Title: A TRANSACTION AND LOGISTICS INTEGRATED MANAGEMENT SYSTEM (TALISMAN) FOR SECURE CREDIT CARD PAYMENT AND VERIFIED TRANSACTION DELIVERY

Abstract: The present invention is a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery.
A TRANSACTION AND LOGISTICS INTEGRATED MANAGEMENT SYSTEM (TALISMAN) FOR SECURE CREDIT CARD PAYMENT AND VERIFIED TRANSACTION DELIVERY

Invented by

Michael C. Bournat

Related Applications

This application claims the benefit of copending U.S. Provisional Application No. 60/257,748, filed December 22, 2000, and copending U.S. Provisional Application No. (Not Yet Assigned), titled Detailed Design Document using Object Oriented Methodology for Talisman, filed December 23, 2001, which are both incorporated here by reference.

Field Of The Invention

The present invention is a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery.

Background Of The Invention

There is constant unsolved need for security and verification of commercial transactions and purchasing by consumers ordering goods by telephone and mail (known as "MOTO" - mail order/telephone order), and, in particular, over the Internet ("e-commerce"). Present ordering methods and systems have not and can not meet today’s security needs secure, verified transactions. In particular, there is a growing unsolved need for secure and verified delivery of goods and services right to the consumer's door.

Unfortunately, reality shows that the described purchasing process
This misuse and fraud is originated from both the unlawful use of corruptly obtained credit card details and merchants who set up sites with the intention of obtaining money but not supplying the goods (merchant fraud).

Whether you are a consumer, merchant, acquirer or issuer you might have to face the costly and unpleasant effects of misuse and fraud in the CNP (Cardholder-Not-Present) transaction environment. As a consumer your card is debited before you receive the ordered goods and there is a strong chance that you will receive wrong or faulty goods or, in the worst case, none at all. The merchant can suffer from the use of a stolen, lost or replica ("skimmed") card whereas banks ultimately stand the losses when the merchant fails or disappears.

The present invention has been designed with the aim to protect all participants: the honest consumer, the honest merchant, the acquirer and the issuer. Though the whole CNP (Cardholder-Not-Present) system is fraught with dangers and possible losses. The present invention produced by CQR Technologies Ltd. is called TALISMAN (transaction and logistics integrated management system) and it addresses the undeniable advantages incorporated in this contemporary way of purchasing. TALISMAN improves the existing banking and credit card clearing system by satisfying the needs of security and protection need for today's consumer market.

The TALISMAN is designed to fully integrate and manage a CNP transaction from the outset to the complete authenticated delivery by a CQR enabled professional logistics company - before the merchant can claim the funds. Equally, will ensure that a consumer cannot deny delivery of the goods. Full adoption of the system will virtually eliminate costly charge backs, repudiation and fraud.
TALISMAN is designed to work with AVS, CVV2, CVC2, CV2 (card security code), PKI, EMV, UKIS and electronic signatures obtained by the logistics company. The interface to the banking environment meets all current banking standards and therefore requires minimal changes to existing operating methods. Modes of payment of the 21st century are highly developed. Now, security is no longer behind: By combining and furthermore managing all links involved in the CNP transaction chain CQR Technologies, consumers, acquirer and issuer banks will only benefit from the true end-to-end solution provide by the present invention.

Summary of the Invention

The present invention is a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery.

In one embodiment of the present invention the TALISMAN system includes a customer ordering sub-system and a communication system such as, but not limited to, an internet connection. The communication system such as the internet provides communication with and between, a merchant sub-system, an acquirer processing sub-system, a credit card issuer processing sub-system, and a carrier verification and delivery sub-system.

Customers, wanting to purchase goods or services remotely when not present at the site of commerce, utilize the customer ordering sub-system. The customer ordering sub-system is in communication with the merchant sub-system, to make credit card purchases with merchants. Upon request for a purchase, the merchant sub-system requests an authorization for payment and/or an ID tag for identification. Authorization for each credit card purchase is issued by
the credit card issuer processing sub-system and the authorization is provided to
the merchant sub-system through either the acquirer processing sub-system or the
carrier verification and delivery sub-system. The ID tag for each credit card
purchase is provided by the carrier verification and delivery sub-system and is
used at the point of delivery to verify the credit card purchase and to establish
proof of delivery at the time of delivery.

In another embodiment of the present invention the TALISMAN system
includes a customer ordering sub-system and an internet connection. The Internet
connection provides communication with and between a merchant sub-system, an
acquirer processing sub-system, a credit card issuer processing sub-system, and a
carrier verification and delivery sub-system. The customers use the customer
ordering sub-system, which is in communication with the merchant sub-system, to
make credit card purchases with merchants.

The merchant sub-system requests an authorization and/or an ID tag from
the credit card issuer processing sub-system for each credit card purchase.
Authorization for each credit card purchases is issued by the credit card issuer
processing system and is provided to the merchant sub-system through either the
acquirer processing sub-system or the carrier verification delivery sub-system.

Payment funds are reserved for the purchase by the credit card issuer
processing sub-system or the acquirer processing sub-system until verification.
The ID tag is issued by the carrier verification and delivery sub-system is used to
verify proof of delivery and the credit card purchase at the point of delivery. Upon
verification of the delivery and the purchase the reserved funds are released to the
merchants.

In another embodiment of the present invention the TALISMAN system
includes a customer ordering sub-system and a communication connection, such
as an internet or intranet, providing communication with and between a merchant sub-system, an acquirer processing sub-system, a credit card issuer processing sub-system, and a carrier verification and delivery sub-system. Customers use the customer ordering sub-system, which is in communication with the merchant sub-system, to make credit card purchases with merchants.

The merchant sub-system requests an authorization code for each credit card purchase. The authorization code (Auth) for each credit card purchases is issued by the credit card issuer processing system. The Auth is provided to the merchant sub-system through either the acquirer processing sub-system or the carrier verification and delivery sub-system. The authorization code is used to verify delivery and the credit card purchase at the point of delivery. Upon verification of the delivery the purchase funds are released to merchants.

In another embodiment of the present invention the TALISMAN system provides an improvement over prior art systems used for credit card holder not present (CNP) transactions. The prior art system allow a purchasing party to request a purchase from a merchant and delivery of ordered product to a receiving party. An acquiring bank makes a request for authorization for a CNP transaction to a card issuer bank.

The improvement includes an electronic authorization ID issued by the issuer bank and/or the acquirer bank and/or a third party. The third party is a logistic entity that coordinates delivery of goods or services purchased, actual delivery, order placement verification, payment instrument verification and the release of reserved payment funds authored for the transaction. A microprocessor is used to verify the issued electronic authorization ID with the identify of the purchasing party and/or the identity of the receiving party and/or the location of delivery at the point of delivery.
In one aspect of the invention the microprocessor is a programmable storage device having the capacity to receive and store credit card authentication data generated by TALISMAN. In another aspect the programmable storage device is a personal digital assistant (PDA) maintained by a carrier delivering the ordered product. The PDA is used to compare the stored credit card authentication with the actual credit card used to initiate the transaction and/or a remote delivery code provided by TALISMAN for remote deliveries.

In another embodiment of the present invention, a method is provided for a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery. The method includes the steps of placing a customer order with a merchant using a customer ordering subsystem. Communicating using an internet connection providing communication with and between a merchant sub-system, an acquirer processing sub-system, a credit card issuer processing sub-system, and a carrier verification and delivery sub-system. Customers use the customer ordering sub-system to make credit cardholder not present purchases with merchant in a manner as described above.

In another embodiment of the present invention, a method for a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery includes the steps of:

- establishing a communication between a first device, a second device, a third device, and a fourth device. Transmitting payment information, corresponding to a payment instrument of a customer, from the first device to the second device;
- forwarding payment information to the third device and the fourth device;
evaluating the payment information based on the payment instrument by the third device;
transmitting approval of the transaction from the third device to the second device;
5 storing a record of the transaction approval at the fourth device; forwarding approval of the transaction from the second device to the first device;
requesting the payment instrument by the fourth device at the point of delivery;
comparing the payment instrument with the payment information by the fourth device at the point of delivery; and transmitting approval to release funds to the first by the fourth device, wherein payment is released to the first by the second device using a direct electronic transmission of monetary value from the second device to the first device.

In one aspect of the invention the first device comprises a merchant device, the second device is an acquirer device, the third device is an issuer device, the fourth device is a carrier verification and delivery device, the party is a consumer, and the payment instrument comprises a card issued by an issuer to a consumer.

In another aspect of the invention at least one communication linkage uses the Internet Protocol (IP). In another aspect of the invention at least one communication linkage uses the Internet Protocol (IP), the transmission via at least one communication linkage is encrypted, and the payment instrument is a credit card and/or a debit card.
In another embodiment of the present invention, a transaction and logistics integrated management apparatus (TALISMANN) is provided for secure credit card payment and verified transaction delivery.

The apparatus includes logic that establishes communication between a first or merchant device, a second or acquirer device, a third or issuer device, and a fourth or carrier verification and delivery device. The apparatus also includes logic that transmits payment information corresponding to a payment instrument of a party, from the first electronic device to the second electronic device. The apparatus further includes logic that forwards the payment information from the second electronic device to the third electronic device. The apparatus further includes logic that receives the payment information at the third electronic device.

The apparatus further includes logic that evaluates the payment information using the payment instrument by the third electronic device. The apparatus further includes logic that transmits approval of the transaction from the third electronic device to the second and fourth electronic devices. The apparatus further includes logic that stores a record of the transaction approval at the fourth electronic device.

The apparatus further includes logic that forwards approval of the transaction from the fourth electronic device to the second electronic device upon verification of the payment instrument with the payment instrument by the fourth electronic device.

Payment is released to the merchant device by the acquirer device using logic that directs electronic transmission of monetary value from the acquirer device to the merchant device.

Again, in one aspect of the apparatus the first device comprises a merchant
device, the fourth device is a carrier verification and delivery device, the party is a consumer, wherein the payment instrument comprises a card issued by an issuer to a consumer.

Also, the apparatus includes at least one communication linkage using the Internet Protocol (IP), and the transmission in at least one communication linkage may be encrypted.

In another embodiment of the invention, the TALISMAN system includes a computer program embodied on a computer-readable medium for executing an electronic transaction between a first device, such as a merchant electronic device, a second device, such as an acquirer device, a third device, such as an issuer electronic device, and a fourth, such as a carrier verification and delivery device.

The computer program includes a code segment that establishes a communication between the first electronic device and the second electronic device. The program also includes a code segment that couples the second, second, third and fourth electronic device via a first communication linkage. And, a code segment that transmits payment information corresponding to a payment instrument of a party, from the first electronic device to the second and third electronic device. And, a code segment that forwards the payment information to the third electronic device. And, a code segment that receives the payment information at the third electronic device.

And, a code segment that evaluates the payment information based on the payment instrument by the third electronic device. And, a code segment that transmits approval of the transaction from the third electronic device to the second and fourth electronic device. And, a code segment that stores a record of the transaction approval at the second electronic device. And, a code segment that
second electronic device upon verification of the payment instrument with the payment instrument by the fourth electronic device.

Payment is released to the first (merchant) device by the second (acquirer) device using logic that directs electronic transmission of monetary value from the second (acquirer) device to the first (merchant) device.

**Brief Description Of The Drawings**

For the purpose of illustrating the invention, there is shown in the drawings a form, which is presently, preferred; it being understood, however, that this invention is not limited to the precise arrangements and instrumentalities shown.

Figure 1 illustrates a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery according to one embodiment of the present invention.

Figure 2 illustrates shipping relationships according to the present invention.

Figure 3 illustrates a shipping document according to the present invention.

Figure 4 illustrates a potential drop-off loophole according to the present invention.

Figure 5 illustrates drop-off loopholes according to the present invention.

Figure 6 illustrates transaction anatomy according to the present invention.

Figure 7 illustrates a remote shopping process according to the present invention.

Figure 8 illustrates PKI and message authentication according to the present invention.
Figure 10 illustrates APACS 29,30 and 50 according to the present invention.

Figure 11 illustrates level 1 DFD—remote shopping service according to the present invention.

Figure 12 illustrates service interactions according to the present invention.

Figure 13 illustrates service components according to the present invention.

Figure 14 illustrates components and interfaces according to the present invention.

Figure 15 illustrates service financial components according to the present invention.

Figure 16. interfaces merchant reporting component according to the present invention.

Figure 17 illustrates remote shopping components and interfaces according to the present invention.

**Detailed Description Of The Invention**

Referring now to the drawings, wherein there is shown in FIGS. 1 through 17 an illustration of the present invention, a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery.

**CNP Transactions**

Cardholder Not Present (CNP) is a banking industry term for remote purchases using a credit or debit card as distinct from a Cardholder Present (CP) transaction when the Cardholder makes a purchase and receives the goods
commonly associated with Mail Order/Telephone Order (MOTO). In the mid 1990’s MOTO was joined by Internet (e-Commerce) purchasing which had the result of rapidly increasing the level of CNP purchasing both actual and potential, but without the regulatory framework.

The process of a Credit Card transaction involves the ‘Issuer’ (BarclayCard) providing the ‘Acquirer’ (Barclays Merchant Services) with an authorisation (‘Auth’) that is then passed to the Merchant. A Merchant having received an “Auth” is able to obtain payment without any further form of verification that the goods have been supplied. It therefore follows that, in such an unregulated market, the banks exercise strict control over the approval of Merchants for CNP transactions.

Research with Bank Paribas demonstrated that 40% of all UK businesses are barred from using CNP transactions because of the risk. Research undertaken subsequently shows the figure to be even higher on an International basis. The banks and Schemes (VISA MASTERCARD EUROPAY) all stand to benefit from growth of the CNP business. Security is a huge subject and regularly associated with ‘Fraud’ in the media and by regulatory bodies. This has pawned a growing industry in ‘Public Key Infrastructure (PKI) encryption and ‘firewall’ developments but these are developments of technology without the bedrock of an application providing a viable economic service.

Background to Development Of TALISMAN

Credit Card technology was designed 30 years ago and always envisaged that the cardholder would be present when a transaction was made. The parties to a conventional Credit Card transaction are:
The Consumer and his bank (known as the Issuing bank)

In a transaction the Merchant takes the Credit Card details and seeks authorization from the Issuing bank or a bank payment services provider. The Issuing bank or services provider authorizes the transaction, the Consumer’s account is debited and the money passes (less fees) from the Issuing bank to the Merchant’s account via the acquiring bank. In a “CNP” transaction (for example a mail order or e-Commerce transaction) the same process is undertaken on authorization of the Credit Card, but on this occasion the Consumer does not have the goods.

The acquiring bank is, nevertheless, obliged by contract to pay the Merchant. Hopefully the correct goods, of satisfactory quality, will be delivered to the Consumer. If they are rejected, or if the Merchant defaults, the Consumer may claim the amount paid for the goods from the Issuing bank (commonly known as a “charge-back”) under the terms of the Consumer Credit Act (Section 75). As a result of banks’ concerns over fraud, payment service providers (PSP) have developed which charge Merchants for authorising Credit Cards in the CNP environment. The Issuing banks, however, remain ultimately responsible for Consumer charge-backs.

Weaknesses In a CNP transaction

- There is no mechanism to ensure the Consumer receives the goods ordered.
- A Merchant can obtain funds from the acquiring bank prior to supplying any goods.
- A Consumer card account can charged before receipt of goods.
- The credit/debit card details may have been obtained fraudulently.
· The Merchant may use Credit Card details fraudulently to make multiple purchases.
· The Consumer may never receive the goods (whether as a result of fraud or otherwise).
· The Acquiring bank will lose in a 'charge-back' if the Merchant defaults (liquidation/receivership).

The Issuing bank loses if a stolen or lost or skimmed card is used fraudulently.

The Merchant loses if the goods are intercepted or the Consumer ‘repudiates’ the delivery. Without TALISMAN, the risks for all parties to the CNP transaction are extremely high. When mail order was the principal type of CNP transaction the risk was limited and manageable. With the onset of e-Commerce, CNP transactions rapidly escalated and the Credit Card companies recognised they were exposed to increasing levels of fraud risk. As a result they sought to reduce the risk whilst taking full advantage of the revenue opportunities represented by e-Commerce.

TALISMAN is the first end-to-end solution for cardholder-not-present credit-card transactions that protects all parties in the credit-card payment scheme: Banks, Consumers and Merchants. The unique TALISMAN process provides acquiring banks with the ability to ensure that payment is only released to Merchants when the cardholder has received the goods. TALISMAN provides a verifiable link between the original order and the receipt of goods; this reduces the ability of a Consumer to deny receipt of the goods and demand fraudulent refunds. By using TALISMAN, payment is released to Merchants only after the customer receives the goods, thus eliminating Merchants fraudulently billing acquiring
Since Merchant payments are released only when goods are received, credit guarantee requirements on accepting new Merchants are greatly reduced, allowing smaller Merchants to join the credit-card scheme, and expanding the card market itself to the major benefit of the banks.

Minimising Banks’ Exposure To Fraudulent Consumers

It is a fact that the incidence of Consumers fraudulently claiming refunds on the basis of non-delivery of goods is constantly growing. By implementing TALISMAN, both Merchants and credit-card companies can verify delivery and significantly reduce fraudulent Consumer claims, diminishing the cost of chargebacks.

Minimising Banks’ Exposure To Fraudulent Merchants

If no authenticated delivery can be provided, TALISMAN will not authenticate the transaction and the funds will remain within the banking system, eliminating the possibility for fraudulent Merchant claims. With TALISMAN, Merchants selling non-existent goods or claiming fictitious sales will not be able to receive payment.

The TALISMAN Process

A Consumer with a SMART credit-card orders goods from a Merchant. The SMART card details are processed using a Secure Socket Layer via the scheme to the Issuing bank. The Consumer validates the card by entering his unique SMART PIN number to confirm the order. An authorisation code (“Auth”) and funds are obtained from the issuing bank, (debiting the cardholder’s account) and the funds are passed into a holding account with the Acquiring bank.

The TALISMAN system gives the transaction a unique tracking identification number. The Merchant advises a TALISMAN equipped carrier of
presents his SMART card, which is inserted into a PDA that is loaded with TALISMAN software, and authentication takes place. The card reader ("PDA") validates the card and, upon validation, the cardholder is required to enter his unique SMART PIN number. Provided the card validates the PIN number the transaction is confirmed. The goods are then released to the cardholder. At the end of each period, all TALISMAN Proofs of Delivery are downloaded to the Carrier’s database, which in turn batch-transfers completed transactions to the TALISMAN data centre. The TALISMAN data centre matches the authenticated deliveries against transactions on its database and transfers confirmations to the Acquiring bank. Having received authentication, the Acquiring bank releases funds to the Merchant in accordance with its normal terms.

Security Benefits

TALISMAN satisfies and secures all the expectations of the parties to a CNP transaction. The 'peace of mind' benefits for each party can be summarised as follows. The Consumer is secure in the knowledge that the Merchant cannot obtain his funds until the Consumer validates the delivery. The bank is secure in the knowledge that, because of validation, there is a significantly reduced chance of repudiation, as only the valid cardholder will know the PIN number of their card. The Merchant bank is secure in the knowledge that funds have been secured on the basis of an authenticated delivery. The logistics business is secure in the knowledge that there is a significantly reduced chance of repudiation of delivery.

Increasing Business Volume

There is a significant additional added benefit derived from the TALISMAN system. Due to the potential losses from fraud and early/new business failure, the banks lay down strict criteria for Merchants to be enabled to
to service this sector they do not in themselves solve the problem of fraud and losses where money is obtained prior to completion of the transaction. The new Merchant pays a heavy price for early entry and the banks are aware that if they have a viable solution for this sector they are the beneficiaries of substantial additional revenues.

TALISMAN and its authentication process enables the Acquiring bank to release funds only after verified delivery. This means that the approval criteria can be dispensed with. A Merchant cannot obtain funds until he has completed the transaction in which case any Merchant could be enabled to take CNP transactions.

FIG. 1 illustrates one embodiment showing a method 10 for a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery according to the present invention.

As shown in FIG. 1, a request is made for a TALISMAN sale 12. A Pre Authorization 14 is requested by the acquiring bank 120 and an Auth Response 16 containing an Auth Code is provided by the issuing bank (not shown). A Merchant Response 18 including a TALISMAN ID is then issued and a Log CQR sale 20 is recorded. A CQR Delivery 22 is initiated containing logistics ID supplied by the merchant 110. The CQR Delivery Register 24 is maintained to track accepted deliveries 26. A transaction status change 28, delivery alert 30, batch ID 32 are also used to facilitate tracking the status monitoring. CQR Consignment Delivery Details 34 are maintained along with CQR Details Accepted 36 and CQR Transaction Status Change 38. The Transaction Status Request 40 is made upon Consignment POD 42 at the point of delivery. Upon Acceptance of POD Details 44 a CQR Point of Delivery 46 is made with Proof of
Delivery Details 52. A Post Authorization Settlement 54 is made upon satisfactory acceptance at the point of delivery or a Cancellation CQR Sale 56 is made should the Proof of Acceptance 48 failed. A Report Acknowledgement 58 is made at the conclusion of the transaction.

These and other advantages of the present invention will be apparent to those skilled in the art from the foregoing specification. Accordingly, it will be recognized by those skilled in the art that changes or modifications may be made to the above-described embodiments without departing from the broad inventive concepts of the invention. It should therefore be understood that this invention is not limited to the particular embodiments described herein, but is intended to include all changes and modifications that are within the scope and spirit of the invention as set forth in the claims.
APPENDIX 1

Talisman™

Secure Payment and Delivery System

Functional Overview and High Level System Design

Consultants to the Project
Document Information

Authors:  
David Griffiths  
Valerie Millington  
David Wilson

Date:  
26 October 2000

Version:  
Version 0.3 draft

Reference:  
349/C1/FS/1

Change History

<table>
<thead>
<tr>
<th>Tool used</th>
<th>Microsoft Word 98</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Date</td>
</tr>
<tr>
<td>Draft 0.1</td>
<td>2/10/00</td>
</tr>
<tr>
<td>Draft 0.2</td>
<td>16/10/00</td>
</tr>
<tr>
<td>Draft 0.3</td>
<td>26/10/00</td>
</tr>
<tr>
<td>Draft 0.3a</td>
<td>09/11/00</td>
</tr>
</tbody>
</table>

Distribution

Consult Hyperion  
CQR Technologies  
and third parties authorised by  
Originator  
Issuer  
CQR Technologies

References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CQR Technologies Secure Payment and Delivery System</td>
<td>0.3</td>
<td>26/9/00</td>
</tr>
<tr>
<td></td>
<td>Requirements Catalogue</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1 INTRODUCTION ............................................................................................................. 1
  1.1 PURPOSE AND SCOPE OF DOCUMENT .................................................................. 1
  1.2 DEFINITION OF TERMS .......................................................................................... 2

2 THE BACKGROUND ......................................................................................................... 3
  2.1 PICK-UP ................................................................................................................. 3
  2.2 TRANSPORT ........................................................................................................... 4
  2.3 DROP-OFF .............................................................................................................. 5

3 THE PROBLEM ................................................................................................................ 6
  3.1 IDENTIFYING SOMEONE TO ACCEPT DELIVERY ............................................... 6
  3.2 OBTAINING A SIGNATURE .................................................................................... 6
  3.3 LEAVING THE PACKAGE ....................................................................................... 7
  3.4 LOOHOLES ............................................................................................................. 7

4 THE PROPOSITION .......................................................................................................... 8
  4.1 THE VISION ........................................................................................................... 8
    4.1.1 Remote Shopping ............................................................................................. 8
    4.1.2 Proof of Collection and Delivery ....................................................................... 8
    4.1.3 Proof of delivery (with escrow) ....................................................................... 9
  4.2 SERVICE ROLL-OUT .............................................................................................. 9

5 REMOTE SHOPPING ....................................................................................................... 10
  5.1 CARD FRAUD ...................................................................................................... 11
  5.2 MERCHANT FRAUD ............................................................................................ 11
  5.3 CONSUMER FRAUD ............................................................................................. 11
  5.4 COLLUSIONAL FRAUD ......................................................................................... 11
  5.5 PLUGGING THE FRAUD ....................................................................................... 11
  5.6 THE CQR SOLUTION ............................................................................................ 11

6 THE CQR REMOTE SHOPPING SERVICE .................................................................... 13
  6.1 SERVICE REQUIREMENTS ..................................................................................... 13
    6.1.1 Authentication .................................................................................................. 13
    6.1.2 Non-repudiation ............................................................................................. 13
    6.1.3 Integrity ......................................................................................................... 13
  6.2 CURRENT TECHNOLOGIES .................................................................................. 14
    6.2.1 Smart Cards .................................................................................................... 14
    6.2.2 Public Key Cryptography (PKC) and Public Key Infrastructure (PKI) ............. 14
    6.2.3 Credit Card Data Authentication ...................................................................... 17
  6.3 UK TECHNOLOGY .................................................................................................. 19
    6.3.1 UK Chip Credit Cards .................................................................................... 19
    6.3.2 Financial Transaction Messages ....................................................................... 20

7 IMPLEMENTATION OF CQR REMOTE SHOPPING .................................................. 22
  7.1 WITHHOLDING FUNDS FROM THE MERCHANT ................................................. 24
  7.2 PROOF OF DELIVERY SERVICE .......................................................................... 26
  7.3 REMOTE SHOPPING (VARIANT 1) ....................................................................... 27
  7.4 REMOTE SHOPPING (VARIANT 2) ....................................................................... 28
  7.5 REMOTE SHOPPING (VARIANT 3) ....................................................................... 30
8 THE CQR SYSTEM ARCHITECTURE .................................................. 32
8.1 SYSTEM COMPONENTS .................................................................. 32
  8.1.1 Financial component ............................................................... 33
  8.1.2 Merchant reporting component .............................................. 33
  8.1.3 Logistics dispatch component ................................................. 33
8.2 INTERFACES ............................................................................. 33
  8.2.1 Merchant Information Management Service (MIMS) ............... 34
  8.2.2 CQR merchant service interface ............................................ 34
  8.2.3 The CQR Merchant Financial interface ................................. 36
  8.2.4 The CQR acquirer interface .................................................. 36
  8.2.5 CQR Dispatch Information Service (CDIS) ............................ 37
  8.2.6 CQR Logistics Dispatch Interface (Internal) ......................... 37
  8.2.7 CQR Reporting Interface ..................................................... 38
9 THE FINANCIAL COMPONENT ..................................................... 40
  9.1 The merchant module .............................................................. 41
    9.1.1 Support for merchant service interface ................................ 41
    9.1.2 Support for the merchant financial interface ....................... 44
  9.2 THE ACQUIRER MODULE ....................................................... 45
    9.2.1 Support for the logistics dispatch interface ......................... 45
    9.2.2 Support for the acquirer interface ....................................... 46
10 LOGISTICS DISPATCH COMPONENT ........................................... 47
11 THE MERCHANT REPORTING COMPONENT ................................. 48
  11.1 OVERVIEW ......................................................................... 48
  11.2 FUNCTIONALITY .................................................................. 48
    11.2.1 Support for MIMS ............................................................ 48
    11.2.2 Support for CQR Reporting Interface ............................... 49
12 CQR REMOTE SHOPPING EXAMPLE ........................................... 52
APPENDICES .................................................................................. 54
  A.1 CQR MERCHANT SERVICE INTERFACE DETAIL ..................... 54
  A.2 CQR MERCHANT FINANCIAL INTERFACE ............................... 56
  A.3 CQR ACQUIRER INTERFACE .................................................. 57
  A.4 CQR LOGISTICS DISPATCH INTERFACE ............................... 58
  A.5 CQR REPORTING INTERFACE ................................................ 60
List of Figures

FIGURE 1. SHIPPING RELATIONSHIPS ................................................................. 3
FIGURE 2. SHIPPING DOCUMENT ................................................................. 4
FIGURE 3. POTENTIAL DROP-OFF LOOPOLES ............................................. 6
FIGURE 4. DROP-OFF LOOPOLES ................................................................. 7
FIGURE 5. TRANSACTION ANATOMY ............................................................ 10
FIGURE 6. THE CQR REMOTE SHOPPING PROCESS ................................... 12
FIGURE 7. PKI AND MESSAGE AUTHENTICATION ....................................... 17
FIGURE 8. SDA KEY HIERARCHY ................................................................. 19
FIGURE 9. APACS 29,30 AND 50 ................................................................. 21
FIGURE 10. LEVEL 1 DFD – CQR REMOTE SHOPPING SERVICE ............. 23
FIGURE 11. CQR SERVICE INTERACTIONS ................................................... 25
FIGURE 12. CQR SERVICE COMPONENTS .................................................. 32
FIGURE 13. COMPONENTS AND INTERFACES ......................................... 34
FIGURE 14. CQR SERVICE FINANCIAL COMPONENT ............................... 41
FIGURE 15. INTERFACES TO THE CQR MERCHANT REPORTING COMPONENT 48
FIGURE 16. REMOTE SHOPPING COMPONENTS AND INTERFACES .......... 52
Introduction

Purpose and scope of document

This document provides an overview of the CQR vision for a secure proof of delivery service and the initial planned implementation of the vision within the UK remote shopping environment. Sections 0 to 0 provide the background and an overview of the issues that the CQR service will address. Section 0 then provides more detail of the vision in the remote shopping arena. Sections 0 and 0 provide an overview of the technological options available to CQR in the marketplace and how these components will be utilised within the CQR service. Sections 0 to 0 provide a more detailed architecture and high level design for a system to support a CQR UK remote shopping solution.
### Definition of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>APACS</td>
<td>Association for Payment Clearing Services</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to Business</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Consumer</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>C2C</td>
<td>Consumer to Consumer</td>
</tr>
<tr>
<td>CHV</td>
<td>Card Holder Verification: A means of verifying the holder of a card is authorised to use that card.</td>
</tr>
<tr>
<td>CNP</td>
<td>Card Holder Not Present</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>DDA</td>
<td>Dynamic Data Authentication: A method available within the specification for Europay, Mastercard and Visa chip credit cards to provide CHV.</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay, Mastercard and Visa combined specifications for chip credit cards.</td>
</tr>
<tr>
<td>MOTO</td>
<td>Mail Order Telephone Order</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary Account Number</td>
</tr>
<tr>
<td>PKC</td>
<td>Public Key Cryptography (see section 0)</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure (see section 0)</td>
</tr>
<tr>
<td>PoD</td>
<td>Proof of Delivery</td>
</tr>
<tr>
<td>Public Key</td>
<td>The cryptographic key from an asymmetric key pair which is made public</td>
</tr>
<tr>
<td>Private Key</td>
<td>The cryptographic key from an asymmetric key pair which is kept secret by the owner of the key pair</td>
</tr>
<tr>
<td>SDA</td>
<td>Static Data Authentication: A method available within the specification for Europay, Mastercard and Visa chip credit cards to provide verification that a card has been legitimately issued by an approved card issuer. SDA does not provide CHV.</td>
</tr>
<tr>
<td>UKIS</td>
<td>The specification for the minimum implementation of EMV within the UK credit card environment.</td>
</tr>
</tbody>
</table>
The Background

*Delivery and postal services provide a means of transferring tangible items from a point of origin to a remote point of delivery. The items transported can vary from documents requiring fast and guaranteed delivery, to samples, spare parts and finished goods to end users. The delivery services are provided for a fee, and this is payable by either the sender or the receiver. However, the payment for the goods being shipped is not normally related to the payment for the shipping, even though the cost may be incorporated in a combined invoice. The financial relationship relating to the goods being shipped (where there is one) exists between the sender and the receiver. The financial relationship for the shipping costs exists between the sender and the delivery service. There is no formal relationship between the delivery service and the receiver.*

![Diagram of shipping relationships](image)

2. **Figure 1. Shipping relationships**

The diagram in Figure 1 shows how the delivery service forms a dynamic link between the sender and the receiver, for the duration of the shipment. The delivery service picks up the item to be shipped from the sender, transports it through its own infrastructure, and delivers it to the receiver.

**Pick-up**

*At the point of pick-up, the shipping item passes from the sender to the delivery service, along with the supporting documentation listing both the sender and the receiver, and uniquely identifying the package. At this point, the sender passes the responsibility for delivery to the delivery service, and is billed accordingly. Both the delivery service and the sender have copies of the shipping documents, recording the transfer.*
The pick-up process is unlikely to be the cause of any major dispute because there is a record of the pick-up signed by both parties, and the process would normally operate under an established relationship.

Transport
From the point at which the shipping item is picked up by the delivery service it is monitored by the internal tracking facilities, until it is finally delivered to the address on the label. Once the shipping item has been accepted by the delivery service, it is they who are responsible for it until it is delivered to its final destination and signed for.

The transportation of the shipping item from the pick-up point to the drop-off point falls entirely within the domain of the delivery service, and within this domain the major players have developed some sophisticated mechanisms for tracking packages, from pick-up right through to drop-off. This means that the sender is able to find out, at any time, exactly where any particular package actually is.
Senders are currently able to track packages by
- quoting the Shipping Number to a Customer Services Representative,
- keying the Shipping Number into the relevant web page,
- sending an e-mail containing the Shipping Numbers to an e-mail ‘robot’,
- sending an SMS to a tracking centre,
- keying the details into a touch-tone phone,
- and now by keying details into a WAP phone.

Senders can also request and receive notification of delivery, including the time and the name of the person receiving the specific package.

Drop-off

*The business of a delivery service is picking up packages at one place and dropping them off at another. Whilst it is likely that the delivery service and the sender will have developed an ongoing business relationship, as a result of the number of packages shipped, the same is not usually true of the relationship between the delivery service and the receiver. In the case of goods ordered through remote shopping services, it is likely that the delivery service and the receiver will only experience a single interaction.*

The business relationship underpinning a specific delivery is between the sender and the receiver, and whilst the delivery service will take care to ensure an effective and efficient service, in most cases they are delivering to an address, and the signature confirms only that the package has been handed over. In the case of remote shopping, the delivery service acts as the transport mechanism to move the shipping item from the sender to the receiver. The drop-off process is the final stage in the lifecycle of a specific delivery contract relating to a specific package, and the signature obtained at the point of delivery marks the end of that specific activity. The signature typically does not provide proof that a shipping item was actually received by the addressee.
The problem

The point at which the delivery of packages from a sender to a receiver is most likely to break down is at the point of delivery. At the Pick-up point, the sender and the delivery service have a business relationship, which is not the case for the receiver and the delivery service. The sender and the receiver have a relationship, but it exists only for the duration of the transaction and the fulfilment, and it does not involve any physical interaction. The delivery service, operating as a limited proxy for the sender, completes the physical interaction link between the sender and the receiver necessary for the handing over of the goods. However, because the sender-receiver relationship is only partly transferred to the delivery service, the sender can never be sure that a package was delivered to the right person, and this leaves the process open to fraud.

![Diagram of potential drop-off loopholes](Image)

Figure 3. Potential drop-off loopholes

The diagram above (Figure 3) shows how the delivery of a package to a receiver might potentially fail. The actions above the dotted line represent the desirable conclusion of the sender, which is the successful delivery of the package to the person named on the label, confirmed with a valid signature.

The process of delivery can be broken into three stages:

1. Identifying someone to accept delivery
2. Obtaining a signature
3. Leaving the package

Identifying someone to accept delivery

The delivery driver arrives at the address printed on the package, and locates someone prepared to accept the package, and this might or might not be the addressee. There is a lower chance of the delivery being disputed in the future if the package is handed over to the person named on the label. However, without demanding identification and making a judgement on the spot, there is no way of knowing that the receiver is who they say they are.

Obtaining a signature

The delivery note is signed by the person accepting delivery, and that person might or might not be the addressee. The signature therefore might or might not be the signature of the addressee, but also, even if it is delivered to the right person, the right person might provide a bogus signature. The person making the delivery has no way of knowing.
Leaving the package

*Once the delivery note has been signed, the delivery driver leaves the package with the signatory, and the delivery is recorded.*

Loopholes

*If the package is received by the right person and signed for correctly by the right person, it is likely that the process will have concluded correctly, in the “Yes” area above the dotted line.*

If any of the steps in the drop-off process fall below the dotted line, then there is a potential for some form of delivery fraud. If the wrong person receives the package, and gives false details and a false signature, then the chances of the right person receiving the package is reduced dramatically. If the right person receives the goods, but provides false details and a false signature, then the right person might be in receipt of the package, but might then claim non-receipt of the goods to the sender.

The process is at risk because there is no way of tying the receiver to the delivery service, and no way of tying the receiver to the sender. The reasons for this are summarised in Figure 4 below, and relate to the processes identified in Figure 3.

| The delivery driver can’t tell to whom he is delivering. | The driver can’t make judgements relating to the signature of the Receiver (nothing to compare them with). | It isn’t possible to prove that a package really was delivered because the proof is based on an unverified signature. |

Figure 4. Drop-off loopholes

*In order to plug the loopholes, the drop-off process needs to establish and maintain a position above the dotted line, highlighted by the red arrows. This is the basis of the CQR proposition.*
The proposition
It is recognised that currently there are no commonly available authenticated “proof of delivery” services or systems and this can cause problems because:

- There is no way of knowing that the person who accepts a package is the person it should be delivered to.
- There is no way of knowing that the person who signs has actually signed with a valid signature.

These are general delivery problems, and the people destined to receive packages frequently claim they have not arrived. This represents a large source of unrecoverable costs that must be borne by either the delivery service or the sender.

The CQR proposition is the provision of a proof of delivery service that would be based on some non-personal identification mechanism. The mechanism needs to be non-personal because the job of a delivery driver is to deliver packages, not to take payment for packages, and not to make judgements regarding the identity of the receiver. The proposition is therefore based on the concept of linking the shipping item to the receiver in such a way as to prevent anyone but the approved receiver taking delivery, which would also provide non-repudiable proof of delivery in the process. If this were the case, the delivery driver would only have to confirm the validity of the link between the shipping item and the receiver, and would not have to prove the identity of the receiver.

The Vision
The Vision involves the development and implementation of a non-repudiable proof of delivery service utilising modern technology, in order to remove the need for the delivery driver to make judgements relating to the receiver at the point of drop-off.

There are also a number of value added services that potentially could be established in the same area using adaptations of the proposed technologies. These, and the original vision, are outlined below, and form the basis of an extended service roll-out plan.

Remote Shopping
The Remote Shopping service will remove much of the risk to the e-retailer and credit card acquirer associated with selling goods remotely. This service works by creating a link between the Receiver and the shipping item, initiated by the sender at the point the transaction is authorised. The link established by the CQR service would mean that only the actual purchaser or a person specifically authorised by the purchaser could take delivery of goods purchased.

The Remote Shopping service can also provide protection for the customer using mail order, telephone order or internet shopping, by delaying the settlement of a credit card transaction until proof that the goods have been delivered is received.

Proof of Collection and Delivery
The Proof of Collection and Delivery service will provide non-repudiable confirmation that a particular item was picked-up, and dropped-off, and also that it was actually accepted by the intended Receiver. This means that the Pick-up process is managed by
an accepted mechanism, as is the Drop-off process, and the two processes are linked through the CQR service.

Proof of delivery (with escrow)
This service is similar to that outlined above, but aimed at peer-to-peer buying and selling services involving the transfer of value, such as on-line auctions. In these cases, CQR would either hold onto the value, or delay the settlement until proof of delivery has been received.

Service Roll-out
The initial CQR service will support the Remote Shopping proposition described above, targeted at the B2C market. This will be followed by the Proof of Collection and Delivery proposition, targeted at the B2B market, and later the Proof of Delivery (with escrow) service targeted at the C2C market.

Most of the remaining analysis work that has gone into the development of this document is focused on the initial service proposition of Remote Shopping, and:

- places the Remote Shopping concept into context,
- develops the principles upon which the proposition is based,
- provides the specification of a system to deliver the proposition.

Section 0 develops the concept of Remote Shopping, and the value of its position in the supply chain. Section 0 identifies the technologies that are currently available, that could be used to provide the infrastructure of the Remote Shopping service. The remainder of the document defines the construction and operation of the Remote Shopping service in terms of the components identified in Section 0.
Remote Shopping
The principles supporting any purchase transaction rely on there being a customer able to make a purchase, and a supplier able to fulfil the demands of the customer. Titles and definitions may change, but there will always be one party holding some sort of value, and another party that has goods to offer in return for that value. The transaction is made when value is exchanged for the goods.

In a face to face cash transaction, a token of value is exchanged for some given item, and the exchange takes place in both directions at the same time, leaving neither party at risk. In a face to face credit card transaction the token of value is typically a piece of paper containing the consumers credit details with authentication provided by a hand written signature. Although the risk is increased in this case as the token has no intrinsic value without authorisation and approval from a bank, mechanisms have been developed to manage and minimise this risk.

Payment

Fulfilment

Figure 5. Transaction anatomy

If the components of the transaction are remote from each other, the process is more complicated. One of the reasons for this is that there is no direct link between the payment side of the transaction and the associated fulfilment side.

In remote transactions it is not possible to directly exchange a physical token of value with the required item. This problem has led to the development of a number of remote payment mechanisms, the most common of which is the use of credit cards. The use of credit cards in an environment where it is not possible to verify the person using the card is the cardholder (for example by matching a hand written signature with that on the card) gives rise to Cardholder Not Present (CNP) transactions. The risk to the merchant is significantly increased in CNP transactions as, not only can they not tell that the customer is using their own card, the merchant is held liable for the fraudulent use of credit cards in this environment.

As well as the recognised issues associated with Cardholder Not Present transactions, there are also issues relating specifically to remote vendors. In a face to face transaction, goods and value are exchanged at the same time, meaning that neither party is ever in possession of both. In the case of a remote transaction, at
some point in the exchange, one party will be in possession of both the goods and the value, and currently that party is more likely to be the vendor.

Where a transaction completes under CNP rules, the merchant is at risk as the card details may be bogus. Stolen cards and stolen card numbers present an ever-increasing element of fraud to remote transactions, and Internet transactions are especially vulnerable. If a card number is used fraudulently, and the transaction is subsequently charged back, the financial loss is passed on to the merchant. Where the fraudulent card numbers are used to obtain low marginal cost goods such as pictures, the merchant may be able to stand the loss. However, where the fraudulent card numbers have been used to acquire real goods, the merchant stands a much higher loss.

There are also risks involved for the card acquirers, from potentially fraudulent merchants who receive the value associated with transactions, but who never deliver the goods.

Card fraud
This involves the use of stolen cards, or card numbers, to purchase goods over the Internet. Provided the transaction is authorised, the merchant accepts the transaction in good faith and, therefore, expects to be paid by the card acquirer. The merchant then delivers the goods to the address provided, and receives payment as the transaction is settled. When the transaction appears on the real cardholder’s statement, which could be a month later, the transaction is challenged, and is charged back to the acquirer, and passed on to the merchant. The merchant has now lost both the goods and the value, and is unable to do anything about it.

Merchant fraud
This involves a legitimate cardholder ordering from a dishonest or bogus merchant. The merchant accepts the transaction from the cardholder, submits the transaction for settlement, but the goods are never delivered. In these circumstances, the merchant is likely to either disappear or go out of business, leaving the card acquirer to foot the bill.

Consumer fraud
This involves a legitimate cardholder ordering from an honest merchant. Provided the transaction is authorised, the merchant accepts the transaction in good faith and, therefore, expects to be paid by the card acquirer. The merchant then delivers the goods to the address provided, and receives payment as the transaction is settled. When the transaction appears on the cardholder’s statement, which could be a month later, the transaction is challenged by the consumer who admits ordering the goods but denies having received them. The transaction is either charged back to the acquirer and passed on to the merchant or the merchant is required to deliver a second set of goods. In either outcome the merchant stands the loss.

Collusion fraud
More advanced fraud schemes often involve the collusion of a number of parties such as the merchant and consumer, the delivery driver and consumer or merchant and logistics company to defraud either the merchant or acquiring banks.

Plugging the fraud
The use of bogus card numbers can be reduced if the physical card is required at the point of delivery, merchant fraud can be prevented if payment for goods can be delayed until after the delivery has been confirmed and consumer fraud can be prevented if a non-repudiable proof of delivery is obtained.

The CQR solution
The CQR solution is to develop an integrated service based on a proof of delivery mechanism that will plug both consumer and merchant fraud scenarios simultaneously. The CQR solution may also be used to reduce the instance of card fraud. The service will close the transaction loop by linking the payment process to the fulfilment process, thereby eliminating the potential for merchants to accept payment for real goods without fulfilling the order and, in some variants of the service, eliminating the potential for the fraudulent use of card numbers at the same time by requiring the valid payment card to be presented at the point of delivery.
Figure 6. The CQR remote shopping process
The CQR Remote Shopping Service

This section identifies technologies that are currently available to CQR, and how these may be used to implement the CQR Services. The same technologies will be available for the development and implementation of each of the CQR propositions, and so the contents of this section can apply to Remote Shopping, Proof of Collection and Delivery, and the Proof of Collection and Delivery (with escrow).

Service requirements

CQR requires a technical solution that will provide the following capabilities:

- Authentication
- Non-repudiation
- Integrity

Authentication

In terms of the CQR services, authentication involves verifying all or some of the purchase details given to the merchant by the consumer and passed to CQR.

The CQR service requires the consumer to specify a card used to receive the goods and provide sufficient details to allow card authentication at the point of delivery.

Non-repudiation

Non-repudiation involves ensuring the consumer cannot deny having ordered goods at the point of purchase and receiving the goods at the point of delivery.

For the CQR services the consumer needs to have 'signed' some data or form at the point of delivery and optionally at the point of purchase ensuring they cannot deny purchasing and receiving the goods.

Integrity

For the purposes of CQR integrity refers to the need for CQR to ensure that the information provided by the consumer at the point of purchase (credit card details, delivery card details,...) remain intact and are not tampered with at any point. Modifying this information would open the system to fraudulent use. Similarly, it is vital that the integrity of the electronic proof of delivery is maintained to allow proof of customer non-repudiation of delivery should the need arise.
Current technologies

The CQR services are able to support the authentication, non-repudiation and integrity requirements by using some, or all, of the following technologies:

- Public Key Infrastructure (PKI)
- Dynamic Data Authentication (DDA)
- Static Data Authentication (SDA)
- Digital Certificates

The above technologies are readily implemented on smart cards, and are discussed in the following sections.

Smart Cards

Smart cards have an intelligent chip mounted on them that holds card applications. One of the common uses currently favoured are identity and authentication applications which may be used in PKI schemes.

The CQR scheme aims to provide integrity, identity, authentication and non-repudiation by means of a smart card, and ultimately, obtain a proof of delivery allowing funds to be released to a merchant by an acquirer. In order to do this, the smart cards used must be acceptable to all parties involved in the CQR scheme. This infers the cards used for the scheme must be from a reputable and trustworthy card issuer, such as a financial institution.

Public Key Cryptography (PKC) and Public Key Infrastructure (PKI)

Overview

Public Key Cryptography (PKC), also known as asymmetric cryptography, is a mechanism that can be used to provide authentication, integrity, non-repudiation and secrecy in electronic communications when used within a trusted Public Key Infrastructure (PKI).

PKC works on the basis that there are one way mathematically functions which may act on a message of any length and a fixed length number (key 1) to generate an encrypted version of the message which it is not possible to reverse or decrypt using the same number. However, there exists another number (key 2) that in combination with a mathematical function will decrypt the message. The use of the keys is also reversible – a message encrypted with key 2 may be decrypted using key 1. The combination of keys 1 and 2 is known as a key pair. PKC works by keeping one of the keys in a key pair secret (the private key) and publicising the second key (the public key). There are a number of different mathematical algorithms and key lengths that may be used in PKC, but the most common currently is the RSA labs asymmetric key algorithm.

A Public Key Infrastructure is the combination of PKC with systems, services and policies to provide authentication, integrity, non-repudiation. PKC in its own right can be used to provide secure communication between two parties who each share a key pair in a closed system. However, anybody can generate and use a PKC key pair. In an open system, PKC does not provide any authentication of the identity of the sender of a message or of the integrity of a message as it is not possible to demonstrate the link between a public key and a particular person or system. PKI addresses this issue by the use of trusted third parties who effectively state that a particular public key belongs to a particular person, identity or system. Providing that the user of a public key trusts the third party then they can rely on the public key and can authenticate and check the integrity of communications from the holder of the corresponding private key. The binding between the trusted third party, identity and public key is provided in a digital certificate.
Digital Certificates

Digital certificates are a means of certifying a person's or system's public key. A Certification Authority (CA) who is a trusted party issues digital certificates. A digital certificate holds the public key of a public/private key pair and some data relating to the person or system whose certificate it is, such as name and address. The ITU(T) standard X.509 is the most common standard for digital certificates worldwide.

A digital certificate is signed by the CA's private key, which ensures the integrity of the certificate contents including the certified body's public key. The CA's private key and hence, the signature, can be verified using the CA's public key which is often self signed. A CA may issue different types of digital certificate requiring different levels of proof of the owner's identity. For instance, some classes of certificate may only require proof in the form of an email address to deliver a certificate to; others require an owner's presence and a proof of identity such as a passport. When deciding to trust a certificate, it is important to consider not only the trust placed in the CA, but also the policy followed when identifying the entity being certified.

A digital certificate is valid for a period of time (specified within the certificate) that may be anything up to a number of years. It may be necessary for a CA to revoke a certificate whilst it is still valid (for example if the private key becomes public). For this reason, CAs maintain directories of revoked certificates and typically publish these as certificate revocation lists (CRL) or 'hot lists' on a regular basis. Prior to trusting a certificate, the relying party should check the current CRL or query the CA directly using OCSP ('online certificate status protocol').
Authentication and Integrity using PKI

Imagine that Sam wishes to verify a received message was really sent by Alex. If the message was handwritten on paper, Alex would typically sign the document as a means of authentication. Alternatively, if the message is sent by electronic means it is possible to attach a digital signature using PKI.

In order to attach a digital signature to a message, Alex’s system first creates a short digest of the message using a one way mathematical hash function. The message digest is then encrypted using Alex’s private key. This encrypted message digest is known as a digital signature.

When Sam receives the message, a system uses Alex’s public key (possibly taken from a digital certificate sent with the message) to decrypt the signature and reproduce the message digest. The system then applies the same hash function to the message and compares the resulting digest with the decrypted signature. If the digests match, the signature has been validated.

If the hash function is collision free (ie no two messages will result in the same digest), then the process of checking the digital signature has also ensured integrity of the message. If the message was modified between Alex and Sam then the digest generated by Sam’s system would not match the decrypted signature and hence Sam would know not to trust the message.
Figure 7 illustrates how PKI can be used for message authentication.

**Figure 7. PKI and message authentication**

Secrecy using PKI

In the above example, the message signed by Alex could be read by any recipient and the signature checked by anyone who had access to Alex’s public key. The message is not secret between Alex and Sam.

In order to securely encrypt the message such that only Sam could read it, Alex would need to make use of Sam’s public key. A message encrypted with Sam’s public key may only be decrypted using Sam’s private key, which is known only to Sam.

Digital signatures may be combined with secrecy in the above example if the message is signed using Alex’s private key and then encrypted using Sam’s public key.

In reality, public key encryption algorithms tend to be too slow to use to encrypt entire messages and as a result are combined with traditional shared key (or symmetric) encryption algorithms which tend to be quicker for encryption and decryption. In this case, the message is encrypted using a shared key. The shared key is then encrypted using the recipient’s public key and sent along with the encrypted message.

**Credit Card Data Authentication**

The major credit card schemes in Europe between them produced a standard for a smartcard based credit card scheme known as EMV (Europay, Mastercard and Visa). EMV supports two data authentication techniques used to validate the data stored on the chip card, Dynamic Data Authentication (DDA) and Static Data Authentication (SDA).
DDA is very similar to PKI and uses a digital signature scheme to authenticate the card. The card contains its own key pair with the public key contained in a certificate signed using the card issuer’s private key. The card also contains a certificate for the issuer’s public key, signed by the card scheme CA. Dynamic data authentication validates the certificates on the card and then issues some random challenge data to the chip card. The chip card encrypts the challenge together with some key data such as card number and expiry date using its private key. The terminal may then decrypt the encrypted data and verify that the results match the information on the card and the random challenge data. If the card forces the use of a pin or biometric (e.g., fingerprint) identification before using the private key, DDA can be used to provide card authentication with card holder verification (CHV) provided by the use of the pin or biometric.

SDA uses a similar trust hierarchy to DDA and PKI, but with no card or cardholder key pair. SDA works because a terminal that knows the scheme CA’s public key can validate that the consumer’s card has been issued by a body approved of by the CA, and that the static data on the card, such as card number and expiry date, has not been tampered with.

In order to use SDA for authentication the following trust hierarchy is utilised:

1. The static data on the card is signed using the card issuer’s private key
2. The card issuer’s private key is verified by the card issuer’s public key
3. The issuer’s public key is signed by the CA’s private key
4. The CA’s private key may be verified by the CA’s public key
The following diagram describes the key hierarchy:

![Key Hierarchy Diagram]

**Figure 8. SDA Key hierarchy**

With this trust hierarchy in place the static data on the card can be taken as genuine and used as a comparison for other data. So, SDA provides a method of authenticating credit card details, which can also be used for identification at the point of delivery.

UK Technology

*The initial implementation of the CQR services is assumed to be in the UK market. This section discusses the technological options available to CQR in the UK and includes information on smart credit cards commonly available. The mechanisms used to communicate financial data between merchants, acquirers and issuers are also discussed.*

UK Chip Credit Cards

The UK implementation of EMV is called UKIS (United Kingdom Integrated Circuit Card Specification). UKIS specifies the minimum level of support for EMV required by UK chip credit cards and does not currently require DDA or CHV. However UKIS does require SDA in all cards that may be used off-line. Cards that require on-line authorisation for every transaction (such as Visa Electron or Solo) are not required to incorporate SDA.

The majority of card issuers who have implemented EMV chip cards to date have implemented the minimum functionality as specified by the UKIS standard. The only significant exception is American Express who have issued a chip version of their Blue card which includes a PKI application and cardholder verification using PIN in addition to the basic UKIS application.

To date, approximately 10% of UK credit cards have been issued as chip cards including the UKIS application. At the end of August, there were 9 million UKIS chip cards in circulation and this number is
expected to grow to 12 million by the end of the year. The Visa scheme has set a deadline of 2005 for all Visa cards to be chip based and incorporate an EMV application.

A number of card issuers have been developing schemes to address consumer concerns regarding the use of their credit card number on the internet. Typically these schemes involve the use of virtual card numbers or one time use credit card numbers for internet transactions, removing the risk that dishonest merchants or unauthorised persons could make use of the card numbers obtained from intercepting internet communications or merchant databases.

**Financial Transaction Messages**

*The communication between merchants and the major acquirers within the UK is defined in various APACS standards.*

- APACS 29 section 4 (sometimes referred to as APACS 29b) defines the batch message format for financial transactions including sales, refunds and cash advance.

- APACS 30 defines the merchant terminal equipment and the conversations between the merchant terminal and the acquirer for the online transaction authorisation process.

- APACS 40 is an extension of APACS 30 that supports online real-time financial transactions and merchant reconciliation in addition to transaction authorisation.

- APACS 50 supports the transfer of financial messages between merchant terminals and a polling bureau. The polling bureau subsequently forms APACS 29 section 4 batches for forwarding to the relevant acquirers.

*At the time of writing, it is believed that the majority of merchants and acquirers in the UK use APACS 50/29 and APACS 30. APACS 40 is less common due to the overhead placed on acquirer systems by the online processes. The initial CQR services will provide a solution that can interoperate with the traditional APACS 29, 30 and 50 processes.*
Figure 9 illustrates the relationship between APACS 29, 30 and 50 messages.

**Figure 9. APACS 29, 30 and 50**
Implementation of CQR Remote Shopping

This section brings together the service CQR wishes to implement with the currently available technology discussed in the previous sections. The technology available in the UK at the moment is enough to implement CQR services with varying levels of security making use of the SDA and PKI applications present on payment cards. The varying degrees of security depend on whether SDA or PKI are used singly or in combination. It is important to note CQR are not aiming to eliminate credit card fraud but to provide proof of delivery to an acquirer before monties are released to merchants and to provide a transaction audit trail. The audit trail is expected to be useful in combating fraud. Some variations of the CQR service will significantly reduce specific fraud by ensuring that the valid payment card is present at the point of delivery, making it harder for a consumer to use a rogue credit card number for a transaction. The delivery will involve the authentication of consumer purchase details and consumer non-repudiation. As the variety of cards increases with different security implementations the CQR services can be adapted to incorporate their features, thereby increasing security.
Figure 10 illustrates the different parties involved and the main data, which is required to be passed around the system for a completed CQR transaction.
The complete CQR Remote Shopping service consists of two elements:

1. A facility to enable the acquirer to withhold funds from the merchant
2. A facility to obtain a proof of delivery from the customer

These two features of the CQR Remote Shopping service mean that merchants will get paid as soon as the goods ordered by a customer have been delivered, and that customers subsequently cannot claim that goods were never received. Withholding funds from the merchant

The initial design for the CQR service assumes that the merchant may use commercial off the shelf solutions for credit card processing / internet commerce servers.

In order to minimise the modifications required to merchant and acquirer systems, CQR will intercept APACS 29 section 4 batches sent to an acquirer, break them down into the individual transactions and hold the individual transaction elements until proof of delivery is received from the logistics company. At that point the individual transaction elements relating to the delivered goods can be re-assembled into a new APACS 29 batch and forwarded to the acquirer. The individual financial transactions are not modified in any way whilst held in the CQR system. As refund and cash advance transactions are not relevant to the CQR system, these will be passed straight through the system and incorporated in the next batch sent to the acquirer.

Figure 11 illustrates the communications between the merchant and acquirer and shows the CQR involvement in the process.

Merchants using the CQR scheme will need to consider the effect of the validity period of transaction authorisations. At the point a merchant authorises a transaction, the authorisation agent may check that the card number is valid and that there are sufficient funds or credit available for the transaction. The available funds or credit for that card are then reduced by the transaction amount to ensure that any balance or credit limits are not exceeded and that the funds are available when the related financial transaction is processed. After a period of time, if the card authorisation has not been used, the authorisation lapses on the assumption that the transaction will not proceed. The available balance is reset to be what it was before the authorisation amount was deducted. If the financial transaction is submitted after the authorisation has lapsed there is no guarantee that the funds will be available to the merchant or that the transaction will be honoured.

The validity period for a credit card authorisation is usually a reasonable amount of time for a delivery to be made, proof obtained for the delivery and CQR to submit the financial transaction to the acquirer. As an example, the validity period is 30 days for Amex and 15 days for Visa cards. However, debit cards such as Switch tend to have a much shorter validity period due to the cumulative effect on customer's available bank balances. Debit cards may have validity periods as short as 24 hours. As a result, it is not recommended that debit cards are used with the CQR system.
Figure 11. CQR Service interactions
Proof of delivery service

There are currently three potential Remote Shopping service variants, defined as follows:

**Variant 1**  Deliver the goods to the UKIS card that made the purchase.

**Variant 2**  Deliver the goods to a PKI card specified at the point of purchase with payment being made by any credit card.

**Variant 3**  Deliver the goods to the PKI and UKIS credit card that signed the purchase using PKI, combined with UKIS SDA for additional authentication at the point of delivery.

Each of these service variants is described in more detail in the following sections.

**Variant 1** is suitable for mail order, telephone order and Internet shopping using the UKIS credit card details as the authenticating details at the point of delivery. Variants 2 and 3 are more suited to Internet shopping and would not work in the mail order and telephone order shopping (MOTO) environments. They involve the use of PKI and require X.509 certificate details to be passed to CQR via the merchant, which is more Internet oriented in implementation.

The variants of the Remote Shopping service have the following features in common:

1. The card used to provide customer authentication at the point of delivery must be specified at the point of purchase.

2. The delivery is to a specified card and not to a person. The customer may choose where they wish to accept delivery, as long as they have the specified delivery card with them.

3. Sufficient information is provided to the logistics company making the delivery to allow them to identify and authenticate the recipient card. However, additional information is required from the chip on the card in order to produce a proof of delivery. This provides consumers, merchants and acquirers with some protection from fraud during the delivery process.

4. Proof of delivery is obtained by the logistics company and is passed to CQR. CQR then pass the merchant’s request for funds on to the credit card acquirer as discussed in section 0.

5. The service provides proof that a delivery has been made, not that the correct goods or services have been provided. It is the recipient’s responsibility to check the goods prior to accepting the delivery or to utilise traditional returns channels should a problem arise after delivery.

The proof of delivery is the mechanism by which an acquirer knows monies can be safely released to the merchant. The acquirer is safe to release the funds, in the
knowledge that the consumer has received the goods, and that the specified delivery card has been authenticated. Additionally, some service variants allow for a digital signature to be provided at the goods ordering stage as a proof of purchase. In order to allow the consumer to digitally sign some of the order details, the consumer will need a smart card reader for their PKI credit card and the merchant must provide a supporting web site. The web site may be required to provide the order and delivery details to the smart card plug-in in the consumer’s browser, allowing the order to be digitally signed. Although fine in theory, this is not current functionality in the majority of commerce servers. It is expected the majority of small internet merchants will use off the shelf products as a basis for their shopping site, and it may be necessary for CQR to implement a service allowing merchant sites to redirect to a CQR hosted site at the point where any PKI processing is required.

Remote Shopping (Variant 1)

Variant 1 requires that the card used for payment is a UKIS chip card, which supports offline transactions and SDA, and the same card is used to accept the delivery. CQR will be passed the credit card details by the merchant. These card details are then used to identify the relevant financial transaction, provide card identification and authentication at the point of delivery and obtain proof of delivery. The proof of delivery will be provided using the static data and SDA on the UKIS card. In order to protect consumer credit card information, the credit card number and expiry date is not transmitted in its entirety to the logistics company delivering the goods. Instead, a collision free, secure one way hash of this data is provided which can be used for authentication at the point of delivery. In order to remind recipients of the required card, the last four digits of the card number will be provided.

**Variant 1 of the Remote Shopping service incorporates the following steps:**

1. The consumer selects some goods for purchase and passes some credit card details to the merchant.

2. The merchant passed the credit card details to CQR to ensure that they are valid for use within this variant of the scheme.

3. Assuming the credit card is suitable for use, CQR assign a transaction identifier enabling the CQR transaction to be tracked from the merchant, to the logistics company and to the acquirer.

4. The merchant seeks credit transaction authorisation from an authorisation host by sending an APACS 30 message.

5. The merchant receives a credit authorisation in response and then passes on the authorisation details to CQR.

6. The merchant supplies the delivery name and address and consignment number to the logistics company. The details needed to authenticate the recipient card at the point of delivery are passed to the logistics company from CQR.
7. At the point of delivery, the consumer hands their card to the delivery driver who uses a hand held device to ensure the signed static data on the card passes SDA and the details match those provided by CQR.

8. A proof of delivery message containing the static data from the recipient card is passed to CQR from the logistics company. CQR validate the proof of delivery to ensure that it is correct. CQR then create an APACS 29 batch corresponding to the valid proofs of delivery received since the previous APACS 29 batch. The acquirer may then release funds to the merchant (see Figure 9 and Figure 11 for the flow of financial data).

Variant 1 of the remote shopping service relies on the same UKIS card details being used at the point of purchase to buy goods and at the point of delivery to authenticate the delivery. Whilst this will not prevent someone from fraudulently using an unreported stolen UKIS card for the purchase and delivery of goods, it will prevent fraudsters from using credit card numbers where they do not posses the valid corresponding chip card. The service does not allow for the consumer to provide non-repudiation of purchase for the remote transaction. To gain consumer non-repudiation at the point of purchase and delivery, PKI can be used to supply a digital signature authenticating the card and the consumer. This option forms variant 3.

There are a small subset of smart credit cards which, although UKIS, are unsuitable for use with variant 1 of the CQR remote shopping services. Credit cards that enforce the use of virtual or single use card numbers for remote transactions may not be used with this service as it is not possible to identify and authenticate the card at the point of delivery. Additionally, on-line only cards such as Visa Electron or Solo may not be used with the scheme as they do not support the SDA application required to provide the proof of delivery.

Remote Shopping (Variant 2)

Variant 2 does not require the consumer to use the same card for payment as the card used for proof of delivery. The payment card can be any credit card, chip or non-chip. A PKI card will be used to digitally sign data at the point of purchase and delivery providing consumer non-repudiation and card authentication. The card used to authorise the purchase and the card specified to be the delivery card at the point of purchase must be PKI cards recognised and accepted by the CQR scheme.

Variant 2 allows the consumer to pay with a different credit card to the delivery card in a secure environment. In terms of flexibility of service, consumer 1 can purchase a gift from a merchant and have it delivered to consumer 2. Consumer 1 enters the purchase details and includes the X.509 certificate of the specified delivery card, which is the PKI card belonging to consumer 2. Consumer 1 may obtain the necessary X.509 certificate of consumer 2 from consumer 2 directly, e.g. via email or from a directory service provided by the PKI card vendor.
It is possible that CQR may, in the future, supply a directory service, allowing consumers to register their certificates along with a means of identification such as an e-mail address. Customers could then obtain the recipient's digital certificate from the CQR directory service simply by knowing the recipient's e-mail address.

As variant 2 of the CQR remote shopping service requires orders and delivery details to be digitally signed, it is not suitable for mail order to telephone order transactions. However, it should be possible to utilise this service using fixed or mobile Internet services (e.g. using a PC with a smart card reader or a dual slot SIM card phone).

**Variant 2 incorporates the following steps:**

1. The consumer selects some goods to purchase and specifies the PKI card to be used for delivery. The consumer digitally signs some of the purchase order data and delivery details, providing consumer non-repudiation for the purchase. The merchant passes the order details and consumer's X.509 certificate to CQR.

2. CQR assigns a transaction identifier enabling the CQR transaction to be tracked from the merchant, to the logistics company, and to the acquirer.

3. The merchant seeks credit card transaction authorisation from an authorisation host by sending an APACS 30 message.

4. The merchant receives a credit authorisation response and then passes on the authorisation details to CQR.

5. The merchant supplies the delivery name and address and consignment number to the logistics company. The card authentication details needed to authenticate the recipient via their PKI card at the point of delivery are passed to the logistics company from CQR.

6. At the point of delivery, the consumer hands their PKI card to the delivery employee who uses a handheld device to generate a random challenge. The recipient enters their PIN and digitally signs the challenge with their private key. The signed challenge is verified using the corresponding public key by the handheld device. The X.509 certificate is verified by its distinguishing ID and by the CA’s public key.

7. The proof of delivery in the form of the consumer’s digital signature is passed to CQR from the logistics company. CQR batch together the APACS 29 requests with the proof of delivery and pass the batch to the acquirer. The acquirer may release funds to the merchant.

*With variant 2, the consumer may order goods and have them delivered to anywhere they want provided the PKI card specified at the point of order is available for authentication at the point of delivery. For the gift scenario, surprise deliveries are not appropriate, the gift recipient has to know when and where the delivery is going to take place and have the assigned delivery card on their person.*
At the point of delivery, there is no SDA check and the card used to actually purchase the goods is not required. This service could, potentially, allow a fraudulent customer to enter invalid, illegal or stolen credit card details. However, the fraudulent purchase order would be signed with the customer's own digital signature. If we assume the PKI card is likely to be used by the valid cardholder because only the valid cardholder would know the PIN, then the fraudulent customer has, by definition, identified themselves to the relevant authorities. The credit authorisation request may be passed initially by the acquirer if there are no current details of fraudulent card use, but if the digital signature has been used a clear audit trail is available, and the customer can be traced easily.

For this reason, CQR may limit the PKI smart cards permitted for use within the scheme to those containing a digital identity from a trusted third party who have performed a reasonable level of card holder identification and authentication prior to issuing a digital certificate. In order to allow investigation of the fraudulent use of the service, the CA will need to be able to provide the physical identity of the card holder to the relevant authorities should the need arise. It is, therefore, inappropriate for the CQR scheme to accept certificates which purely validate that the owner has an active e-mail address and do not verify any further details about the individual.

In comparison, variant 2 provides better consumer identity than variant 1 of the service by offering an audit trail to follow should a fraudulent transaction occur. This is one of the strengths of PKI, allowing a PKI card to authenticate and verify an identity.

Remote Shopping (Variant 3)

Variant 3 combines the UKIS and PKI applications using a single card for both payment and delivery, which can be authenticated by SDA and a digital signature. The limitation of this variant is that the card used for the purchase must be the card used for the delivery, and must implement both the PKI and SDA applications (eg. Amex Blue). To complete this variant of the Remote Shopping transaction, the merchant must forward the credit card details and the X.509 certificate from the card used to purchase the goods to CQR. Credit authorisations are carried out as for the previous service variants, between the merchant and an authorisation host, and the logistics company receives the card details associated with SDA and the X.509 certificate details associated with PKI, to authenticate the card specified for delivery. Customer authentication is provided by the information held in the X.509 certificate and by the SDA, and the digital signature supplied by the private key of the consumer provides the consumer non-repudiation of purchase and delivery.

Variant 3 incorporates the following steps:

1. A consumer selects some goods to purchase and digitally signs the purchase order data, providing consumer non-repudiation at the point purchase. The merchant passes across the credit card details, which will be used to verify the SDA at the point of delivery along with the X.509 certificate details to CQR.
2. CQR assign a transaction identifier enabling the CQR transaction to be tracked from the merchant, to the logistics company and to the acquirer.

3. The merchant seeks credit authorisation by sending an APACS 30 message to the authorisation host.

4. The merchant receives a credit authorisation and then passes on the authorisation details to CQR.

5. The merchant supplies the delivery name and address and consignment number to the logistics company. The card authentication details needed to authenticate the appropriate recipient via their X.509 certificate (public key, X.509 distinguishing Id) and credit card data for SDA, at the point of delivery are passed to the logistics company from CQR.

6. At the point of delivery, the customer hands their PKI/UKIS credit card to the delivery driver. The card data held in the hand held device used by the delivery driver is used to authenticate the SDA information on the card. Following the SDA, a random challenge is generated by the hand held device. The consumer enters their PIN number and digitally signs the challenge with their private key, and the corresponding public key on the hand held device verifies the digital signature.

7. The proof of delivery in the form of the static data and signed challenge is passed to CQR from the logistics company. CQR then assembles an APACS 29 batch corresponding to the proofs of delivery received, and sends this to the acquirer. The acquirer may release funds to the merchant.

**Variant 3 is the most secure of all the offered CQR services with SDA and a digital signature required at the point of delivery. The additional security comes from the same card being used to supply the necessary credit card and X.509 certificate details at the point of purchase and again at the point of delivery. Potential fraudulent use of the card is limited by cardholder verification based on the presence of the card and use of the associated PIN.**
The CQR System Architecture

As CQR are, themselves, a start-up company, it is likely that acquirers may wish to retain a level of control over the service. For this reason, the architecture of the systems that support the CQR service will be such that all credit card data and financial transactions will be stored and processed within a single component, which could be hosted securely by the acquirer. Additional components providing merchants with reconciliation and the interface to the logistics companies could be co-hosted with the main acquirer component or implemented on separate platforms.

![Diagram of CQR service components](image)

**Figure 12. CQR service components**

System components
The CQR system can be split into three independent but interconnected components:

- **Financial component**: deals with all merchant credit card processing transactions.

- **Merchant reporting component**: provides transaction reporting to the merchant.

- **Logistics dispatch component**: provides the pre and post delivery interface to logistics companies.

*These are described in more detail below.*
Financial component

This is the only part of the system which processes and stores credit card details. In addition to providing the generic merchant interface for transaction notification, an acquirer specific component receives batched financial transactions from the merchant and provides the interface to the existing acquirer systems. In the UK, the acquirer specific component will implement APACS 29 section 4 financial transactions.

In addition to this, the financial component will also validate the proofs of delivery, which has been received from the logistics company, prior to passing on a request for funds to the acquirer. The validation is performed within the financial component rather than the logistics dispatch component as it is necessary to use the consumer’s credit card details for SDA.

Merchant reporting component

This component provides information to the merchant to allow tracking and reconciliation of transactions. Information provided to the merchant would include transactions awaiting proof of delivery (e.g. transaction date, CQR id, merchant id, amount) and details of batched financial transactions sent to the acquirer. The component also provides a mapping between merchant financial batches and CQR – acquirer financial batches. Consumer credit card details will not be available from this component.

Logistics dispatch component

The Logistics Dispatch Component stores CQR delivery details (e.g. CQR ID, destination identification details, etc) and data on CQR registered logistics companies. Once proof of delivery is received from the logistics companies, the component will pass this information to the financial component, which will validate the proof of delivery. Consumer credit card number and expiry dates will not be available from this component.

Interfaces

The interfaces between the three CQR service components are defined so no credit card numbers or expiry dates are passed between them ensuring CQR does not have access to such sensitive data. Nevertheless, the interfaces will contain financial information and will therefore be encrypted and require mutual authentication to prevent tampering.

The links from the components to the merchant, acquirer and logistics company are assumed to be Internet links for the remainder of this document. A secure Internet link would be used for the merchant to retrieve transaction data from the reporting component and the logistics company to retrieve card authentication details from the logistics dispatch component. The merchant will have to submit requests to use the CQR service via the internet but may submit the APACS 29’s as usual, using X.25 to the financial interface.

Figure 13 illustrates the internal and external interfaces of the CQR system for the remote shopping services.
Figure 13. Components and interfaces

Merchant Information Management Service (MIMS)

The merchant reporting component of the CQR system provides transaction tracking and accounting management information to merchants who are part of the CQR scheme. The merchant accesses the information on their CQR transactions using the Merchant Information Management Service. MIMS provides two ways for merchants to view and use data relating to their transactions:

- Summary information with drill down capability is provided on a web server, accessed over the internet using HTTP over SSL v3.

- Detailed transaction history and other reports may be downloaded securely as CSV files over the internet using SSL v3 connections. The CSV files are suitable for loading into most spreadsheet or database packages.

In order to use either of these reporting options a secure connection must be set up between the merchant and MIMS. Both parties will authenticate themselves during connection setup before any information is made available to the merchant.

Details of the services offered over MIMS can be found in section 0.

**CQR merchant service interface**

The CQR merchant service interface provides an online bi-directional interface between the merchant and CQR. The interface is used to allow the merchant to request CQR service for a consumer transaction and to notify CQR of any cancelled transactions.

The CQR merchant service interface allows the merchant to send and receive the following data to and from CQR:
1. **Request CQR Sale**: The merchant provides details of a sale and requests to use the CQR service to manage the proof of delivery. The response to this message provides the CQR Transaction ID to the merchant.

2. **Authorise CQR Sale**: Once the merchant has obtained an authorisation code from the acquirer for the CQR credit transaction, the information should be passed to CQR using the **Authorise CQR Sale** message.

3. **Sign CQR Sale**: In order to progress a CQR sale using a PKI service the consumer must digitally sign the order and delivery details. These details and the signature are then passed to CQR.

4. **Cancel CQR Sale**: The merchant provides details of a sale that it no longer wishes to progress using the CQR service.

5. **CQR Merchant Response**: Response from the CQR financial component to the merchant indicating the success or failure of the four messages above.

*The CQR Transaction ID is used throughout the process and provides a way of tracking a CQR transaction from start to finish. The transaction ID must be clearly displayed in machine-readable format on the address label or goods packaging when shipped from the merchant. The format of the transaction ID to be attached to goods by the merchant is to be decided. It will be a machine-readable format such as a barcode or characters suitable for reliable OCR. The hand held device used for proof of delivery will be able to read this ID and use it to drive the proof of delivery process.*

*It is recommended that a merchant submit a Request CQR Sale message before communicating with the acquirer to authorise the credit card transaction. The request to CQR will include the type of card to be used and validates the card being used is suitable and authorised for the CQR service.*

*The Authorise CQR Sale message may take place some time after the sale request as the merchant may wait until he is ready to dispatch the goods before obtaining acquirer authorisation for the transaction. This maximises the available window to obtain the proof of delivery whilst the authorisation is still valid. The merchant must receive a positive CQR Merchant Response for an Authorise CQR Sale message before including the transaction on the CQR merchant financial interface.*

*The Sign CQR Sale message must occur after the Request CQR Sale message. There is no requirement for the sale to be authorised before it is signed or vice versa.*

*Cancellation of a CQR sale shall not result in the transaction details being removed from CQR databases. Instead, they will be marked as cancelled and a date of cancellation attached. This is to ensure that an audit trail is available to the merchant.*
Details of the data contained within these messages and the technical requirements for the interface can be found in appendix A.1

The CQR Merchant Financial interface

The CQR merchant financial interface replaces the traditional direct link between the merchant terminal and acquirer for financial transactions (request of funds). In order to minimise the change required for the merchant and to provide CQR with the necessary information for later use on the CQR acquirer interface, the interface will follow the APACS 29 section 4 messages and batch format. APACS 29 section 4 defines the message and batch format for the following financial transactions:

- Sales
- Refunds
- Cash Advances

In order to utilise the CQR financial interface the merchant/merchant's polling bureau should be able to simply reconfigure the destination for the existing APACS 29 batches from their system to that of the CQR system merchant financial interface.

Details of the data contained within these messages and the technical requirements for the interface can be found in appendix A.2.

The CQR acquirer interface

The CQR acquirer interface is used to pass merchant financial transactions to the acquirer based on the saved APACS 29 data received from the merchant. Refunds and cash advances are passed straight through the CQR system from the CQR merchant financial interface and batched together with Sales for which a proof of delivery has been received and validated. In order to minimise the change required within the acquirer systems, the interface will follow the APACS 29 section 4 standard for financial transactions.

A regular batch will be built for each merchant and transmitted to the acquirer containing:

- All refunds and cash advances passed from the merchant financial interface
- All sales for which proof of delivery has been validated and which have not previously been passed to the acquirer.

Details of the data contained within these messages and the technical requirements for the interface can be found in appendix A.3.

---

1 There is a transaction reversal mechanism built into APACS 29 section 4. Further investigation is required into whether this is used in practice. If this is used, then the CQR system will need to be designed to cope with reversing transactions. For refunds and cash advances, these transactions would be simply built into a reversal batch sent over the CQR acquirer interface. Further thought is required into the impact of reversals of sales in the various states.
CQR Dispatch Information Service (CDIS)
The CQR dispatch information service provides the link between the CQR system and logistics companies. The logistics dispatch component provides the CDIS interface to logistics companies operating the CQR service, allowing them to download the required information to identify the recipient card for CQR deliveries and upload proof of delivery information once the delivery has been completed.

Details of this interface are to be decided following discussions between CQR and logistics companies.

CQR Logistics Dispatch Interface (internal)
The CQR logistics dispatch interface provides the link between the CQR financial component and the logistics dispatch component.

The logistics dispatch interface allows the CQR financial component to pass information on CQR deliveries to the dispatch component (ready for collection by the logistics companies) and receive proof of delivery information back from the dispatch component for validation.

The messages supported by the logistics dispatch interface are:

1. Register CQR Delivery: Information required to organise and validate a delivery is passed from the financial component to the logistics dispatch component.

2. Delivery Accepted: The logistics dispatch component uses this message to indicate that it has successfully received a Register CQR Delivery message.

3. CQR PoD: The logistics dispatch component uses this message to pass proof of delivery information to the financial component.

4. Proof Accepted: The financial component uses this message to indicate that it has successfully received a CQR PoD message.

The contents of the Register CQR Delivery message vary according to whether just UKIS SDA is used or whether PKI is used as well.

UKIS deliveries use a one way hash on the card PAN and expiry date (contained in the Register CQR delivery message) to provide the identification needed to accept a recipient card\(^2\). For these services the recipient card is the card used to purchase the goods. At the point of delivery, the hand held device will perform the same hash algorithm on the card PAN and expiry date and ensure the hashes match prior to authorising the delivery. The delivery authorisation is performed using UKIS SDA to

---

\(^2\) It is therefore, important that the customer is told that they will require the same card to accept the delivery. If the order was made at the end of the validity of the card, the identification and proof of delivery would not work with the customer's replacement card. A mechanism will be required to deal with delivery to customers whose card is lost/stolen between ordering the goods and accepting delivery.
ensure that the card is a legitimate UKIS card. Relevant data is also passed back to CQR to allow a double check prior to releasing funds. In order to aid the recipient of the goods to remember which card they used at the point of order, and as a double check that the correct delivery is being made, the card holder name and last four digits of the card number\(^3\) are also provided. These will be displayed on the hand held terminal.

For PKI deliveries, the Register CQR Delivery message will contain the certificate\(^4\) for the PKI card intended to accept delivery and the delivery card reminder specified by the consumer at the point of sale. The hand held device may display the delivery reminder message to allow the consumer to identify the correct card to be used to receive the goods. At the point of delivery the hand held device will issue a challenge that will be hashed and encrypted with the consumers private key on their PKI card. The public key from the certificate passed by CQR will be used to verify the digital signature (challenge data + encrypted hash) of the consumer, and along with the certificate distinguished id will verify the X.509 certificate and public key on the consumers PKI card.

For PKI + UKIS deliveries, the Register CQR Delivery message will contain both sets of information outlined above.

The logistics dispatch component responds to the Register CQR Delivery message with a Delivery Accepted message once it has successfully received and processed the message. After a timeout, the financial component will periodically resend the Register CQR Delivery message until it receives a Delivery Accepted response.

The financial component responds to the CQR PoD message with a Proof Accepted message once it has successfully received and processed the message. After a timeout, the logistics dispatch component will periodically resend the CQR PoD message until it receives a Proof Accepted response.

Details of the data contained within these messages and the technical requirements for the interface can be found in appendix A.4.

CQR Reporting Interface
The CQR reporting interface is used to notify the merchant reporting component of changes of status of CQR transactions. It also allows CQR to maintain details of responses to the merchant. The purpose of the merchant reporting component is to allow merchants to obtain accurate information on the status of their CQR transactions. The interface also provides financial information to allow the merchant to reconcile financial batches from their terminal equipment with the financial batches submitted to the acquirer by CQR.

The CQR reporting interface therefore supports a number of messages:

\(^3\) It would be possible to expand this to include an issuer description based on the card BIN.

\(^4\) Note that, if required, this may be reduced (by the logistics company) to a certificate identifier and public key before being passed to the hand held device used to authenticate delivery.
1. **Log CQR Sale:** Information is passed from the financial component to the reporting component when a successful CQR Sale Request from a merchant is processed.

2. **CQR Transaction Status Change:** Information is passed from the financial component to the reporting component when a CQR transaction changes status (e.g. Cancelled, Authorised, Signed, Merchant Requests Funds, Delivery in Progress, Delivered, PoD validated or Sale complete).

3. **CQR Merchant Batch Summary:** summary of financial transactions received on the CQR Merchant Financial interface.

4. **CQR acquirer Batch Summary:** summary of financial transactions sent to the acquirer on the CQR acquirer interface.

*The reporting component responds to each of these messages with a Report Acknowledgement once it has been received correctly and stored. The sending component shall re-send transactions at configurable intervals after an initial timeout until an acknowledgement is received.*

*Details of the data contained within these messages and the technical requirements for the interface can be found in appendix A.5.*
The Financial Component

*The financial component is the centre of the CQR system. All financial transactions are processed through the component and it is the central repository for data relating to all CQR transactions. The financial component is effectively a database with a number of supporting processes that provide methods of creating and updating data using the external interfaces. There are a number of interfaces to the financial component:*

- The CQR merchant service interface provides an online bi-directional interface between the merchant and CQR. The interface is used to allow the merchant to request CQR service for a consumer transaction and to notify CQR of any cancelled transactions.

- The CQR merchant financial interface is a unidirectional batch interface, which allows the merchant to pass batched financial transactions to CQR.

- The CQR acquirer interface is a unidirectional batch interface allowing CQR to pass batched financial transaction to an acquirer.

- The CQR logistics dispatch interface is a bi-directional interface, which passes CQR transactions, recipient identification and proof of delivery information between the financial and logistics dispatch components.

- The CQR reporting interface is a bi-directional internal interface, which passes information between the financial and the merchant reporting components of the system.
The above interfaces fit into the financial component as illustrated below:

![Diagram showing interfaces between Merchant and Acquirer](image)

**Figure 14. CQR Service Financial Component**

The merchant module

*The merchant module within the CQR financial component provides the functions that support the merchant service and merchant financial interfaces.*

Support for merchant service interface

Request CQR Sale

*On receipt of a Request CQR Sale message the merchant module checks its validity by checking that:
  a) the message is correctly formatted
  b) the merchant has been registered as a member of the CQR scheme by an acquirer
  c) the consumer's card issuer has approved the CQR scheme
  d) the card scheme (derived from the IIN where possible) is suitable for use with the CQR service requested (eg Visa Electron cards may be acceptable for the PKI service, but not for the UKIS service)*

*If the request is valid the module:*

- generates a unique CQR transaction ID,
- stores the sale data in the CQR financial component database,
- sends a successful **CQR Merchant Response** message back to the merchant that includes the CQR transaction ID, and
• passes relevant information (CQR transaction ID, date, amount, service type...) to the reporting component using the Log CQR Sale message.

If the validity check fails the response to the merchant will be a CQR Merchant Response message indicating the failure, which includes a code describing the reason for failure. No further action is taken.

Authorise CQR Sale

On receipt of an Authorise CQR Sale message, the merchant module performs a validity check which ensures that:

a. the message is correctly formatted
b. the transaction identifier, merchant ID, acquirer ID and value match those stored by CQR
c. the transaction has not previously been cancelled

If the message passes the validity check, the merchant module:

• stores the authorisation data in the CQR financial component database,
• sends a successful CQR Merchant Response message back to the merchant and
• sends a CQR Transaction Status Change message to the reporting component indicating that the credit card sale has now been authorised.

If the message passes the validity check and the sale is using a non-PKI service the merchant module passes details of the transaction and delivery details to the logistics dispatch module using the Register CQR Delivery message.

If the message passes the validity check, the sale is using a PKI service and a successful Sign CQR Sale message has been received the merchant module passes details of the transaction and delivery details to the logistics dispatch module using the Register CQR Delivery message.

If the validity check fails, the response to the merchant will be a CQR Merchant Response message indicating the failure, which includes a code describing the reason for failure. No further action is taken.
Sign CQR Sale

On receipt of a Sign CQR Sale message, the merchant module performs a validity check that ensures that:

a. the message is correctly formatted
b. the transaction identifier, merchant Id, acquirer Id and value match those stored by CQR and the service type includes the use of PKI
c. the transaction has not previously been cancelled
d. the cardholder’s X.509 certificate is valid, has not be revoked and is acceptable to the CQR scheme (i.e. permitted certificate type issued from a trusted CA)\(^5\)
e. the cardholder’s digital signature is valid by verifying it with the cardholders X.509 certificate
f. the recipient certificate details match the order signature if the UKIS + PKI service is in use
g. the recipient’s X.509 certificate is valid, has not been revoked and is acceptable to the CQR scheme, acquirer and the payment card issuer (i.e. permitted certificate type issued from a trusted CA)

If the message passes the validity check, the merchant module:

- stores the data in the CQR financial component database,
- sends a successful CQR Merchant Response message back to the merchant and
- sends a CQR Transaction Status Change message to the reporting component indicating that the PKI sale has now been signed.

If the message passes the validity check and a successful Authorise CQR Sale message has previously been received, the merchant module passes details of the transaction and delivery details to the logistics dispatch module using the Register CQR Delivery message.

If the validity check fails, the response to the merchant will be a CQR Merchant Response message indicating the failure, which includes a code describing the reason for failure. No further action is taken.

\(^5\) To allow tracking of / prosecution resulting from fraudulent transactions CQR should only permit the use of certificates which allow the identification (via the CA) of the person behind the digital identity.
Cancel CQR Sale

On receipt of a Cancel CQR Sale message, the merchant module performs a validity check, which ensures that:

a. the transaction identifier, merchant Id, acquirer Id and value match those stored by CQR
b. the transaction has not previously been cancelled
c. a proof of delivery has not been received for the transaction in question:
d. a logistics company has not requested delivery details within the last five days.  

If the message passes the validity check, the merchant module:

- marks the transaction as cancelled and stores the cancellation date/time in the CQR financial component database,
- sends a successful CQR Merchant Response message back to the merchant and
- sends a CQR Transaction Status Change message to the reporting component indicating that sale has now been cancelled.

If the validity check fails, the response to the merchant will be a CQR Merchant Response message indicating the failure, which includes a code describing the reason for failure. No further action is taken.

Cancellation of a CQR sale shall not result in the transaction details being removed from CQR databases. Instead, they will be marked as cancelled and a date of cancellation attached. This is to ensure that an audit trail is available to the merchant.

Support for the merchant financial interface

When the merchant module receives a batch of financial transactions from a merchant, the CQR system will perform the financial and logical integrity checks defined in APACS 29 to ensure that the batch has not been corrupted in transmission. If either of these checks fail, the batch will be rejected and no further processing will take place.  

The merchant module will then split the batch into its component transactions. CQR is only interested in sales transactions, so any refunds and cash advances in the batch will be passed directly to the CQR acquirer module for inclusion in the next acquirer batch for the merchant.

The merchant module will match the received sale transactions with its records of CQR authorised sales, ensuring that the following fields match:

- Acquirer ID

---

6 This check is designed to ensure that a delivery is not currently in progress, whilst allowing a merchant to cancel a transaction if, for example, it has not been possible to make a delivery. The financial component would need to retrieve the status of the delivery from either the merchant reporting or logistics dispatch components.

7 It is currently unclear how this batch failure is reported back to the merchant – further investigation is required.
Once a match has been found, the merchant module will link the financial transaction to a CQR ID and store the contents of the APACS 29 record for future use. A mechanism shall be provided to report out exceptions and process sales with no corresponding CQR transaction.

Once the batch has been processed, the financial component will post information to the merchant reporting component using the CQR Merchant Batch Summary message. The Acquirer Module

The CQR acquirer module is used to validate proof of delivery and pass merchant financial transactions to the acquirer from the saved APACS 29 data received from the merchant.

Support for the logistics dispatch interface

When a delivery is made, the proof of delivery is passed to the logistics dispatch component by the logistics company. The logistics component passes the proofs of delivery to the acquirer module using a CQR PoD message. Upon receiving a PoD message, the module performs a validity check as follows:

a. For UKIS deliveries, the relevant information in the PoD message is combined with the card number and expiry date, which are stored locally and a UKIS SDA check is performed.

b. For PKI deliveries, the signed challenge is decrypted using the consumer's public key, which is stored locally, the challenge hash is recomputed and compared to the decrypted hash.

For UKIS+PKI deliveries both checks must pass in order for the proof of delivery to be considered valid.

The SDA check validates that delivery has been made to a valid UKIS chip card matching the card number and expiry date provided by the consumer during the original transaction. The PKI check ensures the digital signature forwarded by the logistics company is valid according to the consumer's public key and has not been tampered with. If the checks pass, the consumer has provided proof they have received the goods.

The data from the CQR PoD message is stored within the financial component to allow subsequent auditing of the system and independent verification if necessary. Once a proof of delivery has been received the financial component notifies the merchant reporting component by passing the CQR transaction Id and an indicator of the validity of the PoD in a CQR Transaction Status Change message.
If the proof of delivery is valid, the corresponding financial transaction is marked for inclusion in the next batch on the acquirer interface.

The module responds to the CQR PoD message with a Proof Accepted message once it has successfully received and stored a valid PoD message.

Support for the acquirer interface

In order to minimise the change required within the acquirer systems, transactions will be combined into batches formed in accordance with the APACS 29 section 4 standard for financial transactions.

A regular batch will be built for each merchant and transmitted to the acquirer containing:

- All refunds and cash advances passed from the merchant financial interface
- All sales for which proof of delivery has been validated and which have not previously been passed to the acquirer.

Financial and logical validity checks will be performed on the batch prior to transmission to the acquirer.

Once the batch has been successfully transmitted to the acquirer\(^8\), the financial component will post information to the merchant reporting component using the CQR Acquirer Batch Summary message on the CQR reporting interface.

\(^8\) It is currently unclear how the acquirer would indicate whether the batch is acceptable or not. Further work is required in this area.
Logistics Dispatch Component

Details TBD
The Merchant Reporting Component

Overview

The merchant reporting component of the CQR system provides transaction tracking and accounting management information to merchants who are part of the CQR scheme.

The merchant reporting component is essentially a database that is updated via the CQR reporting interface by both the financial and logistics dispatch components. The merchant accesses the information on their transactions using the Merchant Information Management Service (MIMS).

Functionality
Support for MIMS
MIMS provides two ways for merchants to view and use data relating to their transactions:

- Summary information with drill down capability is provided on a web server, accessed over the internet using HTTP over SSL v3.

- Detailed transaction history and other reports may be downloaded securely as CSV files over the internet using SSL v3 connections. The CSV files are suitable for loading into most spreadsheet or database packages.

Figure 18. Interfaces to the CQR Merchant reporting component

In order to use either of these reporting options a secure connection must be set up between the merchant and MIMS. Both parties will authenticate themselves during connection setup before any information is made available to the merchant.
In order to make the service more useful to the merchant the selection of records to be included in reports may be parameterised, for example by allowing the merchant to specify a date range or CQR transaction id range.

MIMS shall initially provide a standard set of reports to all merchants, however, the service shall include the capability to customise the reports available and report layout/format according to merchant preference. This personalisation may in the future be offered by CQR to merchants as an added value service.

The reports to be offered through MIMS shall include but not be limited to:

- Counts of transactions in each status with the ability to drill down to provide transaction details.
- Counts of non-canceled transactions not in each status with the ability to drill down to provide transaction details. For example, all transactions which are sales but not authorised, all PKI transactions which are not signed, valid transactions awaiting delivery and transactions for which the merchant has requested funds but for which the request for funds has not been submitted to the acquirer.
- Counts of cancelled transactions by the most recent status prior to cancellation with the ability to drill down to provide transaction details.
- Summary details and drill down for batches on the CQR merchant financial interface.
- Summary details and drill down for batches on the CQR acquirer interface.

Support for CQR Reporting Interface

The CQR reporting interface is an internal interface used by both the financial and logistics dispatch components to communicate with the merchant reporting component.

On receipt of a message on the reporting interface, the component stores the relevant data against the transaction and updates any pre-defined reports. Once the data has been stored successfully, the merchant reporting component responds with a Report Acknowledgement message.
In addition to storing the data received on this interface, the reporting component shall update the CQR transaction status as documented below.

**CQR Transaction Status**

The table below defines each of the statuses for a CQR transaction, specifying which component notifies the reporting component and any requirements for the pre-existing status of a transaction. The status of a transaction may be viewed as a bit mask (i.e., multiple values may be valid at any one time). Typically, status updates can only add bits to the status – i.e., it is not generally possible to remove information from the status value. There is one exception to this rule, the receipt of a PoD Validated status shall cause a status of PoD invalid to be removed.

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Description</th>
<th>Notified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>X'0001'</td>
<td>Sale Requested</td>
<td>The merchant has notified CQR of a valid sale using the Request CQR Sale message. A CQR transaction ID has been assigned</td>
<td>Log CQR Sale issued by financial component</td>
</tr>
<tr>
<td>X'0002'</td>
<td>Authorised</td>
<td>The merchant has authorised a credit card transaction for the sale and notified CQR of the authorisation details using the Authorise CQR Sale message. Not permitted unless status contains X'0001' – sale requested.</td>
<td>CQR Transaction Status Change issued by financial component.</td>
</tr>
<tr>
<td>X'0004'</td>
<td>Signed</td>
<td>A PKI service is being used and a valid digital signature and delivery information for the sale has been provided by the consumer/merchant using the Sign CQR Sale message. Not permitted unless status contains X'0001' – sale requested.</td>
<td>CQR Transaction Status Change issued by financial component.</td>
</tr>
<tr>
<td>X'0008'</td>
<td>Merchant Requests Funds</td>
<td>A valid sale transaction has been received on the merchant financial interface corresponding to the CQR transaction. Not permitted unless status contains X'0002' – authorised.</td>
<td>CQR merchant batch summary</td>
</tr>
<tr>
<td>X'0010'</td>
<td>Delivery information available</td>
<td>The financial component has collated all information required for delivery and passed this information to the logistics dispatch component. Not permitted unless status contains X'0004' – signed if the transaction service is PKI.</td>
<td>CQR Transaction Status Change issued by logistics dispatch component.</td>
</tr>
<tr>
<td>X'0020'</td>
<td>Delivery information collected</td>
<td>A logistics company has collected the delivery information from CQR, indicating that at delivery is in progress. Not permitted unless status contains X'0010' – Delivery information available</td>
<td>CQR Transaction Status Change issued by logistics dispatch component.</td>
</tr>
</tbody>
</table>

---

9 The action to be taken if a “not permitted” status change occurs is to be defined.
| X'0040' | Delivered | A logistics company has delivered the goods and obtained a proof of delivery. Not permitted unless status contains X'0020' - Delivery information collected |
| X'0080' | PoD validated | The financial component has validated and accepted the proof of delivery provided by the logistics company. Not permitted unless status contains X'0040' - Delivered. Causes the status X'0100' PoD invalid to be removed |
| X'0190' | PoD invalid | The financial component has failed to validate the proof of delivery provided by the logistics company. Not permitted unless status contains X'0040' - Delivered or if status contains X'0080' PoD validated. |
| X'0200' | Funds requested from acquirer | A financial batch has been submitted to the acquirer requesting funds be released to the merchant as the sale has completed successfully and the goods have been delivered. Not permitted unless status contains X'0080' - PoD validated. |
| X'8000' | Cancelled | The CQR transaction has been cancelled and will not progress further. Not permitted if status contains X'0200' - Funds requested from acquirer. |
CQR Remote Shopping Example

The following diagram and text illustrates the CQR Remote Shopping model in terms of the system components and interfaces as described in section 0.

**Figure 16. Remote shopping components and interfaces**

1. A Request CQR Sale message is sent from the Merchant to the CQR Financial Component on the Merchant Service Interface when a consumer has purchased some goods. A CQR Merchant Response message is sent in return across the Merchant Service Interface. This contains the CQR Transaction Id.


3. The merchant uses APACS 30 to get the credit card authorisation.

4. Having obtained an authorisation code from the acquirer, the merchant sends an Authorise CQR Sale message on the Merchant Service Interface to the CQR Financial Component. The CQR Financial Component replies with a CQR Merchant Response message across the Merchant Service Interface and updates the transaction status by sending a Transaction Status Change message to the Merchant Reporting Component.
5. If the transaction is using service 2 or 3 (PKI based) the digitally signed customer order is passed to CQR using the Sign CQR Sale message. The CQR Financial Component replies with a CQR Merchant Response message across the Merchant Service Interface and updates the transaction status by sending a Transaction Status Change message to the Merchant Reporting Component.

6. The CQR Financial Component sends a Register CQR Delivery message over the Reporting Interface to the Logistics Dispatch Component, which holds the delivery details for the logistics company to retrieve the information.

7. The Logistics Dispatch component module replies to the Financial component with a Delivery Accepted message.

8. The merchant submits a request for funds in the form of an APACS 29 Request (maybe using APACS 50 via a polling bureau), which is received by the CQR Financial Component across the Merchant Financial Interface.

9. The CQR Financial Module passes summaries of all batches appearing at the Merchant Financial Interface to the Reporting Interface for the Merchant to retrieve using MIMS.

When the Merchant Reporting Component receives any of the reporting messages (see section 0) it responds to the CQR Financial Component with a Report Acknowledgement across the Reporting Interface. The CQR Financial Component can send a CQR Transaction Status Change message on the Reporting Interface to the Merchant Reporting Component at any point during a transaction in order to keep the merchant informed on the current state of a delivery.

10. Prior to making a CQR delivery the logistics company will retrieve delivery card information from CQR using CDIS. After a successful delivery the logistics company will forward the proofs of delivery to the Logistics Dispatch component using CDIS.

11. The Logistics Dispatch component will pass a CQR PoD message to the CQR Financial Component across the Logistics Dispatch interface.

12. Upon receiving the CQR PoD message the CQR Financial Component will reply with a PoD Accepted message across the Logistics Dispatch Interface.

13. The CQR Financial Component reconstructs the APACS 29 messages along with the relevant proofs of delivery and sends batched APACS 29's to the acquirer to the acquirer who will then arrange for release of funds to the merchant.

14. The CQR Financial Module passes summaries of all batches appearing at the acquirer Interface to the Reporting Interface for the merchant to retrieve using MIMS.
Appendices

A.1 CQR merchant service interface detail

Message Data

This section lists the data included in each of the messages on the CQR merchant service interface. All fields are mandatory except where explicitly marked as optional.

### Request CQR Sale

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00&lt;sup&gt;10&lt;/sup&gt;</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0001' = Request CQR Sale</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>n 11</td>
<td>6</td>
<td>right justified and padded with x'0'</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>ans 15</td>
<td>15</td>
<td>Assigned by acquirer. Left justified and padded with x'0'</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>int</td>
<td>2</td>
<td>Assigned by merchant to allow interleaved requests</td>
</tr>
<tr>
<td>Transaction date</td>
<td>n</td>
<td>8 CCYYMMDD</td>
<td>4 left justified, padded with spaces</td>
</tr>
<tr>
<td>Cardholder name</td>
<td>ans 26</td>
<td>26</td>
<td>card number obtained from consumer left justified and padded with x'F'</td>
</tr>
<tr>
<td>PAN</td>
<td>n 20</td>
<td>10</td>
<td>obtained from consumer</td>
</tr>
<tr>
<td>Card Expiry date</td>
<td>YYMM</td>
<td>2</td>
<td>as defined by ISO 4217</td>
</tr>
<tr>
<td>Currency code</td>
<td>n 3</td>
<td>2</td>
<td>Total amount of transaction in smallest unit of currency eg 100 = £1.00 or Lira 100 depending on currency code. Right justified and padded with x'0'</td>
</tr>
<tr>
<td>Amount</td>
<td>n 12</td>
<td>6</td>
<td>Service Required</td>
</tr>
<tr>
<td></td>
<td>b</td>
<td>2</td>
<td>X'0001' = UKIS, delivery to payment card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0002' = PKI signed, delivery to PKI card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0003' = UKIS + PKI, delivery to payment card with PKI check</td>
</tr>
</tbody>
</table>

### Authorise CQR Sale

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0002' = Authorise CQR Sale</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>n 11</td>
<td>6</td>
<td>right justified and padded with x'0'</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>ans 15</td>
<td>15</td>
<td>Assigned by acquirer. left justified and padded with x'0'</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td>right justified and padded with x'0'</td>
</tr>
<tr>
<td>Currency code</td>
<td>n 3</td>
<td>2</td>
<td>as defined by ISO 4217</td>
</tr>
<tr>
<td>Amount</td>
<td>n 12</td>
<td>6</td>
<td>total amount of transaction as authorised by acquirer in smallest unit of currency eg 100 = £1.00 or Lira 100 depending on currency code. Right justified and padded with x'0'</td>
</tr>
<tr>
<td>Auth code</td>
<td>an 6</td>
<td>6</td>
<td>Received from acquirer. left justified and padded with x'0'</td>
</tr>
<tr>
<td>Authorisation date</td>
<td>n</td>
<td>8 CCYYMMDD</td>
<td>4 Date Auth Code was received from acquirer.</td>
</tr>
</tbody>
</table>

### Sign CQR Sale

<sup>10</sup> Interface shall be extended in such a way that they provide backwards compatibility.
<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0004' = Sign CQR Sale</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td>right justified and padded with x'0'</td>
</tr>
<tr>
<td>Currency code</td>
<td>n 3</td>
<td>2</td>
<td>as defined by ISO 4217</td>
</tr>
<tr>
<td>Amount</td>
<td>n 12</td>
<td>6</td>
<td>total amount of transaction as authorised by acquirer in smallest unit of currency eg 100 = £1.00 or Lira 100 depending on currency code, right justified and padded with x'0'</td>
</tr>
<tr>
<td>Delivery to payment card</td>
<td>bool</td>
<td>1</td>
<td>True / False</td>
</tr>
<tr>
<td>Delivery to signature card</td>
<td>bool</td>
<td>1</td>
<td>True / False – Must be true is delivery to payment card is true</td>
</tr>
<tr>
<td>Delivery X.509 certificate</td>
<td></td>
<td></td>
<td>Optional - certificate for PKI card to be delivered to 11. Mandatory if delivery to signature card is False. If not present, CQR use Customers X.509 certificate for delivery.</td>
</tr>
<tr>
<td>Delivery Card reminder</td>
<td>ans</td>
<td>20</td>
<td>Optional – text supplied by customer to remind them which card is to be used for delivery.</td>
</tr>
<tr>
<td>Customers X.509 certificate</td>
<td></td>
<td></td>
<td>X.509 public certificate from a consumer’s PKI card</td>
</tr>
<tr>
<td>Signed hash</td>
<td>n48</td>
<td>24</td>
<td>A hash of the data contained in this message signed using the customer’s private key. Right justified and padded with x'0'</td>
</tr>
</tbody>
</table>

**Cancel CQR Sale**

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0008' = Cancel CQR Sale</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>n 11</td>
<td>6</td>
<td>Right justified and padded with x'0'</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>ans</td>
<td>15</td>
<td>Assigned by acquirer. Left justified and padded with x'0'</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td>Right justified and padded with x'0'</td>
</tr>
<tr>
<td>Currency code</td>
<td>n 3</td>
<td>2</td>
<td>As defined by ISO 4217</td>
</tr>
<tr>
<td>Amount</td>
<td>n 12</td>
<td>6</td>
<td>Total amount of transaction as authorised by acquirer in smallest unit of currency eg 100 = £1.00 or Lira 100 depending on currency code, Right justified and padded with x'0'</td>
</tr>
</tbody>
</table>

**CQR Merchant Response**

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>Taken from request</td>
</tr>
<tr>
<td>Sequence number</td>
<td>int</td>
<td>2</td>
<td>Taken from request if present, else 0</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td>For sale response, generated by finance component and only present if success else, all x'0'. For other responses, taken from request Right justified and padded with x'0' (note 13 digits in typical bar code)</td>
</tr>
<tr>
<td>Reason code</td>
<td>b</td>
<td>4</td>
<td>if success,</td>
</tr>
</tbody>
</table>

11 Customer may get this info from recipient (eg by e-mail) or from a directory service provided by a PKI card issuer
Technical
This section will define the technical interface mechanism. This is currently to be decided, but may be XML over an SSL 3 connection.

Consideration should be given to the error rate and error correction characteristics of the chosen underlying transport mechanism. It may be appropriate to add a cyclic redundancy check (CRC) or some other form of data integrity checking to the messages on this interface.

A.2 CQR merchant financial interface

Message Data
The data requirements for this interface are completely defined in APACS 29 section 4 and the common attachment to APACS standards 29, 30, 40 and 50.

Technical
The APACS 29 standard defines a data transfer mechanism for use with magnetic tape or disks. This is clearly inappropriate for Internet shopping and APACS 29 does acknowledge that the batches defined may be passed by other means including transmission. However, there is no defined transmission mechanism within the standard.

It is believed that the APACS 29 batches are typically transmitted over X.25 from the merchant to the acquirer, and as such, the CQR system would need a connection to an X.25 PAD to receive batches from a merchant. Further investigation is required in this area to fully define the technical requirements for this interface.
A.3 CQR acquirer interface

Data
The data requirements for this interface are completely defined in APACS 29 section 4 and the common attachment to APACS standards 29, 30, 40 and 50. All required data will be sourced from the merchant financial interface. The CQR system shall not modify the contents of individual APACS 29 messages between the merchant financial interface and the acquirer interface.

Technical
The APACS 29 standard defines a data transfer mechanism for use with magnetic tape or disks. This is clearly inappropriate for Internet shopping and APACS 29 does acknowledge that the batches defined may be passed by other means including transmission. However, there is no defined transmission mechanism within the standard.

It is believed that the APACS 29 batches are typically transmitted over X.25, and as such, the CQR system would need a connection to an X.25 PAD to receive the batches. Further investigation is required in this area to fully define the technical requirements for this interface.

It may be appropriate for the CQR system to digitally sign financial batches sent over this interface. This would provide some integrity checking for the acquirer at a minimal cost of implementing a wrapper function to validate the signature and then pass the batch through to existing APACS 29 batch handling systems.
### A.4 CQR logistics dispatch interface

**Delivery Message Data**

#### Register CQR Delivery

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0010' = Register CQR Delivery</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>CQR Delivery Service</td>
<td>b</td>
<td>2</td>
<td>X'0001' = UKIS, delivery to payment card X'0002' = PKI signed, delivery to PKI card X'0003' = UKIS + PKI, delivery to payment card with PKI check</td>
</tr>
<tr>
<td>Cardholder name</td>
<td>ans 26</td>
<td>26</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present. Left justified, padded with spaces</td>
</tr>
<tr>
<td>Card ID</td>
<td>n 4</td>
<td>2</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present. Last four digits of PAN</td>
</tr>
<tr>
<td>Recipient hash</td>
<td>tbd</td>
<td>tbd</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present. Result of a one way hash of PAN and expiry date</td>
</tr>
<tr>
<td>Hash type</td>
<td>b</td>
<td>1</td>
<td>Type of hash used. Values tbd</td>
</tr>
<tr>
<td>Delivery X.509 certificate</td>
<td></td>
<td></td>
<td>Mandatory if CQR delivery service is X'0002' or X'0003', else not present.</td>
</tr>
<tr>
<td>Delivery Card reminder</td>
<td>ans</td>
<td>20</td>
<td>Optional if CQR delivery service is X'0002' or X'0003', else not present.</td>
</tr>
</tbody>
</table>

#### Delivery Accepted

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0020' = Delivery Accepted</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td>Taken from register CQR delivery</td>
</tr>
</tbody>
</table>
### CQR PoD

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0040' = Register CQR Delivery</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Logistics company ID</td>
<td>int</td>
<td>2</td>
<td>Logistics company identifier within CQR system</td>
</tr>
<tr>
<td>Terminal ID</td>
<td>tbd</td>
<td>tbd</td>
<td>unique identifier of hand held device used at point of delivery</td>
</tr>
<tr>
<td>Terminal type</td>
<td>int</td>
<td>2</td>
<td>identifier of type of hand held device used. Values tbd</td>
</tr>
<tr>
<td>Date</td>
<td>n 8 CCYYMMDD</td>
<td>4</td>
<td>Date of delivery recorded on hand held device</td>
</tr>
<tr>
<td>Time</td>
<td>n6 HHMMSS</td>
<td>3</td>
<td>Time of delivery (24hr clock) recorded on hand held device</td>
</tr>
<tr>
<td>UKIS Certification Authority Public Key Index</td>
<td>1</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Issuer Public Key Certificate</td>
<td>40-128</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Issuer Public Key Exponent</td>
<td>1-32</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Signed Application Data</td>
<td>40-128</td>
<td>Mandatory if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Issuer Public Key Remainder</td>
<td>1-36</td>
<td>Optional (mandatory if present on chip card) if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Application Effective Date</td>
<td>3</td>
<td>Optional (mandatory if present on chip card) if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Application PAN Sequence Number</td>
<td>1</td>
<td>Optional (mandatory if present on chip card) if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Issuer Action Code – Default</td>
<td>5</td>
<td>Optional (mandatory if present on chip card) if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Issuer Action Code – Denial</td>
<td>5</td>
<td>Optional (mandatory if present on chip card) if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>UKIS Issuer Action Code – Online</td>
<td>5</td>
<td>Optional (mandatory if present on chip card) if CQR delivery service is X'0001' or X'0003', else not present.</td>
<td></td>
</tr>
<tr>
<td>Challenge</td>
<td>Tbd</td>
<td>Tbd</td>
<td>Mandatory if CQR delivery service is X'0002' or X'0003', else not present.</td>
</tr>
<tr>
<td>Hashed and signed challenge</td>
<td></td>
<td></td>
<td>Mandatory if CQR delivery service is X'0002' or X'0003', else not present.</td>
</tr>
</tbody>
</table>

### PoD Accepted

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0080' = PoD Accepted</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td>taken from CQR PoD</td>
</tr>
</tbody>
</table>
Technical
This section will define the technical interface mechanism. This is currently tbd, but may be XML over an SSL 3 connection. The chosen mechanism shall support variable length and optional fields. The interface may support batches of messages if appropriate.

Consideration should be given to the error rate and error correction characteristics of the chosen underlying transport mechanism. It may be appropriate to add a CRC or some other form of data integrity checking to the messages on this interface.

A.5. CQR reporting interface

Message Data

Log CQR Sale

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0100' = Log CQR Sale</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>int</td>
<td>4</td>
<td>Assigned by financial component to allow interleaved requests</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>n 11</td>
<td>6</td>
<td>right justified and padded with X'0'</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>ans 15</td>
<td>15</td>
<td>Assigned by acquirer, left justified and padded with X'0'</td>
</tr>
<tr>
<td>CQR Delivery Service</td>
<td>b</td>
<td>2</td>
<td>X'0001' = UKIS, delivery to payment card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0002' = PKI signed, delivery to PKI card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0003' = UKIS + PKI, delivery to payment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>card with PKI check</td>
</tr>
<tr>
<td>Transaction date</td>
<td>n</td>
<td>8</td>
<td>CCYYMMDD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>as defined by ISO 4217</td>
</tr>
<tr>
<td>Currency code</td>
<td>n 3</td>
<td>2</td>
<td>as defined by ISO 4217</td>
</tr>
<tr>
<td>Amount</td>
<td>n 12</td>
<td>6</td>
<td>total amount of transaction in smallest unit of currency eg 100 = £1.00 or Lira 100 depending on currency code, right justified and padded with X'0'</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

CQR Transaction Status Change

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0200' = CQR Transaction Status Change</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>int</td>
<td>4</td>
<td>Assigned by financial component to allow interleaved requests</td>
</tr>
<tr>
<td>CQR Transaction ID</td>
<td>n 13</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>New status</td>
<td>b</td>
<td>2</td>
<td>X'0002' = Authorised</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0004' = Signed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0008' = Merchant Requests Funds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0010' = Delivery information available</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0020' = Delivery information collected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0040' = Delivered</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0080' = PoD validated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X'0100' = PoD invalid</td>
</tr>
<tr>
<td>New status date</td>
<td>n 8</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>------</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CCYYMMDD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

X'0200' = Funds requested from acquirer
X'8000' = Cancelled
### CQR Merchant Batch Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0400' = CQR Merchant Batch Summary</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>int</td>
<td>4</td>
<td>Assigned by financial component to allow interleaved requests</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>n 11</td>
<td>6</td>
<td>right justified and padded with x'0'</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>ans 15</td>
<td>15</td>
<td>Assigned by acquirer. left justified and padded with x'0'</td>
</tr>
<tr>
<td>Batch Date</td>
<td>n 8 CCYYMMDD</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Merchant batch ref</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Sales transaction count</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Sales total</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Refund transaction count</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Refund total</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Cash Advance count</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Cash Advance total</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>CQR Transaction ID 1</td>
<td>n 13</td>
<td>7</td>
<td>included in batch</td>
</tr>
<tr>
<td>CQR Transaction ID 2</td>
<td>n 13</td>
<td>7</td>
<td>included in batch</td>
</tr>
<tr>
<td>CQR Transaction ID n</td>
<td>n 13</td>
<td>7</td>
<td>included in batch</td>
</tr>
<tr>
<td>Number of Sales with no</td>
<td>int</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>matching CQR Transaction ID</td>
<td></td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>

### CQR Acquirer Batch Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length (bytes)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>X'0800' = CQR Acquirer Batch Summary</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>int</td>
<td>4</td>
<td>Assigned by financial component to allow interleaved requests</td>
</tr>
<tr>
<td>Acquirer ID</td>
<td>n 11</td>
<td>6</td>
<td>right justified and padded with x'0'</td>
</tr>
<tr>
<td>Merchant Number</td>
<td>ans 15</td>
<td>15</td>
<td>Assigned by acquirer. left justified and padded with x'0'</td>
</tr>
<tr>
<td>Batch Date</td>
<td>n 8 CCYYMMDD</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>CQR batch ref</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Sales transaction count</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Sales total</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Refund transaction count</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Refund total</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Cash Advance count</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>Cash Advance total</td>
<td>tbd</td>
<td>tbd</td>
<td>as defined in APACS 29</td>
</tr>
<tr>
<td>CQR Transaction ID 1</td>
<td>n 13</td>
<td>7</td>
<td>included in batch</td>
</tr>
<tr>
<td>CQR Transaction ID 2</td>
<td>n 13</td>
<td>7</td>
<td>included in batch</td>
</tr>
<tr>
<td>CQR Transaction ID n</td>
<td>n 13</td>
<td>7</td>
<td>included in batch</td>
</tr>
</tbody>
</table>

### Report Acknowledgement

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Length</th>
<th>Comment</th>
</tr>
</thead>
</table>

12 More thought is required on how to deal with sales transactions in the APACS29 from the merchant, which do not correspond to a COR transaction ID.
<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Version</td>
<td>b</td>
<td>2</td>
<td>X'0100' = v1.00</td>
</tr>
<tr>
<td>Message ID</td>
<td>b</td>
<td>2</td>
<td>taken from report message being acknowledged</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>int</td>
<td>4</td>
<td>taken from report message being acknowledged</td>
</tr>
<tr>
<td>Response code</td>
<td>b</td>
<td>2</td>
<td>X'0000' = success</td>
</tr>
</tbody>
</table>

Technical

*This section will define the technical interface mechanism. This is currently to be decided, but may be XML over an SSL 3 connection. The chosen mechanism shall support variable length messages containing repeating fields. The interface may support batches of messages if appropriate.*

*Consideration should be given to the error rate and error correction characteristics of the chosen underlying transport mechanism. It may be appropriate to add a CRC or some other form of data integrity checking to the messages on this interface.*
CLAIMS

What is claimed is:

1. A transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery, the system comprising:
   a customer ordering sub-system; and
   an internet connection providing communication with and between,
   a merchant sub-system,
   an acquirer processing sub-system,
   a credit card issuer processing sub-system, and
   a carrier verification and delivery sub-system

wherein, customers use the customer ordering sub-system, which is in communication with the merchant sub-system, to make credit card purchases with merchants, the merchant sub-system requests an authorization and/or an ID tag for each credit card purchase, authorization for each credit card purchases is issued by the credit card issuer processing sub-system and is provided to the merchant sub-system through either the acquirer processing sub-system or the carrier verification and delivery sub-system, the ID tag for each credit card purchase is provided by the carrier verification and delivery sub-system and is used at the point of delivery to verify the credit card purchase and to establish proof of delivery at the time of delivery.

2. A transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery, the system comprising:
   a customer ordering sub-system; and
an internet connection providing communication with and between,
a merchant sub-system,
an acquirer processing sub-system,
a credit card issuer processing sub-system, and
a carrier verification and delivery sub-system

wherein, customers use the customer ordering sub-system, which is in communication with the merchant sub-system, to make credit card purchases with merchants, the merchant sub-system requests an authorization and/or an ID tag from the credit card issuer processing sub-system for each credit card purchase,

authorization for each credit card purchases is issued by the credit card issuer processing system and is provided to the merchant sub-system through either the acquirer processing sub-system or the carrier verification and delivery sub-system, funds are reserved for the purchase by the credit card issuer processing sub-system or the acquirer processing sub-system until verification, the ID tag is issued by the

carrier verification and delivery sub-system is used to verify proof of delivery and the credit card purchase at the point of delivery, upon verification of the delivery and the purchase, the reserved funds are released to the merchants.

3. A transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery, the system comprising:
a customer ordering sub-system; and

an internet connection providing communication with and between,
a merchant sub-system,
an acquirer processing sub-system,
a credit card issuer processing sub-system, and
a carrier verification and delivery sub-system
wherein, customers use the customer ordering sub-system, in communication with the merchant sub-system, to make credit card purchases with merchants, the merchant sub-system requests an authorization code for each credit card purchase, the authorization code for each credit card purchases is issued by the credit card issuer processing system and is provided to the merchant sub-system through either the acquirer processing sub-system or the carrier verification and delivery sub-system, the authorization code is used to verify proof of delivery and the credit card purchase at the point of delivery, upon verification of the delivery and the purchase funds are released to merchants.

4. A transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery, providing an improvement over prior art systems used for credit card holder not present (CNP) transactions, the prior art system having a purchasing party requesting a purchase from a merchant and delivery of ordered product to a receiving party, an acquiring bank requesting authorization for a CNP transaction from a card issuer bank, the improvement comprising:

   an electronic authorization ID issued by the issuer bank or the acquirer bank or a third party, and

   a microprocessor to compare the issued electronic authorization ID with the identify of the purchasing party and/or the identity of the receiving party at the point of delivery.

5. The system according to claim 4, wherein the microprocessor is a programmable storage device having the capacity to receive and store credit card authentication data generated by TALISMAN.

6. The system according to claim 5, wherein the programmable storage device is a personal digital assistant (PDA) maintained by a carrier delivering the
ordered product, wherein the PDA is used to compare the stored credit card
authentication with the actual credit card used to initiate the transaction and/or a
remote delivery code provided by TALISMAN for remote deliveries.

7. A method for a transaction and logistics integrated management system
(TALISMAN) for secure credit card payment and verified transaction delivery, the
method comprising the steps of:

placing a customer order with a merchant using a customer ordering
sub-system; and

communicating using an internet connection providing communication
with and between,

a merchant sub-system,

an acquirer processing sub-system,

a credit card issuer processing sub-system, and

a carrier verification and delivery sub-system

wherein, customers use the customer ordering sub-system, which is in
communication with the merchant sub-system, to make credit card purchases with
merchants, the merchant sub-system requests an authorization and/or an ID tag for
each credit card purchase, authorization for each credit card purchases is issued by
the credit card issuer processing sub-system and is provided to the merchant sub-
system through either the acquirer processing sub-system or the carrier verification
and delivery sub-system, the ID tag for each credit card purchase is provided by
the carrier verification and delivery sub-system and is used at the point of delivery
to verify the credit card purchase and to establish proof of delivery at the time of
delivery.
8. A method for a transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery, the method comprising the steps of:

establishing a communication between a first (merchant) device, a second (acquirer) device, a third (issuer) device, and a fourth (carrier verification and delivery) device;

transmitting payment information, corresponding to a payment instrument of a customer, from a first (merchant) device to a second (acquirer) device;

forwarding payment information to the third (issuer) device and the fourth (carrier verification and delivery) device;

receiving the payment information at the third (issuer) device;

evaluating the payment information based on the payment instrument by the third (issuer) device;

transmitting approval of the transaction from the third (issuer) device to the second (acquirer) device;

storing a record of the transaction approval at the fourth (carrier verification and delivery) device;

forwarding approval of the transaction from the second (acquirer) device to the first (merchant) device;

requesting the payment instrument by the fourth (carrier verification and delivery) device at the point of delivery;

comparing the payment instrument with the payment information by the fourth (carrier verification and delivery) device at the point of delivery, and transmitting approval to release funds to the first (merchant device) by the fourth device, wherein payment is released to the first (merchant device) by the
second (acquirer) device using a direct electronic transmission of monetary value from the second (acquirer) device to the first (merchant) device.

9. The system according to claim 8, wherein the first device comprises a merchant device, the second device is an acquirer device, the third device is an issuer device, the fourth device is a carrier verification and delivery device, the party is a consumer, wherein the payment instrument comprises a card issued by an issuer to a consumer.

10. The system according to claim 8, wherein at least one communication linkage uses the Internet Protocol (IP).

11. The system according to claim 8, wherein at least one communication linkage uses the Internet Protocol (IP).

12. The system according to claim 1, wherein the transmission via at least one communication linkage is encrypted.

13. The system according to claim 1, wherein the payment instrument is a credit card.

14. The system according to claim 1, wherein the payment instrument is a debit card.

15. A transaction and logistics integrated management apparatus (TALISMAN) for secure credit card payment and verified transaction delivery, the apparatus comprising:

   logic that establishes communication between a first (merchant) device, a second (acquirer) device, a third (issuer) device, and a fourth (carrier verification and delivery) device;

   logic that transmits payment information corresponding to a payment instrument of a party, from the first electronic device to the second electronic device;
logic that forwards the payment information from the second electronic device to the third electronic device;
logic that receives the payment information at the third electronic device;
logic that evaluates the payment information using the payment instrument by the third electronic device;
logic that transmits approval of the transaction from the third electronic device to the second and fourth electronic devices;
logic that stores a record of the transaction approval at the fourth electronic device;
logic that forwards approval of the transaction from the fourth electronic device to the second electronic device upon verification of the payment instrument with the payment instrument by the fourth electronic device, wherein payment is released to the first (merchant) device by the second (acquirer) device using logic that directs electronic transmission of monetary value from the second (acquirer) device to the first (merchant) device

16. The apparatus according to claim 15, wherein the first device comprises a merchant device, the second device is an acquirer device, the third device is an issuer device, the fourth device is a carrier verification and delivery device, the party is a consumer, wherein the payment instrument comprises a card issued by an issuer to a consumer.

17. The apparatus according to claim 15, wherein at least one communication linkage uses the Internet Protocol (IP).

18. The apparatus according to claim 15, wherein the transmission via at least one communication linkage is encrypted.

19. The apparatus as recited in claim 15, wherein the payment instrument is a credit card.
20. The apparatus as recited in claim 15, wherein the payment instrument is a debit card.

21. A transaction and logistics integrated management system (TALISMAN) for secure credit card payment and verified transaction delivery having a computer program embodied on a computer-readable medium for executing an electronic transaction between a first electronic device, a second electronic device, a third electronic device, and a fourth electronic device, the computer program comprising:

- a code segment that establishes a communication between the first electronic device and the second electronic device;
- a code segment that couples the second, second, third and fourth electronic device via a first communication linkage;
- a code segment that transmits payment information corresponding to a payment instrument of a party, from the first electronic device to the second and third electronic device;
- a code segment that forwards the payment information to the third electronic device;
- a code segment that receives the payment information at the third electronic device;
- a code segment that evaluates the payment information based on the payment instrument by the third electronic device;
- a code segment that transmits approval of the transaction from the third electronic device to the second and fourth electronic device;
- a code segment that stores a record of the transaction approval at the second electronic device; and
a code segment that forwards approval of the transaction from the fourth electronic device to the second electronic device upon verification of the payment instrument with the payment instrument by the fourth electronic device, wherein payment is released to the first (merchant) device by the second (acquirer) device using logic that directs electronic transmission of monetary value from the second (acquirer) device to the first (merchant) device.

22. The computer program as recited in claim 21 wherein the first electronic device is a consumer device, the second electronic device comprises an acquirer device, the third electronic device comprises an issuer device, the fourth electronic device is a credit card issuer processing sub-system, wherein the payment instrument comprises a card issued by an issuer to a consumer.