

VETT represents a new paradigm for: Authentication and User security

VETT (Verified Electronic Transaction Technology) is a new paradigm for transaction security. This paper provides a brief introduction to the technology and shows the combination of elements used to deliver a new safe environment for remote commerce.

The elements of this new paradigm combine to deliver a safe environment to conduct payments and many other types of financial transactions. These elements are:

- Third Parties do not need a User's sensitive account data
- Transactions are conducted via two separate channels
- The User always initiates 'Access to Service' (never follow links)
- Authentication of the User and the Transaction
- Internet, Mobile, Telephone, Face-to-face (Channel neutral)
- Education – Ubiquity, learn once
- No special device or software required by Users

This paper also looks at an outline for the development of payment transaction systems set out in chronological order. Further, there is a description together with a diagram to show a generic VETT transaction.

VETT is a generic solution that can be deployed to enable security for a range of transaction types. The system offers many advantages which are shown in relation to each participant.

- VETT facilitates access via the Internet, Landline, Mobile Phone and can also be deployed for face-to-face transactions.

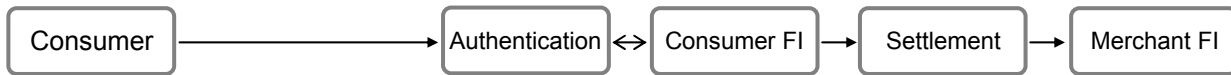
The final section of the paper looks at the distribution of components to facilitate the operational environment for VETT technology.

+44 (0)1636 707 777 t
+44 (0)1636 700 747 f
enquires@vettuk.com e

Vett UK Limited
Balderton Hall Fernwood
Nottinghamshire NG24 3JR
© VETT ltd - All rights reserved



1980s Telephone Banking



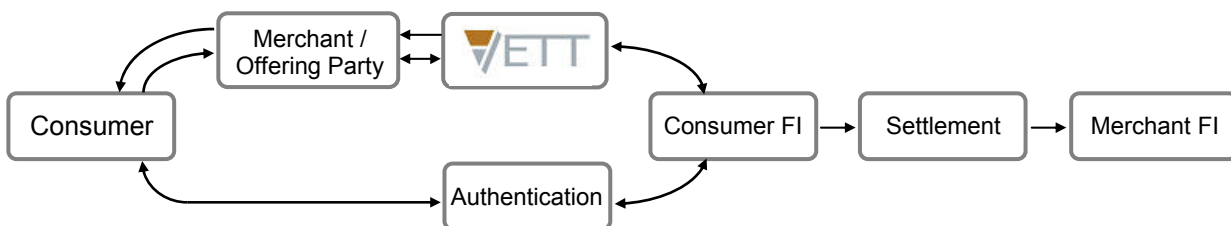
Telephone banking was introduced with limited capabilities in the late 1980s. Early versions of this type of service relied upon the Consumer (business or individual) using a battery powered tone generator to let the user transmit tones to a computer to initiate predefined functions. Telephones in the UK are now DTMF enabled removing the necessity for the tone device.

1998 Credit Card via the Internet



In the early days of internet commerce Merchants collected credit card data and manually transferred card numbers to gain authorisation by telephone. Automating the process via a dedicated payment system became widely used from circa 1998 onwards. However, card holder not present (CNP) transactions are very susceptible to fraud.

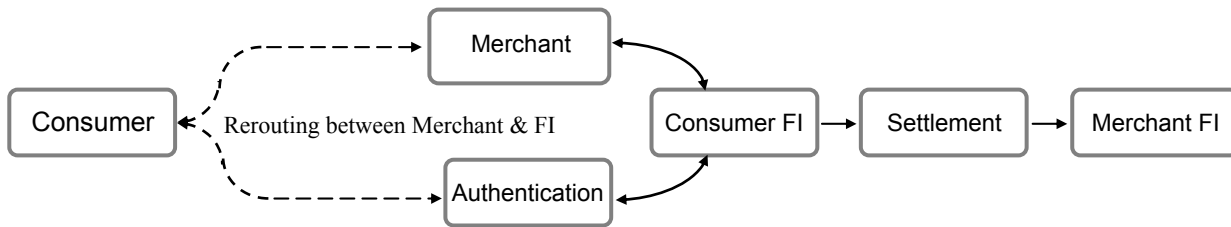
2000 VETT, patent application filed



VETT enables multi channel access for Consumers such as the internet, landline, mobile phone and face-to-face. VETT provides additional layers of security for ecommerce rendering data obtained through hacking valueless; VETT transactions are immune to phishing. VETT does *not* require the User to use any special device or software. Third Parties do not need to see user sensitive account data.

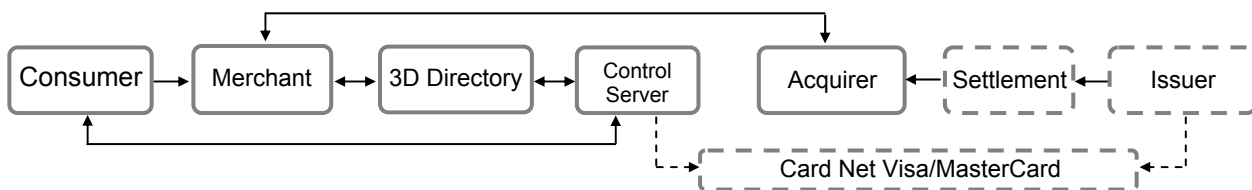


2000 NACHA Online Two Channel



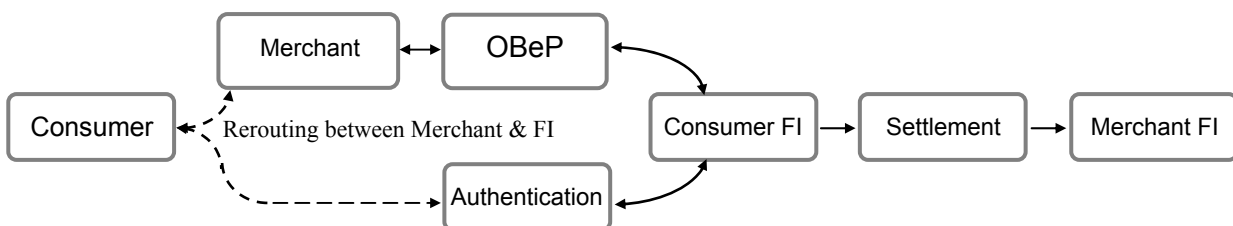
NACHA (National Automated Clearing House Association - USA) Set-up a research project in 2000 to test consumer reaction to a two channel internet payment system. In 2005, NACHA commissioned 'proof of concept' to test the technology. A pilot system was rolled out in 2007.

2002 3D Secure



The 3D secure model is web based and used to authenticate credit card payments. Developed by Visa and adopted by JCB and MasterCard, cardholders must first register with their card issuer. Cardholders still expose their account number, expiry date and CVV to third parties.

2005 EPC Task Force published an outline for OBeP



The European Payments Council (Online Banking electronic Payments) OBeP scheme is a point solution dependent upon the internet. The model shown here is designed for real time online purchasing. OBeP relies on Banks to provide authentication and protection against fraud. Currently the favoured method for authentication is to issue 'two factor' tokens to online Users. At present there is no single uniformly accepted solution. The EPC have also recognised that OBeP is vulnerable to fake site phishing.



Description of Consumer paying a bill through VETT

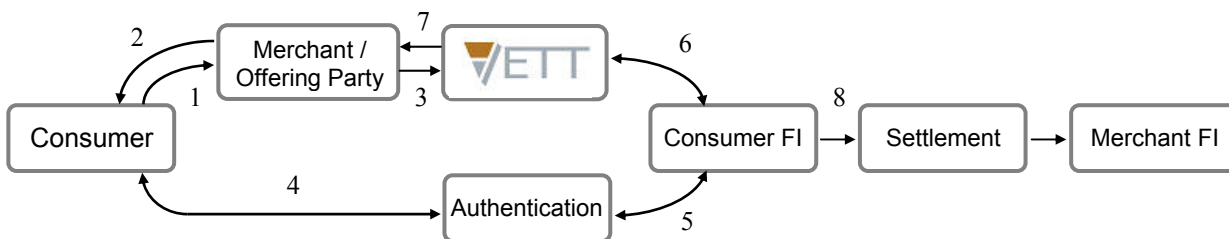
A Biller sends a bill (statement) with a unique identity number to a Consumer requesting payment.

The Consumer checks the bill (Is it for me, Do I know the biller and is it the right amount?). Assuming all is as it should be the Consumer will connect to their online account and log-in.

After an authentication routine the Issuer system will request the 'unique identity number' of the bill. The VETT system locates the bill and reports a summary to Consumer.

Assuming the summary matches the bill, the Consumer accepts the data and is asked to 'authorise payment'. Selecting 'authorise' generates a message to report payment made and the Consumer can then 'log-out'.

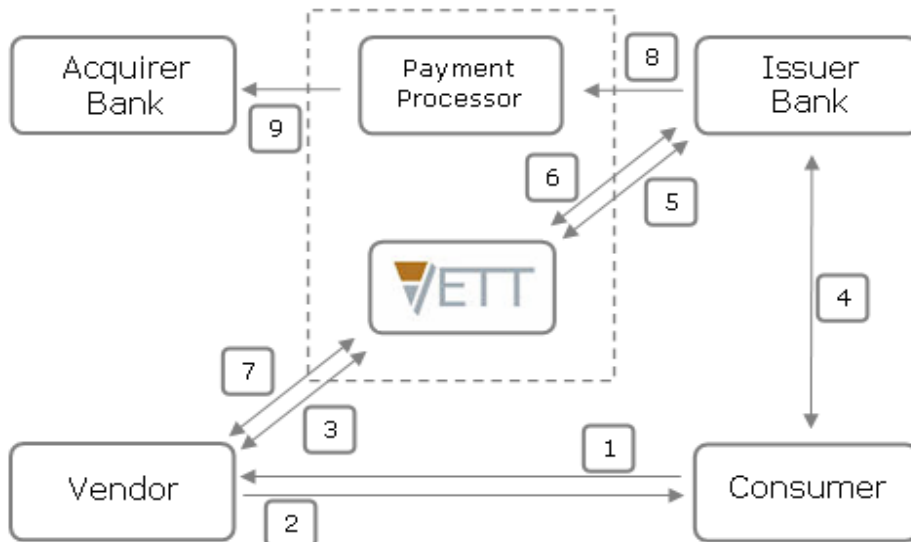
Detail of a VETT transaction



1. The User (Consumer/Business) connects to a Merchant and will submit their instruction via an order form indicated by arrow [1]. The VETT function issues a unique identifier for the transaction and stores a copy of the order (transaction) pending authorisation.
2. A copy of the order message is posted to the User (via SMS or email) asking for User authorisation [2].
3. A duplicate copy of the order is registered with VETT [3].
4. To authorise a transaction the User must log-in to their Financial Institution (FI) and use a prescribed authentication routine. When authenticated the User is required to enter the transaction's unique identifier [4].
5. The User checks the details of data reported for that unique identifier. The User must confirm the transaction to initiate authorisation of payment [5].
6. Subject to the result of an available balance check (cash on hand in consumer's account), FI functions issue an authorisation code which is transmitted to VETT [6].
7. VETT compiles and forwards an authorisation message to the Merchant system [7].
8. VETT forwards payment data to 'Payment Processor to enable settlement between the User FI and the Merchant's FI [8].



Diagram – VETT in the four corner model



This diagram shows:

The steps involved in a VETT transaction

The potential location for the VETT platform

(VETT technology can be deployed for many differing applications other than the billing and payment scheme described here. An optimal operational location can only be determined and specified in light of requirements for the use of the technology).

The payment message resulting from an authorised transaction

Also:

This diagram also represents the commercial relationship for a new payment scheme

Vendors are sponsored into the scheme through an Acquirer

Consumer must hold an account with an Issuer registered with the scheme

Additional information:

Suitable for Business to business as well as Consumer to business

Orders can be placed by Internet, Telephone, Mobile and Face-to-face

Payment can be authorised by Internet, Mobile, Telephone or Authorised Agents

A registered Vendor can issue 'one-off' and/or scheduled bills (invoices, pro-forma-invoices, statements, subscription requests). Such requests for payment can also include a timing element (cooling off period) which must be observed before payment can be authorised.



Distribution of VETT components

Merchant system

To enable a VETT transaction the Merchant system requires a plug-in component to facilitate the following tasks:

- Create a unique identity number for each transaction
- Compile and store a record of the transactions
- Forward copy of an enquiry to the consumer and submit duplicate copy to VETT
- Store a copy of consumer enquiries pending authorisation
- Report functions are provided to maintain operational efficiency

Financial Institution system

To enable a VETT transaction the Financial Institution system requires a plug-in component to facilitate the following tasks:

- Authenticate access to VETT server
- Perform 'available balance' check on Users' account
- Generate and forward authorisation code for transactions
- Compile payment message and forward to Payment Processor
- Exception functions

VETT System

The VETT system is a separate and dedicated system to facilitate the transaction flow. To ensure security, VETT's dedicated operation or functionality should not be integrated with any other system.

VETT functions include the following:

- Automatically receive and negotiate connection with authorised Merchant systems
- Store transaction records submitted from Merchant using unique identifier
- Stores transaction records pending authorisation
- Time parameters are employed to control record retention
- System receives and negotiates connection with Financial Institution server
- Receive authorisation code/s and forward to Merchant server
- Reporting functions
- Automatic routines are used to maintain operational efficiency.



Consumer

No special device or software required. Consumers can conduct a VETT transaction via the internet, by telephone, by Mobile phone and face-to-face through an Authorised Agent.

Advantages of separating the Instruction and authorisation actions

Consumer	<ul style="list-style-type: none">• No sensitive financial data is shared with any third party• Specifies delivery address• Certainty, safety and control of timing• Protects against identity theft
Merchant	<ul style="list-style-type: none">• Certainty of payment• Confirmation of delivery instructions• No charge back or associated costs
Financial Institution	<ul style="list-style-type: none">• Minimise repudiation• End-to-end automation• Secure - Protects against identity theft and fraud• Potential for new revenue streams
System	<ul style="list-style-type: none">• Enables multi channel access via Internet, landline, mobile and face-to-face• Thwarts all known threats to consumers such as fake site, email and telephone phishing.

For further information on the VETT solution contact Garry Gibson email: enquiries@vettuk.co.uk or telephone:

Office: +44 (0) 1636 707 777

Fax: +44 (0) 1636 700747.

Footnote on Phishing and Fake-site scams

An attacker can use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack and it is very difficult to spot without specialist knowledge.

A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.

Source: *Wikipedia, Dec, 2007*