN may have been provided it by their employer for a specific use, and may be for a limited set of merchants, merchant categories, or time period. VCNs can be limited-use or even single-use, which has significant benefits when it comes to control and security. Should the details of a VCN be misappropriated, the subsequent use of those details is mitigated or even prevented, e.g. by disabling or deleting the virtual card. Further restrictions can be placed on the use of VCNs. For example, where the VCN details include information relating to a supplier, the VCN may be restricted such that it may only be used with that particular supplier or class of suppliers. There may also be restrictions on the amount available to spend in any given transaction. Finally there may also be restrictions on how long the VCN is valid for (e.g. an employer may make it valid only for the duration of a planned business trip). Restrictions may instead be based on other components of the VCN details or combinations thereof.

A company may want to issue a VCN to an employee for a specific use and period of time (e.g. a business trip up to £4,000 valid from 14 June to 30 August, only valid in hotels, airlines, taxis etc…). VCNs currently can only easily be used online (e.g. typed into an e-commerce site), but the use in face-to-face (e.g. hotels, taxis etc…) is challenging. A payment platform like MDES could solve this by creating a token on a device, however the payment platform cannot create a token that can be used in 'traditional' e-commerce - as the payment platform token must not be shown to the user, but the user needs the token PAN (e.g. VCN) to make the transaction.

As used herein, references to a virtual card management system (such as the Mastercard Purchase Control™ system/Mastercard inControl™ system) are understood to refer to VCN-based payment systems. A well-known example of a VCN-based commercial payment system is the Mastercard Purchase Control™ system/Mastercard inControl™ system. Web-based systems such as these enable organisations to provide their employees with limited-use VCNs with which transactions can be performed, instead of providing employees with physical

purchasing cards. This improves the control, efficiency, compliance and security of transactions.

An organisation utilising a VCN-based payment system can create unique rules for each employee using the system. For example, an administrator may provide a custom set of rules for each employee. Alternatively, a blanket set of rules for the whole organisation may be created. Should one or more of the transaction parameters exceed the limits of the relevant pre-defined rules, the transaction request may either be automatically rejected or the request may be held while an administrator is notified. The administrator can then as a secondary input perform a manual analysis of the transaction request and either reject or approve the transaction request.

As used herein, references to a payment platform (such as the Mastercard Digital Enablement Service (MDES) platform) are understood to refer to a collection of computer-implemented services that transform any connected device into a commerce device to make and receive payments. The platform helps power user devices to enable secure payments to take place for contactless, e-commerce, and in-app payments. The platform validates a transaction, maps from the token back to the PAN and forwards it to the issuer for authorization. The MDES platform as described herein may additionally or alternatively be a token vault or tokenization platform.

As used herein, the Funding Primary Account Number (FPAN) means the primary account number of a payment account that is to be used to supply funds to pay for a transaction. The FPAN may appear on a physical card (or similar device). The FPAN may also be referred to as a real card number (RCN), which may be the same as the PAN described above. The RCN is the term that is typically used when referring to VCN platforms, and the FPAN is the term that is typically used when referring to tokenization platforms, however they both refer to the underlying PAN that is to be used for the purchase.

As used herein, authentication refers to the process by which a user is able to prove that they are who they purport to be. Typically, the user provides more than one of something they know (e.g. a PIN or passcode), and/or something they are (e.g. biometric information) and/or something they have (e.g. a smart card) in order to prove that they are who they purport to be and hence authenticate themselves with a party requesting the authentication.

Figure 1 shows a block diagram of a system 100 suitable for implementing embodiments of the invention. System 100 includes a merchant

website 102 that is communicatively coupled 120 to an application programming interface (API) 114, e.g. via a public network such as the internet, or a private network or virtual private network, or combination thereof. Here, 'communicatively coupled' in the context of an API means that the relevant components which support the API can hence communicate with one another via the API. The merchant website 102 may be an e-commerce website. The API 114 is also communicatively coupled 122 with an issuer computer 116. Alternatively (and not shown), another third party directory service may help facilitate this lookup. The API 114 is further communicatively coupled 124 to a mobile application 106 (e.g., a consumer facing application, a customer portal, etc.) on a user device (e.g., a smartphone, laptop, desktop computer, tablet, gaming console, smart TV, wearable, etc.). A user 107 of the user device communicates 125 with the mobile application 106 via the user device. The user 107 of the user device is a consumer. The mobile application 106 on the user device is further communicatively coupled 126 with a tokenization server 110 (e.g. a tokenization service provided by the MDES platform), which itself communicates 128, 140, 142 with a virtual card management service 112 (e.g. the InControl™ service as provided by the applicant). The tokenization server 110 is further communicatively coupled 130 with the API 114. The API 114 is communicatively coupled 132 with the merchant website 102. The merchant website 102 further communicates 134, 152 with an acquirer 104, which itself communicates 136, 150 with a payment network 108. The payment network 108 is communicatively coupled 138, 144 with the tokenization server 110 and communicative coupled 146, 148 with the issuer 116 and the issuer 116 optionally communicates 154 with the tokenization server.

Figure 2 shows a block diagram of another system 200 suitable for implementing embodiments of the invention. System 200 includes a merchant website 202 that is communicatively coupled 220, 232, e.g. via a public network such as the internet, or a private network or virtual private network, or combination thereof, to a mobile application 206 (e.g., a consumer facing application, a customer portal, etc.) on a user device (e.g., a smartphone, laptop, desktop computer, tablet, gaming console, smart TV, wearable, etc.). The merchant website 202 may be an e-commerce website. A user 207 of the user device communicates 225 with the mobile application 206 via the user device. The user 207 of the user device is a consumer. The mobile application 206 on the user device is further communicatively coupled 226, 230 with

a tokenization server 210 (e.g. a security service provided by the MDES platform), which itself communicates 228, 240, 242 with virtual card management service 212 (e.g. the InControl™ service as provided by the applicant). The merchant site 202 further communicates 234, 252 with an acquirer 204, which itself communicates 236, 250 with a payment network 208. The payment network 208 is communicatively coupled 238, 244 with the tokenization server 210 and communicatively coupled 246, 248 with the issuer 216 and the issuer 216 communicates 254 with the tokenization server.

In Figure 1, the merchant website 102 is integrated with the API 114. Whereas in Figure 2, the merchant site 202 is not integrated with an API. While both system 100 and 200 can be used to implement the invention, system 100 offers some advantages relative to system 200. Having the merchant website 102 integrated with the API 114, as in system 100, improves transaction efficiency and speed and user experience when compared with the configuration of system 200. Furthermore, the use of the API 114 allows the merchant website 102 and the mobile application to hide the VCN token and pass a cryptogram through the API 114, improving security.

It will be appreciated that while only one merchant website 102, 202 is shown in Figure 1 and Figure 2, it is not necessary for the user 107, 207 to make use of the same merchant website 102, 202 for each transaction. A user 107, 207 of a user device is the consumer. In some cases the consumer is a legal person e.g. a service-providing corporation, rather than a natural person; in such cases, the merchant website 102, 202 can be a computer operated by, or on behalf of, the corporation. The consumer can be the corporation themselves, e.g. a merchant providing a good or service.

In the embodiment in which the merchant website 102 is integrated with the API 114, the process for making a payment using a VCN can be as follows.
Description of user experience

First the user selects items on a merchant website 102 to buy and proceeds to the checkout on the merchant website 102. The user may select the option of paying with their banking mobile application.

The merchant website 102 displays the transaction amount to the user. The merchant website 102 may additionally display the transaction currency, shipping details, taxes, and other standard checkout items to the user.

The merchant website 102 gives the user the option to use a virtual card. For example, this may be a button, a new branded program, a specific checkout option or some other way to clearly guide the consumer to the right checkout experience.

An API 114 performs a re-direct or push of the transaction details, such as the merchant name, transaction amount and transaction currency, to the mobile application 106.

Optionally, a call is made to the issuer 116 to route the re-direct or push of the transaction details to the correct mobile application 106. Alternatively, a lookup service may help route the user to the right application.

The user opens the mobile application 106 and authenticates themselves to the mobile application. Alternatively, the user may already be authenticated on the mobile application.

Assuming the authentication is successful, the transaction details are re-directed or pushed from the merchant website 102 to the mobile application 106 by the API 114. The user confirms that the transactions details are correct. Particularly, that the merchant and the amount in the mobile application 106 match that of the merchant website 102 and the amount at the checkout on the merchant website 102. The user selects the virtual card to be used for payment from a list of possible virtual cards. There may be no physical card associated with the virtual card. There may be multiple virtual cards associated with a single payment account. The virtual card may be single use. The virtual card may be issued to a user as an employee of a company. The virtual card may be restricted in the payments made with it, for example, time limit restrictions, monetary limit restrictions, number of uses restrictions, and/or merchant restrictions.

Alternatively, if a VCN already exists (e.g. from a prior transaction made with the mobile application 106), the transaction details are automatically pre-entered in the mobile application 106. The user validates the pre-entered transaction details and selects the VCN which has already been generated by the tokenization server 110.

Optionally, the user device generates a cryptogram specific to the transaction in the mobile application 106. The cryptogram specific to the transaction generated by the user device in the mobile application 106 is sent to the tokenization server 110 at step 308 for processing and/or validation, as detailed below. This is a

dynamic cryptogram that changes for each transaction, for each VCN, for each transaction amount etc.. This means that the cryptogram is valid for use only with a single transaction, improving security by preventing attacks such as replay attacks.

The tokenization server 110 then proceeds to carry out step 302, as detailed below.

In the embodiment in which the merchant website 202 is not integrated with an API 114, the process for making a payment using a VCN can be as follows.

First the user selects items on a merchant website 202 to buy and proceeds to the checkout on the merchant website 202.

The merchant website 202 displays the transaction amount to the user. The merchant website 202 may additionally display the transaction currency, shipping details, taxes, and other standard checkout items to the user.

The merchant website 202 gives the user the option to use a virtual card. For example, this may be a button, a new branded program, a specific checkout option or some other way to clearly guide the consumer to the right checkout experience. Alternatively, the merchant website 202 is not changed from a standard checkout experience and the user checks out as normal, but uses their virtual card as describe below.

The user opens the mobile application 206 and authenticates themselves to the mobile application. Alternatively, the user may already be authenticated on the mobile application.

Assuming authentication is successful, the user selects the virtual card to be used for payment on the mobile application 206 from a list of possible virtual cards. There may be no physical card associated with the virtual card. There may be multiple virtual cards associated with a single payment account. The virtual card may be single use. The virtual card may be issued to a user as an employee of a company. The virtual card may be restricted in the payments made with it, for example, time limit restrictions, monetary limit restrictions, number of uses restrictions, and/or merchant restrictions. The user enters the transaction amount and currency from the merchant website 202 into the mobile application 206. Optionally, the user also enters the merchant website 202 details into the mobile application 206.

The user confirms that the merchant and the transaction amount and currency in the mobile application 206 match that of the merchant website 202 and the amount and currency at the checkout on the merchant website 202.

Optionally, the user device generates a cryptogram specific to the transaction in the mobile application 206. The cryptogram specific to the transaction generated by the user device in the mobile application 206 is sent to the tokenization server 210 at step 308 for processing and/or validation, as detailed below. This is a dynamic cryptogram that changes each transaction. This means that the cryptogram is valid for use only with a single transaction, improving security by preventing attacks such as replay attacks. Alternatively, the tokenization server 210 may generate the cryptogram, and store it for later validation.

The tokenization server 210 then proceeds to carry out step 302, as detailed below.

Figure 3 sets out a method for use of VCNs in e-commerce transactions. The method of Figure 3 can be performed by a tokenization server 110, 210 such as the Mastercard Digital Enablement Service (MDES).

In step 302, the tokenization server 110, 210 receives a transaction request corresponding to the transaction with the merchant website 102, 202 from the mobile application 106, 206 on the user device as discussed above.

In step 304, the tokenization server 110, 210 generates a virtual card number (VCN) which corresponds to a virtual card selected to be used for payment and has no correspondence to any physical payment instrument. The use of this VCN makes merchant integration easier and it is possible to use this VCN in e-commerce transactions, transactions using mobile-device wallets, etc.

Alternatively to step 304, in step 306 the virtual card management service 112, 212 generates a virtual card number (VCN) and transmits it to the tokenization server 110, 210. Currently, VCNs are usually generated by the payment network owning the BINs of the FPAN. By having the tokenization server 110, 210 or the virtual card management service 112, 212 generate the VCN, the need to use three different identifiers (a token, a virtual card number and a funding primary account number) during a transaction is removed. Instead, only the VCN and the FPAN/RCN are used, as the VCN acts as in place of a token. This is more efficient, simpler to implement and reduces latency of the transaction, resulting in simpler integration and faster transactions, as well as increased security. Furthermore, back end tokens (e.g. MDES tokens) cannot be exposed to a user, so unlike the present VCN, cannot be entered into a merchant site for an e-commerce transaction. The mapping of the VCN to the actual account number may be known to the tokenization

server which operates a token vault securely storing the mapping, the merchant, and the acquirer. The issuer may build up a mapping of VCNs and/or tokens to FPANs through notification of the token and FPAN in an authorisation request. The VCN may have the same format as the actual account number, and thus be recognised by the payment network as an account identifier that can be used in a transaction.

Optionally, once the tokenization process is complete, the tokenization server 110, 210 sends the issuer 116, 216 a notification network message that the tokenization process has been completed. If the issuer opted in to receive this network message, this completes the tokenization process.

In step 308, the tokenization server 110, 210 generates a cryptogram specific to the transaction with the merchant website 102, 202 and then stores the generated cryptogram for processing and/or validation. Alternatively to step 308, in step 310 a cryptogram specific to the transaction is received by the tokenization server 110, 210 from the mobile application 106, 206 and stored by the tokenization server 110, 210 for processing and/or validation. This cryptogram is generated by the mobile application 106 on the user device. This adds extra security to the transaction, as the same entity is not both generating the cryptogram and verifying the transaction. In either case above the cryptogram is dynamic as it changes from transaction to transaction, improving the security around use of virtual cards.

In step 312, the tokenization server 110, 210 provides the VCN to the merchant website 102, 202.

In the embodiment in which the merchant website 102 is integrated with the API 114, the tokenization server 110 can provide the VCN to the merchant website 102 via the API 114, for future use. The merchant website 102 receives the VCN details. No information has to be entered into the merchant website 102 manually.

In the embodiment in which the merchant site 202 is not integrated with an API 114, the tokenization server 210 can provide the VCN to the merchant website 202, for future use, by providing the VCN to the user via the mobile application 206. The VCN is displayed to the user in the mobile application 206. The user manually enters the VCN details displayed on the mobile application 206 onto the merchant site 202 checkout page. Alternatively, the user may transfer the VCN details displayed on the mobile application 206 onto the merchant site 202 checkout page via NFC Mobile to Mobile, Mobile to Terminal, using 3D Bar Codes, Bluetooth,

Bluetooth Low Energy, copy and paste, manual key entry, or any other transfer method.

The merchant website 102, 202 generates a transaction request and transmits the transaction request to the acquirer 104, 204. The transaction request may include details such as the VCN, the checkout amount, and the merchant details. In the embodiment in which the merchant website 102 is integrated with the API 114, the transaction request may further include the cryptogram. The acquirer 104, 204 receives the transaction request and generates an authorisation request. The payment network 108, 208 processes the authorisation request as part of the authorisation process and forwards it on to the tokenization server 110, 210. The tokenization server 110, 210 looks up the underlying funding primary account number (FPAN) of the virtual card from the authorisation request.

In step 316, the tokenization server 110, 210 obtains the underlying funding primary account number (FPAN) of the virtual card from the payment network 108. Optionally, the tokenization server 110, 210 may obtain the FPAN from the virtual card management service 112, 212, e.g. by the virtual card management service using the VCN to look it up in a database.

In step 318, the stored cryptogram specific to the transaction is retrieved by the tokenization server 110, 210.

In step 320, the validity of the retrieved cryptogram is checked. The validity checks may include one or more of checking that the time of the cryptogram is valid (as the cryptogram may only be valid for a limited time to help prevent fraud), checking that the transaction amount and the amount at the checkout on the merchant site checkout match, checking the transaction currency and the currency at the checkout on the merchant site checkout match, and checking the channel the cryptogram is being used for is correct (as the cryptogram may only be valid for a certain channel, for example, e-commerce, CVC2, etc.). The retrieved cryptogram may have been generated by the tokenization server 110, 210. In this embodiment, the cryptogram may use symmetric cryptography, as the cryptogram was generated by the tokenization server 110, 210 and eventually ends back at the tokenization server 110, 210 for validation.

In another embodiment, a digital signature may be used instead of, or in addition to, a cryptogram. The digital signature may use asymmetric cryptography and may be used instead or as well as a cryptogram using symmetric cryptography.

The use of asymmetric cryptography has the benefit for the merchant site being able to verify the cryptogram has been sent by the tokenization server 110, 210, and if not, stop the transaction. This reduces the steps needed in the process. Any entity which has the right Payment System public key could validate that the signature is genuine, giving confidence about the transaction. The digital signature could end up back at the tokenization server 110, 210, to ensure that it has not been tampered with. Alternatively, it could contain a symmetric cryptogram, such as 8-byte MAC, that would be extracted and sent back in the authorisation request for validation.

As a result of the validity check of step 320, in step 321 an indication may be provided to the merchant website 102, 202 detailing if the cryptogram is valid or not valid. The indication may detail that the cryptogram is valid if all of the one or more validity checks completed in step 320 are valid. For example, the time of the cryptogram is valid, the transaction amount and the amount at the checkout on the merchant site checkout match, the transaction currency and the currency at the checkout on the merchant site checkout match, and/or the channel the cryptogram is being used for is correct. The indication may detail that the cryptogram is not valid is any of the one or more validity checks completed in step 320 are not valid. For example, if any one of the time of the cryptogram is not valid, the transaction amount and the amount at the checkout on the merchant site checkout do not match, the transaction currency and the currency at the checkout on the merchant site checkout do not match, and/or the channel the cryptogram is being used for is not correct. The merchant website 102, 202 may process the indication and display an approve or decline response to the user, depending on the validity of the cryptogram.

Alternatively or additionally to step 321, if, as a result of step 320, it is decided that the cryptogram is valid the method may proceed to step 324. In step 324, the tokenization server 110, 210 sends the valid cryptogram to virtual card management service 112, 212 to perform one or more further checks on the virtual card used for the transaction, such as whether the virtual card is being used within any pre-configured timeframe, whether the transaction is at an allowed merchant and/or merchant category, whether the transaction amount is within a specified range, whether the transaction is for a specific amount, whether the aggregate of spend is less than or equal to a specified amount, whether the aggregate spend by merchant and/or merchant category is within a specified amount, whether the spend and/or aggregate spend at a merchant/merchant category is within a specified amount and within a

specified time period (e.g. no more than £100 on clothing in a calendar month), whether these, or any other configured rules are a hard rule (which would typically generate a decline) or a soft rule (which may allow the transaction but trigger an alert). Further checks on the virtual card used for the transaction are not limited to just the above and other further checks may be required depending on the situation.

Alternatively or additionally to step 321, if, as a result of step 320, it is decided that the cryptogram is not valid, the tokenization server 110, 210 may decline the transaction or pass the information on to the issuer 116, 216 that the cryptogram is not valid, so that the issue 116, 216 may make their down authorization decision. Alternatively if, as a result of step 320, it is decided that the cryptogram is not valid the method may proceed to step 322. In step 322, the tokenization server 110, 210 sends the invalid cryptogram to a payment network 108, 208, which returns a declined authorisation response to an acquirer. When step 322 is completed the following steps may follow.

The acquirer 104, 204 receives the decline authorisation response from the payment network 108, 208. The acquirer 104, 204 sends a response to the merchant website 102, 202. The merchant website 102, 202 processes the response and displays a decline response to the user.

As set out above, in step 324 the tokenization server 110, 210 sends the valid cryptogram to virtual card management service 112, 212 to perform the further checks discussed above. When step 324 is completed, the following steps may follow.

If the further checks performed by virtual card management service 112, 212 result in an invalid result, the virtual card management service 112, 212 sends the invalid cryptogram to the payment network 108, 208, which returns a declined authorisation response and sends the declined authorisation response to an acquirer 104, 204.

The acquirer 104, 204 receives the authorisation response from the payment network 108, 208. The acquirer 104, 204 sends a response to the merchant website 102, 202. The merchant website 102, 202 processes the response and displays a decline response to the user.

If the further checks performed by virtual card management service 112, 212 result in a valid result, the virtual card management service 112, 212 sends

the valid cryptogram to the payment network 108, 208, which updates the authorisation request as needed, e.g. with On-Behalf of Services (OBS) results.

The payment network 108, 208 performs any other core processing needed. Other core processing needed may include validating that all mandatory data elements in the request are present and/or validating that all data elements that are present are correctly formatted, regardless of whether they are mandatory, conditional, or optional data elements. The payment network 108, 208 sends an updated authorisation request to the issuer 116, 216 for authorisation. The issuer 116, 216 processes the authorisation request. The issuer 116, 216 creates and sends an authorisation response to the payment network 108, 208. The payment network 108, 208 receives the authorisation response and sends it to the acquirer 104, 204.

The acquirer 104, 204 receives the authorisation response from the payment network 108, 208. The acquirer 104, 204 sends a response to the merchant website 102, 202. The merchant website 102, 202 processes the response and displays an approve response to the user.

It will be appreciated that the processes set out above enable merchant integration to be made easier. These processes also enable a virtual card to have a dynamic cryptogram, further enhancing security.

Having described aspects of the disclosure in detail, it will be apparent that modifications and variations are possible without departing from the scope of aspects of the disclosure as defined in the appended claims. As various changes could be made in the above constructions, products, and methods without departing from the scope of aspects of the disclosure, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

While the disclosure has been described in terms of various specific embodiments, those skilled in the art will recognize that the disclosure can be practiced with modification within the spirit and scope of the claims.

It will be appreciated that the processes described above can be implemented using a computer. Here, 'computer' is understood in the broad sense to refer to any collection of processing resources capable of operating on digital data. This includes traditional physical computers such as laptops, desktop computers, tablets, mobile phones, etc. and also virtual computers such as cloud-based virtual machines, servers, server clusters, and the like.

As used herein, the term "non-transitory computer-readable media" is intended to be representative of any tangible computer-based device implemented in any method or technology for short-term and long-term storage of information, such as, computer-readable instructions, data structures, program modules and sub-modules, or other data in any device. Therefore, any one or more steps of the methods described herein may be encoded as executable instructions embodied in a tangible, non-transitory, computer readable medium, including, without limitation, a storage device, and/or a memory device. Such instructions, when executed by a processor, cause the processor to perform at least a portion of the methods described herein. Moreover, as used herein, the term "non-transitory computer-readable media" includes all tangible, computer-readable media, including, without limitation, non-transitory computer storage devices, including, without limitation, volatile and non-volatile media, and removable and non-removable media such as a firmware, physical and virtual storage, SD cards, memory chips and any other digital source such as a network or the Internet, as well as yet to be developed digital means, with the sole exception being a transitory, propagating signal.

As will be appreciated based on the foregoing specification, the above-described embodiments of the disclosure may be implemented using computer programming or engineering techniques including computer software, firmware, hardware or any combination or subset thereof, wherein the technical effect is enabling the use of VCNs with systems such as a payment platform like MDES. Any such resulting program, having computer-readable code means, may be embodied or provided within one or more computer-readable media, thereby making a computer program product, i.e., an article of manufacture, according to the discussed embodiments of the disclosure. The article of manufacture containing the computer code may be made and/or used by executing the code directly from one medium, by copying the code from one medium to another medium, or by transmitting the code over a network.

CLAIMS

1. A computer-implemented method for enabling use of virtual cards in e-commerce transactions, the method performed by a tokenization server (110), the method comprising:

receiving (126, 226, 302), from a user device, a transaction request corresponding to a transaction with a merchant (102);

generating (304) a virtual card number, VCN, which corresponds to a virtual card;

generating and storing (308) a cryptogram specific to the transaction with the merchant (102);

providing (312) the VCN to the merchant (102);

obtaining (316) an underlying funding primary account number, FPAN, of the virtual card;

retrieving (318) the cryptogram;

checking (320) the validity of the cryptogram; and

providing (321) an indication to the merchant (102) if the cryptogram is valid or not valid.

2. The computer-implemented method of claim 1, wherein providing (312) the VCN to the merchant (102) further comprises:

transmitting the VCN to an API (114) which transmits the VCN to the merchant (102).

3. The computer-implemented method of claim 1, wherein providing (312) the VCN to the merchant (102) further comprises:

providing the VCN to the user device for display to a user who manually transfers the VCN to the merchant (102).

4. The computer-implemented method of any preceding claim, wherein obtaining (316) an underlying funding primary account number, FPAN, of the virtual card further comprises:

receiving the FPAN of the virtual card from a virtual card management service (112).

5. The computer-implemented method of claim 4, wherein the virtual card management service retrieves the FPAN by querying a database with the VCN to return the FPAN.

6. The computer-implemented method of any preceding claim, wherein when the cryptogram is not valid, a response declining authorisation is provided to the merchant (102) via an acquirer (104).

7. The computer-implemented method of any preceding claim, wherein when the cryptogram is valid, the cryptogram is provided to the merchant (102) with a virtual card management service (112) which performs further checks.

8. The computer-implemented method of claim 7, wherein the further checks comprise one or more of determining whether:

the transaction is within a pre-configured timeframe;

the transaction is at an allowed merchant and/or merchant category;

the transaction amount is within a specified range;

the transaction is for a specific amount;

the aggregate of spend with the virtual card is less than or equal to a specified amount;

the aggregate spend with the virtual card by merchant and/or merchant category is within a specified amount;

the spend and/or aggregate spend with the virtual card at a merchant/merchant category is within a specified amount and within a specified time period.

9. The computer-implemented method of claim 8, wherein it is determined whether the further checks result in the transaction being declined or allowed with an alert.

10. The computer-implemented method of any preceding claim, wherein the VCN is an alphanumeric string.

11. The computer-implemented method of any preceding claim, wherein checking (320) the validity of the cryptogram further comprises one or more of:

checking that a time of the cryptogram is valid;

checking that a transaction amount and currency matches the amount and currency at the merchant; and

checking a channel the cryptogram is being used for is correct.

12. A tokenization server configured to perform the method of any one of claim 1 to 11.

13. A computer-readable medium comprising instructions which, when executed by a processor cause the processor to perform the method of any one of claims 1 to 11.

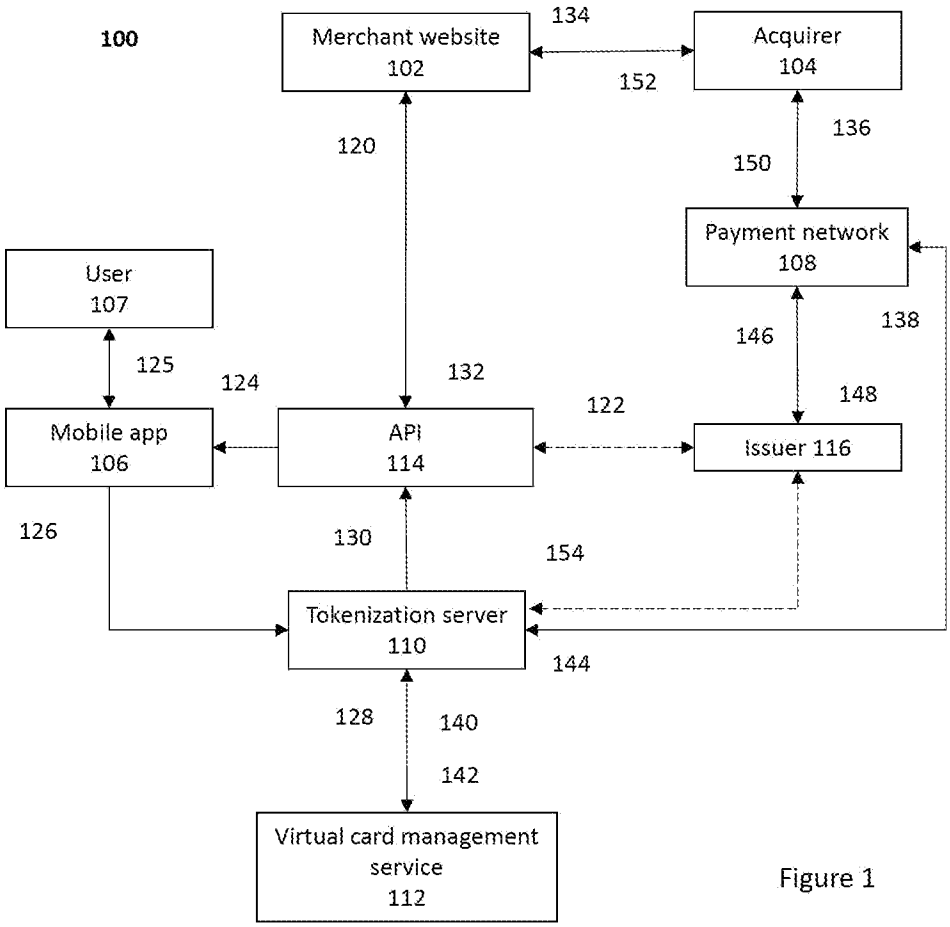
100
Merchant website
102
134
152
Acquirer
104
120
136
150
Payment network
108
User
107
138
146
125
124
132
148
122
Mobile app
106
API
114
Issuer 116
126
130
154
Tokenization server
110
144
128
140
142
Virtual card management service
112

Figure 1

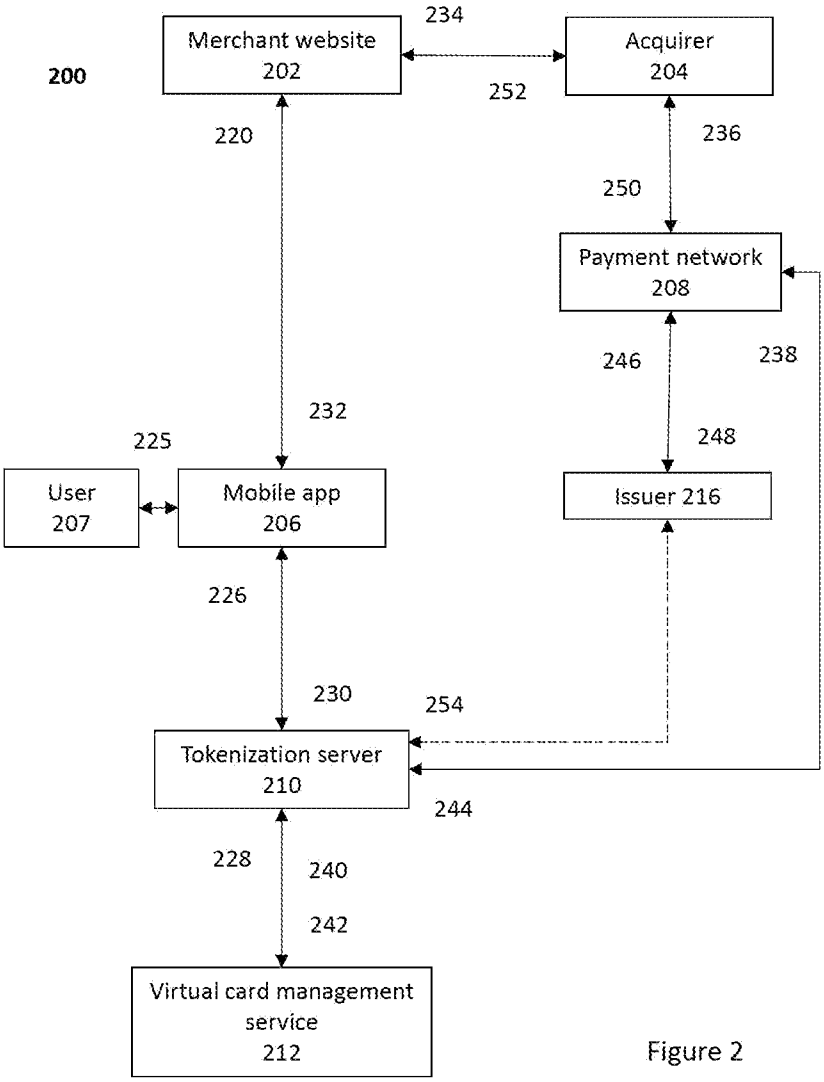
200
Merchant website
202
234
252
Acquirer
204
220
236
250
Payment network
208
246
238
232
225
248
User
207
Mobile app
206
Issuer 216
226
230
254
Tokenization server
210
244
228
240
242
Virtual card management
service
212

Figure 2

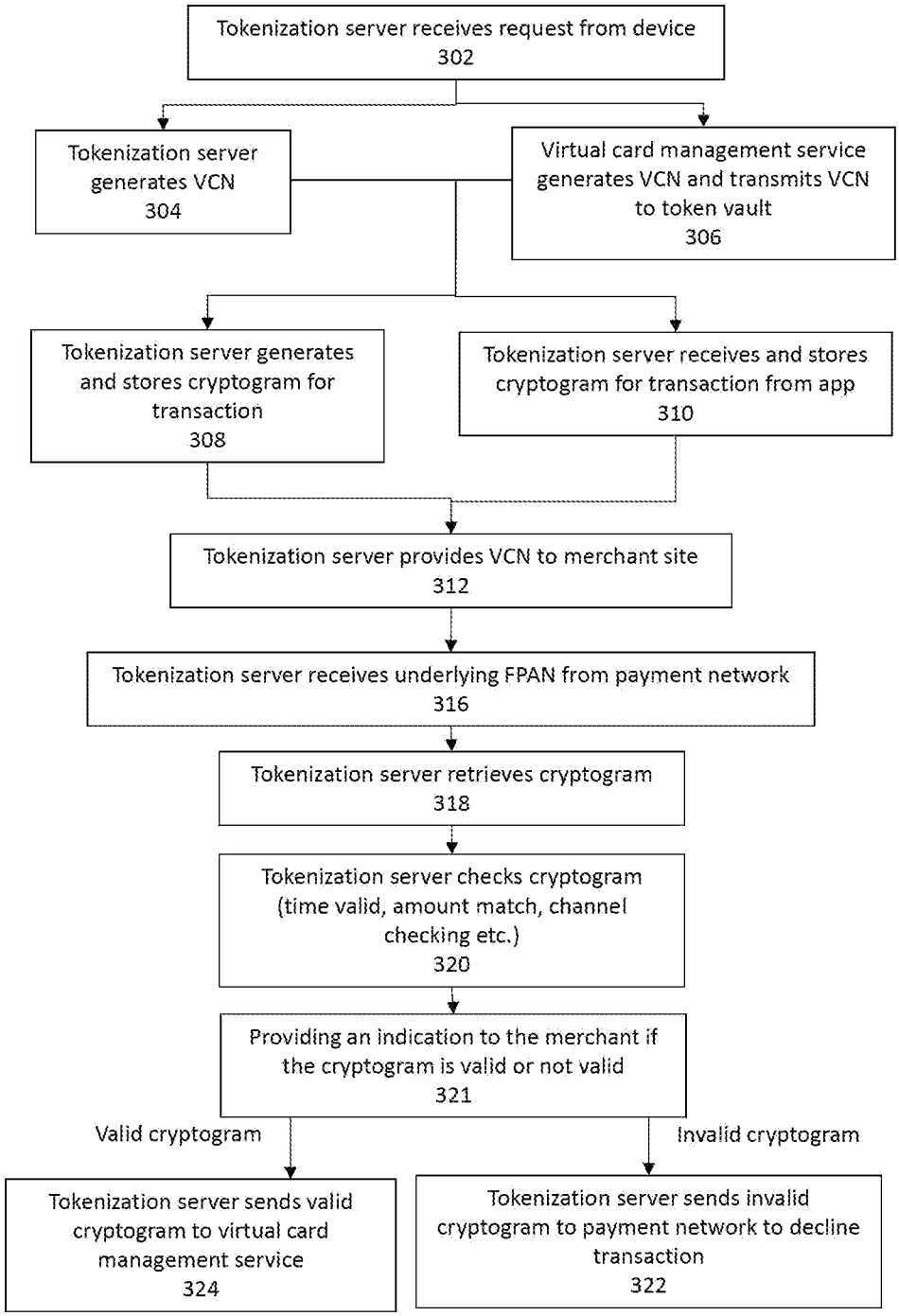
Tokenization server receives request from device
302
Tokenization server generates VCN
304
Virtual card management service generates VCN and transmits VCN to token vault
306
Tokenization server generates and stores cryptogram for transaction
308
Tokenization server receives and stores cryptogram for transaction from app
310
Tokenization server provides VCN to merchant site
312
Tokenization server receives underlying FPAN from payment network
316
Tokenization server retrieves cryptogram
318
Tokenization server checks cryptogram (time valid, amount match, channel checking etc.)
320
Providing an indication to the merchant if the cryptogram is valid or not valid
321
Valid cryptogram
Invalid cryptogram
Tokenization server sends valid cryptogram to virtual card management service
324
Tokenization server sends invalid cryptogram to payment network to decline transaction
322

Figure 3

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/US2023/019576**

## A. CLASSIFICATION OF SUBJECT MATTER

**G06Q 20/34**(2012.01)i; **G06Q 20/38**(2012.01)i; **G06Q 20/40**(2012.01)i; **H04L 9/32**(2006.01)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)

G06Q 20/34(2012.01); G06Q 20/36(2012.01); G06Q 20/40(2012.01); G06Q 40/00(2006.01); H04L 9/32(2006.01)

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: tokenization server, virtual card number (VCN), funding primary account number (FPAN), cryptogram, validity

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 2015-0134540 A1 (SALT TECHNOLOGY, INC.) 14 May 2015 (2015-05-14)<br>See paragraphs 41, 117, 124, 135, 176, 179, 184, 187, claims 4, 19 and figure 13. | 1-5 |
| Y | US 2021-0073813 A1 (ENTERSEKT INTERNATIONAL LIMITED) 11 March 2021 (2021-03-11)<br>See claims 1, 3, 7. | 1-5 |
| Y | US 2014-0129435 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 08 May 2014 (2014-05-08)<br>See paragraph 167. | 2 |
| A | US 2014-0019352 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 16 January 2014 (2014-01-16)<br>See the whole document. | 1-5 |
| A | US 10210507 B2 (ALIBABA GROUP HOLDING LIMITED) 19 February 2019 (2019-02-19)<br>See the whole document. | 1-5 |

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| **16 August 2023** | **16 August 2023** |

| Name and mailing address of the ISA/KR | Authorized officer |
|---|---|
| **Korean Intellectual Property Office**<br>**189 Cheongsa-ro, Seo-gu, Daejeon**<br>**35208, Republic of Korea** | **LEE, KANG HA** |
| Facsimile No. **+82-42-481-8578** | Telephone No. **+82-42-481-5003** |

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/US2023/019576**

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☑ Claims Nos.: **8-9**
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

Claims 8-9 are unclear, because they refer to multiple dependent claims 7-8 which do not comply with PCT Rule 6.4(a).

3. ☑ Claims Nos.: **6-7,10-13**
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| US 2015-0134540 A1 | 14 May 2015 | CA 2909081 A1 | 24 October 2013 |
| | | CA 2909081 C | 10 May 2022 |
| | | CN 104603809 A | 06 May 2015 |
| | | CN 104603809 B | 05 July 2019 |
| | | EP 2842092 A1 | 04 March 2015 |
| | | EP 2842092 A4 | 20 January 2016 |
| | | EP 3848874 A1 | 14 July 2021 |
| | | WO 2013-155627 A1 | 24 October 2013 |
| US 2021-0073813 A1 | 11 March 2021 | WO 2019-145905 A1 | 01 August 2019 |
| | | ZA 202105811 B | 28 April 2022 |
| US 2014-0129435 A1 | 08 May 2014 | AU 2013-337340 A1 | 21 May 2015 |
| | | AU 2017-254850 A1 | 23 November 2017 |
| | | AU 2019-264670 A1 | 05 December 2019 |
| | | AU 2022-200201 A1 | 17 February 2022 |
| | | CA 2890335 A1 | 08 May 2014 |
| | | CA 2890335 C | 30 July 2019 |
| | | CA 3044977 A1 | 08 May 2014 |
| | | CA 3044977 C | 21 June 2022 |
| | | CN 104903926 A | 09 September 2015 |
| | | CN 104903926 B | 14 May 2019 |
| | | CN 110245933 A | 17 September 2019 |
| | | HK 1214670 A1 | 29 July 2016 |
| | | JP 2016-500182 A | 07 January 2016 |
| | | JP 2018-028926 A | 22 February 2018 |
| | | JP 2020-042838 A | 19 March 2020 |
| | | JP 6266638 B2 | 24 January 2018 |
| | | JP 6625105 B2 | 25 December 2019 |
| | | JP 6951401 B2 | 20 October 2021 |
| | | KR 10-2015-0082564 A | 15 July 2015 |
| | | KR 10-2018-0108885 A | 04 October 2018 |
| | | KR 10-2039847 B1 | 27 November 2019 |
| | | US 11222329 B2 | 11 January 2022 |
| | | US 2022-0058619 A1 | 24 February 2022 |
| | | WO 2014-071338 A2 | 08 May 2014 |
| | | WO 2014-071338 A3 | 10 July 2014 |
| US 2014-0019352 A1 | 16 January 2014 | AU 2011-203954 A1 | 26 July 2012 |
| | | AU 2011-268026 A1 | 31 January 2013 |
| | | AU 2011-293250 A1 | 21 March 2013 |
| | | AU 2011-316955 A1 | 30 May 2013 |
| | | AU 2011-316955 B2 | 01 December 2016 |
| | | AU 2012-205511 A1 | 18 July 2013 |
| | | AU 2012-217606 A1 | 09 May 2013 |
| | | AU 2012-220669 A1 | 02 May 2013 |
| | | AU 2012-262317 A1 | 19 December 2013 |
| | | AU 2012-278963 A1 | 23 January 2014 |
| | | AU 2012-278963 B2 | 23 February 2017 |
| | | AU 2013-214801 A1 | 25 September 2014 |
| | | AU 2013-214801 B2 | 21 June 2018 |
| | | AU 2013-221323 A1 | 25 September 2014 |
| | | AU 2013-221323 B2 | 08 November 2018 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | | | Publication date (day/month/year) |
|---|---|---|---|---|---|
| | | AU | 2013-277083 | A1 | 22 January 2015 |
| | | AU | 2014-204010 | A1 | 23 July 2015 |
| | | AU | 2014-232707 | A1 | 05 November 2015 |
| | | AU | 2016-201087 | A1 | 10 March 2016 |
| | | AU | 2016-203811 | A1 | 30 June 2016 |
| | | AU | 2016-203811 | B2 | 07 December 2017 |
| | | AU | 2016-204018 | A1 | 07 July 2016 |
| | | AU | 2016-219581 | A1 | 15 September 2016 |
| | | AU | 2016-219582 | A1 | 15 September 2016 |
| | | AU | 2017-200131 | A1 | 02 February 2017 |
| | | AU | 2017-203295 | A1 | 08 June 2017 |
| | | AU | 2017-203341 | A1 | 08 June 2017 |
| | | AU | 2017-210537 | A1 | 17 August 2017 |
| | | AU | 2017-218967 | A1 | 07 September 2017 |
| | | AU | 2017-254844 | A1 | 16 November 2017 |
| | | AU | 2018-201066 | A1 | 08 March 2018 |
| | | AU | 2018-204218 | A1 | 05 July 2018 |
| | | AU | 2018-204218 | B2 | 30 April 2020 |
| | | AU | 2018-204759 | A1 | 19 July 2018 |
| | | AU | 2018-204759 | B2 | 12 March 2020 |
| | | AU | 2018-214967 | A1 | 30 August 2018 |
| | | AU | 2018-247237 | A1 | 01 November 2018 |
| | | AU | 2019-200882 | A1 | 28 February 2019 |
| | | AU | 2019-200882 | B2 | 25 June 2020 |
| | | AU | 2019-202797 | A1 | 16 May 2019 |
| | | AU | 2019-204966 | A1 | 25 July 2019 |
| | | AU | 2019-232775 | A1 | 03 October 2019 |
| | | AU | 2019-240636 | A1 | 24 October 2019 |
| | | AU | 2019-246813 | A1 | 31 October 2019 |
| | | AU | 2019-253898 | A1 | 14 November 2019 |
| | | AU | 2019-275656 | A1 | 02 January 2020 |
| | | AU | 2020-239652 | A1 | 15 October 2020 |
| | | AU | 2021-212099 | A1 | 26 August 2021 |
| | | AU | 2021-229141 | A1 | 30 September 2021 |
| | | AU | 2021-236487 | A1 | 21 October 2021 |
| | | AU | 2021-236489 | A1 | 21 October 2021 |
| | | AU | 2021-261960 | A1 | 02 December 2021 |
| | | AU | 2022-221528 | A1 | 10 November 2022 |
| | | BR | 112013021057 | A2 | 10 November 2020 |
| | | BR | 112013021059 | A2 | 27 October 2020 |
| | | CA | 2635500 | A1 | 22 December 2008 |
| | | CA | 2635500 | C | 17 May 2016 |
| | | CA | 2786264 | A1 | 14 July 2011 |
| | | CA | 2802687 | A1 | 22 December 2011 |
| | | CA | 2802687 | C | 25 September 2018 |
| | | CA | 2809822 | A1 | 01 March 2012 |
| | | CA | 2837208 | A1 | 06 December 2012 |
| | | CA | 2837208 | C | 16 August 2022 |
| | | CA | 2845580 | A1 | 11 September 2014 |
| | | CA | 2846522 | A1 | 15 September 2014 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | | | Publication date (day/month/year) |
|---|---|---|---|---|---|
| | | CA | 2846601 | A1 | 14 September 2014 |
| | | CA | 2864743 | A1 | 22 August 2013 |
| | | CA | 2864743 | C | 25 August 2020 |
| | | CA | 2897145 | A1 | 10 July 2014 |
| | | CA | 2912066 | A1 | 13 May 2016 |
| | | CA | 3014255 | A1 | 22 December 2011 |
| | | CA | 3161647 | A1 | 06 December 2012 |
| | | CA | 3193605 | A1 | 14 September 2014 |
| | | CN | 102645849 | A | 22 August 2012 |
| | | CN | 102645849 | B | 20 May 2015 |
| | | CN | 103038790 | A | 10 April 2013 |
| | | CN | 103038790 | B | 16 November 2018 |
| | | CN | 103299331 | A | 11 September 2013 |
| | | CN | 103635920 | A | 12 March 2014 |
| | | CN | 103718200 | A | 09 April 2014 |
| | | CN | 103765453 | A | 30 April 2014 |
| | | CN | 103765453 | B | 14 August 2018 |
| | | CN | 105144216 | A | 09 December 2015 |
| | | CN | 106803175 | A | 06 June 2017 |
| | | CN | 106803175 | B | 30 July 2021 |
| | | CN | 106803176 | A | 06 June 2017 |
| | | CN | 109118199 | A | 01 January 2019 |
| | | CN | 109460990 | A | 12 March 2019 |
| | | CN | 109461050 | A | 12 March 2019 |
| | | EP | 1829352 | A2 | 05 September 2007 |
| | | EP | 1829352 | A4 | 06 July 2011 |
| | | EP | 1829352 | B1 | 31 January 2018 |
| | | EP | 1829354 | A2 | 05 September 2007 |
| | | EP | 1829354 | A4 | 25 February 2009 |
| | | EP | 1829354 | B1 | 23 January 2019 |
| | | EP | 2521999 | A1 | 14 November 2012 |
| | | EP | 2521999 | A4 | 07 January 2015 |
| | | EP | 2580729 | A2 | 17 April 2013 |
| | | EP | 2580729 | A4 | 13 April 2016 |
| | | EP | 2601632 | A1 | 12 June 2013 |
| | | EP | 2601632 | A4 | 27 April 2016 |
| | | EP | 2678812 | A1 | 01 January 2014 |
| | | EP | 2810242 | A1 | 10 December 2014 |
| | | EP | 2973276 | A1 | 20 January 2016 |
| | | GB | 2505382 | A | 26 February 2014 |
| | | GB | 2523972 | A | 09 September 2015 |
| | | GB | 2523972 | B | 07 October 2020 |
| | | GB | 2581282 | A | 12 August 2020 |
| | | HK | 1213076 | A1 | 24 June 2016 |
| | | IN | 11079DEN2013 | A | 05 June 2015 |
| | | JP | 2012-175106 | A | 10 September 2012 |
| | | JP | 2014-519657 | A | 14 August 2014 |
| | | JP | 2016-524198 | A | 12 August 2016 |
| | | JP | 2018-063729 | A | 19 April 2018 |
| | | JP | 2020-123405 | A | 13 August 2020 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| | | JP 2023-016836 A | 02 February 2023 |
| | | JP 5638550 B2 | 10 December 2014 |
| | | JP 6377125 B2 | 22 August 2018 |
| | | KR 10-1416842 B1 | 08 July 2014 |
| | | KR 10-1903963 B1 | 05 October 2018 |
| | | KR 10-2013-0103512 A | 23 September 2013 |
| | | KR 10-2013-0114633 A | 17 October 2013 |
| | | KR 10-2014-0038473 A | 28 March 2014 |
| | | KR 10-2019-0015588 A | 13 February 2019 |
| | | KR 10-2019-0041539 A | 22 April 2019 |
| | | KR 10-2020-0032753 A | 26 March 2020 |
| | | KR 10-2020-0138828 A | 10 December 2020 |
| | | KR 10-2021-0097840 A | 09 August 2021 |
| | | KR 10-2022-0137795 A | 12 October 2022 |
| | | KR 10-2023-0010808 A | 19 January 2023 |
| | | MX 2007006924 A | 11 February 2008 |
| | | MX 2007006925 A | 23 October 2007 |
| | | MX 2012007926 A | 03 August 2012 |
| | | MX 2013013903 A | 22 July 2014 |
| | | NZ 605666 A | 27 March 2015 |
| | | SG 11201404555 A | 28 August 2014 |
| | | SG 193481 A1 | 30 October 2013 |
| | | SG 193510 A1 | 30 October 2013 |
| | | US 10013423 B2 | 03 July 2018 |
| | | US 10037526 B2 | 31 July 2018 |
| | | US 10096022 B2 | 09 October 2018 |
| | | US 10102516 B2 | 16 October 2018 |
| | | US 10121129 B2 | 06 November 2018 |
| | | US 10154084 B2 | 11 December 2018 |
| | | US 10163121 B2 | 25 December 2018 |
| | | US 10205721 B2 | 12 February 2019 |
| | | US 10210506 B2 | 19 February 2019 |
| | | US 10223684 B2 | 05 March 2019 |
| | | US 10223691 B2 | 05 March 2019 |
| | | US 10223730 B2 | 05 March 2019 |
| | | US 10242358 B2 | 26 March 2019 |
| | | US 10262001 B2 | 16 April 2019 |
| | | US 10296891 B2 | 21 May 2019 |
| | | US 10296895 B2 | 21 May 2019 |
| | | US 10318941 B2 | 11 June 2019 |
| | | US 10320992 B2 | 11 June 2019 |
| | | US 10354240 B2 | 16 July 2019 |
| | | US 10372712 B2 | 06 August 2019 |
| | | US 10419529 B2 | 17 September 2019 |
| | | US 10430381 B2 | 01 October 2019 |
| | | US 10438176 B2 | 08 October 2019 |
| | | US 10500481 B2 | 10 December 2019 |
| | | US 10552824 B2 | 04 February 2020 |
| | | US 10586227 B2 | 10 March 2020 |
| | | US 10614447 B2 | 07 April 2020 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | | | Publication date (day/month/year) |
|---|---|---|---|---|---|
| | | US | 10621611 | B2 | 14 April 2020 |
| | | US | 10672022 | B2 | 02 June 2020 |
| | | US | 10688385 | B2 | 23 June 2020 |
| | | US | 10726439 | B2 | 28 July 2020 |
| | | US | 10755261 | B2 | 25 August 2020 |
| | | US | 10755298 | B2 | 25 August 2020 |
| | | US | 10803449 | B2 | 13 October 2020 |
| | | US | 10825001 | B2 | 03 November 2020 |
| | | US | 10841433 | B2 | 17 November 2020 |
| | | US | 10846670 | B2 | 24 November 2020 |
| | | US | 10846685 | B2 | 24 November 2020 |
| | | US | 10915887 | B2 | 09 February 2021 |
| | | US | 10915917 | B2 | 09 February 2021 |
| | | US | 10983960 | B2 | 20 April 2021 |
| | | US | 11010753 | B2 | 18 May 2021 |
| | | US | 11010756 | B2 | 18 May 2021 |
| | | US | 11023886 | B2 | 01 June 2021 |
| | | US | 11036681 | B2 | 15 June 2021 |
| | | US | 11037138 | B2 | 15 June 2021 |
| | | US | 11062342 | B2 | 13 July 2021 |
| | | US | 11074218 | B2 | 27 July 2021 |
| | | US | 11216468 | B2 | 04 January 2022 |
| | | US | 11288661 | B2 | 29 March 2022 |
| | | US | 11311797 | B2 | 26 April 2022 |
| | | US | 11354649 | B2 | 07 June 2022 |
| | | US | 11354723 | B2 | 07 June 2022 |
| | | US | 11397931 | B2 | 26 July 2022 |
| | | US | 11475436 | B2 | 18 October 2022 |
| | | US | 11532010 | B2 | 20 December 2022 |
| | | US | 11599873 | B2 | 07 March 2023 |
| | | US | 2003-0095646 | A1 | 22 May 2003 |
| | | US | 2005-0008132 | A1 | 13 January 2005 |
| | | US | 2005-0061872 | A1 | 24 March 2005 |
| | | US | 2005-0123112 | A1 | 09 June 2005 |
| | | US | 2005-0229003 | A1 | 13 October 2005 |
| | | US | 2006-0120519 | A1 | 08 June 2006 |
| | | US | 2007-0047703 | A1 | 01 March 2007 |
| | | US | 2008-0165941 | A1 | 10 July 2008 |
| | | US | 2008-0319868 | A1 | 25 December 2008 |
| | | US | 2010-0036743 | A1 | 11 February 2010 |
| | | US | 2010-0254522 | A1 | 07 October 2010 |
| | | US | 2010-0280911 | A1 | 04 November 2010 |
| | | US | 2010-0299221 | A1 | 25 November 2010 |
| | | US | 2010-0299733 | A1 | 25 November 2010 |
| | | US | 2011-0178924 | A1 | 21 July 2011 |
| | | US | 2011-0270693 | A1 | 03 November 2011 |
| | | US | 2012-0123924 | A1 | 17 May 2012 |
| | | US | 2012-0124496 | A1 | 17 May 2012 |
| | | US | 2012-0209677 | A1 | 16 August 2012 |
| | | US | 2012-0209749 | A1 | 16 August 2012 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| | | US 2012-0212715 A1 | 23 August 2012 |
| | | US 2012-0215648 A1 | 23 August 2012 |
| | | US 2012-0215701 A1 | 23 August 2012 |
| | | US 2012-0233073 A1 | 13 September 2012 |
| | | US 2012-0239556 A1 | 20 September 2012 |
| | | US 2012-0317028 A1 | 13 December 2012 |
| | | US 2013-0010941 A1 | 10 January 2013 |
| | | US 2013-0013430 A1 | 10 January 2013 |
| | | US 2013-0013499 A1 | 10 January 2013 |
| | | US 2013-0013510 A1 | 10 January 2013 |
| | | US 2013-0018783 A1 | 17 January 2013 |
| | | US 2013-0024364 A1 | 24 January 2013 |
| | | US 2013-0024371 A1 | 24 January 2013 |
| | | US 2013-0036019 A1 | 07 February 2013 |
| | | US 2013-0036048 A1 | 07 February 2013 |
| | | US 2013-0041768 A1 | 14 February 2013 |
| | | US 2013-0054454 A1 | 28 February 2013 |
| | | US 2013-0054470 A1 | 28 February 2013 |
| | | US 2013-0066701 A1 | 14 March 2013 |
| | | US 2013-0066735 A1 | 14 March 2013 |
| | | US 2013-0121633 A1 | 16 May 2013 |
| | | US 2013-0151417 A1 | 13 June 2013 |
| | | US 2013-0159081 A1 | 20 June 2013 |
| | | US 2013-0159154 A1 | 20 June 2013 |
| | | US 2013-0166332 A1 | 27 June 2013 |
| | | US 2013-0197986 A1 | 01 August 2013 |
| | | US 2013-0204686 A1 | 08 August 2013 |
| | | US 2013-0204723 A1 | 08 August 2013 |
| | | US 2013-0204886 A1 | 08 August 2013 |
| | | US 2013-0204894 A1 | 08 August 2013 |
| | | US 2013-0218657 A1 | 22 August 2013 |
| | | US 2013-0218684 A1 | 22 August 2013 |
| | | US 2013-0246215 A1 | 19 September 2013 |
| | | US 2013-0246261 A1 | 19 September 2013 |
| | | US 2013-0246342 A1 | 19 September 2013 |
| | | US 2013-0290181 A1 | 31 October 2013 |
| | | US 2013-0290203 A1 | 31 October 2013 |
| | | US 2013-0290234 A1 | 31 October 2013 |
| | | US 2014-0006268 A1 | 02 January 2014 |
| | | US 2014-0012640 A1 | 09 January 2014 |
| | | US 2014-0052617 A1 | 20 February 2014 |
| | | US 2014-0108170 A1 | 17 April 2014 |
| | | US 2014-0122331 A1 | 01 May 2014 |
| | | US 2014-0129436 A1 | 08 May 2014 |
| | | US 2014-0195425 A1 | 10 July 2014 |
| | | US 2014-0197234 A1 | 17 July 2014 |
| | | US 2014-0200997 A1 | 17 July 2014 |
| | | US 2014-0213344 A1 | 31 July 2014 |
| | | US 2014-0214567 A1 | 31 July 2014 |
| | | US 2014-0214575 A1 | 31 July 2014 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| | | US 2014-0214653 A1 | 31 July 2014 |
| | | US 2014-0222594 A1 | 07 August 2014 |
| | | US 2014-0229319 A1 | 14 August 2014 |
| | | US 2014-0249999 A1 | 04 September 2014 |
| | | US 2014-0337175 A1 | 13 November 2014 |
| | | US 2014-0344149 A1 | 20 November 2014 |
| | | US 2015-0019944 A1 | 15 January 2015 |
| | | US 2015-0026049 A1 | 22 January 2015 |
| | | US 2015-0039462 A1 | 05 February 2015 |
| | | US 2015-0046241 A1 | 12 February 2015 |
| | | US 2015-0058162 A1 | 26 February 2015 |
| | | US 2015-0154588 A1 | 04 June 2015 |
| | | US 2015-0170128 A1 | 18 June 2015 |
| | | US 2015-0186873 A1 | 02 July 2015 |
| | | US 2015-0220914 A1 | 06 August 2015 |
| | | US 2015-0227919 A1 | 13 August 2015 |
| | | US 2015-0248664 A1 | 03 September 2015 |
| | | US 2015-0302394 A1 | 22 October 2015 |
| | | US 2015-0348018 A1 | 03 December 2015 |
| | | US 2016-0063486 A1 | 03 March 2016 |
| | | US 2016-0086166 A1 | 24 March 2016 |
| | | US 2016-0232513 A1 | 11 August 2016 |
| | | US 2016-0379192 A1 | 29 December 2016 |
| | | US 2017-0046679 A1 | 16 February 2017 |
| | | US 2017-0053302 A1 | 23 February 2017 |
| | | US 2017-0134479 A1 | 11 May 2017 |
| | | US 2017-0228711 A1 | 10 August 2017 |
| | | US 2017-0235786 A9 | 17 August 2017 |
| | | US 2017-0236117 A1 | 17 August 2017 |
| | | US 2017-0243199 A1 | 24 August 2017 |
| | | US 2017-0364940 A1 | 21 December 2017 |
| | | US 2017-0372301 A1 | 28 December 2017 |
| | | US 2017-0372343 A1 | 28 December 2017 |
| | | US 2018-0018690 A1 | 18 January 2018 |
| | | US 2018-0025376 A1 | 25 January 2018 |
| | | US 2018-0046623 A1 | 15 February 2018 |
| | | US 2018-0053157 A1 | 22 February 2018 |
| | | US 2018-0053203 A1 | 22 February 2018 |
| | | US 2018-0056179 A1 | 01 March 2018 |
| | | US 2018-0130047 A1 | 10 May 2018 |
| | | US 2018-0165705 A1 | 14 June 2018 |
| | | US 2018-0189756 A1 | 05 July 2018 |
| | | US 2018-0285987 A1 | 04 October 2018 |
| | | US 2018-0341650 A1 | 29 November 2018 |
| | | US 2019-0026729 A1 | 24 January 2019 |
| | | US 2019-0034921 A1 | 31 January 2019 |
| | | US 2019-0075156 A1 | 07 March 2019 |
| | | US 2019-0147523 A1 | 16 May 2019 |
| | | US 2019-0188691 A1 | 20 June 2019 |
| | | US 2019-0205288 A1 | 04 July 2019 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| | | US 2019-0236588 A1 | 01 August 2019 |
| | | US 2019-0244192 A1 | 08 August 2019 |
| | | US 2019-0251550 A1 | 15 August 2019 |
| | | US 2019-0295054 A1 | 26 September 2019 |
| | | US 2019-0361845 A1 | 28 November 2019 |
| | | US 2019-0361901 A1 | 28 November 2019 |
| | | US 2020-0051064 A1 | 13 February 2020 |
| | | US 2020-0094133 A1 | 26 March 2020 |
| | | US 2020-0327538 A1 | 15 October 2020 |
| | | US 2020-0349553 A1 | 05 November 2020 |
| | | US 2021-0042726 A1 | 11 February 2021 |
| | | US 2021-0125215 A1 | 29 April 2021 |
| | | US 2021-0272101 A1 | 02 September 2021 |
| | | US 2021-0272102 A1 | 02 September 2021 |
| | | US 2022-0129470 A1 | 28 April 2022 |
| | | US 2022-0253832 A1 | 11 August 2022 |
| | | US 2022-0270078 A1 | 25 August 2022 |
| | | US 2023-0044764 A1 | 09 February 2023 |
| | | US 2023-0081174 A1 | 16 March 2023 |
| | | US 6526130 B1 | 25 February 2003 |
| | | US 7131578 B2 | 07 November 2006 |
| | | US 7280644 B2 | 09 October 2007 |
| | | US 7477731 B2 | 13 January 2009 |
| | | US 7522716 B2 | 21 April 2009 |
| | | US 7676030 B2 | 09 March 2010 |
| | | US 7909242 B2 | 22 March 2011 |
| | | US 8464938 B2 | 18 June 2013 |
| | | US 8472594 B2 | 25 June 2013 |
| | | US 8479980 B2 | 09 July 2013 |
| | | US 8571937 B2 | 29 October 2013 |
| | | US 8594286 B2 | 26 November 2013 |
| | | US 8849075 B2 | 30 September 2014 |
| | | US 8867713 B2 | 21 October 2014 |
| | | US 8967464 B2 | 03 March 2015 |
| | | US 8973820 B2 | 10 March 2015 |
| | | US 9182683 B2 | 10 November 2015 |
| | | US 9355393 B2 | 31 May 2016 |
| | | US 9558484 B2 | 31 January 2017 |
| | | US 9582598 B2 | 28 February 2017 |
| | | US 9710807 B2 | 18 July 2017 |
| | | US 9757644 B2 | 12 September 2017 |
| | | US 9785961 B2 | 10 October 2017 |
| | | US 9785962 B2 | 10 October 2017 |
| | | US 9792619 B2 | 17 October 2017 |
| | | US 9830328 B2 | 28 November 2017 |
| | | US 9852414 B2 | 26 December 2017 |
| | | US 9892406 B2 | 13 February 2018 |
| | | US 9953378 B2 | 24 April 2018 |
| | | US 9959531 B2 | 01 May 2018 |
| | | WO 2004-107280 A2 | 09 December 2004 |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/US2023/019576**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| | | WO 2004-107280 A3 | 18 August 2005 |
| | | WO 2006-062832 A2 | 15 June 2006 |
| | | WO 2006-062832 A3 | 02 November 2006 |
| | | WO 2006-062842 A2 | 15 June 2006 |
| | | WO 2006-062842 A3 | 22 February 2007 |
| | | WO 2008-013945 A2 | 31 January 2008 |
| | | WO 2008-013945 A3 | 03 April 2008 |
| | | WO 2008-013945 B1 | 29 May 2008 |
| | | WO 2011-085241 A1 | 14 July 2011 |
| | | WO 2011-159579 A2 | 22 December 2011 |
| | | WO 2011-159579 A3 | 22 March 2012 |
| | | WO 2012-027664 A1 | 01 March 2012 |
| | | WO 2012-054785 A1 | 26 April 2012 |
| | | WO 2012-054786 A1 | 26 April 2012 |
| | | WO 2012-097108 A1 | 19 July 2012 |
| | | WO 2012-112822 A2 | 23 August 2012 |
| | | WO 2012-112822 A3 | 18 October 2012 |
| | | WO 2012-116125 A1 | 30 August 2012 |
| | | WO 2012-166790 A1 | 06 December 2012 |
| | | WO 2013-006725 A2 | 10 January 2013 |
| | | WO 2013-006725 A3 | 11 April 2013 |
| | | WO 2013-009660 A1 | 17 January 2013 |
| | | WO 2013-012876 A1 | 24 January 2013 |
| | | WO 2013-044175 A1 | 28 March 2013 |
| | | WO 2013-049329 A1 | 04 April 2013 |
| | | WO 2013-075071 A1 | 23 May 2013 |
| | | WO 2013-090611 A2 | 20 June 2013 |
| | | WO 2013-090611 A3 | 18 June 2015 |
| | | WO 2013-116806 A1 | 08 August 2013 |
| | | WO 2013-123438 A1 | 22 August 2013 |
| | | WO 2013-192443 A1 | 27 December 2013 |
| | | WO 2014-011691 A1 | 16 January 2014 |
| | | WO 2014-107594 A2 | 10 July 2014 |
| | | WO 2014-107594 A3 | 12 September 2014 |
| | | WO 2014-145708 A1 | 18 September 2014 |
| US 10210507 B2 | 19 February 2019 | EP 3146484 A1 | 29 March 2017 |
| | | EP 3146484 A4 | 27 December 2017 |
| | | JP 2017-517061 A | 22 June 2017 |
| | | JP 6446474 B2 | 26 December 2018 |
| | | KR 10-2016-0136415 A | 29 November 2016 |
| | | US 11010751 B2 | 18 May 2021 |
| | | US 2015-0339661 A1 | 26 November 2015 |
| | | US 2019-0197523 A1 | 27 June 2019 |
| | | WO 2015-179082 A1 | 26 November 2015 |