(12) UK Patent Application (19) GB (11) 2598311 (13) A

(43) Date of A Publication 02.03.2022

(21) Application No: 2013230.4

(22) Date of Filing: 24.08.2020

(71) Applicant(s):
MasterCard International Incorporated
2000 Purchase Street, Purchase 10577-2509,
New York, United States of America

(72) Inventor(s):
Mehdi Collinge
Alan Edward Johnson

(74) Agent and/or Address for Service:
Murgitroyd & Company
Murgitroyd House, 165-169 Scotland Street,
GLASGOW, G5 8PL, United Kingdom

(51) INT CL:
G06Q 20/36 (2012.01) ***G06Q 20/38*** (2012.01)
G06Q 20/40 (2012.01)

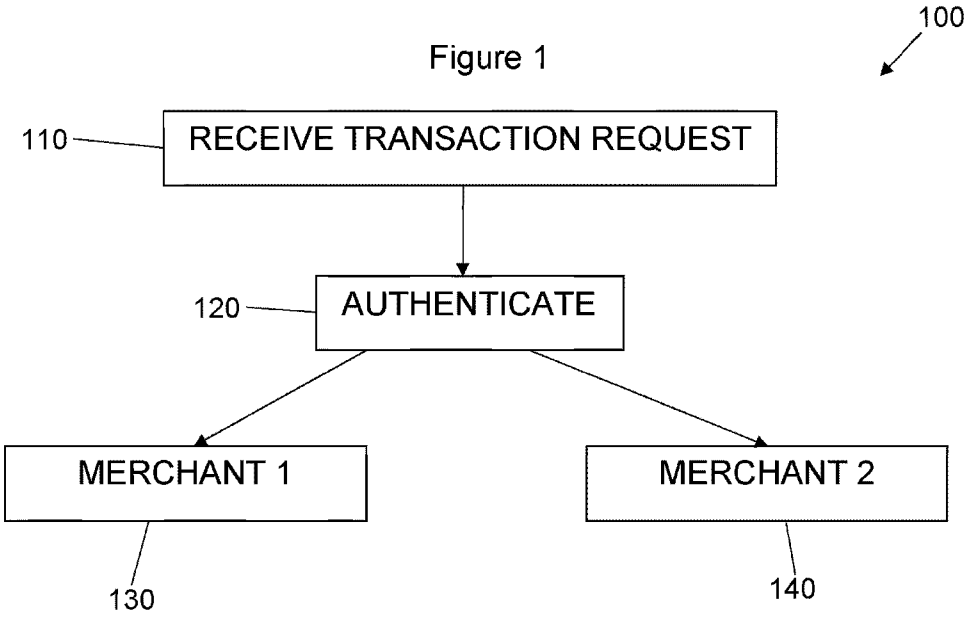
(56) Documents Cited:
None

(58) Field of Search:
Other: **No search performed: Section 17(5)(b)**

(54) Title of the Invention: **A multiple payee digital transaction authentication method**
Abstract Title: **Multiple payee transaction from a single cryptogram**

(57) A method of paying multiple payees where unique transaction credentials are provided to each of the payees upon receipt of a transaction request including a single cryptogram. The method involves receiving a transaction request including a cryptographic payer identifier and payment information for at least two payees. The transaction request is authenticated based on the identifier. Each of the payees is provided with a unique account number, expiry data, and verification code that are all bound using a cryptographic process. These transaction credentials are usable by the payee to make a payment request that facilitates payment from the payer. One of the account number, expiry data and verification code is time limited so that the payment request is only facilitated within a predetermined length of time of the credentials being provided. The invention finds use with payers having a mobile wallet application on their smart device.

Figure 1



GB 2598311 A

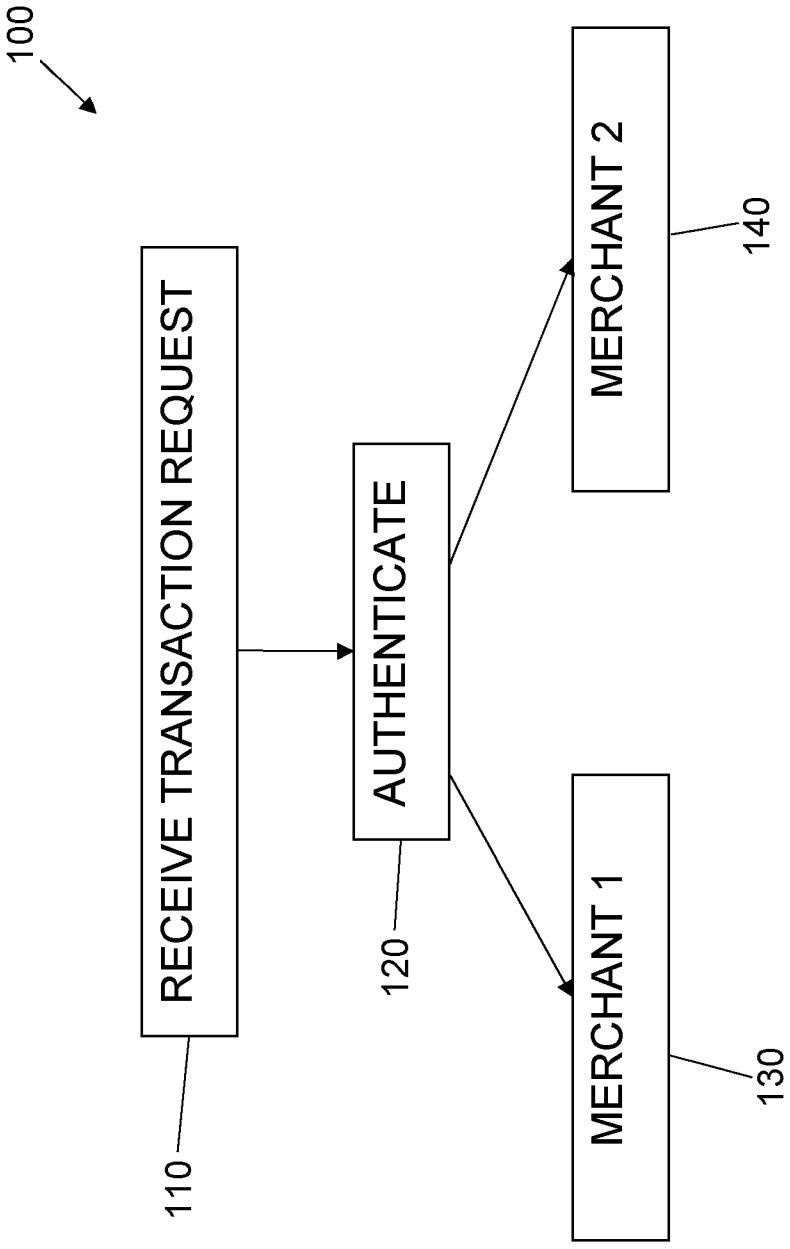

100
RECEIVE TRANSACTION REQUEST
110
AUTHENTICATE
120
MERCHANT 1
130
MERCHANT 2
140

Figure 1

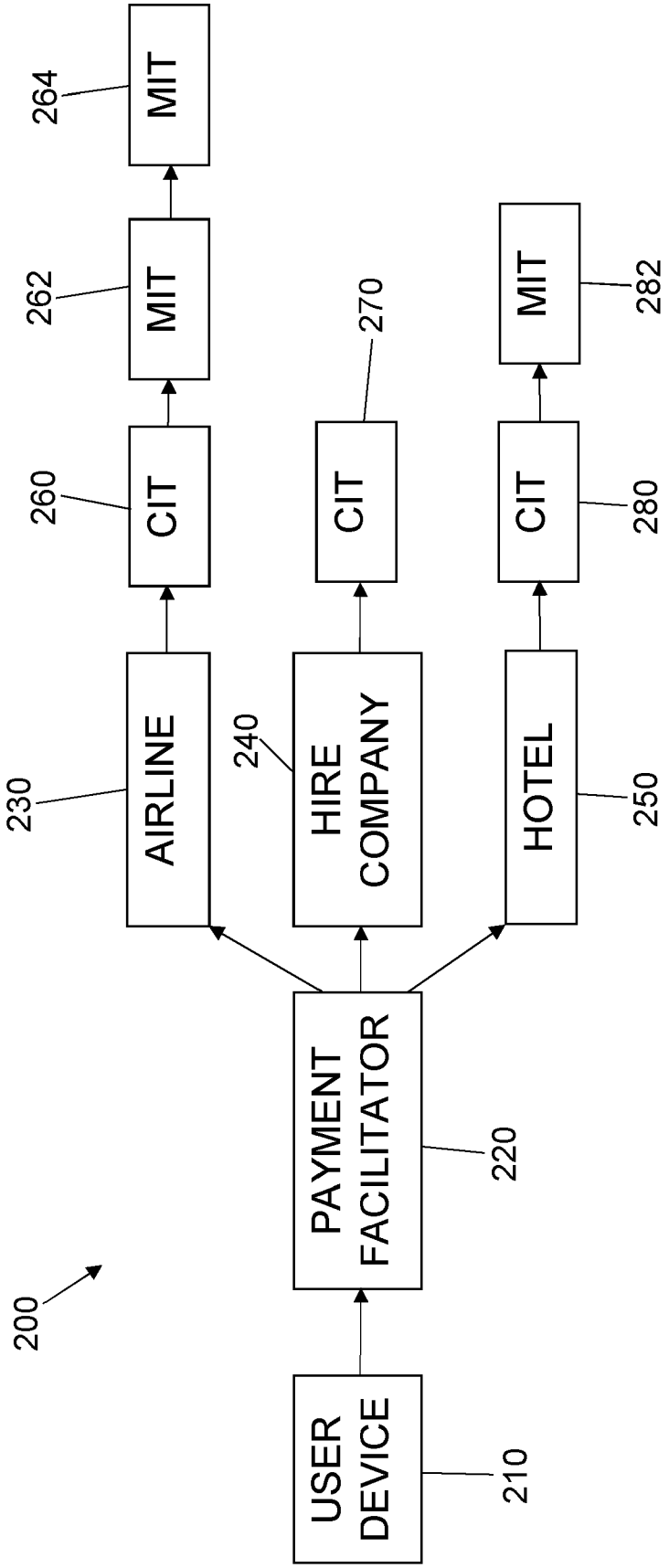

200
USER DEVICE
210
PAYMENT FACILITATOR
220
AIRLINE
230
HIRE COMPANY
240
HOTEL
250
CIT
260
CIT
270
CIT
280
MIT
262
MIT
264
MIT
282

Figure 2

A MULTIPLE PAYEE DIGITAL TRANSACTION AUTHENTICATION METHOD

Field of the Invention

The present invention relates to a multiple payee digital transaction authentication method and finds particular, although not exclusive, utility in providing a digital transaction authentication method in which a plurality of payees or merchants are provided with unique transaction credentials.

Background to the Invention

Typically, merchants have the capability to process payments by taking a 16-digit primary account number, an expiry date in YYMM format, and a card verification code/value (CVC/CVV), usually found on a bank or credit card, from a customer or payer. However, exposing these transaction credentials to a merchant over a network, such as the Internet, may be viewed as a security risk. Accordingly, recent developments have been made to secure these single payments with message authentication codes or similar mechanisms. One such method is by paying via a mobile wallet application on a smart device, such as a smart phone or smart watch.

The smart device may store a token, which may be a 16-digit number, that is unique to the device. Furthermore, the device may store a set of keys capable of creating unique cryptograms. A fingerprint or face scan may be taken to create a cryptogram. For each transaction made from the device, the device will send the token along with a unique cryptogram created by the set of keys. Each transaction will have a unique cryptogram that can only be used once, for the transaction for which it was created, and is, as such, single use. The 16-digit token and the cryptogram may be used to facilitate the transaction. Accordingly, even if the token and/or a cryptogram is exposed or otherwise obtained by an unauthorised person, it cannot be used to facilitate a further payment, thereby providing some security.

However, in some circumstances, a user may use their smart device to purchase an item or a service from several merchants with a single transaction. For example, when using an online travel shopping company, a single transaction may be used to purchase a flight from an airline, a car hire from a hire company, and a hotel room

booking from a hotel. In this case, as there is only a single transaction, the token is provided along with only a single unique cryptogram. Accordingly, there is not a unique cryptogram for each of the three merchants requiring payment, which means that payments cannot be secured using the single use cryptogram.

Another example of when a single transaction may be used to pay several merchants is when a medical bill is to be paid. When settling a medical bill, a single monetary amount may be presented for payment. However, this single monetary amount will typically include payment for many services, medicines and other goods that may each be supplied by separate merchants. Accordingly, the single cryptogram provided with the token may not be suitable to allow for a transaction with each of the merchants.

Therefore, presently known transaction methods are not suitable for use in scenarios wherein two or more merchants require payment with a single transaction.

Objects and aspects of the present invention seek to alleviate at least these problems and improve prior known digital transaction authentication methods.

Summary of the Invention

According to a first aspect of the present invention, there is provided a multiple payee digital transaction authentication method comprising: receiving a transaction request including a cryptographic payer identifier and payment information including at least two payees and corresponding payment amounts; authenticating the transaction request based on the cryptographic payer identifier; and providing each of the at least two payees with a unique account number, unique expiry data and a unique verification code which is usable by the payee to facilitate payment of the corresponding payment amount from the payer, wherein: the account number, the expiry data and the verification code are bound using a cryptographic process ; and one of the account number, the expiry data and the verification code is time limited such that a payment request from the respective payee is facilitated only if the payment request is received within a predetermined length of time of the account number, the expiry data and the verification code being provided.

A key advantage of the present invention is that unique and secure transaction credentials may be provided to several merchants or payees, such that secure payments may be made to several payees. In addition, the provision of an account number, expiry data and a verification code may be suitable for use in legacy payment system which typically require a primary account number, an expiry date and a card verification code/value.

A payee may use the account number, the expiry data and the verification code to process a payment via legacy digital payment systems wherein the account number takes place of the primary account number, the expiry data takes place of the expiry date and the verification code takes place of the card verification code/value (CVC/CVV). In this way, payees may make use of existing legacy digital payment systems to process a payment, whilst some cryptographic operations are performed for security with generation and validation of a payment proof.

A multiple payee digital transaction may be a transaction in which a single payer pays a plurality of payees. The transaction may be carried out via a broker or a third party. For example, a user, the payer, may book a holiday via an online travel shopping company. The holiday booking may include a flight booking, a hotel booking, and a car hire booking. Each of these bookings may be made with different providers. Accordingly, the single holiday booking made by the user with the online travel shopping company includes three bookings, each with different providers. As a further example, a user, the payee, may have required medical treatment. The treatment may include an ambulance, an x-ray, surgery and the user may be provided with medicine to be administered at home. Each of these services and the medicine may each be provided by a different merchant. Accordingly, the treatment may include several different merchants, paid via a single medical bill transaction.

Receiving a transaction request may mean that a request for a payment is received. The transaction request may be received from the payer. Alternatively, the transaction request may be received from a broker or a third party, such as an online travel shopping company.

A cryptographic payer identifier may be generated by the payer's digital device, such as a smart phone.

Payment information may include an amount of money due, goods and/or services requested, a date of payment and/or any other information related to a transaction. The payment information may include payment amounts that may be monetary amounts to be paid to each respective payee.

At least two payees may mean only two payees. Alternatively, the method may be used to pay more than two payees. As described above, the present invention provides a method which allows for secure payments to be made to several payees.

Authenticating the transaction request may mean that the transaction request is checked or otherwise considered and is verified as being a genuine request from the payer. Authentication is important to reduce or eliminate fraudulent transactions.

Providing each of the at least two payees with a unique account number, unique expiry data and a unique verification code may allow the payee to facilitate payment from the payer without providing payer information typically required to facilitate a payment, such as the primary account number, expiry date and card verification code/value. Accordingly, there is less exposure of the payer's financial details which may reduce the risk or opportunity for fraudulent activity involving the payer's details.

The account number, the expiry data and the verification code being cryptographically bound may mean that the integrity and use of these pieces of information is protected, which may also reduce the risk or opportunity for fraudulent activity involving the payer's details.

One of the account number, the expiry data and the verification code being time limited may mean that a payment may not be facilitated using the time limited information if the predetermined time period has expired. In this way, some certainty regarding the time and/or date of the payment may be provided and payments outside of an allowable period may be barred.

One or more of the account number, the expiry data and the verification code provided to a payee may include a payee identifier. The payee identifier may correspond to the payee to which the account number, the expiry data and the

verification code are provided. In this way, the identity of the payee may be derivable from this information. Furthermore, when this information is received back from the payee, to facilitate a payment or otherwise, the identity of the payee may be established and/or verified.

The method may further comprise receiving a payee request for payment of the payment amount from a payee. The payee request may include the account number, the expiry data and the verification code. The method may further comprise comparing the payee identifier with an identity of the payee from which the payee request is received. In this way, the source of the request from the payee for payment of the payment amount may be verified in that the identity of the payee from which the payee request is received may be matched to the payee identifier. The method may further comprise facilitating payment of the payment amount from the payer to the payee only if the payee identifier and the identity of the payee from which the payee request is received match. Accordingly, some verification of the payee identity is required to facilitate payment from the payer to the payee. Therefore, the likelihood of a fraudulent payment being facilitated is reduced.

Furthermore, a transaction that is not facilitated may be given further consideration to determine whether fraudulent activity has been attempted, and any such determinations may be provided to the relevant law or standards agency.

The predetermined length of time may be 24 hours. In this way, typical generation and management of date control may be used, without requiring amendment to typical and widely used transaction practices.

The method may further comprise receiving a further transaction request from the respective payee. The further transaction request may include a further payment amount and the account number and the expiry data. The further transaction request may be a request for payment for goods and/or services not covered by the original transaction. For example, the original transaction may be payment for a hotel room, and the further transaction request may be for payment for items consumed from the hotel room mini bar, after the guest has left the hotel. Other scenarios wherein a further payment is required are envisaged. One of the account number and the expiry data may include the payee identifier. Accordingly, the payee

may be identified, and the further payment facilitated, without need of the verification code. The method may further comprise facilitating payment of the further payment amount from the payer to the payee. Accordingly, a further transaction may occur. In this way, the payee may receive payment for goods and or services not covered by the original transaction.

The original transaction may be a consumer initiated transaction and is, as such, initiated by the payer by submitting the transaction request. The further transaction may be a merchant initiated transaction and is, as such, initiated by a payee by submitting the further transaction request without the involvement of the payer. Additionally, the further transaction may be a refund which may be considered to be initiated by the consumer, but may not require the verification code.

The further payment may be facilitated if the further transaction request is received within a further predetermined time of receipt of the transaction request. The further predetermined time may be dependent on the type of business and/or another characteristic of the payee. For example, it is common for further payments to be made to a hotel or a car hire company, whereas it may be unusual for a further payment to be made to a clothing store. Accordingly, upon receipt of a further payment request wherein a further payment request is not expected or is unusual, further checks may be undertaken and/or the further payment request may be denied.

The unique account number, unique expiry data and/or the unique verification code may be recycled once it is no longer usable due to expiry of the further predetermined time or when a merchant initiated transaction would require a new consumer initiated transaction to be approved using newly created credentials. In this way, a finite number of unique account numbers, unique expiry data and/or the unique verification codes may be continually used.

The further payment may be facilitated if the further transaction request conforms to predetermined criteria selected from the list: a payment amount, a number of previous payments and/or a characteristic of the payee. In this way, a check is applied to further payments, thereby improving security.

The further payment may be facilitated if the further transaction request includes reference to a previously facilitated payment from the payer to the respective payee. In this way, the further payment may only be facilitated if it follows an original payment authorised by the payer.

The cryptographic payer identifier may comprise a proof of biometric authentication. The biometric authentication proof may be obtained via an authentication method. The authentication method may comprise a fingerprint identification, facial recognition, a retina scan, an iris scan, a palm vein scan, a hand geometry scan, voice analysis, behavioural pattern recognition or any combination thereof.

Alternatively, or additionally, the cryptographic payer identifier may comprise a password, a passcode, a personal identification number (PIN), security questions and corresponding answers, a verification code received by the user via their device, an identification token from a list or any combination thereof.

The payee identifier may comprise sufficient information such that at least 16 payees can be assigned a unique payee identifier. The payee identifier may comprise at least 4 characters, or bits. For example, if the payee identifier is expressed in a binary system, 4 binary characters allows for 16 unique payee identifiers to be provided, whereas 5 binary characters allows for 32 unique payee identifiers to be provided. The number of characters used for the payee identifier may be dependent on the expected number of payees.

The account number and the validation code may be provided as a character string. The characters may be numbers 0 to 9, letters A to Z, values from any other character set or a combination thereof. The character string may include 18 character positions. Positions 1 to 15 may relate to the account number. Positions 16 to 18 may relate to the validation code. Other combinations are envisaged. Alternatively, the character string may include 19 character positions, with positions 1 to 16 relating to the account number and positions 17 to 19 relating to the verification code. The character strong may comprise a checksum. The checksum may be computer over, or related to, a subset or the entire list of characters.

The payee may be required to delete, wipe or otherwise destroy the verification code after the original transaction, as is typically required by law or official standards, for example PCI compliance. The payee may retain the account number and the expiry data such that a further payment may be requested and facilitated.

The transaction request may be received from a user, the payer, via a mobile wallet application on a user device. For example, the transaction request may be received via Apple Pay, Google Pay, or some other application capable of sending a transaction request including a cryptogram. The user device may be a smart device. For example, the user device may be a smart phone, a smart watch, smart eyewear, an RFID chip, or any other suitable device. Alternatively, the generation of the transaction request may be delegated to a service provider when no user device is available to deliver the transaction request.

More than one of the account number, the expiry data and the verification code may be time limited such that the payment request from the respective payee is facilitated only if the payment request is received within the predetermined length of time of the account number, the expiry data and the verification code being provided.

A broker or third party, such as an online travel shopping company, may receive the transaction request and forward the transaction request to a payment facilitator. The broker or third party may also provide a number of payees to be paid. The payment facilitator may then, after authenticating the transaction request, provide each of the payees, directly or via the broker or third party, with a unique account number, unique expiry data and a unique verification code.

A list of mapping information between the transaction request and the account number, the expiry data and the verification code provided to each payee may be stored. The list of mapping information may be accessed and used by a payment authorisation system.

According to a second aspect of the present invention, there is provided a computer readable storage medium system configured to store computer executable code that when executed by a computer configures the computer to carry out the method of the first aspect of the present invention.

Brief Description of the Drawings

Figure 1 is a first schematic process diagram showing a method of authenticating a payment and providing unique transaction credentials to multiple merchants; and

Figure 2 is a second schematic process diagram showing a method of authenticating and facilitating a secure remote transaction via an online travel provider.

Detailed Description

Figure 1 is a first schematic process diagram 100 showing a method of authenticating a payment and providing unique transaction credentials to multiple merchants.

The method 100 includes receiving a transaction request 110 from a user. The transaction request 110 includes a cryptogram which allows the identity of the user to be verified. The user will typically submit the payment request from a digital device, such as a smart phone, which has the capability to take a biometric scan or otherwise verify the identity of the user.

The transaction request 110 also includes payment information including details of at least two merchants and monetary values to be paid to each of the merchants. The transaction request 110 may be received via a third party, which may provide some or all of the payment information.

The transaction request 110 is then authenticated 120 based on the cryptogram provided in the transaction request 110, such that the likelihood of fraudulent or otherwise unauthorised transactions being allowed is reduced.

Once the transaction request 110 has been authenticated 120, transaction credentials are provided to each of the merchants 130, 140. The transaction credentials include a unique account number, unique expiry data and a unique verification code. The merchants 130, 140 can then use the transaction credentials to process payments using legacy transaction systems which require a primary

account number, an expiry date and a card verification code/value. To ensure transaction security, the account number, the expiry data and the verification code are cryptographically bound.

Furthermore, one of the account number, the expiry data and the verification code is time limited such that it may only be used to successfully process a transaction within a predetermined time period. The predetermined time period may be 24 hours.

Figure 2 is a second schematic process diagram 200 showing a method of authenticating and facilitating a secure remote transaction via an online travel provider.

A user, via a user device 210, may browse the website or an app of an online travel provider and select a holiday package to book. The holiday package may be displayed on the website or app as a single purchasable item, but in reality the holiday package may include several purchases bundled into one larger purchase.

Once the user decides to book the holiday package, they may pay with a mobile wallet application on their device 210. A transaction request may then be sent to a payment facilitator 220, via the online travel provider or directly. The payment facilitator 220 may then authorise the transaction request and provide transaction credentials as described with reference to Figure 1 above.

The holiday package may include a flight booking, transport, and accommodation. Accordingly, payments may be due to an airline 230, a hire company 240 and a hotel 250, or other similar providers. As such, the payment facilitator 220 will provide unique transaction credentials to the airline 230, the hire company 240 and the hotel 250.

The airline 230 may then use the unique transaction credentials provided to them by the payment facilitator 220 to undertake a Consumer Initiated Transaction (CIT) 260 to take payment for the airline's 230 portion of the holiday package. The airline 230 may make use of existing legacy payment systems to process the payment. Once

the CIT 260 has been undertaken, the airline may be required to delete the verification code provided to them, to comply with law or regulation.

The hire company 240 may also use the unique transaction credentials provided to them by the payment facilitator 220 to undertake a Consumer Initiated Transaction (CIT) 270 to take payment or pre-authorize a given amount for their portion of the holiday package. The hire company 240 may make use of existing legacy payment systems to process the payment. Once the CIT 270 has been undertaken, the hire company may be required to delete the verification code provided to them, to comply with law or regulation.

The hotel 250 may also use the unique transaction credentials provided to them by the payment facilitator 220 to undertake a Consumer Initiated Transaction (CIT) 280 to take payment for the hotel's 250 portion of the holiday package or use a pre-authorization process to get the assurance that the card is in good standing, with the full outstanding amount charged on checkout using one or more Merchant Initiation Transactions (MITs). The hotel 250 may make use of existing legacy payment systems to process the payment. Once the CIT 280 has been undertaken, the hotel may be required to delete the verification code provided to them, to comply with law or regulation.

Accordingly, each of the airline 230, the hire company 240 and the hotel 250 will have received the payment due to them for the holiday package or will have received assurance that later payment via the processing of one or more MITs is possible.

The user may also make use of services, or consume goods, whilst on the holiday that were not covered by the original payment. Accordingly, the airline 230, the hire company 240 and/or the hotel 250 may undertake one or more Merchant Initiated Transactions (MIT) to take payment for these services or goods. The stored account number and expiry data may be used to process the MITs via legacy payment systems. The allowability of MITs may be decided by the payment facilitator 220, based on a number of predetermined criteria such as a previous approval of a corresponding CIT, time since the CIT, a value of the MIT, or the number of MITs already allowed.

For example, the airline 230 may undertake a first MIT 262 to take payment for excess baggage not covered by the original booking. Furthermore, the airline 230 may undertake a second MIT 264 for a upgrade package requested after the original CIT 260 has been completed. The hotel 250 may also undertake a single MIT 282 to take payment for items taken from a minibar that were not paid for upon check out. Other additional goods and services are envisaged.

The methods shown schematically in Figures 1 and 2 may include further steps. The sequence of steps shown does not exclude preceding, intermediate or following steps. Furthermore, although the use of a smart phone for sending the transaction request has been described above, it is to be understood that any suitable digital device may be used, such as a smart watch. Figure 1 has been described above in relation to two merchants. However, other numbers of merchants are envisaged, and the number of merchants is dependent on the specific transaction. An exemplar predetermined time period of 24 hours is discussed above. However, other time periods are contemplated. The transaction credentials described above may include further information and is not limited to including only the information detailed above.

Figure 2 is described in relation to a transaction with an online travel provider. However, it is to be understood that the method described is applicable to any scenario in which a single transaction request is used to facilitate payment of two or more merchants. For example, any type of package payment, such as a medical bill, may be facilitated with the method described above. In addition, although Figure 2 is described in relation to three merchants, it is to be understood that the method is application to scenarios in which any two or more merchants require payment.

Claims

1. A multiple payee digital transaction authentication method comprising:

receiving a transaction request including a cryptographic payer identifier and payment information including at least two payees and corresponding payment amounts;

authenticating the transaction request based on the cryptographic payer identifier; and

providing each of the at least two payees with a unique account number, unique expiry data and a unique verification code which is usable by the payee to facilitate payment of the corresponding payment amount from the payer, wherein:

the account number, the expiry data and the verification code are bound using a cryptographic process; and

one of the account number, the expiry data and the verification code is time limited such that a payment request from the respective payee is facilitated only if the payment request is received within a predetermined length of time of the account number, the expiry data and the verification code being provided.

2. The method of claim 1, wherein one or more of the account number, the expiry data and the verification code provided to a payee includes a payee identifier corresponding to the payee to which the account number, the expiry data and the verification code are provided.

3. The method of claim 2, further comprising:

receiving a payee request for payment of the payment amount from a payee, wherein the payee request includes the account number, the expiry data and the verification code;

comparing the payee identifier with an identity of the payee from which the payee request is received; and

facilitating payment of the payment amount from the payer to the payee only if the payee identifier and the identity of the payee from which the payee request is received match.

4. The method of any preceding claim, wherein the predetermined length of time is 24 hours.

5. The method of any one of claims 2 to 4, further comprising:

receiving a further transaction request from the respective payee, wherein the further transaction request includes a further payment amount and the account number and the expiry data, wherein one of the account number and the expiry data includes the payee identifier; and

facilitating payment of the further payment amount from the payer to the payee.

6. The method of claim 5, wherein the further payment is facilitated if the further transaction request is received within a further predetermined time of receipt of the transaction request.

7. The method of claim 5 or claim 6, wherein the further payment is facilitated if the further transaction request conforms to predetermined criteria selected from the list: a payment amount, a number of previous payments and/or a characteristic of the payee.

8. The method of any one of claims 5 to 7, wherein the further payment is facilitated if the further transaction request includes reference to a previously facilitated payment from the payer to the respective payee.

9. The method of any preceding claim, wherein the cryptographic payer identifier comprises a proof of biometric authentication.

10. The method of any one of claims 2 to 10, wherein the payee identifier comprises sufficient information such that at least 16 payees can be assigned a unique payee identifier.

11. The method of any preceding claim, wherein the account number and the validation code are provided as a character string.

12. The method of claim 11, wherein the character string includes 18 character or number positions, wherein positions 1 to 15 relate to the account number and positions 16 to 18 relate to the validation code.

13. The method of any preceding claim, wherein the transaction request is received from a user via a mobile wallet application on a user device or the generation of the transaction request is delegated to a service provider when no user device is available to deliver the transaction request.

14. The method of any preceding claim, wherein the verification code is time limited such that the payment request from the respective payee is facilitated only if the payment request is received within the predetermined length of time of the account number, the expiry data and the verification code being provided.

15. A computer readable storage medium system configured to store computer executable code that when executed by a computer configures the computer to carry out the method of any preceding claim.