Page left Intentionally Blank

*Introducing E*MERGE® powered by 3DAS™*

GUARANTEEING IDENTITY AND SECURE PAYMENTS THE FOUNDATION FOR ECOMMERCE

The explosive growth of the Internet promises much. Organisations can extend their reach to hundreds of millions of new and profitable customers. Unfortunately, a powerful brake is holding back the growth of eCommerce: ***Distrus*t**. Fear is firmly fixed in the minds of businesses about the true identity of parties on the Internet. Simultaneously consumers fear sending sensitive personal and financial information over an open and insecure Internet. Both these fears are fuelled by regular Press reports telling of fraud by criminals and easy intrusion by hackers. *And with no viable, ready-to-market, bank-led solutions to turn to,* these reports will continue to discourage millions of businesses and consumers from buying through this inexpensive and *already available* sales channel.

For Business-to-Business eCommerce to thrive, a means of guaranteeing the *Identity* of the parties on the Internet is a mandatory requirement. Moreover, for Business-to-Consumer eCommerce to thrive, consumer must be confident and have access to a proven economically sound *secure payment system*. One that the banks can trust, is cost-effective for sellers, and is mobile while easy to use for buyers. Ultimately digital trust capable of assuring the irrefutability of any Internet transaction is essential.

Unicate believes that E*MERGE® powered by 3DAS™ provides the answer. Not only does this new technology give complete security, it is portable, providing a cost-effective method to authenticate the identity of each party in a transaction anywhere on the Internet. Being intuitively obvious for the buyer to use, user confidence is maximised.

E*MERGE® powered by 3DAS™ provides *today* the perfect identification and Secure payment system for everyone to securely trade over the Internet.

*Why is E*MERGE® powered by 3DAS™ superior to other solutions?*

A number of companies and consortia have attempted to assure authenticity using Smart Cards. Others propose digital certificates locked inside insecure PCs. From this work, SET or "Secure Electronic Transaction" has been proposed. However, SET is not the answer. It is generally agreed that SET will impose a costly and unacceptable cryptographic computational burden. Nor is SSL a solution. This is only a line encryption system between two points and simply cannot secure sensitive information inside a PC or merchant server. Some propose adding a Public Key system on top of SSL. However, as with SET, this demands a single, global, legal and technical Public Key certification infrastructure. Even if anyone would be willing to accept the cost of the incremental computational power required in PCs and Internet servers to unravel each cryptographic level of hierarchy, *these software-based solutions do not offer mobility*. Hence, no other system can offer the security and cost-effectiveness that E*MERGE® and 3DAS™ does.

For eCommerce to prosper, corporations, merchants and consumers demand an easy to use, mobile and inexpensive means of proving identity and transacting payments. *Moreover, this is precisely what E*MERGE® ® powered by 3DAS™ can deliver.*

Why 3DAS™?

3DAS™ is the simple solution for creating a cost-effective and secure Internet transaction and payment system. It gives the card issuer, acquiring bank and seller a proven Card Authentication Method (CAM). Unicate has demonstrated that a 3DAS™ CAM cannot be reproduced and that transactions digitally signed by a 3DAS™ Card are irrefutable. More importantly, rejection of a legitimate buyer is near impossible. 3DAS™ also eliminates the need for the expensive security hardware required by magnetic stripe based Cardholder Verification Methods (CVM) used to support PIN. 3DAS™ therefore provides a secure off-line CAM and an inexpensive CVM to protect MasterCard, Visa and other payment cards. 3DAS™ offers:

- **Cardholder (buyer) Authenticity**
- **Buyer mobility**
- **Payment Data Confidentiality**
- **Seller (merchant) Authenticity**
- **Transaction Irrefutability**
- **Transaction Integrity**

3DAS™ is the **easiest to use** and most cost-effective solution to credit and debit card security. To implement, the buyer simply installs a 3DAS™ "Plug and Play" reader and the issuer adds the 3DAS™ authentication and personalisation modules to their system. The result is authenticity of all parties to the transaction, data integrity, data confidentiality and transaction irrefutability

*Why E*MERGE®?*

*Based on 3DAS™ and the work done to combat card fraud, Unicate has now created E*MERGE®, Unicate's transaction and payment solution for the Internet.*

*The benefits of E*MERGE® to banks:*

✓ Banks can profit from the growth in eCommerce and extend their full range of electronic payment products into this environment.

✓ Banks can cost-effectively and securely introduce on-line PIN and debit cards for Internet payments without the need for expensive cryptographic technology.

✓ Banks need not alter their existing EFTPOS networks and systems.

*The benefits of E*MERGE® to sellers:*

✓ Sellers are secure that the buyer is authentic; the transaction is irrefutable so when the sale is completed payment is guaranteed.

✓ Sellers can use the same technology to support a range of payment options.

✓ Sellers can benefit from favorable Card Present payment terms.

*The benefits of E*MERGE® to buyers:*

✓ Buyers can easily choose from an array of payment methods knowing critical payment details are entirely confidential.

✓ Buyers know that they are buying from an Acquiring Bank's authenticated seller and can be confident of the integrity of the seller's invoice and the terms of sale.

✓ Buyers are mobile. They can use their 3DAS™ Card on any device, from the PC at home, to a colleague's laptop, in a Cyber Café, or with their PDA, GSM, or at a Point of Sale terminal in so far as these devices are E*MERGE® enabled.

✓ 3DAS™ works the same way anywhere**, at anytime, in any device.**

The Unicate solution (US $0.30 per card and $ 49.95 without considering volume discount) affords the ultimate in fraud protection. The 3DAS™ CAM eliminates the costly systems, and network changes that expensive EMV Smart Cards proposals demand. The E*MERGE® protocol is simple, easy to implement and protects both the issuing and acquiring banks' current investments in payment technology.

*How can you benefit from E*MERGE® and 3DAS™?*

Unicate believes that E*MERGE® powered by 3DAS™ is an opportunity your company can capitalise upon. The following Appendices have been provided for your Senior IT officers to scrutinise. We are confident that the observations and conclusions made in this document will be fully substantiated.

TABLE OF CONTENTS

I Guaranteeing Identity - The Key Issue of Security In eCommerce

A series of real problems face the convergence of Internet eCommerce with internal corporate information policies or with high street commerce. The first is the problem of *trust*. Trust must be created between the buyer, the seller, and the banks before a transaction can take place. Trust, in a virtual world, can only exist when the identity of each of the parties involved has been guaranteed. Guaranteeing identity is such a basic requirement, that eCommerce will not be fully successful until it is solved.

The Goals for Secure Electronic Commerce

Numerous organizations and consortiums in seeking to solve this problem have set themselves the goal of creating a transaction and payment system to do the following:

1. Uniquely identify the client (*authenticity*)
2. Authorize the user (*verification*)
3. Guarantee the confidentiality of the employee's or client's identity and the instructions given over a public network (*confidentiality*)
4. Guarantee that the instructions given by the employee or client cannot be challenged and that the terms are as agreed (*irrefutability*)
5. Allow the employee or client to operate anywhere and at anytime (*mobility*)

A successful solution must also be cost-effective and user-friendly, requiring only the simple skills needed to operate a browser, insert a card, and conduct eCommerce.

Assuring Identity - Some Current Approaches

Three options exist today to assure identity of parties doing business over the Internet. Only one guarantees ease of use, mobility, authenticity and irrefutability.

A The account number and password system

This option can operate from any computer connected to the Internet. It relies on assigning an account number and a password to a user. These typically involve a string of at least fifteen characters. In most systems, the account number is at least twelve digits and the password eight characters. The problem with this approach is that only the server is sure of the authenticity of the user. While having to managing a growing number of passwords, employees or consumers can only be confident that they are connected to the right server by relying on the visual images presented on screen.

B. Wallets, software, and certificates

Here, data and software are loaded into each employee or client's machine. This software authenticates the server. After an electronic dialogue, it can state that the machines at both ends hold authentic certificates. This approach is limited in three ways. First it is not the person that is being authenticated, it is the machine. Second, it is not a mobile solution (unless the individual carries a laptop everywhere he/she goes). Third, unless both parties have exchanged something in advance, the authentication process does not function.

This approach is in principle a SET approach, except that SET offers a more complex solution based on a Public Key infrastructure (PKi) with Certification Authorities (CAs) to create the chain of trust and the third-party to guarantee that this trust is current.

Machine dependency has to led a layer of protection being added above the software in the machine. The user must enter a password to confirm that they are at the correct machine. They are then authorized to use this machine for the purpose intended. External parties however can copy or alter the software inside the computer. Because of these difficulties, many do not believe that a software solution can be successful.

C. Physical token or key

This uses a machine-readable physical token, which is given to the parties and authenticated when read. The essence of this approach is that the carrier treasures the token. If lost, the carrier will feel obliged to report it. To assure identification from any location, all that is needed is that the physical token can be machine-read anywhere. Keys of course can be stolen. Approximately 50% of bankcard fraud is due to lost or stolen cards. The answer is to add a second level of security such as a password/PIN or a biometric.

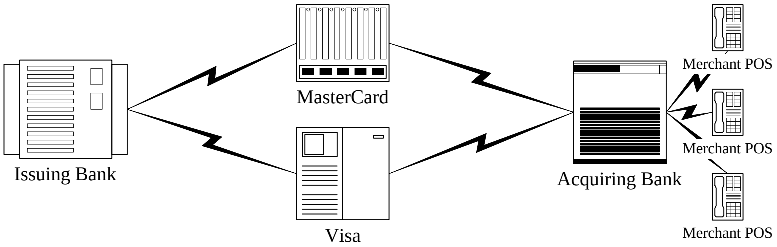
Means of Security	Ease of use	Mobility	Authenticity	Irrefutability
Account Number	Medium	High	Low	Low
With Password	Low	High	Medium	Medium
Software	High	Zero	Medium	Medium
With Password	Medium	Zero	High	High
Physical Token	High	High	High	High
With Password	Medium	High	High	High

Please note many people do not believe a software solution can be secure.

II ePayments - The Enabler of eCommerce

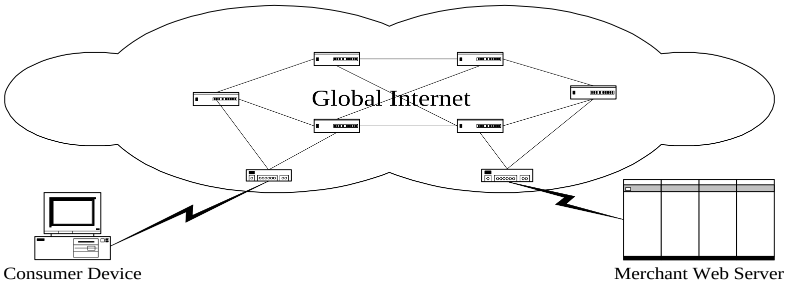
Assuming identity can be guaranteed, deciding which payment system to make available on the Internet is the next most important issue holding back the growth of eCommerce. Obviously, paper notes and coins will not work. The system must be electronic. Most people are already aware of electronic payment systems such as American Express, Diners, JCB, MasterCard, and Visa, and can rightly ask, "Why should we use anything else?" Security is an essential attribute of these networks. They have been introduced and accepted by buyers and sellers worldwide. Rather than inventing something completely new, these existing systems offer an obvious starting point for an ePayment system[1].

EFTPOS - The Virtual Private Network



The bank payment associations such as Visa, MasterCard and Europay have built a secure global network designed to carry authorization, clearing and settlement data. These are all Virtual Private Networks. Core to their design is an assurance of security necessary to protect sensitive payment details while guaranteeing that no transactions are lost. Other networks, such as those managed by S.W.I.F.T. in addition, the ACH operators have a similarly construction. All have well-defined messaging standards, comprehensive operating procedures, and certification processes to assure security and reliability.

The Internet - A Public Utility



In contrast to the VPNs, the Internet has evolved as a public utility with no inherent security or guarantee that transactions are complete. Its power is to allow any buyer to find a seller anywhere on the globe. Organizations see the Internet as an extremely powerful distribution channel without the cost of building and managing a physical storefront or the expense of running a global mail order and telephone order operation.

Consumer Fear - The Brake to Exponential Growth

Media publicity about the ever-present reality of fraud over the Internet has created suspicion and distrust in the minds of buyers about entering their personal or their company credit card details onto the Internet. The fear of fraud is real; particularly when one considers the open architecture of the Internet and the ease this offers hackers and criminals to intercept credit card data transiting the Internet. Fear has been fueled by stories of hackers breaking into merchant web sites, collecting details for a large number of credit cards and using this information to defraud card payment systems. Stories also abound of people receiving erroneous bank statements, or of fake ATMs being installed on high streets and in shopping malls to capture PIN and the debit card details. *The fact*

[1] Small value purchases is the one exception. Today only notes and coins are effective. The Internet will need something to take on this low value payment function.

that no viable and ready-to-market bank solutions are in sight only stimulates this decline in the confidence of buyers.

In a recent informal meeting, it was pointed out that based on a leading credit card organization's transactions, 90+% of mail order and telephone order fraud in Europe is Internet based. 15% of Internet clearing volume is charged back while 50% of digital goods purchased over the Internet are charged back. The solution, and the challenge, is to devise a way to use this insecure environment while retaining all the advantages of the proven and secure EFTPOS network.

The Internet Identification Requirements

To give organizations the confidence to reveal corporate secrets, divulge privileged client information or grant access to powerful transaction processing capabilities means it is essential to be able to trust that people on the Internet are indeed who they claim to be. Furthermore, the growth of one-to-one marketing has focused marketing strategies on segmenting the client based down to *one*. To be confident that access has been granted to the proper authorized party demands a solution that can:

- Assure the authenticity of the employee or client
- Assure the confidentiality of privileged information
- Assure the integrity of data
- Assure the irrefutability of the transaction

Internet Payment Security Requirements

The Internet is a user-friendly and open environment. For a payment solution to be successful, it must maintain this ease and openness without putting the current EFTPOS network at risk. This means finding a payment transaction solution that can establish trust between buyer and seller by addressing the following security issues:

- Authenticity of the buyer and the seller
- Verification through the use of PIN of the identity of the card user
- Confidentiality and privacy of information relating to content of the Transaction
- Integrity of transmission data
- Irrefutability of the transaction.

Nevertheless, to be completely successful, the Internet payment system must also be capable of dealing with the following additional issues:

- Guaranteed payment upon fulfilled terms of delivery
- Mobility that allows the buyer to conduct business on the Internet from any point of interaction, regardless of the device type or location
- Support for an array of existing payment products
- Incorporation of an effective (i.e. economical) micro-payment system

III The Failure of Current Solutions

Since the advent of the Internet and the World Wide Web, a number of players have been searching for a secure way to enable payments.

SET-Secure Electronic Transactions

- SET, the specification developed by MasterCard and Visa with the advice and assistance of GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa, and VeriSign, has been slow in its uptake due to its cumbersome protocol and its requirement for excessive processing. Complaints abound on the cost of implementing SET due to its demand for the computation power to perform complex cryptography. Cumbersome registration/enrolment procedures also concern consumer advocates and trouble bank managers who are responsible for assuring customer satisfaction.
- In recognising the enormous interest buyers/consumers have in the Internet, some banks have installed Cyber Cafes in their prime branch locations. *Nevertheless, the banks must accept that mobility is not part of SET.*

EMV - The Bank Card Specification for Smart Cards

- Europay, MasterCard and Visa, who have been working on the introduction of Smart Cards based on EMV specifications to combat fraud, are currently investigating the possible integration of EMV with SET. EMV would offer increased mobility. Yet, with regard to EMV, its implementation has been equally as slow as SET. The two different PKi structures of SET and EMV also create the need for more expensive processing power and software
- Smart cards have not yet proven cost-effective in most markets. In the largest payment card market, the United States, banks are particularly concerned about the economics of EMV.

SSL - The Default Solution

- While concerned about the complexity of SET, yet under pressure to make eCommerce a reality, a number of merchants have turned to SSL as a way of securing information *while it transits* the Internet.
- SSL is only a line encryption method between two points. SSL does not protect card details stored within the merchant server or inside the buyer's PC.
- For a criminal intent on attacking the system, the easiest place to attack is the insecure web server of an unsuspecting merchant. Once inside, it is not one card that they can counterfeit, but hundreds if not thousands.
- A PKi can be built on top of SSL, introducing the need to manage and authenticate public key certificates. This is fraught with politics. Defining who shall be the entity responsible for offering trusted certificates is a much-debated issue. When it involves a guarantee of payment, the banks believe they should be more responsible. When it involves assurance of identity, the question becomes more complex.

  What is it about the individual that needs to be trusted? Their name? The address they give. Is it that the individual is indeed employed by the named organization?

  There are issues of national verse global responsibility. PKi can support complex structures. Its "trust tree" is elegant in structure allowing digital trust to be both global and decentralized. Unfortunately serving this need for decentralization comes at a cost. Each layer requires incremental processing as the PC or server attempts to work its way up the tree until it finds a trusted entity that it recognizes.
- As a means of authentication, SSL must establish a comprehensive trust structure. Like SET, it will require that the banks agree to a global PKi architecture. This structure is not efficient in supporting the need for product, regional and national Certification Authorities. In fact, this PKi structure will create the need for complex cryptographic authentication processes within the PC and the web servers.
- SSL cannot secure card details and authenticate the counter-party.
- SSL is not a solution that can give the buyer both authentication and mobility
- SSL does not meet the requirements of the financial institutions as stated in SET

A Vision for the Internet

The vision behind all these current proposals for an Internet payment mechanism is very simple. It is to create:

- An easy to use
- Cost-effective
- Mobile
- Secure
- Irrefutable system for buyers and sellers to effect all transactions (including payment) over the Internet
- Via an assortment of payment options

However, realizing this vision has been difficult and slow. The political issues, the excessive complexity of processor intensive approaches, the standardization issues, the inter-operational problems, and the very significant implementation costs provide major obstacles to their uptake.

The result is that consumers continue to fear using the Internet as a purchasing channel.

The successful solution will be one that can meet all the demands of SET, overcome all the obstacles imposed by the complexity of SET, and deliver the mobility and security promised by EMV. At the same time, it will assure that payment details are safe, not only on the Internet but also in the insecure computers and servers connected to the Internet.

IV Identity & Transaction Irrefutability–The Solution Powered by 3DAS™

The Internet is a cost-effective channel for the sale and support of goods and services. Without a secure, easy to use and mobile solution for identification and ePayments, the growth and the success of eCommerce is at risk. As an advocate of the Internet and the power of 3DAS™, Unicate set itself the following objective:

> **To design a solution that will achieve all the goals of SET, overcome all the obstacles imposed by the complexity of SET, and deliver the mobility and security promised by EMV.**

This required Unicate to develop a solution that would specifically:

1. Resolve the Internet security issues.
2. Ensure that the act of payment is easy to use, safe, secure and mobile.
3. Avoid the cost and complexity of PKi and processor intensive approaches.
4. Protect the investment in the EFTPOS infrastructure by eliminating any need to modify these networks.

The result is a solution **without** expensive Certificate Authorities, laborious processor dependent Public Key verification, the complex legal issues of data encryption, and the need to upgrade legacy EFTPOS networks, or complex Internet protocols.

This solution, called **E*MERGE**, is made possible by Unicate's unique 3DAS™ technology. The use of the parallax of a Three-Dimensional Authentication System provides the basis for a coherent transaction and payment mechanism. It is simple to use, efficient to manage, and is not complicated by complex cryptography. It assures all parties of *authenticity, confidentiality, transaction integrity, mobility and irrefutability.*

The 3DAS™ Break-through

In 1994, Unicate discovered that by employing non-woven fibers and stereoscopic imaging technology, an authentication mechanism could be made that was cost-effective, process efficient and impervious to external attack. Research performed by TNO (the Dutch National Laboratory) revealed that the digital representation of this three dimensional authentication system, known as the "3DAS™ Table", is capable of assuring that **the item associated with the marker is unique in a sample of 10^{36}.** The result is a cost-effective method for providing the highest level of security allowed by international regulations. (See Appendix I for 3DAS™ details)

3DAS The Perfect CAM

Unicate and its team of experts have developed its 3DAS™ technology to produce a Card Authentication Method "CAM". This gives the ***issuing bank*** the following benefits:

1. ***Cost-effectiveness:*** An external business model produced by an international payment association has demonstrated that the 3DAS™ approach is a minimum US$ 10-15 billion less expensive over a five year aggregate than the prevailing Visa and MasterCard plans to deploy Smart Cards to combat counterfeit fraud. Using 3DAS™, cash flow will be positive within the third year whereas Smart Cards continue to be negative beyond the fifth year.
2. ***Secure card authentication and PIN verification without cryptographic technology:*** The 3DAS™ approach can implement on-line PIN without the need for any expensive cryptographic technology inside the public network. 3DAS™ provides data integrity, data confidentiality and transaction irrefutability (see below). This enables the use of PIN-based debit and credit cards on the Internet. A capability that does not yet exist.
3. ***Transaction integrity and irrefutability:*** To guarantee the integrity of card-based payment systems, Unicate has developed an effective algorithm, which creates a CAM that fits into as few as four digits. This allows the 3DAS™ approach to protect magnetic stripe cards in today's point of sale networks. The approach does not require any modifications to the existing EFTPOS systems, ATM networks or computer systems.
4. ***Security against criminal attack:*** **Compared** with current chip technology, the 3DAS™ approach is not open to criminal attack by digital replay or cloning of the smart card.

V The Ultimate Internet Authentication & Payment Solution: E*MERGE®

E*MERGE® has been designed to follow the basic guidelines and principles defined by the payment card industry for a coherent payment mechanism. It is simply to use and efficient to manage. E*MERGE® is also not complicated by a complex cryptographic overhead[2] or a complex protocol.

E*MERGE® can support any means of payment. These can range from small value payments to credit and debit card payments, to checks and electronic wire transfers. Whatever the method, ***by using the 3DAS™ technology,*** E*MERGE® is able to create the trust required between all parties involved (seller, buyer, Issuer and Acquirer**). <u>The payment details needed to construct payment instructions *never* traverse the Internet and are therefore impervious to attack</u>.** E*MERGE**®**, powered by 3DAS™, stands to be the most cost-effective and application transparent offering on the market today.

E*MERGE® delivers to **all** the parties involved the following fundamental capabilities:

- **Cardholder (buyer) Authenticity**
- **Seller (merchant) Authenticity**
- **Payment Data Confidentiality**
- **Transaction Integrity**
- **Transaction Irrefutability**
- **Mobility**

Unicate's E*MERGE® Design Principles

5. The Internet is an open on-line environment.
6. The exponential growth of the Internet and information technology-based services dictates that complex issues of software maintenance and data management are more cost-effectively handled in network servers than in millions of personal computers.
7. Buyers do not want to worry about managing certificates. They also do not want to discover that their re-issued card no longer works on the Internet.
8. Avoid the need for an extensive Public Key Certification infrastructure.

   The central issue is one of trust. Does the public key that is presented belong to the rightful (claimed) owner? To answer this requires the search for a common Certification Authority (CA) known by the party that delivered the public key and by the party that needs to verify the public key. Two paths must be followed:

   - The first leads from the owner to his/her CA, then from this CA to the next higher level CA until a common, known (and trusted) CA has been found.
   - The second leads from the verifier to his/her CA, then to the next higher-level CA until a common, known (and trusted) CA has been found.

   If no single global CA exists then this authentication process could end without a result. A further issue for a Public Key Certification infrastructure is that it must rely on the secure storage of the secret key. Arguments continue to rage between proponents of hardware solutions and proponents of software solutions, further slowing down the creation of an accepted, global solution.

9. Avoid the need to encrypt data. In general, the laws governing the use of cryptography around the world are complex. In some cases, its use is illegal. Data encryption presents two specific problems:
   - Legislation does not always allow for long keys. This diminishes the value of encryption because an eavesdropper can decrypt the information.

[2] The SET Secure Electronic Transaction Specification Book 1: Business Description includes fifteen pages devoted to the subject of cryptography in a document oriented to business people.

- Encryption requires key-synchronisation. Both the sender and the receiver need to know the key(s) required for successful encryption and decryption. Depending on the type of encryption used, this requires several extra messages to be sent between sender and receiver before the encrypted data can be exchanged. The result is that additional costs are incurred.

10. Do not allow secure payment details to be stored in insecure buyer and seller computers
11. Create a solution capable of supporting all existing banking payment products and adhere to the standard developed during the European Union funded SEMPER programme and the agreements reached by W3C and IETF.
12. Adhere to the principles set out by the payment card industry, and defined in the "Secure Electronic Transaction Specification Book 1: Business Description

"Primary motivations for the payment card brands to provide specifications for secure payments are to:

- *"Encourage the payment card community to take a leadership position in establishing a secure payment specification and, in so doing, to avoid costs associated with future reconciliation of implemented approaches,*
- *"Respect and preserve the relationship between merchants and Acquirers and between cardholders and Issuers,*
- *"Facilitate rapid development of the marketplace,*
- *"Respond quickly to the needs of the financial services market, and*
- *"Protect the integrity of payment card brands."*

SET also defines seven business requirements for an Internet payment mechanism:

1. *"Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.*
2. *"Ensure the integrity of all transmitted data.*
3. *"Provide authentication that a cardholder is a legitimate user of a branded payment card account.*
4. *"Provide authentication that a merchant can accept branded payment card transactions through its relationship with an Acquiring financial institution.*
5. *"Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.*
6. *"Create a protocol that neither depends on transport security mechanisms nor prevents their use.*
7. *"Facilitate and encourage interoperability among software and network providers.”*

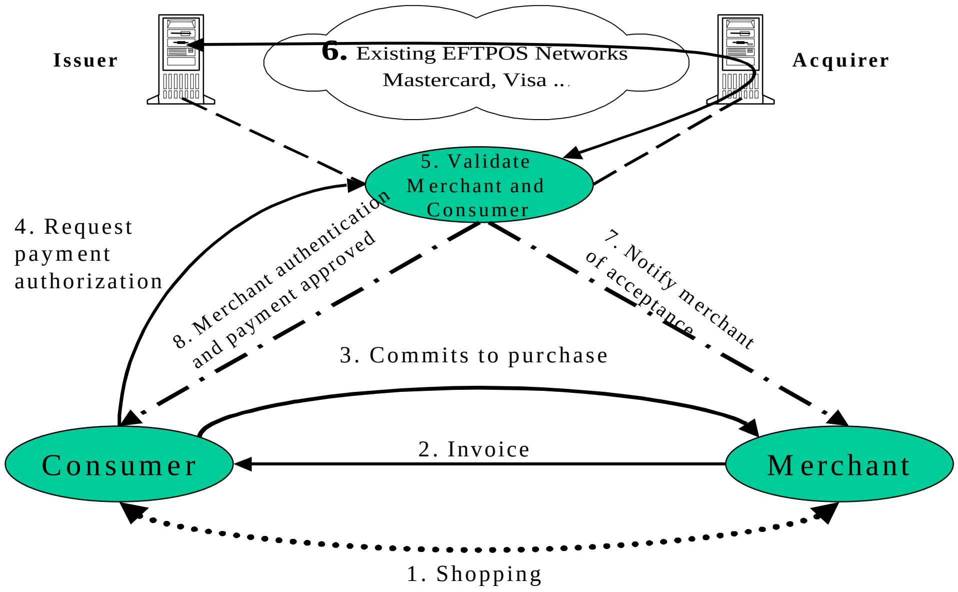
Unicate believes that these principles should be the basis for evaluating the viability of any system claiming to be an easy to use and cost-effective merchant and consumer mechanism for effecting, in total confidence, all transactions and payments over the Internet.

Eight Easy Steps for payment transactions

E*MERGE® mimics the way payment transactions take place in the real world.

5. The buyer locates a seller on the Internet and shops
6. The seller prepares an invoice and offers a set of payment options to the buyer
7. The buyer confirms to the seller their plan to buy with a selected payment option
8. The authorization for payment is requested
9. The buyer and seller are authenticated inside a secure environment
10. Without requiring any modifications to today's EFTPOS systems, the Issuer is asked to approve the payment
11. The seller is informed of the approval or decline of the payment
12. The buyer receives confirmation of the payment.

E*MERGE® - Internet Transaction and Payments Made Simple


Issuer
6. Existing EFTPOS Networks
Mastercard, Visa ..
Acquirer
5. Validate Merchant and Consumer
4. Request payment authorization
8. Merchant authentication and payment approved
7. Notify merchant of acceptance
3. Commits to purchase
Consumer
2. Invoice
Merchant
1. Shopping

The eight E*MERGE® steps assure the buyer, the seller, the Issuer and the Acquirer that sensitive details for payment never traverse the Internet. The seller is assured that they will be paid, the buyer that the goods will be delivered and the banks, that customers can securely take advantage of the power of eCommerce on the Internet.

What E*MERGE® Means for the Seller

The seller is able to offer buyers an assortment of payment systems within a mechanism that assures the buyer that the seller can be trusted. The entire technical infrastructure to interface with a chosen payment system is part of the solution.

The seller can be paid by any one of the following means of payment[3]:

- Acquiring bank relationships supporting, for example, Visa, MasterCard, Maestro, Interlink, JCB, and domestic debit card schemes
- A set of bank relationships capable of accepting electronic cheques, or direct debits.
- An American Express relationship
- A micro-payment service

E*MERGE® also provides the seller with:

- Irrefutable proof of the uniqueness and integrity of the invoice sent to the buyer, which is subsequently recorded as part of the buyer's agreement to pay.
- An approval of payment that is based on the trusted authentication of the buyer and designed to match the business conditions of a card present transaction. *Note that this card present feature translates into lower discounts for the merchant and offsetting lower risk costs for the card issuer.*
- A means of proving to the buyer that they are paying the trusted seller.

What E*MERGE® Means for the Buyer

E*MERGE® creates a simple and secure payment and transaction environment in which the buyer is assured that the seller can be trusted. Enrollment is very straightforward and easy. The buyer is provided with a unique 3DAS™ Payment Card and an inexpensive 3DAS™ Reader. The reader may optionally contain a secure and low cost PIN pad allowing the support of PIN-based payment products. The 3DAS™ Reader is plugged into the PC and the plug & play software automatically loads the E*MERGE™ Browser Plug-in. The plug-in automatically connects to the Issuer's designated payment server and organizes the activation of the buyer's 3DAS™ payment card.

After the buyer has selected the goods and services they wish to purchase, the seller submits an invoice. After inserting the 3DAS™ payment card, the E*MERGE® Browser Plug-in presents the buyer with a list of payment methods that buyer and the seller both employ (including credit and debit cards and a micro-payment mechanism). By simply clicking on the payment method the buyer wishes to use for the transaction, the buyer accepts the seller's terms and authorizes payment.

The banks are convinced of the authenticity of the buyer and seller and the buyer's bank authorizes the payment. The buyer and seller then receive confirmation of completion from their E*MERGE® Payment Server. These two messages authenticate the seller to the buyer and the buyer to seller that the buyer's bank will make payment and seller will comply with the terms and conditions of the sale.

[3] Unicate has only validated that these payments can be supported, others simply require a technical validation.

What E*MERGE® Means for the Banks

Unicate offers both Issuing and Acquiring banks a mechanism that supports their existing means of payment, without the need for any changes to their existing EFTPOS infrastructure.

3DAS™ can guarantee that both the seller and the buyer are who they claim to be, even when using the Internet. Furthermore, the E*MERGE® system offers irrefutable proof that the terms of payment, as agreed by the buyer, were as issued by the seller. This all happens on-line while simultaneously creating a suitable audit trail able to provide evidential proof to assure irrefutability in the event of a dispute.

Unicate offers the Issuing and Acquiring banks a cost effective means of guaranteeing payments over the Internet that is mobile, simple, efficient for the buyer and cost-effective for the seller.

Business Relationship Assumptions of E*MERGE®

E*MERGE® has been established based upon the principal that the payment card Issuer maintains control over the buyer relationship, and the payment card Acquirer maintains control over the seller relationship.

Unicate assumes that the E*MERGE® system will be set-up and managed by a consortium (most likely the payment schemes) who will establish the rules, manage the secure VPN and commission the associated MP and CP servers.

It is therefore assumed that the relationship with the buyer will be a three party relationship with the Issuing Bank taking the lead. The operator of the CP server is a trusted agent of the Issuing Bank.

It is also assumed that the relationship with the seller would be via a three party relationship with the Acquiring Bank taking the lead. Thus, the operator of the MP server becomes a trusted agent of the Acquiring Bank.

In many markets, sellers do not restrict processing their payment activity through any one Acquiring Bank. As is true with any payment system, acceptance is the key. So the E*MERGE® system assumes that the primary relationship for technical processing is between the seller and the operator of the E*MERGE® MP Server, while the primary relationship for payment processing is between the Acquiring Bank and the seller.

The banks must trust the operators of the MP Servers.

Appendix 1 - 3DAS™ The Ultimate in Security

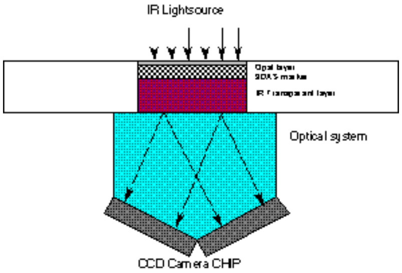
3DAS™ is a marker embedded into any object, for example a credit card. Once embedded into the designated object, 3DAS™ becomes that machine-readable token that provides a coherent solution to all the issues surrounding assuring trust and insuring security over the Internet.

The digital interpretation of 3DAS™ is a unique means of identification capable of authenticating and therefore guaranteeing that the genuine object/card is present. By binding data or transaction details to a unique read of 3DAS™ a digital signature is established that assured the irrefutability of that card being present when that data or transaction was altered or created.

Using a simple 3DAS™ Reader connected to the users PC and adding a unique 3DAS™ value as an index to a database, Unicate has been able to create this authenticity of identity. Moreover, 3DAS™ can become the employee number, client account number or credit card number.

By upgrading the 3DAS™ Reader to include an integrated keypad, it is further possible to establish a relationship between 3DAS™ and the cardholder's 4 to 8 character password or PIN.

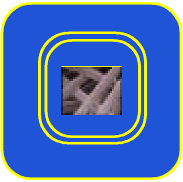
The Birth of 3DAS™ - the Ultimate Token for Identification and Authenticity



In 1994 Unicate BV discovered that by employing non-woven fibers and stereoscopic imaging technology, a physical authentication mechanism, "A Secure Token", was now available that is process efficient and impervious to external attack. The result of original research, conducted by TNO the Dutch Research laboratory, revealed that the digital representation of the 3DAS™ "Three Dimensional Authentication System" is unique in a sample of 10^{36}.

In terms that are more technical, the False Acceptance Rate FAR[4] or "type one error" is one in 10^{36}. The other key measure, the False Reject Rate[5] FRR or "type two error" is one in a number approaching infinity. Compared to any known physical token or human biometrics these results stagger the imagination and offer the users of 3DAS™ a level of security and customer service that is near perfect.

3DAS™ Marker



To take advantage of the unique power of 3DAS™, the un-woven fibers are put through a unique Unicate coating process and ultimately inserted into a frame. This frame is then affixed to or embedded inside a plastic card, paper check, brand label or any other object that one wishes to be assured is authentic. Depending on the application the marker can either be visible or invisible allowing the security solution to be overt or covert.

[4] The FAR is the measure of how many times a fraudulent individual will be able to pass themselves off as valid consumers. The FAR is a pure economic loss for the banks. Furthermore when billed to the rightful consumer, an easy way to alienate your important clients.

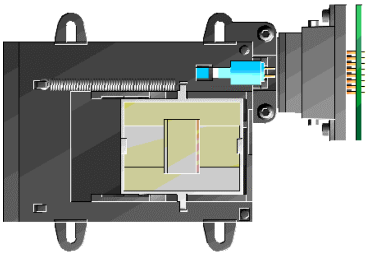
[5] The FRR is the frequency a customer suffers rejection. Each rejection is a customer relationship nightmare!

The object now has a one to one association with a 3DAS™ Marker[6]. This physical token can be read at any time during the object's life and by checking with an authority that has registered the 3DAS™ Marker one can be assured that the object is the original one.

In order to assure that the concept and technology was capable of operating in the real world a series of trials took place in Holland. The results proved that under field conditions the 3DAS™ Marker could be read accurately and that its integration into existing computer systems could be achieved without significant effort[7]. Simultaneously, Unicate performed the necessary tests to prove that the 3DAS™ Marker adhered to all the ISO standards. This therefore assures users of 3DAS™ that the marker will last longer than the plastic card it is embedded in.

3DAS™ Reader

After the successful completion of the trials, the Unicate team began the work to industrialize the optical element of the reader and to miniaturize the sensor, processor, memory and electronics used to perform the optical read and create a unique digital representation of the 3DAS™ Marker. The production prototype shown below resulted in a component designed to read the 3DAS™ Marker embedded in a standard ISO 7810 plastic card integrated with an ISO 7816 Integrated Circuit Card ICC.



Inside the 3DAS™ reader is an infrared LED, a light train, the sensor array, a digital signal processor, a gate array, volatile and non-volatile memory, chip card contacts and appropriate input output logic. Given that its core function is to guarantee that an optic read has occurred and that external agents cannot view what is taking place during the processing cycle, security is inherent in its design.

Unlike smart cards and other hardened security devices, no secrets are stored within the device thus eliminating the risk from an external attack. In the event that applications employing 3DAS™ require enhanced security to protect the algorithm or other persistent elements of application specific data, then the design already includes the ability to add an ICC, like those used for the GSM SIM, bank issued electronic purses and proposed by EMV.

Core to the 3DAS™ philosophy is that the **3DAS™ Reader must be able to fit inside any device** that one might consider using to authenticate an individual or effect an electronic transaction. This has led the Unicate team to further miniaturize the 3DAS™ Reader. Future releases of the hardware are being designed in such a way that they can fit into set top box, personal digital assistants, mobile phones and an array of emerging Internet access devices.

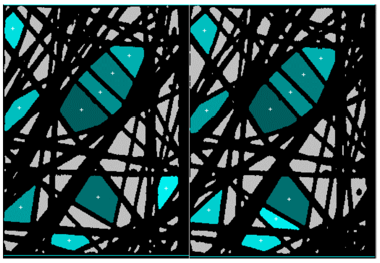
Later in the description of the 3DAS™ capabilities, there is a description of how to perform cardholder verification using 3DAS™. In the case that this function is required, a tamper evident keypad is integrated into the 3DAS™ Reader allowing the buyer to enter their PIN and then allowing the internal logic to perform PIN verification or create a mechanisms to facilitate on-line PIN verification ***without*** need for network security. The 3DAS™ solution eliminates the need for hardened security hardware used to encipher the PIN during transmission.

[6] Research performed by Akzo Nobel, Unicate and TNO has identified that the only way to replicate a 3DAS™ Marker is to be able to steer the production of a random mass of filaments, on average 38 microns in diameter, in three dimensions. Furthermore a deviation of 4 microns in the selected geometry is a different marker

[7] In one case a large array of databases where linked together by simply providing each patient a 3DAS™ card and adding the 3DAS™ Key to each patient record during admission. Then by using 3DAS™ as the common index all the associated information collected about that patient was linked together.

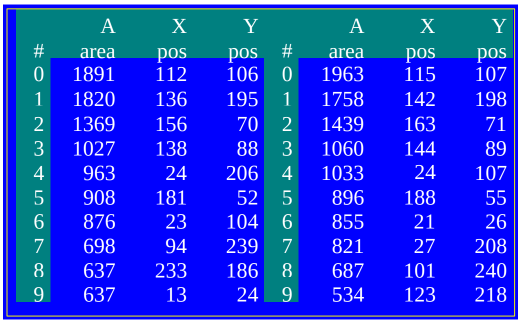
3DAS™ Table

To create the 3DAS™ Table, the optics generates a stereoscopic image of the 3DAS™ Marker on a single sensor (camera chip). The result, as seen by the sensor, is two images. The first, the right view at +20°. The second, the left view at -20°. These two images result in a digital representation of the black or white value of each pixel. In other terms, where the filaments of the 3DAS™ Marker exist the pixel is black and the space between is white.



Working with this digitized image, the software identifies the ten largest planes. The process within the 3DAS™ Reader then calculates the area and the center of gravity for each of these planes. The software then sorts the 10 planes of the left and the 10 planes of the right in descending order. The result is the 3DAS™ Table[8].

3DAS™ Key



	A	X	Y		A	X	Y
#	area	pos	pos	#	area	pos	pos
0	1891	112	106	0	1963	115	107
1	1820	136	195	1	1758	142	198
2	1369	156	70	2	1439	163	71
3	1027	138	88	3	1060	144	89
4	963	24	206	4	1033	24	107
5	908	181	52	5	896	188	55
6	876	23	104	6	855	21	26
7	698	94	239	7	821	27	208
8	637	233	186	8	687	101	240
9	637	13	24	9	534	123	218

To activate a 3DAS™ Marker the 3DAS™ Table must be registered in an organization's database. The registration takes place during the card personalization process and includes a few of reads of the marker. The result of merging the 3DAS™ Tables creates the 3DAS™ Key. The 3DAS™ Key is then linked within the organizations database, to the card.

From this point forward card authentication and identification is achieved by comparing a 3DAS™ Table to the 3DAS™ Key. If they match, the card is authentic with a risk of one in 10^{36}.

3DAS™ Algorithms

Since the initial trials of the 3DAS™ technology, the power has been in the ability to apply the 3DAS™ Table. The first application saw the table as a pointer to a database. The most recent innovation has identified how to use 3DAS™ as a mechanism to secure information in such a way that any number of copies can exist. However, to read the data the 3DAS™ Marker, a trusted 3DAS™ Reader (with the appropriate algorithm inside) and the owner of the information must be present.

As Unicate looks to the Internet all of these algorithms can be put too good use. The power is that 3DAS™ is a physical token not limited by mathematics. However, mathematics can exploit it.

During the development of a 3DAS™ solution to fraud problems of the plastic payment card industry, Unicate discovered a series of additional capabilities of 3DAS™. Most of these resulted from determining that the entire 80 byte 3DAS™ Table does not need to be transmitted to the card Issuer in order to guarantee unparalleled levels of authenticity.

In fact, after consulting with TNO, it was determined that 8 bytes would produce a FAR of 1 in 60 billion and by increasing the number of bytes transmitted to 16, results in a false acceptance rate of $1.5x10^{21}$. These findings allowed Unicate to propose a solution to the payments industry that does not require any modifications to the numerous systems that attach the point of sale device to the Issuing Bank's host. More importantly, Unicate was able to create a solution that secured today's magnetic stripe and cheap secure memory chip based relationship cards.

[8] This is only one-way of interpreting the 3DAS™ Table. Additional variables can be derived for each plane or an organization may employ other values unique to them.

Bottom line, Unicate has designed a series of functions that assure the ***Identity, Authenticity, Irrefutability, Integrity and Uniqueness*** of any object and the transactions it engages in.

The 3DAS™ FastKey

The 3DAS™ FastKey is an extract of the 3DAS™ Table that can be used as a common index to extremely large databases. The 3DAS™ ™ FastKey is the digital representation of a physical key belonging to an object, card or person.

A simple application of the 3DAS™ FastKey is to use it as the employee's key to corporate access control systems. The solution requires a simple plastic card with a 3DAS™ Marker inside. The 3DAS™ Marker is read at a door, a security gate or the terminal with access to corporate secrets.

The 3DAS™ Reader would create the 3DAS™ FastKey and request from the corporate security database permission to allow this person through a particular door in a building or campus complex. An inexpensive solution that is impervious to attack, easy to install and comparable in price to the magnetic stripe and PIN based systems in use today.

Unlike today's magnetic stripe cards, or for that matter chip cards, **a 3DAS™ Marker cannot be duplicated. It must be located from within a pile of 10^{36} markers.**

The algorithm implemented within the 3DAS™ Reader to create the employee id simply must know the length of the security systems database's index and understand which elements of the 3DAS™ Table will be used to define the 3DAS™ FastKey. In essence, the 3DAS™ Marker becomes the employee’s identity card. Thinking in terms of payment systems the 3DAS™ FastKey can be an account number.

As an example, using the 3DAS™ Table represented on page 22, and applying an organisations specific algorithm[9], the 3DAS™ FastKey of this marker would be 112 106 136 195 115 107 142 198.

The 3DAS™ FastKey is the unique an indisputable means of identifying that that physical token is or was present and read by a 3DAS™ Reader.

The Hash

In the development of solutions to assure the integrity of data transmitted electronically, mathematicians have been exploring the field of large numbers. During their research they have developed a series of mechanisms that allow one to calculate a value that offers the sender of electronic data assurance that the receiver of the same element of data will know that no one has altered the content of the message. Simultaneously these mechanisms, unlike what we all learned in mathematics, cannot be reversed, they are "one way" functions. Because of this unique property and their acceptance in the marketplace, they have become an integral part of the 3DAS™ solution.

To receive the assurance of **data integrity** the recipient simply takes the data received and performs the exact same mathematical calculation. The result will be a value that must be the same as the value calculated by the sender, or, the recipient knows that data has been altered.

Various forms of these algorithms, a Hash, have been defined and tested by a number of recognised authorities. Which Hash algorithm is employed is not important, the only requirement is that all parties agree on the one that will be used.

[9] Assume that an 8-byte index is required. Define an algorithm that selects the X and Y values of two largest planes from of both the left and the right image. Within this algorithm take the X value from the largest plane on the left followed by the right value followed by the X value of the second largest plane of the left and so on. This would result in a 3DAS™ FastKey which ultimately would be converted to the hexadecimal value of 112 106 136 195 115 107 142 198. Insert this value as the index of the record belong to that card and you have a means of accessing the data associated with that card with an assurance that that marker is unique in a population of 60 billion

In the E*MERGE® solution, data pertinent to the terms of the payment transaction are input into the Hash calculation, thus, providing the consumers, merchants and banks comfort in knowing that the contents of the transaction have not been altered by outside parties.

What the Hash does do is provide data or transaction integrity. The Hash does not provide a means of identifying and authenticating who sent the message. To achieve this more important task of identification and authentication of the parties engaged in the transaction is where the 3DAS™ Marker is employed.

3DAS™ Signature

The 3DAS™ Signature is the means of assuring the parties engaged in a transaction that the identity of the individual involved in the transaction can be authenticated and that the Hash can be proven to be the one created by that individual. In the case of a payment transaction, it proves that an authorised seller and an authorised buyer were present and executed that particular transaction.

To achieve the security goals of *authenticity, irrefutability and integrity* the only requirement is that the party interested in being assured of the identity of the physical token register the 3DAS™ Marker in their database. In the E*MERGE® payment system this means that the Consumer Bank and the Merchant Banks register the 3DAS™ Marker of their customers card.

To be able to assure authenticity of who signed the transaction, the party who registered the 3DAS™ Marker simply compares a 3DAS™ Signature they create, using the 3DAS™ Key stored in the database, to the 3DAS™ Signature generated, by the 3DAS™ Marker, used to sign the transaction.

To create a unique 3DAS™ Signature for each transaction, a Hash is created over pertinent data such as the terms and condition, the date, the time and the location of the transaction. This Hash is submitted to the 3DAS™ Reader. The reader uses the Hash as a set of pointers[10] to select values from the 3DAS™ Table of the optical read of a 3DAS™ Marker present at the time of the transaction. The resulting **3DAS™ Signature provides irrefutable proof that** the card belonging to **the person** authorising the transaction **was present**.

Upon receipt of the Hash and the 3DAS™ Signature, the bank duplicates this process using the 3DAS™ Key as its equivalent of the read. By comparing this value to the <u>**3DAS™ Signature**</u> just received <u>**provides irrefutable proof**</u> that <u>**the card was present**</u>.

If irrefutability of the terms of the transaction is the requirement then all that is required is that the bank receives the data (terms and conditions) that was hashed, and the original 3DAS™ Signature. By using the 3DAS™ Key as its base, the bank can re-compute the Hash and the 3DAS™ Signature and prove that those are the terms and conditions that the parties agreed to.

In the event that the cardholder disputes that their card was present, then by simply asking them to submit their card as part of the dispute resolution process the bank can use the 3DAS™ Card to re-calculate the 3DAS™ Signature and prove that that card was or was not used to sign the transaction. Obviously, if the card was stolen then the same issue exists as today unless PIN was also used. The cardholder must report this event allowing the Issuer to block future transactions.

[10] As an example, the algorithm to create the 3DAS™ Signature could be defined as follows. The right four bits of each byte of an eight byte Hash will act as a pointer to either an X or a Y value from the left or right plane. Each of the eight pointers of the Hash is numbered from 0 to 7, using the three rightmost bits from the pointer. The first bit of the pointer indicates if the X values or the Y values are taken (e.g. 0 means X and 1 means Y). Further, the first six values are selected from the left image and the last two from the right image. The resulting eight bytes is the 3DAS™ Signature.

The Unique 3DAS™ Transaction Serial Number

One of the properties of the 3DAS™ system is that each optic read of a 3DAS™ Marker is a random event. Therefore, converting this random characteristic into a digital value creates a unique serial number. This unique value can then be used to assure the bank that no one is attempting to defraud the system by signing multiple transactions with a single read of a 3DAS™ Card.

This random feature results from the fact that each sensor converts a visual image into a digital image based on a defined number of pixels. Each time a card is read the position of the marker is spatially unique, therefore which pixels are black or white will never be the same. In the case of the X and Y values Unicate has developed software specifically to eliminate the randomness of the output whereas in the case of the areas of each plane the randomness has been emphasised.

Combining an appropriate set of these values creates a unique serial number. This data element is then included in the message. Later the recipient checks this value against any previous message making sure there are no duplicates. ***This assures the Issuer this transaction was signed by a unique read of a 3DAS™ Marker***.

On-line Card and Data Authentication

The first enhance Unicate can offer to the typical credit card payment process is to develop a means of assuring in an on-line authorisation request that the card present is the one that the Issuing Bank had registered to that cardholder. To achieve this goal, a Hash (see page 24) and a 3DAS™ Signature (see page 25) of each transaction is created. This digital signature guarantees that the transaction details were not altered and ***the card was present***. Next, the 3DAS™ Reader creates the unique transaction serial number (see page 26). This unique value assures the Issuer that this transaction resulted from ***a unique read*** of the 3DAS™ Marker. As the ultimate warning, this unique transaction serial number can identify any duplicate transactions generated by fraudulent merchants or criminals.

The 3DAS™ Signature and the unique transaction serial number are transmitted within both the standard authorisation and clearing messages to the Issuer’s host. Once received, the Issuer can authenticate the card in the 3DAS™ Reader and issue an authorisation. In the case of the clearing message the Issuer is in a position to further validate the transaction before authorising payment.

In reviewing the specifications of the authorisation and clearing messages of Europay, MasterCard and Visa, Unicate identified two existing fields that can carry this information without modification to the intervening systems. The net result is an on-line solution that requires the inclusion of the 3DAS™ Reader in the terminal and two modules within the Issuers environment. The first module adds the 3DAS™ Key to their database. The second, to compare the 3DAS™ Table to the 3DAS™ Key when an authorisation or clearing transaction is received.

When considering typical business to business transactions, the key is to be assured that the person present is authorised to transact and that the content of the instructions are as entered. When considering other types of transactions simply substitute the appropriate transaction for the authorisation and clearing message, just described, and the organisation can achieve the exact same guarantee of card authenticity and transaction integrity.

Off-line Card, Data and PIN Authentication

Merging the 3DAS™ technology with the power of Public Key cryptography "PKi" Unicate has been able to develop a series of algorithms in the 3DAS™ Reader. These algorithms assure the seller, **off-line,** of the authenticity of a card, the integrity of data associated with the card and optionally that the rightful cardholder is present.

By creating a digital certificate, a card authentication method "a CAM" and optionally a cardholder verification method "a CVM" is available. To create the certificate the 3DAS™ Table along the data on the card and optionally the buyer PIN is Hashed together and signed with the secret component of a public key algorithm. This is then stored in track three of the magnetic stripe or within an inexpensive memory chip.

The certificate allows a public key algorithm within the 3DAS™ Reader to authenticate that the 3DAS™-enabled card is present, the data is unaltered and the consumer knowing the PIN is there with unparalleled accuracy and at an extremely reasonable per card cost[11]. When the card is present, the 3DAS™ Marker is read, the appropriate data is retrieved and optionally the cardholder enters their PIN. A standard algorithm within the 3DAS™ Reader is executed and it uses the appropriate public key to validate the certificate. The result, without the expense of on-line communications, the merchant has irrefutable proof of the authenticity of the card, the data and the cardholder.

3DAS™ Can Protect Today's Magnetic Stripe Payment Cards

While validating the ability to implement the 3DAS™ off-line PKi based solution, it became clear that many countries employed track three and many banks could not justify the expense of implementing even cheap chip cards.

This meant that Unicate had to create a new algorithm that could provide an off-line CAM that could use a certificate that was a maximum of seven digits[12] long.

Unicate created a solution that offered a level of protection (6.5 million to one) with certain associated risks[13]. The solution employs a randomising algorithm that can use a mere four digits to provide a CAM. In order to protect the algorithm, it is stored and executed within a smart card chip identical to those supporting EMV[14].

Furthermore, there is minimal financial risk to the banks. The clearing message contains the much more robust On-line CAM employing the 3DAS™ Signature. Therefore, no payment would occur unless the merchant can prove they are not in collusion with the cardholder who has broken the secure algorithm.

Like the on-line approach, the off-line approach does not require any modifications to any of the network and systems between the POS or ATM device and the Issuers host.

Cost-effective Implementation of an On-line PIN

Today's use of PIN demands encryption of the PIN inside a secure box at each point on a network where it passes to another legal entity. A typical debit card transaction could involve transiting nine security modules with five sets of security keys and associated procedures.

The Unicate team has designed a means of implementing on-line PIN without the need for expensive cryptographic hardware or associated technology inside the Internet or todays secure networks. To achieve the result Unicate acknowledges that the PIN is simply a piece of data known to two parties: the Issuing Bank and the cardholder.

[11] If one assumes that the cost of certificate generation is equal to that associated with employing smart cards as proposed in EMV, and that the 3DAS™ Reader is $30 more expensive than a simply chip reader and the 3DAS™ card is $.70 as compared to $1.50. Then if there are only 37 cards per terminal the 3DAS™ solution will be less expensive. The ratio in the United States today is 67 cards per terminal and in the UK 170 cards per terminal.

[12] Public key certificates are large numbers and require all the space in track one, two or three. This therefore limits the amount of space available to carry an off-line CAM to all of track three or the unused portion of both track one and track two. Based on the ISO 7811 and the MasterCard and Visa specification the maximum available is seven digits.

[13] Unicate acknowledges that there are certain risks associated with this approach. The criminal must acquire; the algorithm, 3DAS™ Markers, valid card data and never allow the fraudulent transactions to go on-line.

[14] When one considers the issue of protecting smart cards from attack one must think about the number of terminals in a 3DAS™ based solution that would have an EMV like smart card inside as compared to the number of cards that would require an EMV smart card. Sixty-seven cards to one terminal represent the ratio in the United States while 170 to 1 represents the ratio in the United Kingdom.

By requesting the cardholder to enter the PIN into the keypad, that optionally comes with the 3DAS™ Reader, the reader is in a position to produce a 3DAS™ Signature that hides the PIN from anyone but the cardholder and the secure computer system of the Issuer.

To provide cardholder verification, the Hash of the transaction and the PIN are merged together, using Modulo 16 arithmetic, by the 3DAS™ Reader. The resulting value is a set of pointers used to produce the 3DAS™ Signature.

Knowing the PIN the Issuer is able to replicate the calculation and create a 3DAS™ Signature from the 3DAS™ Key. The two 3DAS™ Signatures are compared and if they match the Issuer is confident that the **card is present, then that card is authentic** and the **cardholder entered the correct PIN**.

The 3DAS™ Tunnel

Data confidentiality is a critical issue when an organisation considers the sensitivity of data that it may wish to provide to its mobile work force over the Internet. Built into most browsers is either SSL or PGP: both tools to provide a measure of confidentiality.

Unicate began looking at the issue of confidentiality not from the perspective of the Internet but from the perspective of data carried by an individual in an inexpensive protected memory chip or a diskette. What Unicate is able to create, is a solution that enciphers the data by deriving a symmetric key from the 3DAS™ Table employing a password known to the individual authorised to read the information. To achieve the result the encrypted data is read, the 3DAS™ Marker is read and the authorised individual enters a password. Software in a 3DAS™ Reader designed to support this capability then decrypts the data and returns it to the authorised individual. When altered, the authorised individual resubmits the data to the specially configured 3DAS™ Reader and the information is re-encrypted.

When Unicate began to look at the Internet it developed a way of adapting this process to allow the server that has a registered copy of the 3DAS™ Key to send a challenge to the PC who would present this challenge to the 3DAS™ Reader. The 3DAS™ Reader would return a key 3DAS™ that could then be used as the symmetric session key by SSL or other line or data encryption software. **The mechanism makes it possible to tie the encryption of client specific data to the 3DAS™ Marker and eliminate any dependency on exchanging keys over the network or requiring keys to be stored within software in a PC**. 3DAS™ is capable of establishing data confidentiality.

The All in One Solutions

3DAS™ the Simplest Means of Identification

By exploiting the power of 3DAS™, Unicate has been able to create a solution that allows an organization to ***identify and authenticate*** both off-line and on-line its card bearing clients or employees. 3DAS™ can then be employed to create ***irrefutable proof*** that the card and cardholder were present and did execute the transaction.

Considering the growth of business-to-business eCommerce and the desire to be able to provide secured access to business partners and effect transactions in a secure and confidential way the 3DAS™ family of services is one of the most effective solutions available.

3DAS™ & E*MERGE® the Securest Means of Payment

When considering the world of consumer to business eCommerce the issues that must be addresses begin with the need for a means of authenticating both the buyer and the seller but it also requires a means of payment that does not demand the use of cryptography to protect the sensitive payment details from external elements. This protection of consumer and merchant details is the responsibility of the banks, the third party to any payment transaction.

3DAS™ affords the *Issuer* secured irrefutability by card authentication, cardholder "PIN" verification and unique transaction integrity. Simultaneously the 3DAS™ solution makes sure that **the *Acquirer* remains in complete control of the merchant relationship**, <u>**UNLIKE**</u> the EMV approach that transfers the decision to go on-line from the merchant's terminal to the smart card.

> The power of the off-line authentication method is that can be used to protect today's magnetic stripe cards with the robust on-line authentication method that will assure that only authentic transactions involve the transfer of money. Unicate has created a solution that allows the payments industry to bridge the period between today and when track three can be made available or the Issuers decide to add inexpensive (.15 to .20 US dollars) protected memory chip cards to create customer relationship cards. This approach is a cost effective solution to fraud and a profitable strategy focused on allowing the Issuers to segment their card portfolios and only offer relationship programs requiring additional memory capacity of a 3DAS™ secured inexpensive chip cards to their profitable clients.

The net result is that Unicate expanded the capabilities of the 3DAS™ Reader from simply analyzing the digital image to also perform the following on-line and off-line functions;

- **On-line account identification**
- **On-line card authentication**
- **Off-line card authentication**
- **On-line data authentication**
- **Off-line data authentication**
- **On-line PIN verification**
- **Off-line PIN verification**
- **Generation of a digital signature or transaction certificate**
- **Protection from replay with a unique transaction serial number**

3DAS™ and the Chip Card

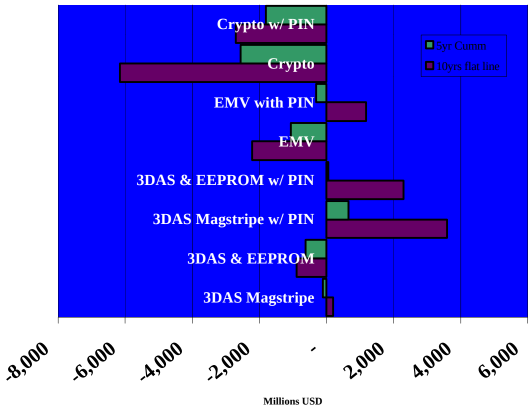
One of the most important results of the work Unicate has been doing to develop a solution to the banking industries payment card fraud problem, is the recognition that 3DAS™ offers an effective way of employing inexpensive (.15 to .20 US Dollar) protected memory chips. 3DAS™ is able to provide all the security benefits much more expensive smart cards claim to provide, for a fraction of the cost.

By using 3DAS™, public key cryptography and these inexpensive protected memory cards Issuers can quickly introduce profitable value-added programs to targeted segments of their cardholders. These applications are assured that only authorized entities can alter the data held within the cheap memory and more importantly can link that data to a unique 3DAS™ Marker and the bona-fide cardholder, thus protecting the Issuer from external fraud and consumer abuse.

By simply reading the 3DAS™ Marker and the data held within the memory and verifying that the data and the marker belong together and are unaltered provides all the protection loyalty schemes, electronic ticketing programs, stored value systems, identification mechanisms, logical access controls and consumer information profiles require.

The 3DAS™ Business Case

As part of the work to develop a business proposition for 3DAS™ as the cost effective solution to the problem of fraud on plastic payment cards Unicate developed a set of business cases that demonstrates that 3DAS™ is the most ***cost effective*** means of creating a ***Card Authentication Method*** as well as enabling a ***secure Cardholder Verification Method.*** The banking industry would no longer suffer losses resulting form counterfeit and lost & stolen fraud.



In this graph data acquired for USA Visa and MasterCard cards in issue, terminal population, transaction values, transactions volumes and fraud levels circa 1996, were put through a model similar to the one employed by MasterCard and Europay when they justified the migration to smart cards. Please note that this model grossly underestimated the implication of systems changes imposed by EMV and yet it still demonstrates that the 3DAS™ approach that does not have these same costs is significantly less expensive.

The results are clear. 3DAS™ is the only solution that makes economic sense.

The Migration to Customer Relationship Management

As banks work to improve shareholder value, the focus has shifted from product to customer profitability. With this focus on customer relationship management, banks now recognize that 10% of their clients generate 110%[15] of the profit. The realization that many clients are not profitable has lead segmentation of the custom and unique value propositions that serve the interests of thee profitable client while maximizing the bank's return on investment.

The 3DAS™ solution is *110%* compatible with this approach. The solution allows an Issuer to determine when it makes sense to spend money to expand the feature functionality it offers its clients. It does not force them to implement expensive smart card technology on a portfolio wide basis, as EMV seems to suggest, simply to achieve the tangible and intangible benefit of fraud reduction. Instead, it protects today's investment in magnetic stripe technology while leveraging the expanded memory capabilities afforded by inexpensive chip cards to those individuals in its portfolio that will generate a profitable return.

Furthermore, once a bank determines that it makes sense to add new value added programs to its cards the security provided to the basic credit or debit function is instantaneously increased. Migrating from off-line authentication of the magnetic stripe to off-line authentication using e^2PROM and PKi enhances security. The result, security increases from 6,500,000 to 1 to 1,000,000,000,000,000,000,000,000,000,000,000,000 to 1 and the risk is that someone can replicate a specific 3DAS™ Marker.[16]

The Unicate approach is an affordable approach to creating consumer value while also affording fraud protection without the enormous up front expense of EMV.

The 3DAS™ solution affords all of the requisite requirements of a robust security solution. It assures the *identification* and *authentication* of the token (the card) associated with the person performing a transaction. By providing a means *cost effective means* of *verification*, assuring that the person holding the card is the rightful owner, the solution is then complete. The 3DAS™ Reader finally provides a digital signature and a transaction identifier designed to guarantee that the transaction is both *unique* and *irrefutable*.

All of this security, without the need for complex cryptographic or expensive and disruptive changes to the existing EFTPOS networks and systems. Moreover, the one element never qualified in the EMV business case, *the implementation of an infrastructure to create the opportunity to create value added services*, is finally cost effectively assured.

[15] The Dr. Roberts, founder of one to one marketing, repeatedly quotes this finding in her books and speeches

[16] To replicate a marker one must find one in a random sample of 10^{36th} markers.

Appendix 2 - 3DAS™ Identification and Irrefutability

To serve the blossoming world of business-to-business eCommerce expanded by the Internet, Unicate offers a unique means of ***identification*** and assurance of ***irrefutability.*** The goal of the 3DAS™ mechanism is to assure that the corporations token was present, an authorized individual did agree and those are the instructions agreed. 3DAS™ is well suited to serve the needs of emerging Internet enabled applications such as

- Analytics
- Cash management
- Email
- Home banking
- Logistics management
- Money transfer
- One to one marketing
- Stockbrokerage
- Self service human resources
- Customer relationship management
- Order processing
- Enterprise resource management
- Supply chain management
- Strategic enterprise management
- Corporate knowledge management
- Sales force automation

All of these applications have one thing in common. They access confidential corporate information or allow the execution of transactions that can have mission critical consequences. Therefore, before an organization can consider enabling access via the Internet it is essential that there is adequate assurance that only authorized individuals have access and that any instruction given is prepared and authorized by the individual.

This being said security comes at a price. Unicate believes that the cost of security must commensurate with the value of the asset in question. More importantly, security should not subject the user to unnecessarily cumbersome procedures or the need to remember various account numbers and passwords.

The design of the Unicate solution allows clients, employees and partners, to use standard Internet browsers to connect through any insecure network to confidential and mission critical applications and knowledge. For the user, the solution is easy to use and only requires them to enter their first name, insert their 3DAS™-enabled Card and if security dictates, enter their PIN. The user no longer is required to remember an account number and password associated with each system they access.

Behind a firewall are the Internet enabled corporate applications employed to provide the appropriate services to client, partner or employee “users”.

The 3DAS™ solution involves installing a 3DAS™ Identification Server as the secure gateway between the public network and the corporations secure private network. The goal, to provide a transparent interface allowing any Internet enabled applications to be accessed from anywhere without requiring any modification. By eliminating the need to modify operational systems, assures the corporation's investment in training and application development. The 3DAS™ solutions cost effectively assure that these same applications can exploit the ability of the insecure Internet to reach an ever larger population of mobile workers, strategic partnerships and self services business processes.

The 3DAS™ Environment

To achieve these goals the following is required:

- A 3DAS™ Identification Server located in-between the public networks and the Intranet of organization.
- A 3DAS™ Reader with keypad connected to the user's computer and the 3DAS™ Plug-in connected to the standard Internet browser.
- A 3DAS™ Marker inside a plastic card issued to the user.
- A secure tunnel created using SSL or the stronger 3DAS™ Tunnel.

The 3DAS™ Identification Architecture

1. A user connects to the Internet and logs on to the corporations web site.
2. The 3DAS™ Identity Server determines that a 3DAS™ reader is present and formats the log-on screen.
3. The user is requested to insert their 3DAS™-enabled Card.
4. The user enters their first name and a 3DAS™ FastKey is generated.
5. A log on message is prepared and sent to the server.
6. The user is identified and authenticated
7. A welcome screen is prepared and applications he has access to are presented
8. The user selects what applications they wish to access
9. Eventually a transaction entry screen "Form" is presented to the user
10. The user fills in the form
11. Upon completion of the form a 3DAS™ Signature is created
12. The transaction is transmitted to the server
13. The Server validates the 3DAS™ Signature
14. The form is returned to the originating application for processing.
15. The user continues to work.

Leveraging the tools described in Appendix 1 - 3DAS™ The Ultimate in Security ***Unicate can offer irrefutable authenticity of identify, irrefutable transaction integrity, user centric confidentiality, ease of use and mobility.***

3DAS™ Reader & 3DAS™ Plug-in

The 3DAS™ Reader is a secure device designed to afford protection over all of its functions and to protect the PIN and the generation of the 3DAS™ Signatures.

The 3DAS™ Reader and its associated 3DAS™ Plug-in has been designed as a plug and play standalone device that is either attached to the UTP port or PCMCIA slot. Where required, the 3DAS™ Reader can also be inserted into an empty slot of a 3½-inch diskette drive. This unit can be provided with an integrated chip card reader and when required fitted with a secure PIN pad.

Each 3DAS™ Reader is capable of allowing any client possessing a 3DAS™ Card to access the organization's services. This unique capability offers mobility to organization's clients.

The installation is easy, the user plugs the 3DAS™ Reader in to the USB port, the Plug & Play routine identifies the reader and requests the insertion of the install CD. The rest of the installation process is automatic. The 3DAS™ Plug-in is loaded and communication to the 3DAS™ Reader and Internet is tested.

The 3DAS™ Reader and Plug-in are now ready. Whenever the Browser is operational, the Plug-in awaits a request from a 3DAS™ Identity Server to do something.

3DAS™ Identification Server – ID Server

The 3DAS™ ID Server contains all of the security, logic and controls necessary to manage the organization's 3DAS™ Cards, client authentication, 3DAS™ Readers and the controls necessary to assure irrefutability.

The 3DAS™ ID Server offers a transparent window to the organization's applications. Only using the user's first name[17] and a four byte 3DAS™ FastKey, user's identity is protected from eavesdroppers while it transits through a public network.

[17] In the event that the user does not wish their name, it is possible to use any value the user wishes.

Recognizing that components of the total environment are constantly evolving, the overall architecture of the 3DAS™ solution will have the ability to upgrade the 3DAS™ Plug-in installed with the customers PC or software housed within the 3DAS™ Reader. These functions are integral to the operation of the 3DAS™ ID Server.

The 3DAS™ ID Server supports a secure database the “3DAS™ ID Profile” that links the 3DAS™ Card to the user. In this profile the linkage between the card and the account numbers and passwords for those applications, the user has access to, necessary to access the existing legacy applications.

The 3DAS™ ID Server will transparently add data and instructions used to communicate with the 3DAS™ Plug-in and 3DAS™ Reader. The secure server will then transmit these modified HTML pages to the user's browser. It will await response from the browser that will contain information for the application and from the 3DAS™ Plug-in. The Server will extract those elements sent from the plug-in and act accordingly. Assuming all is well, it will pass the application specific information to the appropriate application.

Unicate’s approach allows the organization to augment security without having to upgrade or modify any of their existing legacy systems.

As an additional benefit the 3DAS™ ID Server can be used to implement a consistent look and feel to all of the organization’s applications again without impacting the existing legacy applications. The 3DAS™ solution is mobile, easy to use, secure and capable of assuring consistency of brand image.

The 3DAS™ ID Profile

For each user the 3DAS™ ID Server maintains a 3DAS™ ID Profile. This profile contains the 3DAS™ Key, the first name & 3DAS™ FastKey, the proper name and other appropriate reference information. It then contains a series of associated records that link the 3DAS™ Card to each of the applications this user is granted access to. These records maintain any logon information or other static data needed to complete the log-on form. Where corporate applications require periodic change of password, specific modules capable of executing password change will perform this function independent of the user.

When preparing the User’s 3DAS™ Card their database record is created. The first action is to enter the 3DAS™ Key and other user specific reference information such as the first name. During user initialization, the account number and password information of each application, the user currently has access to, is loaded into the database.

The database requires routinely maintenance. As new applications are made available or the user is no longer allowed access then the updates are made. From an administrative perspective, by removing the user for the 3DAS™ ID Profile all access can be immediately restricted.

The User at Work

From any location, with a 3DAS™ Reader the user is assured of secure and irrefutable access to the partner, employer or vendor's systems. All they need to do is enter the URL of the corporation. The corporate server responds by sending it home page and including a message designed to determine if a 3DAS™ Reader is present. Assuming the 3DAS™ Plug-in positively responded the 3DAS™ ID Server is passed control and prepares a log-on screen.

When the browser receives the login screen, it passes control to the 3DAS™ plug-in. Through a 3DAS™ plug-in window the plug-in requests the user to enter their first name and optionally a PIN. Using information contained in the log-on message, the first name, date and the time the plug-in prepares a Hash. The PIN and the Hash are sent to the 3DAS™ Reader who responds by reading the 3DAS™ Card and returning a 3DAS™ Signature that includes the PIN. This information is encapsulated in a particular format and returned to the server.

The 3DAS™ ID Server receives the message and uses the first name & 3DAS™ FastKey as the index to the user’s 3DAS™ ID Profile. Employing the same mathematical function used to create the 3DAS™ Signature, the secure 3DAS™ ID Server authenticates that the 3DAS™ Card is registered and that the user knows the PIN.

Knowing that an authentic user with a registered and active 3DAS™ Card is present, the 3DAS™ ID Server employs the 3DAS™ ID Profile to produce an application selection page. By simply clicking on the application, the user selects application they wish to access. The 3DAS™ ID Server prepares the necessary login message and connects to the application on behalf of the user. The application then formats the queries, execution forms and information displays as it does today. Upon receipt, the ID Server imposes the corporate look and feel to the page and sends it to the user's browser.

In the event the screen is requesting input of information that is of a transactional nature the 3DAS™ ID Server will also include a request to the 3DAS™ Plug-in to arrange to have the 3DAS™ Card sign the transaction.

If the application is simply displaying data the 3DAS™ Plug-in is passive. In the event that the 3DAS™ ID Server requested that the user's response be signed, it awaits completion by the user and, just before transmission captures the data, prepares a Hash and requests the 3DAS™ Reader to read the 3DAS™ Card and sign the transaction.

The 3DAS™ Reader produces the 3DAS™ Signature and returns the 3DAS™ Signature and the 3DAS™ Unique Transaction Serial Number to the 3DAS™ plug-in. The 3DAS™ Plug-in appends this information to the message and sends it to the 3DAS™ ID Server. The ID Server is now in a position to validate the integrity of the message, the authenticity of the user and produce a log that can be used to assure irrefutability in the event of a dispute.

If the message is authentic and irrefutable, the 3DAS™ specific information is stripped off and the application receives the user input information as it originally request.

The application can now execute in the knowledge that the transaction is irrefutable, the source of the instructions are confidential, the user is authentic and the identity and the content of the message was sent unaltered by that particular user.

Data Confidentiality

Many services that corporations want to make available require that confidential information be transmitted to the user over the insecure Internet. For most, this is an unacceptable proposition. Several mechanisms are available to solve this problem. Unicate recommend is that SSL be used, as the default option, given that it is already available in the browsers, is recognized by most users and offers a reasonable level of security. In the event that the corporation wishes to introduce an enhanced level of security then both the 3DAS™ Reader and the 3DAS™ ID Server can be configured to support this much more robust means of assuring data confidentiality.

By employing 3DAS™, the user will have secure access to all corporate services. The corporation will be safe in knowing that they have irrefutable proof of identity and of the instructions input by that particular user. Furthermore, the solution is mobile and can operate from any 3DAS™ enabled mobile location capable of connecting to the Internet.

Appendix 3 - The Architecture of E*MERGE®

The essence of the design involves the development of a set of interconnected Payment Servers that securely manage consumer and merchant trust and the payment details necessary to interface with the existing bank card payment networks i.e. EFTPOS networks.

Built into this secure environment are all the firewalls and appropriate interfaces necessary to securely interface the Internet with the card accepting side of appropriate EFTPOS networks. Inherent in the design is the isolation of where confidential merchant and consumer data resides. This thus established the trust and security that is fundamental to the relationships the banks have had and desire to retain between their end users - the consumers and merchants.

The design assumption is that a trusted party would operate these secure Payment Servers. Either this trusted third party operated on behalf of a group of banks or the Issuing and Acquiring Banks may own and operate these trusted Payment Servers.

In order to assure the level of authenticity demanded by the consumers, merchants and banks the following hardware and software is required.

The Buyer Requires

- A 3DAS™ Payment Card
- An inexpensive Plug & Play 3DAS™ Reader with a secure PIN pad
- A CD with E*MERGE® Browser Plug-in and a set of device drivers

The installation is simple plug the 3DAS™ Reader in and let the Plug & Play routine request the insertion of the install CD. The rest is automatic. The E*MERGE® Browser Plug-in is loaded and communication to the 3DAS™ Reader and Internet is tested.

When the buyer receives the 3DAS™ Card and starts the new card program, the E*MERGE® Browser Plug-in will automatically connect to the Payment Server of the card Issuer and the consumer's payment profile is loaded. The buyer is ready to start shopping, secured by E*MERGE®.

The Seller Requires

In order to avail themselves of the security afforded by the E*MERGE® service the seller will need to integrate into their Web hosting environment.

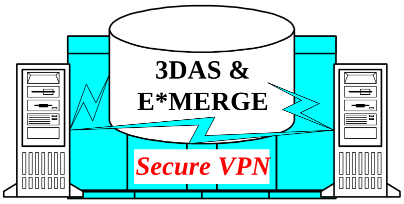
- A number of 3DAS™ Readers18.
- The software required that drives the 3DAS™ Readers.
- The E*MERGE® Merchant OLTP Control Software.19
- A set of documents defining the 3DAS™ and E*MERGE® APIs
- A guide to assuring interoperability both with
- The consumer E*MERGE® Browser Plug-in
- The Payment Server interfacing to the EFTPOS networks on the seller’s behalf
- A 3DAS™ Merchant card for each 3DAS™ Reader

[18] The number is a function of the throughput of a 3DAS™ Reader at 150 milliseconds per read and the number of simultaneous transactions that require a 3DAS™ Signature.

[19] This module replaces any payment functionality that may already exist. Built into this software will be the logic to conduct an E*MERGE® transaction or decide to employ a standard SSL form to allow input of credit card details.

Once these have been integrated into the seller web server environment, the seller has performed the interoperability test, the payment methods the sellers will accept have been set-up and the seller has activated the 3DAS™ Cards through the one time registration process, the seller is live and ready to trade secure in E*MERGE®.

The Payment Server



5 Validate
Merchant & Consumer

The payment server is the trusted party that offers a range of services to its users - the Issuing Banks, Acquiring Banks, consumers and merchants. Inherent in the E*MERGE® design is the user profile. It is the responsibility of the operator of the payment server to securely manage the user profile that contains the confidential details necessary to prepare valid instructions based on the prevailing EFTPOS interface specifications.

The payment server will interface to the existing EFTPOS networks used to execute electronic payments for the assortment of payment methods that the buyers, sellers and banks will wish to employ over the Internet. The specifications and many cases off the shelf software modules for the appropriate electronic interchange protocols *already exist* and simply have to be integrated into the payment servers. An example is the UK Implementation of the MasterCard and Visa ISO 8583 specification defined by APACS[20].

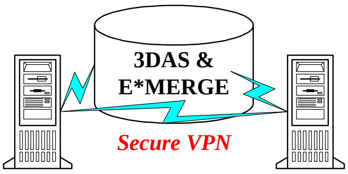
For purposes of simplicity and acknowledging that, there must be a competitive environment for the provision of this trusted service, also acknowledging that the Issuers and Acquires may wish to perform the function of the payment server, E*MERGE® segments the payment server's into two components:

- The first component is associated with the trust relationship between the banks and the buyers, consumers or cardholders.
- The second component is associated with the trust relationship between the banks and the sellers or "merchants".

Any number of trusted parties can exist and it is business and technically possible for a party to operate both functions.

Secure E*MERGE® VPN

To interconnect the trusted merchant and consumer payment servers a secure "VPN" Virtual Private Network exists to assure the confidentiality of data transmitted between the trusted payment servers.



In the specification of the Secure E*MERGE® VPN, a set of transactions[21] are defined. This network allows the independent seller or buyer payment servers to communicate with the payment server associated with the counter-party to the purchase-taking place over the Internet. These messages define how either party will communicate in order to complete the transaction and to assure the authenticity of the buyer, the seller and the transaction.

[20] APACS is the Association of UK clearing banks.

[21] In the schematics included later in this document, these transactions are in lower case roman numerals.

The E*MERGE® Profile is simple in structure:

- ✓ Each registered user - seller or buyer - has a random pseudonym assigned, which identifies the user on the Internet
- ✓ Each payment method the buyer is willing to use has a random pseudonym assigned which identifies the payment method over the Internet.
- ✓ Each payment method the seller is willing to use has a random pseudonym assigned which identifies the payment method over the Internet.
- ✓ The 3DAS™ Key is secure inside the payment server database along with the confidential information necessary to populate the EFTPOS message formats.

Four E*MERGE Profiles exist.

Two matching consumer payment profiles one on the payment server the other in the E*MERGE Browser Plug-in.

Two matching merchant payment profiles one on the payment server the other in the E*MERGE® Merchant OLTP Control Software.

The E*MERGE® Consumer Payment Server (EMERGE®CP Server)

The CP server is responsible for assuring the seller that the buyer can be trusted (see 5) Validate Seller and Buyer) and that the Issuing Bank can process a legitimate payment transaction.

The operator of the CP server will build relationships with the Issuers. They will develop and operate a mechanism to make sure that the information necessary to insert the buyer’s details into the payment instructions is accurate and up to date. It will provide appropriate support to the customer service center that will be in contact with buyer during the installation and registration process.

During the transaction process it will assure buyer authenticity, provide the necessary payment details, monitor the progress of the payment authorization and provide feedback to the buyer through the E*MERGE® Browser Plug-in.

The payment server maintains electronic logs that prove that documents buyer’s action. In the event of a dispute the Issuer is assured that the customer was present, that a valid copy of the invoice was provided, that the seller was authentic and that the buyer’s card was present at the time of the transaction. To perform this function the bank simply asks the buyer to provide the invoice as originally received and compares this to the seller’s signature of the invoice generated at the time of the transaction and approved with a signature by the buyer's card. Assuming the seller has fulfilled the terms of the invoice then the buyer's responsibility to payment is irrefutable. In the event that the card was lost and not reported, then the Issuer, like today will have agreed to specific terms with cardholder, which define the cardholder liabilities.

It will also be responsible for monitoring buyers using E*MERGE® to assure overall system integrity.

The E*MERGE® Merchant Payment Server (EMERGE®MP Server)

Is responsible for assuring the buyer that the seller can be trusted (see 5) Validate Seller and Buyer). The MP server also handles communications with the EFTPOS networks. To support these networks the operator of the MP server must build and support the requisite interfaces to the existing EFTPOS systems necessary to support the payment methods that it wants to offer to its clients the merchants. The role of these interfaces is to simulate, on behalf of the seller, a point of sale terminal connecting to the Acquiring Bank authorization and clearing system.

The operator of the MP server will build relationships with the Acquirer’s operations and systems people to develop and operate a mechanism that will be used to make sure the information necessary to insert the seller’s details into the payment instructions is accurate and up to date. It also has responsibility to develop and manage the technical interface to the appropriate EFTPOS networks used to process authorization and payment instructions.

The operator will work with sellers to install the E*MERGE® Merchant OLTP software, 3DAS™ Readers and the 3DAS™ Cards required to meet peak performance. As appropriate it may provide proprietary interfaces to the sellers' management and logistical systems.

During the transaction process, the payment server will assure seller authenticity, provide the necessary MP details, monitor the progress of the payment authorization and provide feedback to the seller of approval or rejection. Given that many payment systems work on the concept of payment on delivery it must also support the ability to subsequently receive a confirmation of delivery, from the seller, and submit the appropriate EFTPOS clearing message to initiate payment.

Electronic logs shall exist that can be used to prove claims of seller irrefutability. In the event of a dispute the Acquirer is assured that the customer was present, that a valid copy of the invoice was provided, that the seller was authentic and that the buyer's card was present at the time of the transaction. To perform this function the bank simply asks the seller to provide the invoice as originally sent and compares this to the seller's signature of the invoice generated at the time of the transaction and approved with a verifiable signature by the buyer's card. Assuming the seller has fulfilled the terms of the invoice, payment is guaranteed.

Payment Server Authenticity

Both the seller and the buyer must be confident that the E*MERGE® CP or MP Server that they are communicating with is authentic. The simplest way to achieve this essential level of trust is to require each payment server to create a secret key and then to derive a public key using an E*MERGE® specified public key algorithm

E*MERGE® employs the most basic form of Public Key cryptography and therefore does not requires a certification authority or any registration authorities.

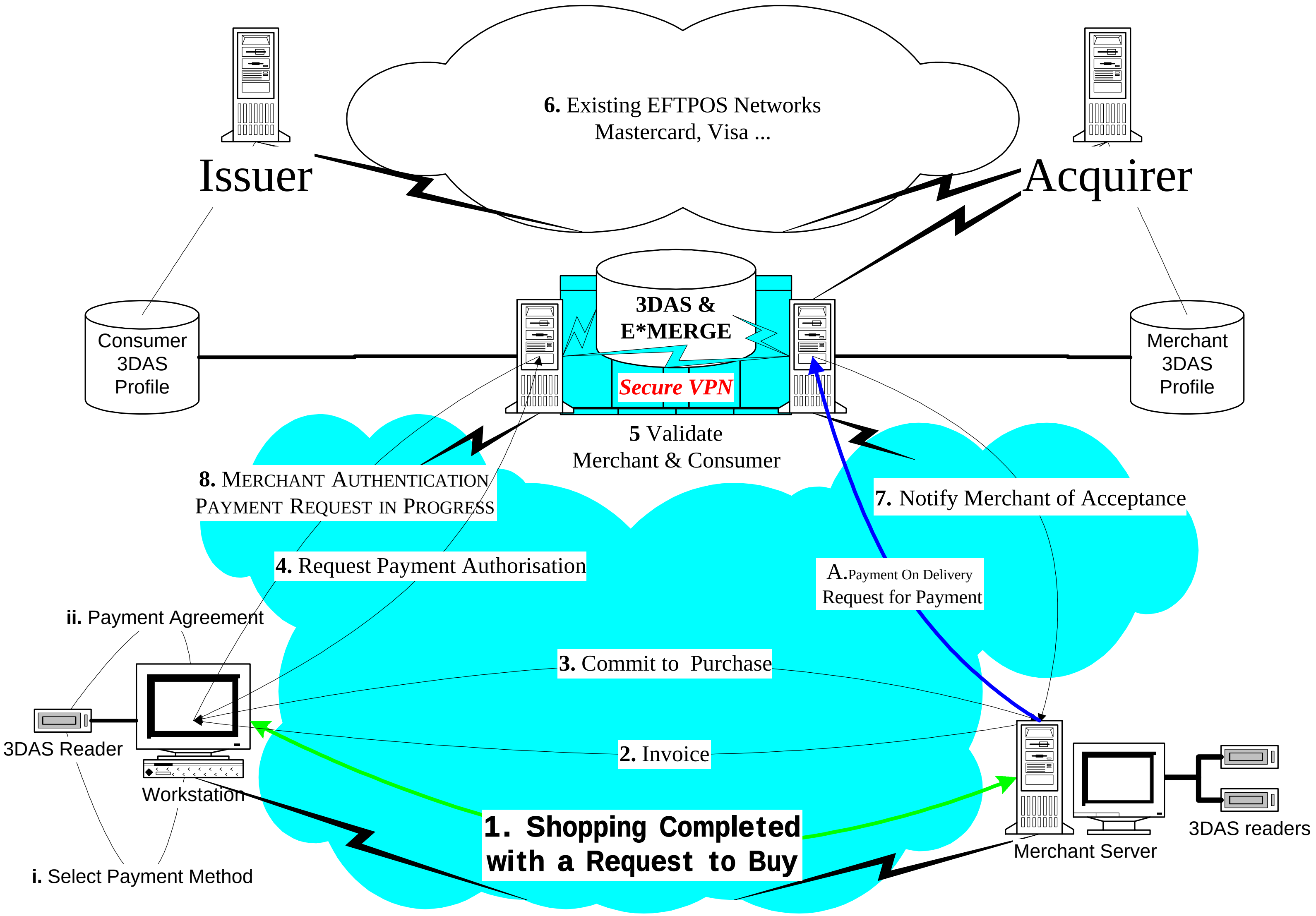
When the buyer or seller initialises the payment profile, the public key of the trusted payment server is automatically loaded. The matching public key held by the buyer or seller therefore can validate each message signed with the payment server's unique secret key.

3DAS.ORG

Unicate has insisted in developing a solution that is easy to use and mobile. To achieve this result its effort to assure an easy to use mobility option required the creation of an easy to form URL. As will be described in Appendix 4 - Consumer Mobility - The E*MERGE® Difference **by** the E*MERGE® Browser Plug-in simply needs to know the name of the cardholders issuer to make a connection to www.issuerID.3DAS.org. Employing the power of the Internet addressing scheme makes this simply to do and only requires the management of a DNS server responsible for the sub addresses of the domain 3DAS.org. The task simply to provide the central domain server capable of populating the Internet with the IP addresses of the appropriate E*MERGE® CP Servers.

Further recognizing that parties do cease to operate or that the addresses of servers connected to the Secure VPN may change a single master directory of currently authorized payment servers will need to exist. The same entity responsible for managing 3DAS.org can manage this secure directory.

The Transaction Flow (Flow Chart) of E*MERGE®


6. Existing EFTPOS Networks
Mastercard, Visa ...
Issuer
Acquirer
Consumer
3DAS
Profile
3DAS &
E*MERGE
Secure VPN
Merchant
3DAS
Profile
5 Validate
Merchant & Consumer
8. Merchant Authentication
Payment Request in Progress
7. Notify Merchant of Acceptance
4. Request Payment Authorisation
A.Payment On Delivery
Request for Payment
ii. Payment Agreement
3. Commit to Purchase
3DAS Reader
2. Invoice
Workstation
1. Shopping Completed
with a Request to Buy
3DAS readers
Merchant Server
i. Select Payment Method

E*MERGE® Data Elements Relationship between Profiles, Logs, Hashes and Messages

E*MERGE Data Elements in the Profiles, Logs, Hash and Messages		Merchant Payment		Consumer Payment		Hash M	2	Hash C	3	4	5	6	7
		Profile	Log	Profile	Log		Invoice		Commit	Verify	Enrich	EFTPOS	Approval
Merchant Identification	Merchant Pseudo	1	1		1	1	1	1		1	1		
	Merchant Card Pseudo	1	1		1	1	1	1		1	1		
Payment Identification	Merchant Payment Pseudo	1 to n				1 to n	1 to n						
	Payment Server Address	1 to n				1 to n	1 to n						
	Payment Method Type (MasterCard, Visa, Amex, Discover, Check)	1 to n				1 to n	1 to n						
Consumer Identification	Consumer Pseudo		1	1	1			1	1	1	1		
Payment Identification	Consumer Payment Pseudo			1 to n									
	Payment Server Address			1 to n									
	Payment Method Type (MasterCard, Visa, Amex, Discover, Check)			1 to n									
Transaction Details	Invoice		1		1	1	1						
	Date		1		1	1	1	1		1	1	1	1
	Time		1		1	1	1	1		1	1	1	1
	Amount		1		1	1	1	1	1	1	1	1	1
	Currency		1		1	1	1	1	1	1	1	1	1
	Reference number		1		1	1	1	1	1	1	1		1
Merchant Validation	Hash M		1		1	====>	1	1		1	1		
	TCM		1		1		1	1		1	1		
	3DAS Sign M		1		1		1	1		1	1		
Payment method To Use	Merchant Payment Pseudo		1		1			1	1	1	1		
	Payment Server Address		1		1			1	1	1	1		
	Consumer Payment Pseudo		1		1			1	1	1	1		
	Payment Server Address		1		1			1	1	1	1		
	Payment Method Type		1		1			1	1	1	1		
Consumer Validation	Hash C		1		1			====>	1	1	1		
	TCC		1		1				1	1	1		
	3DAS Sign C		1		1				1	1	1	1	
8583 Data	Consumer Details										1	1	
	Merchant Details										1	1	1
	Approval Code		1		1							1	1

The 3DAS™ E*MERGE® Transaction Flow (narrative)

1) Shopping Completed with a Request to Buy

The buyer has located a shop on the web and goes shopping.

During this shopping experience the sellers will want to find out if they will receive **card present** or **card not present** terms on the sale. In E*MERGE® this means that the seller wants to know if a 3DAS™ Reader is attached to the buyer's PC.

Sometime during the buyer's shopping process the merchant OLTP server will send a message to the buyer's browser asking if it can talk to an E*MERGE® Browser Plug-in.

If the E*MERGE® Browser Plug-in does not respond then the merchant web server can plan to use a payment request form protected by SSL. If this were case then transaction are **card not present** or as a Mail Order Telephone Order transaction.

If the E*MERGE® Browser Plug-in does respond, then the seller can assume there is a high probability that it will be a **card present** transaction.

In the case the goods will be delivered to a buyer the seller could request specified address information contained in another plug-in performing services like the Microsoft Wallet plans to offer[22]. The E*MERGE® assumption is that this information forms part of the seller's final terms and conditions.

At the end of the shopping experience, the buyer will agree to purchase a set of goods under a set of the terms & conditions and for a specific price.

2) Seller's Invoice

The seller encapsulates all of this information into a digital format that can be displayed by the buyer's browser and processed by the E*MERGE® Browser Plug-in. For the purpose of this write up, the plug-in was located during the shopping experience. This message contains:

- ✓ The invoice
- ✓ A unique reference number
- ✓ A random pseudonym used to identify the seller
- ✓ An random pseudonym used to identify the 3DAS™ Merchant Card
- ✓ The payment options the seller accepts (AMEX, electronic check, Electron, Maestro, MasterCard, Visa)
- ✓ A random Pseudonym used to identify each payment method
- ✓ The Hash of the invoice and other elements of the message
- ✓ The seller's 3DAS™ Signature
- ✓ The unique 3DAS™ serial number

[22] A more appropriate solution is to integrate the functionality of these wallets into the 3DAS™ Browser Plug-in. At the time of the preparation of this document dialogues with the key suppliers of wallet software have not taken place.

3) Buyer Commits to Purchase

Assuming the buyer is happy with the deal, the buyer should be ready to commit to pay for the goods or services offered. The E*MERGE® Browser Plug-in will request the buyer to insert a 3DAS™ Card. Using the results of this first read of the 3DAS™ Card the E*MERGE® Browser Plug-in will identify which payment profile the buyer wants to use. (See **4) Initialize and Authenticate Buyer** and Card on page 61 for further details).

In the event that the buyer does not insert a card, the E*MERGE® Browser Plug-in sends an error message back to the merchant web server. The seller then defaults to requesting payment through an SSL script, assuming they wish to take the risk of a card not present transaction. It would also be recommended that they display a warning and an E*MERGE® advertisement.

The E*MERGE® Browser Plug-in compares the consumer payment profile, associated with that card, to the list of payment methods found in message **2) Seller's Invoice**. In the E*MERGE® Browser Plug-in payment window the payment methods that both parties employ are displayed with easy to recognize icons. The screen prompt requests the buyer to choose a payment method or decline the purchase. The buyer clicks on a payment method and the E*MERGE® Browser Plug-in calculates a Hash and requests the 3DAS™ Reader to create a 3DAS™ Signature.

In the event that the buyer wishes to change the terms of the invoice, then the E*MERGE® Browser Plug-in assumes the seller will resubmit the invoice and this request to pay session is closed.

If appropriate, the 3DAS™ Reader can include a PIN Pad to allow the PIN as a second security mechanism. By including this ***inexpensive, tamper evident keypad*** allows the bank's customers to **use debit cards as a secure payment product on the Internet**. Simultaneously the E*EMERGE allows banks the ability to introduce PIN on credit cards, eliminating fraud loses attributed to lost and stolen cards.

If this is the case, the plug-in will instruct the buyer to enter the PIN into the appropriate PIN Pad before the creation of the 3DAS™ Signature. For a complete description of the process please see the description of a Cost-effective Implementation of an On-line PIN on page 27.

At the completion of this session, the merchant web server receives a message from the plug-in with the buyer's commitment to pay. This message contains selected information from the merchant invoice message and adds the following

- ✓ The address of the CP server
- ✓ A random pseudonym used to identify the buyer
- ✓ The payment method selected
- ✓ The random pseudonym of the payment method selected
- ✓ The Hash of elements of this message
- ✓ The buyer's 3DAS™ Signature
- ✓ The unique 3DAS™ serial number

4) Request Payment Authorization

The E*MERGE® Browser Plug-in sends a message to the address of the CP server, stored during the registration process described on page 60. This message contains all the information necessary to allow the payment servers to authenticate both the buyer and seller and submit a request for payment authorization through the existing EFTPOS networks.

Since both the seller’s and the buyer’s identities are masked by a set of random pseudonyms known only to the payment servers and the respective E*MERGE® Browser Plug-in, their identities are secure over the public Internet.

The only other information that must pass across the Internet to the banks (payment servers) is:

- ✓ The amount
- ✓ A code indicating the type of merchandise, as specified by the payment system
- ✓ A time stamp
- ✓ The 3DAS™ Signatures that confirm authenticity
- ✓ The address of the MP server
- ✓ A set of random numbers that are meaningless to outside parties

The E*MERGE® Browser Plug-in creates an electronic log of the event and statuses the log record as pending the results of the request for payment.

If the buyer wishes to await further information the status of the request for payment is monitored and displayed in the plug-in's window.

5) Validate Seller and Buyer

Employing the random pseudonyms sent in the message by the E*MERGE® Browser Plug-in the E*MERGE® CP Server identifies the buyer and the selected means of payment from the E*MERGE® Consumer Profile. The authenticity of the buyer is validated as described in the section on the **3DAS™ Signature** on page 25 to 3DAS™ Key held in the E*MERGE® Consumer Profile. If appropriate, the buyer’s PIN is verified using the logic described in the section on a Cost-effective Implementation of an On-line PIN on page 27

The data, held in the secure 3DAS™ Consumer Profile, needed to fill in the appropriate EFTPOS message, i.e. the ISO 8583, MT or domestic electronic clearing houses formats, is inserted and sent over the Secure VPN to the E*MERGE® MP Server.

The E*MERGE® MP Server employs the random pseudonyms of the seller, passed from by the E*MERGE® Browser Plug-in, to identify the seller and its selected means of payment. The E*MERGE® MP Server validates the authenticity of the seller using the 3DAS™ Key held in the E*MERGE® Merchant Profile. Then using the content of the E*MERGE® Merchant Profile the necessary details to complete the requisite EFTPOS message are inserted into the EFTPOS message already containing the buyer's details.

In the event either party does not pass the 3DAS™ authentication process, both the buyer and the seller receive error messages.

- ➢ In the case of the seller, this is essential to further processing of the order. If the buyer is not authentic, the seller will want to halt the delivery of goods or services.
- ➢ If the buyer does not know that there was an error, no deduction of funds from their account will occur and the seller will lose a sale.
- ➢ Obviously appropriate fraud alerts will be created and further investigation can begin.

Assuming both parties are authentic, all of the necessary items required to assure irrefutability from this point forward are logged by the payment servers and held for as long as E*MERGE® and the EFTPOS networks dictate.

6) Existing EFTPOS Networks, Domestic, MasterCard, SWIFT … VISA

Knowing that the seller is authentic, the buyer is authentic and acknowledging the capability of assuring irrefutability, the merchant OLTP server starts the EFTPOS payment process as defined by the authorities responsible for its management.

All the information required by the EFTPOS network to prove that a card was present becomes part of an appropriate EFTPOS record. The E*MERGE® MP Server sends the record to the appropriate EFTPOS network and a response is awaited. In the case of a credit card, a response will come back within a matter of seconds, approved or declined. The results are electronically logged.

Based on the terms agreed with the buyer and seller notification of the final status of the payment is returned to the seller and/or buyer on-line or via an off-line process. If the worst was to happen and the bank denied the request for payment, then MP Server must informs the seller and the CP Server shall informs and the buyer. The CP and the MP notify their client be using the same logic, described below, to notify the buyer and seller of the decline.

7) Notify Seller of Acceptance

In the case of the seller, a confirmation is important given that the seller will not wish to ship until confirmation that the bank has authorized payment. In the case of real-time delivery of goods, this would want to be an instant response. In the case of physical goods, this may be a file sent every hour, formatted based on the seller's requirements. For example, the seller may wish it formatted for direct input into the organization’s logistics system.

8) Notify Buyer of Seller Authentication & Payment Approval

In most cases, the buyer assumes that everything is ok after they have agreed to pay.

In some cases, a buyer may be concerned that the bank will not approve. Therefore they will wish to remain connected to the status screen of the E*MERGE® Browser Plug-in started at step 4. In the event of a decline, the buyer would then be in a position to propose another payment method.

This willingness to stay connected will also apply to soft goods delivery, which will require a download, an electronic process, the E*MERGE® Browser Plug-in could be used to facilitate.

This background connection to the E*MERGE® CP Server also affords the server the ability to send any enhancements or updates.

A) Request for Payment on Delivery

Acknowledging that the terms of payment for goods bought and sold over the Internet is a subject of much regulatory discussion, our design approach is to assume that present conditions covering mail order telephone order transactions will prevail.

When the seller rightfully believes that they have delivered the goods to the rightful buyer then they can either submit through the Internet or through a proprietary interface a request for payment message.

The MP server will authenticate the seller and prepare the necessary EFTPOS message using information in the transaction log and further information included in the request for payment message.

This clearing message will be submitted to the appropriate EFTPOS interface. Settlement will occur, as today, employing existing settlement procedures.

• Physical and Soft Goods Delivery

Independent of the payment process the seller may wish to send the buyer an e-mail or surface mail to provide details associated with delivery of goods.

Working on the assumption that the merchant is delivering soft goods then E*MERGE® Browser Plug-in, on acknowledgement of merchant authentication and payment approval, can organize the connection to the appropriate merchant download site. When this message and the "notify merchant of acceptance" match, then the download site can authorize the transfer.

Assuming the E*MERGE® Browser Plug-in successfully connects to the download site, all is well. If not, the seller can use other means to deliver the soft goods to the buyer such as sending the hyperlink of the download site in e-mail.

The Customer Interface

To describe what is taking place at the consumer site it is important to understand how 3DAS™ and E*MERGE® are integrated into the consumer’s Internet access device. This device could be a personal computer a mobile phone, a set top box, a digital TV or a personal digital assistant. In the case of many of these devices, the 3DAS™ Reader would be integrated during the manufacturing process. IN THE CASE OF A PC, it is probable that the installation would occur after the initial purchase; as would be the case will the 100s of millions of PCs now in operation.

This specification will dwell on this PC environment.

In simple terms, the buyer is provided with or purchases a 3DAS™ Reader, connects the 3DAS™ Reader to the PC and loads the E*MERGE® Browser Plug-in. The 3DAS™ embedded card is received and the plug-in is registered with E*MERGE® CP Server.

i) Select Payment Method

Picking up from the point during the shopping experience when the E*MERGE® Browser Plug-in became aware, and informed the buyer, that the seller also supports E*MERGE® it sits idle awaiting receipt of a message **2) Seller’s Invoice**.

After the invoice is received and while the invoice is being displayed by the browser, the E*MERGE® Browser Plug-in AUTOMATICALLY updates a local electronic log indexed by the Ref# and validates the Hash, thus assuring the integrity of the data sent by the seller.

An E*MERGE® Browser Plug-in window will appear and request the buyer to enter their 3DAS™ Card. A 3DAS™ read is performed and the E*MERGE® Browser Plug-in determines if it has a payment profile associated with that card. (See 4) Initialize and Authenticate Buyer and Card for more details)

The E*MERGE® Browser Plug-in then compares the list of payment options sent by the seller to the set of payment options found in the seller's payment profile.

The E*MERGE® Browser Plug-in will state that the buyer has requested secure E*MERGE® payment and offers the list of matching payment options. The buyer has the option to select one or cancel.

In the event that the buyer wishes to cancel

The seller receives a response based on the information found in the invoice message defining how to respond to the buyer selecting the cancel button.

ii) Payment Agreement

The buyer has selected which means of payment and committed to pay. The E*MERGE® Browser Plug-in sends a commit message, message 3, to the seller and issues the request payment authorization message, message 4, to the CP server.

The E*MERGE® Browser Plug-in window will begin to display the status of the payment process. The buyer can either decide to wait and watch or go and surf somewhere else. Assuming the buyer's Internet connection is still active the E*MERGE® Browser Plug-in remains active and awaits a response to confirm the commit to pay. If the buyer disconnects from the Internet the E*MERGE® Browser Plug-in is left in a pending response state.

iii) E*MERGE® Browser Plug-In Status Screen and Electronic Log Functions

In the event that the user leaves the E*MERGE® Browser Plug-in window visible the first update will be acknowledgement of seller authenticity. Acknowledgement of payment approval by the bank will follow.

In any case the E*MERGE® Browser Plug-in will need a response to the request for authorization so that it can internally acknowledge completion of the transaction. If the Internet connection is not interrupted and the E*MERGE® Browser Plug-in remains active the CP server will return confirmation of seller authentication and approval of the payment.

In the event the connection is lost, the ability for the plug-in is not longer able to receive a response. Therefore, upon reactivation of the plug-in, the plug-in will (in the background) connect to each of the CP servers in the profile, that should have outstanding messages, requesting delivery of any outstanding messages targeted for that buyer's plug-in.

In some cases, the buyer will disconnect from the Internet. In other cases, the buyer will not always use their designated home device. In order to keep the electronic log up to date and to assure the customer they have all the information they might need in the event of a dispute. The E*MERGE® Browser Plug-in must have a means of synchronizing itself and collecting information about E*MERGE® purchases performed on other devices.

To assure that the home E*MERGE® Browser Plug-in is fully synchronized it must have the ability to automatically connect to the various CP servers it is registered with. So periodically when the home device is connected to the Internet the 3DAS™ Browser Plug-in will request permission from the buyer to synchronize itself. Assuming the buyer grants permission, the plug-in will automatically connect to each payment servers it knows and perform a synchronization process.

During these synchronization sessions the plug-in will request downloads of any pending messages concerning seller authentication and payment approval. It then requests a download of the messages associated with the mobile purchases kept on the buyer's that have taken place since the last synchronization session.

All messages are logged and as appropriate matched to any the pending commits to pay records.

This electronic log offers the buyer all he needs to track goods purchased over the Internet using E*MERGE®. The buyer uses a simple viewer, installed at the time the E*MERGE® Browser Plug-in was loaded, to monitor his Internet purchasing activity.

As described in the section 7) Notify Seller of Acceptance the E*MERGE® Browser Plug-can be used to authorize the download of soft goods. Part of the function of the status screen would be to inform the buyer to initiate the download. Assuming the buyer agrees the plug-in can initiate the FTP session and provide any corrective action as may be appropriate.

In the event of dispute the E*MERGE® Viewer can be used to print the necessary information to support the claim that the seller has not fulfilled their commitment to deliver.

Services that extend the features of the E*MERGE® solution, such as integration to Quicken or MS Money, can use this file to offer expanded value added capabilities.

Appendix 4 - Consumer Mobility - The E*MERGE® Difference

One of the challenges in providing an effective means of payment for the Internet is to make sure the buyer can make purchases from any Internet enabled device. Providing mobility does not, mean that security can be subjugated nor should it mean that the buyer's option of payment methods is limited or that procedures become more cumbersome.

Most of secure payment methods available today depend on a software module and some associated data commonly referred to as a "Wallet". The "Wallet" must be loaded and becomes part of the software of a PC. Banks must create Cryptographic keys and certificates associated with each payment method and arrange to load them into this “insecure” PC. This dependence on software restricts the buyer purchasing only from those PCs they have arranged to load the cryptographic information. Unless they figure out how to copy these cryptographic keys and certificates to securely carry them around.

The one solution that MasterCard and Visa are discussing to solve this problem is to employ smart cards, defined by the EMV “Europay, MasterCard and Visa” Integrated Circuit Card Specification, as the mechanism to carry the consumer’s SET “Secured Electronic Transaction” certificates.

Unicate's concern is that this solution does nothing to reduce the complexity of SET nor does it eliminate the costs associated with issuing these EMV smart cards. A 5 to 10 year mega billion dollar negative business case that no one has been able to sensibly justify.

Other methods currently being experimented with implement the consumer's wallet inside a network server thus allowing the consumer to access their network wallet from any PC. Although these solutions begin to resolve the problem of mobility, it does not successfully resolve the associated issues of security and ease of use.

These network solutions are hampered by the fact that assuring an acceptable level of security forces the user into having to remember account numbers and passwords. This requirement imposed to assure protection ends up defeating the primary goal -

Provide The Consumer A Mobile And Easy To Use Payment System.

Mobility - Device and Location

In designing E*MERGE® Unicate began by considering the devices and locations that a consumer may wish to effect Internet purchases from. This holistic approach recognized that without an effective ePayment mechanism the success of eCommerce was at risk. Unicate also thought about the needs of all the players and remembered, “The consumer is king”. This customer focus has assured the users of E*MERGE that makes payments from a Cyber Café is as secure and easy as they are from home.

Home & Office Devices

If we simply consider the home, there is an assortment of devices a consumer may wish to use (PC, TV, …, Smart Phone). They do not expect to be limited to use the one supported by some specification just because the authors of that payment solution did not design mobility and device independence in from the beginning.

Simultaneously many office workers, during their lunch and breaks, surf the web and locate goods they wish to purchase. On the other hand, for business reasons they may wish to be able to effect payments against their expense account or a corporate payment card from their home office.

As Local Area Networks expand, users will end up working from a variety of devices in the office environment. The list could include the PC in their office, a PC in a conference room, PCs installed in locations away from their main place of work or on their laptop. All of these locations must be positions from where consumers should have the ability to spend money using the new channel provided by the eCommerce revolution.

Devices at both the home and office have one thing in common. There is a degree of trust assumed by the user.

The Cyber Café and Alien Locations

In contrast the Cyber Café and locations such as hotels, outdoor kiosks, PCs in building lobbies and other public locations are locations from where consumers will have a heightened security concerns. This being said, the design of the E*MERGE® system assumes that every location is a threatening location and views that payments should operate the same no matter where the consumer is.

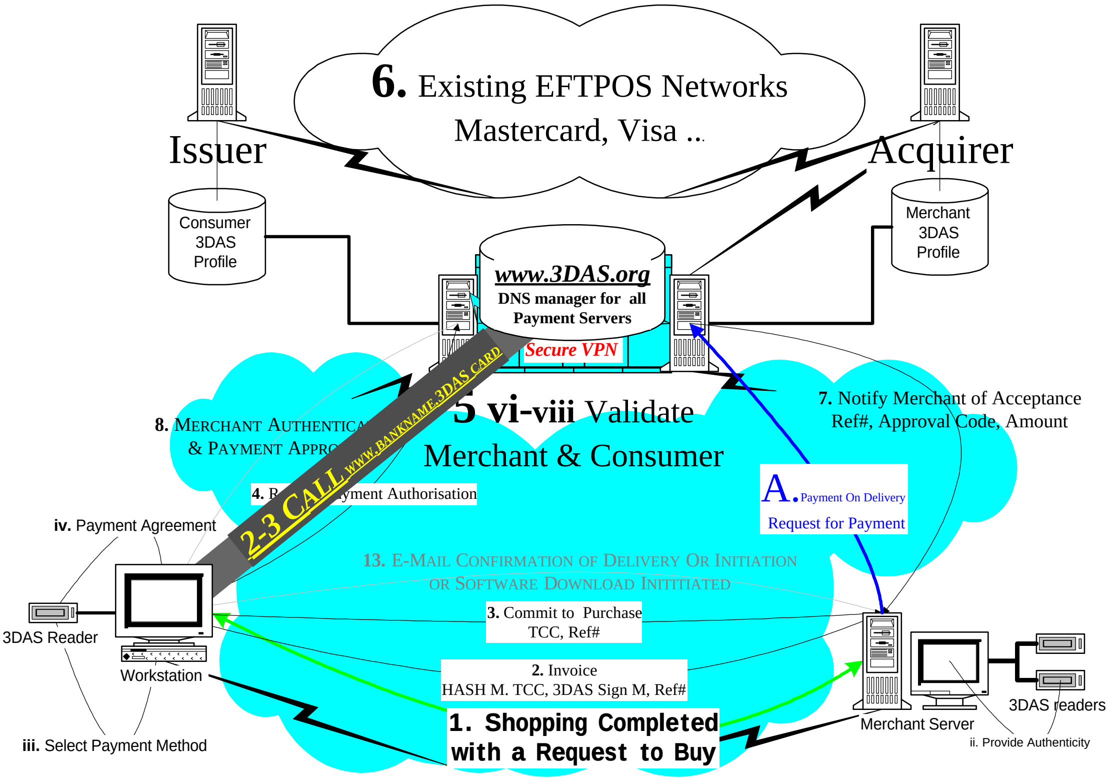
Unicate appreciates that certain communities will wish to provide distinguishing features on public terminals to assure the consumer that their payments are secure and cannot be tampered with. Therefore it assumes that some of these public locations will require some form of external certification to assure trust in both the software and the hardware being employed by the E*EMERGE® system.

How this certification should take place and how it can be policed must be the subject of multi-lateral discussions with the E*MERGE Consortium, International agencies, local authorities in each country or community planning to employ E*MERGE® in such public locations

GSM and other low powered digital devices

As eCommerce expands, eCommerce merchants will wish to enable payments from a raft of small low powered devices that do not have the display capabilities or the computational power of a PC or, for that matter, a digital television. Three issues must be addressed when considering how to serve these locations. First, how the E*MERGE® *Browser* Plug-in interacts with the consumer? Second, how much memory or storage is available on these devices to allow the plug-in to store consumer profiles etc? Third, can the 3DAS™ Reader be made small enough?

Contrary to other initiatives Unicate has assumed mobility and the variety of devices a consumer may wish to use as key to the overall design criteria. Simultaneously, Unicate's management demands that the 3DAS™ solution avoids the use of cryptography and assures the consumer the highest level of ease of use. Equally, Unicate’s management has spent a great deal of time making sure that the 3DAS™ reader is as small as possible. Unicate will continue in its efforts to further reduce production cost and further miniaturization of the reader.



www.issuerID.3DAS.org/mobile - The Key To Consumer Mobility

With E*MERGE® and leveraging the power of 3DAS™, all that is required is that the device the consumer wishes to use be equipped with an inexpensive 3DAS™ Reader.

3DAS™ the Key to Mobile Payments

The solution Unicate proposes simply requires the user to insert their 3DAS™ Card into a 3DAS™ Reader when prompted by the E*MERGE® Browser Plug-in to do so[23]. The E*MERGE® Browser Plug-in reads the card and does not find a matching E*MERGE® Browser Plug-in Consumer Profile. (See **i) Select Payment Method** for more details.) It therefore assumes the consumer is a mobile user and initiates the Mobile user routine.

The E*MERGE® Browser Plug-in operates under the assumption that it is there to serve. Therefore it wants to locate the right E*MERGE® CP Server. It can follow one of two routes to server this mobile consumer.

E*MERGE® Mobility with A Little Bit of Print

Not finding a mobility file on the card, it asks the consumer to enter the Issuer Id, as found printed on face of the card. The user is then requested to enter their first name exactly as printed on the card.

Based on this very simple to remember, *its printed on the card,* information the plug-in can now prepare an E*MERGE® Mobility Message "No Mobility file present" consumer with ID is present. It first requests the 3DAS™ Reader to produce a 4 character FastKey

Using the Issuer Id entered by the buyer and a 3DAS™ FastKey it creates the URL **www.issuerID.3DAS.org/mobile** and connects to the Internet. Assuming the connection is established and recognising that the mobility file is not present, the E*MERGE® CP Server responds with request to produce a 3DAS™ Signature based on a random challenge value.

The E*MERGE® Browser Plug-in takes the value of the challenge plus the User ID, issuer ID, date and time and creates a Hash. Using this Hash the plug-in requests the 3DAS™ Reader to produce a 3DAS™ Signature. The plug-in then creates a message including the Hash, date and time and the 3DAS™ Signature and sends it back to the E*MERGE CP Server. The payment server validates that it the card is present by verifies the Hash and the 3DAS™ signature against the Consumer Profile is located using the User ID found in the first message. It is now ready to allow the E*MERGE® Browser Plug-in to serve its 3DAS™ authenticated consumer.

E*Merge® Mobility File

Consumer mobility ID	First and Last Name with a sequence number	27 Characters
E*MERGE® CP Server Address	The URL of the of the CP server	Variable
E*MERGE CP Server Public Key	Last CP Server Public Key used to validate authenticity of messages from the payment server	8 digits1024 bits

E*EMERGE® Mobility Facilitated by an Inexpensive Protected Memory Chip

(Or other machine readable media on the card)

[23] This occurs immediately after the E*MERGE® Browser Plug-in has received the Merchant Invoice.

Finding an inexpensive (.15 to .20 US dollars) protected memory chip (or other machine readable data store) present and locating an E*MERGE® Mobility File, the E*MERGE® Browser Plug-in proceeds to read the information in the E*MERGE Mobility File.

The E*MERGE Browser Plug-in prepares a mobility message that includes the Consumer Mobility ID, a calculated Hash[24], the data, the time and a 3DAS®™ Signature[25]. Using the address in the Mobility File[26] and adding a /mobile to the URL it connects to the E*MERGE CP Server[27] and sends the message that initiates the request to download a temporary consumer profile.

The server looks up the consumer record from within the E*MERGE Consumer Payment Profile using the Consumer Mobility ID as the index. The payment server validates that it the card is present by verifies the Hash and the 3DAS™ signature against the Consumer Profile is located using the Consumer Mobility ID. It is now ready to allow the E*MERGE® Browser Plug-in to serve its 3DAS™ authenticated consumer.

The E*MERGE Mobility Routine returns, after positive verification of the Hash and the 3DAS™ signature, a temporary Consumer Profile to the Plug-in

An Authentic Card is Mobile

In either of the two cases described above, the E*MERGE CP Server has used 3DAS™ to prove that the **Card is Present** so that the Issuing Bank can offer their treasured clients an easy to use mobile service.

Assuming the card is authentic, the E*MERGE CP Server creates a **temporary** copy of the E*MERGE® Consumer Payment Profile, inserting new pseudonyms in for both the consumer pseudonym and the payment method pseudonyms.

In the event that a protected memory chip was present[28] with an E*MERGE® Mobility File inside the payment server also sends a new Consumer Mobility ID. This new ‘Consumer Mobility ID’ is written to the chip, replacing the old value.

This temporary file and additional information is sent by the E*MERGE® CP Server to the E*MERGE® Browser Plug-in serving the mobile user. The E*MERGE® Browser Plug-in creates an additional temporary consumer profile using the standard structure describer in the section on the E*MERGE® Browser Plug-in Consumer Profile.

[24] The Hash is of the data in the mobility file along with the date and the time.

[25] The 3DAS™ Reader produced the 3DAS™ Signature based on the Hash

[26] Each E*MERGE® Consumer Payment Server must have a unique IP Address that links to the URL www.issuerID.3DAS.org in a central DNS *Domain Name System.* A DNA is a database system that translates an IP address into a domain name. The E*MERGE Consortium would manage the DNS for the domain 3DAS.org.

[27] The extension /mobile will allow the E* MERGE® Consumer Payment Server to direct the request to the mobility routine.

[28] Note: As an alternative a SSL connection may be set-up for retrieving the Consumer Profile. The ‘Last Mobility ID’ then remains unchanged. This is especially recommended if the data storage on the card is read-only and the ‘Last Mobility ID’ thus is a constant value.

The E*MERGE® Browser Plug-in is now able to continue with the standard secure E*MERGE® payment process at the stage that the plug-in compares the payment options the consumer has available to the payment options the merchant is willing to accept (See **i) Select Payment Method** on Page 45).

Recognising that exceptions do occur the E*MERGE® browser plug-in will maintain a temporary log of the transaction. Either after the Internet connection is terminated and a specified period has elapsed or after receipt of message 8 these log records will be deleted.

In order to assure the consumer that the log at the primary E*MERGE® Browser Plug-in is up to date, the E*MERGE® payment server will store and create the log records necessary to update the consumer home plug-in's log. This feature will allow the home E*MERGE® Browser Plug-in, see page 46 describing the iii) E*MERGE® Browser Plug-In Status Screen and Electronic Log Functions, to automatically update the consumers home log file when it is next connected to the Internet.

Technical Considerations

The software in the E*MERGE® Browser Plug must include logic that says that if it does not find a consumer profile linked to the card in the 3DAS™ Reader it executes the logic associated with the E*MERGE® mobility option.

The plug-in must also have within it logic to purge consumer profiles that are no longer active. This suggests that when a mobile users effects a mobile internet payment the 3DAS™ Browser Plug-in asks the user to enter the number of days their temporary consumer profiles can remain persistent[29]. This being said many consumers will not understand the security issue surrounding the temporary E*MERGE® Consumer Profiles. Therefore, as part of each payment servers automated maintenance procedures it will have fraud prevention logic capable of instruct an E*MERGE® Browser Plug-in to purge mobile consumer profiles.

The E*MERGE® CP Server will be able to recognize the URL extension /mobile and in an inbound message and recognize that an E*MERGE® Browser Plug-in attempting to serve one of the payment server mobile consumers. The CP Servers mobility logic will also include specific fraud detection logic designed to monitor irregular activity.

In order to make sure the consumer's host plug-in's logs are kept up to date the server will retain all pertinent information, so that the consumers host E*MERGE® Browser Plug-in' log can be updated.

[29] This feature would allow a consumer at a hotel to set the plug-in to keep the their profile for say 3 days. At a Cyber Café for only another hour. Their office could be set to maintain the profile for 120 days. The machine of a friend could be set for 30 days. The goal is to improve performance for repeat users, while at the same time protect the system from criminal activities. The default being to delete after each use.

Appendix 5 - System Components of E*MERGE®

In all attempts to implement payment systems, Interoperability has been the greatest obstacle. Therefore, Unicate has set out to make sure that throughout the design there is assurance that E*MERGE® can be implemented on a global scale and remains true to the tenants of open competition and guarantee interoperability.

The following components make up the E*MERGE® system:

- The E*MERGE® Specifications
- The 3DAS™ Card
- The 3DAS™ Reader
- The E*MERGE® Message Protocol
- The E*MERGE® Browser Plug-in
- The E*MERGE® Merchant OLTP Server Components
- The E*MERGE® Secure VPN, MP and CP Servers

The intention of this section, and in conjunction with the description provided in Appendix 1 - 3DAS™ The Ultimate in Security, is not to specify each of these components. Its goal is to provide a high level overview of these components, how they are to be made available to the appropriate parties and how through the overall management of the E*MERGE® scheme, interoperability can be guaranteed.

The E*MERGE® Specifications

Obviously in order to assure interoperability the specification must be singular and extremely proscriptive.

Unicate will develop this document and submit it as a draft to the consortium that will be ultimately responsible for the management of E*MERGE® System. Inherent in this document will be the specifications that define the unique characteristics of the components defined below.

The 3DAS™ Card

The card is made up of two elements the plastic body (as it exists today) and the 3DAS™ Marker.

Unicate will provide for the secure and auditable provision of 3DAS™ Markers. In time, other entities can be licensed to provide the markers so long as these entities adhere to the security regulations defined in the specifications.

The insertion of the 3DAS™ Marker into the card is a simple operation and equipment already exists and is employed by many of the organizations that produce plastic payment cards gearing up to embed smart cards[30]. Therefore, the suppliers of payment cards will procure markers and arrange for the insertion of the 3DAS™ Marker into the card body.

[30] Unicate has already validated that the equipment used to embed smart cards can just as easily be used to embed the 3DAS™ Marker

NOTE A MARKER IS ONLY VALID
AFTER IT HAS BEEN REGISTERED AND STATUSES AS LIVE.
BEFORE THAT TIME IT IS WORTH LESS TO THE CRIMINAL
THAN THE PRE-PRINTED BODY OF A CREDIT CARD.

The 3DAS™ Reader

The reader includes a specific sub-assembly capable of reading and interpreting the 3DAS™ Marker. Only qualified suppliers under license should be permitted to manufacture this 3DAS™ specific intelligent optic sub-assembly.

The integration of this 3DAS™ specific component and the electronics that interface to the PC or server into the PCMCIA, free-standing or rack mounted form can be accomplished by virtually any manufacturer of computer components. The key is assuring interoperability is making sure that the hardware is provided with software that guarantees that applications written by others can talk to it and that the hardware and software package matches the computer equipment that it will be attached to (Windows, Unix, Linux…). (See section on **3DAS™ Reader** on page 22 for further details)

Core to the E*MERGE® specification will be a defined set of APIs that describe how applications communicate with the 3DAS™ Reader. This specification will define how the application software requests the generation of a 3DAS™ Signature and how it will return the result.

✓ It will define the structure of the input that the application software must provide.
✓ It will define the structure of the output the 3DAS™ Reader will provide.
✓ It will define the error conditions that may be returned.
✓ It will articulate how to incorporate a buyer PIN in the 3DAS™ Signature.
✓ It will define how the application software specifies the length of the signature
✓ It will define how the application software can specify that the signature must come from a new read of the same Card.[31].

The sale and support of the 3DAS™ Reader can be through any number of distributors. These distributors can range from the local PC store through to systems integrators involved in developing merchant web sites. Alternately the banks may wish to provide this component as a branded part of the banking relationship.

The E*MERGE® Message Protocol

As part of the release of the specifications a specific document will be prepared that defines the flow, message content, message format and data structure governing the Internet protocol that has been defined in **The Transaction Flow (Flow Chart)** on page 39.

The E*MERGE® Browser Plug-in

At this stage in the design of the E*MERGE® system the assumption is that the E*MERGE® Browser Plug-in is a software component that will be provided by one vendor, both as a specification and a reference model. This initial version will be capable of being employed through either Netscape or Internet Explorer running under a yet to be defined list of operating systems.

[31] This particular requirement is required during both card personalization and during consumer profile activation.

In the future, software suppliers may determine that it is appropriate to embed this component into future releases of the software or banks may decide to include this as part of an overall-banking package provided to the buyer. As long as all implementations are capable of supporting the full range of 3DAS™ Reader APIs and responding to, and issuing the appropriate messages as defined in The E*MERGE® Message Protocol assures interoperability.

The E*MERGE® Merchant OLTP Server

At this stage in the design of the E*MERGE® system the assumption is that the E*MERGE® Merchant OLTP Server is a set of software modules that will be integrated into the online transaction processing environment of the merchant. Web transaction processing system software suppliers may determine that it is appropriate to embed this component into future releases of their software. As long as all implementations are capable of supporting the full range of 3DAS™ Reader APIs and receiving and issuing the messages defined in The E*MERGE® Message Protocol then interoperability is assured.

Later in the specification it will refer to the E*MERGE® Merchant OLTP Control Software. As the project moves into detailed design it is hoped that a component similar to the E*MERGE® Browser Plug-in can be developed for the merchant server environment thus improving the lead-time on merchant server development.

The Merchant and Consumer Payment Servers

A limited number of implementations are anticipated of these systems and it is recognized that this will be the most complex part and requires the highest level of security of the entire E*MERGE® system. Unicate proposes that a limited number of suppliers work together to develop the core aspects of these applications. It is then assumed that these suppliers will work with the organizations that will operate these systems to customize them to afford each operator competitive advantage.

As a baseline, these systems must be able to respond to and support The E*MERGE® Message Protocol. These systems will also have to support a secure environment capable of storing and managing the 3DAS™ Key and the related payment instructions. On the Merchant/Acquiring side, the appropriate interfaces to the existing payment systems will have to be included in the overall solution.

As part of the ongoing payment authorization process, and in a secure way, the MP server will be responsible to format the EFTPOS messages and transmit them through the appropriate Acquiring Bank interface. This will involve

- Inserting the consumer information received over the Secure VPN from the 3DAS™ Consumer Servers into the appropriate EFTPOS message e.g. PAN, Expiry Date …
- Inserting the appropriate elements of the static payment details held in the E*MERGE® Merchant Profile into the EFTPOS message
- Inserting any transaction specific data into the EFTPOS Message e.g. (amount, date …
- Awaiting response from the Acquiring Bank interface
- Returning to the CP server status of payment authorization

The Secure VPN

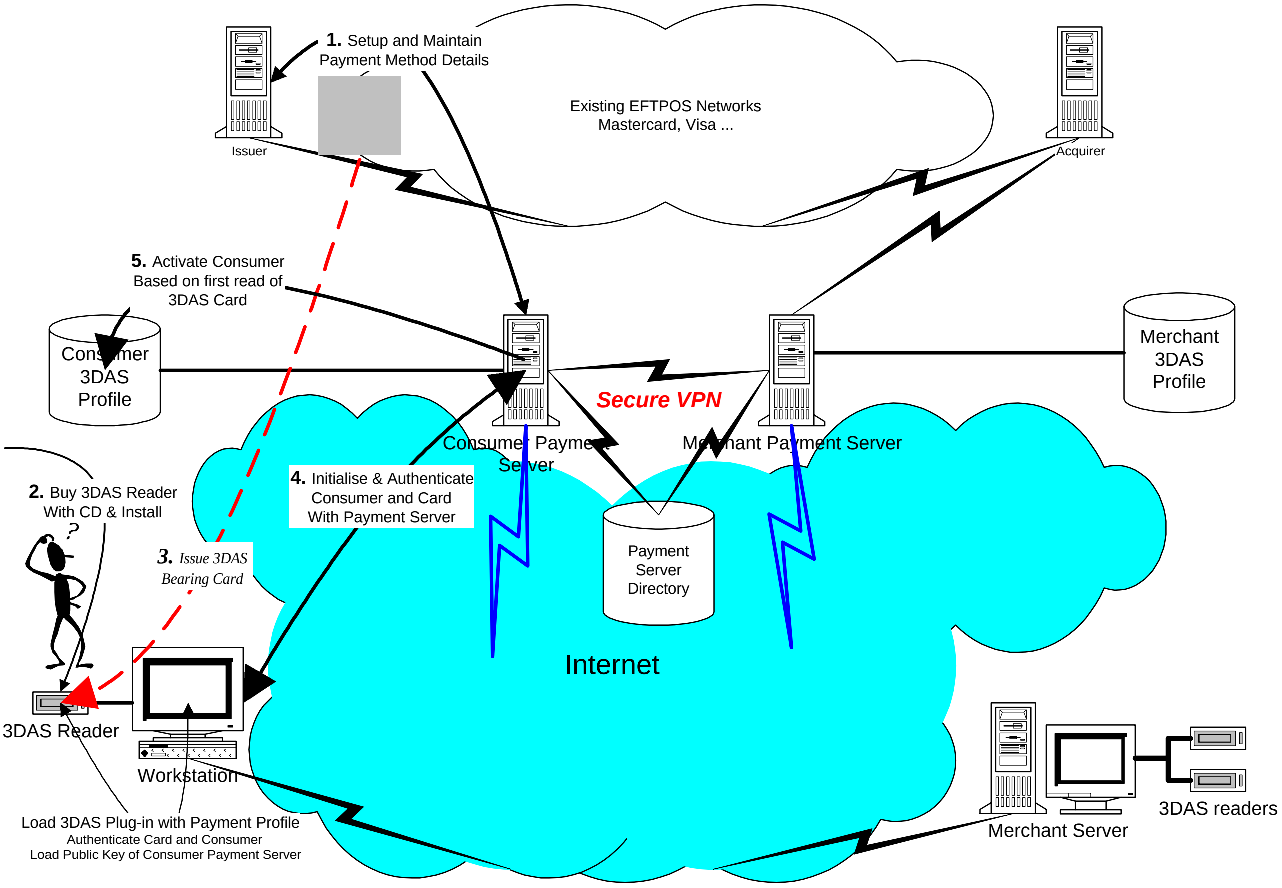
The Secure VPN supports secure communication of a set of messages that will be defined in the detail transaction flow included as a further addendum to this document and a secure network capable of assuring the confidentiality of the payment instructions. The overall architecture of the VPN will be a function of the number of payment servers that will ultimately operate and is identical to numerous networks currently in operation.

For any pilot installation, these three components can be assembled as one system.

3DAS.org

In order to assure the success of the mobility option and assist in making sure that the Secure VPN and the links between the trusted payment servers are current a set of redundant DNS servers will need to be maintained by the E*MERGE consortium.

Appendix 6 - Consumer Enrolment in E*MERGE®



Buyer Enrolment Flowchart

The assumed business relationships between the three parties involved in the buyer enrollment process are as follows:

- Buyers have a series of relationships with banks that provide them with an assortment of payment options.
- Based on the assumption defined in Business Relationship Assumptions of E*MERGE®, banks select from the list of accredited payment system operators an operator to manage the banks E*MERGE® CP Server. A number of banks may decide to develop and operate E*MERGE® CP Servers.
- The operator of the payment server will have a tertiary relationship with the buyer, based on the terms of their relationship with the bank.
- The delivery of the 3DAS™-enabled Card to the buyer is the responsibility of the bank and the establishment of the payment methods that can be employed. Using that payment card is the responsibility of that same bank.

Name	Description	Source	Size
Buyer Name	First and last name	Issuer	27 Characters
Buyer Pseudonym	Randomly generated and changed on a random cycle	CP server	12 bytes
3DAS™ Key	Data Table of 3DAS™ Marker in the bank's buyers card	Issuer - at card personalization	80 bytes
Payment Method Type	E*MERGE® wide standard used to define if the method is MasterCard, Visa, Check, Micro-payment …	Issuing Bank	4 Bytes with a .JPG or .BMP file stored with the E*MERGE® Browser Plug-in
Payment Method Pseudonym	Randomly generated and changed on a random cycle	CP server	12 bytes
Payment Details	Static Information required to complete EFTPOS Message	Issuing Bank	Variable - based on payment scheme specifications
Payment Method Type	E*MERGE® wide standard used to define if the method is MasterCard, Visa, Check, Micro-payment …	Issuing Bank	4 Bytes with a .JPG or .BMP file stored with the E*MERGE® Browser Plug-in
Payment Method Pseudonym	Randomly generated and changed on a random cycle	CP server	12 bytes
Payment Details	Static Information required to complete EFTPOS Message	Issuing Bank	Variable - based on Payment Scheme specifications
Payment Method	As many as required		

E*MERGE® Consumer Profile

1) Set up & Maintain E*MERGE® Consumer Payment Profile

Key to the responsibilities defined in the relationship between the Issuing Bank and the operator of the E*MERGE® CP Server is a record referred to as the E*MERGE® Consumer Profile.

The role of this record is to record the payment methods the bank defines the buyer is allowed to use over the Internet. Further, it will securely hold the static information required to submit the EFTPOS message associated with that particular payment method.

For example, the Issuing Bank may decide that John Smith can use his MasterCard and his USA checking account.

- For a MasterCard credit card the Issuer would provide the complete content of track 1 and/or track 2.

- For a USA Checking Account the Issuer would provide the content of the MICR line and any other information employed when submitting electronic checks to the ACH system.

Periodically, the Issuer will be required to update this record. For example when issuing a new card when the expiries date changes.

As described in *The E*MERGE® Consumer Payment Server* (EMERGE®CP Server)on page 37, the operator of the CP server will establish the procedures and technology necessary to maintain the accuracy of this secure payment information.

2) Buyer Obtains 3DAS™ Reader with CD and Installs

The working assumption is that the E*MERGE® system will be widely accepted and that the buyer will be able to go to any store that sells personal computers and purchase a 3DAS™ Reader.

On the other hand, the buyer’s bank may wish to brand the 3DAS™ Reader and the CD.

At some point the buyer will sit down in front of their PC ready to set-up their E*MERGE® environment. Core to the buyer proposition is that all the buyer does is plug the 3DAS™ Reader in and be ready to insert the CD when prompted to do so. The Plug and Play mechanism will identify the new device and ask the user if they have the disk.

The working assumption is that the E*MERGE® Browser Plug-in is included on the install CD. Another option is that the E*MERGE® Browser Plug-in is included as part of the Microsoft wallet. This would allow integration of customer profile related capabilities of the wallet with the payment related services of the E*MERGE® system.

As part of the automated installation process, the plug-in and the drivers are loaded into the PC. Next the E*MERGE® Browser Plug-in will attach to the appropriate browser within the user’s configurations. The E*MERGE® Browser Plug-in can test communication with the 3DAS™ Reader. It can then go on to automatically register itself with the distributor responsible for the warranty and service of the 3DAS™ Reader and E*MERGE® Browser plug-in. Assuming successful connection to the distributor’s site, further automated tests can take place and the download of any software upgrades can occur.

3) Issue 3DAS™ Card

The next step in the buyer enrolment process is to create the 3DAS™-enabled Card.

At the time that the card is produced and personalized, the 3DAS™ Key must be created as described in section on the **3DAS™ Key**. The 3DAS™ Key is registered in the E*MERGE® Consumer Profile. The entry associated with this particular buyer begun during the **1) Set up & Maintain E*MERGE® Consumer Payment Profile** described on page 59.

After the 3DAS™ Key is loaded into the CP server database, two files containing information pertinent to creating the E*MERGE® Browser version of the buyer profile and supporting the mobility option are prepared.

The Issuer delivers the card to the buyer in much the same manner as today, by mail or by asking the buyer to pick it up at their bank branch.

The delivery of files can occur in one of three ways.

- It could be loaded onto a CD and sent with the card.

- It could be built within the payment server. A mail insert can be prepared with an Internet address printed on it.
- It could be loaded into an inexpensive chip on the card.

The advantage to this approach is that the chip facilitates the user mobility option (see Appendix 4 - Consumer Mobility - The E*MERGE® Difference). In addition, independent of E*MERGE® this inexpensive chip[32] can provide a platform to offer value added services to these Internet aware and computer literate customers.

Everything is now prepared to move to the next step.

4) Initialize and Authenticate Buyer and Card

The Issuer, in conjunction with the E*Merge® CP Server operator, can send the buyer the 3DAS™-enabled Card

- ✓ With an inexpensive, protect memory chip in it.
- ✓ With a CD inside the envelope.
- ✓ With a mail insert with a URL printed on it.

In order to assure the highest level of security there is a separate secure mailer, with an initialization secret[33] inside.

When the buyer has the envelope with the card and the separate envelope with the secret, they will read the instructions, sit down at their PC and do one of the following:

- Insert the card into the 3DAS™ Reader.
- Insert the CD into the CD drive.
- Launch the browser and connect to the URL.

Whichever option is employed, the E*MERGE® Browser Plug-in will automatically start and begin the initialization process.

The E*MERGE® Browser Plug-in will acquire either from the chip card, CD or URL, two files. These two files will be used to create the E*MERGE® Browser Plug-in's Consumer Profile.

One of the data elements in the first file is the public key of the E*MERGE® CP Server. This key is used to assure trust between the buyer and the E*MERGE® CP Server. To provide this assurance, a simple public key infrastructure is required.

In the future, when the E*MERGE® Browser Plug-in receives information and instructions it will know that it came from this trusted payment server. The payment server will sign its outbound messages with its Private Key and the plug-in will authenticate these messages with the payment server's Public Key.

[32] The E*MERGE® system would require two files inside the chip. The first file includes basic information used to simplify the mobility option and initialize the E*MERGE® Browser Plug-in. The second file carries the content of the E*MERGE® Browser Consumer Profile and is only used once to initialize the home PC of the consumer and is subsequently erased. This therefore allows the card Issuer to use the space for other applications.

[33] The use of the secret is described in the subsequent section **5) Activate Consumer on Payment Server** and is a security mechanisms to protect against **not received** fraud and **application** fraud.

Name	Description	Size
3DAS™ Code	Result of read of 3DAS™ Marker Associated With Issuer	4 bytes
Buyer Pseudonym	Randomly generated and changed on a random cycle	12 bytes
E*MERGE® CP Server Address	The URL of the of the CP server on the secure VPN	Variable
E*MERGE CP Server Public Key	Public Key used to validate authenticity of messages from the payment server	1024 bits
Payment Method Type	E*MERGES® wide standard	4 Bytes with a .JPG or .BMP file stored with the E*MERGE® Browser Plug-in
Payment Method Pseudonym	Randomly generated and changed on a random cycle	12 bytes
Payment Method Type	E*MERGE® wide standard	4 Bytes with a .JPG or .BMP file stored with the E*MERGE® Browser Plug-in
Payment Method Pseudonym	Randomly generated and changed on a random cycle	12 bytes
Payment Method	As many as required	

E*MERGE® Browser Plug-in Consumer Profile

At this stage the E*MERGE® Browser Plug-in is ready to activate the card.

The plug-in will recognize either that a card is in the reader or request the buyer to insert their 3DAS™ Card

The plug-in will prompt the buyer to type in the secret[34] known to them and the Issuing Bank.

[34] There is a risk that a criminal may intercept the card in the mail and attempt to register it fraudulently. Therefore, it is prudent to include a secret **only** in the registration process that the consumer payment server and the consumer know. This would then be used as part of the data used to generate this 3DAS™ signature. Specifics of how this secret is established are up to the Issuer and the E*MERGE Consumer Payment Server Operator to define. After this procedure is complete, this secret would only be used if the Browser plug-in fails and requires reinitialized.

The E*MERGE® Browser Plug-in will calculate a Hash (see The Hash for details) using the buyer pseudonym, the secret, the data and the time as input. It then asks the 3DAS™ Reader to read the 3DAS™ Marker and generate a 3DAS™ Signature.

Using the URL, now stored in the buyer's profile, the E*MERGE® Browser Plug-in will establish and connect to the E*MERGE® CP Server and request authentication of the buyer's card. The CP server will use the buyer pseudonym to locate the buyer profile and authentication the 3DAS™ Signature and respond accordingly.

During this communication session any new E*MERGE® .JPG or .BMP files containing visual icons for the payment methods that user is authorized to employ can be added to the plug-in's library.

Assuming authentication, the E*MERGE® Browser Plug-in will ask the 3DAS™ Reader to read the marker one more time[4]. The output of this read will be inserted into the E*MERGE® Browser Plug-in Consumer Profile as the 3DAS™ Code used in the future to identify the appropriate consumer payment profile and pre-authenticate the user.

When multiple banks send cards to the buyer, this 3DAS™ Code is used to determine which payment methods the buyer is allowed to use with the card then in the reader.

At the end of this short process, the buyer can use their E*MERGE® Card to securely shop on the Internet.

5) Activate Consumer on Payment Server

If the customer enrolment completed successfully and the E*MERGE® Browser Plug-in was loaded properly the E*MERGE® CP Server activates the card.

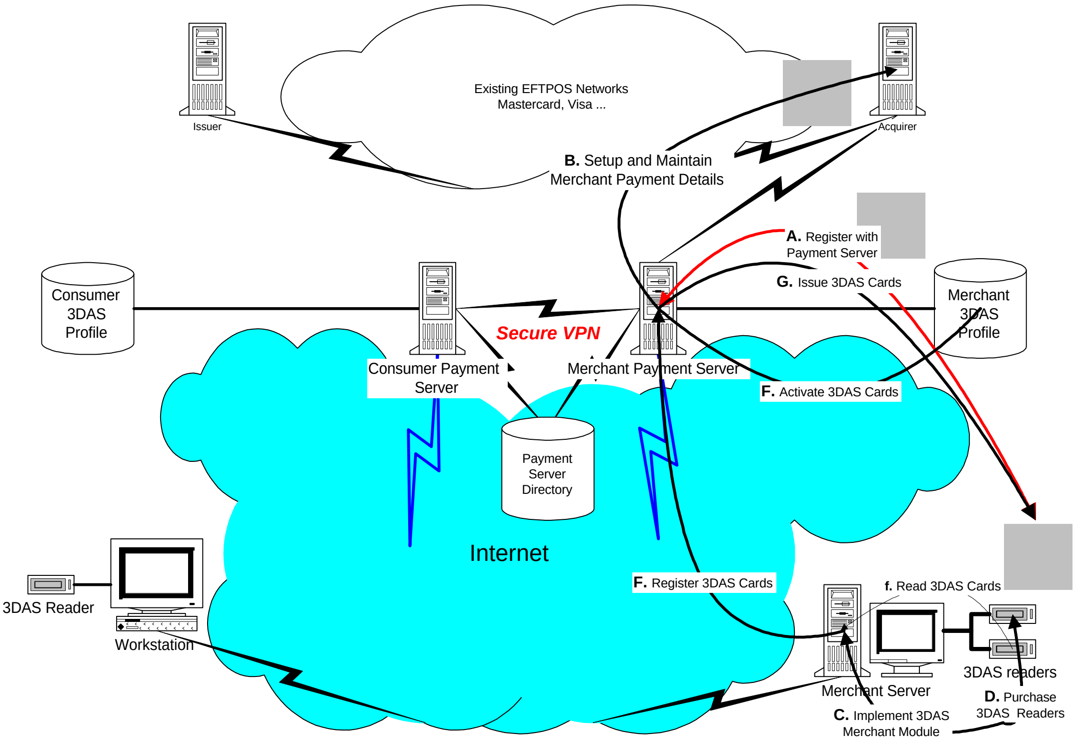
From this point forward, or until the Issuer states otherwise, the E*MERGE® CP Server will accept requests for payment from the buyer and issue appropriate authentication information to the seller.

[4] As part of the software in the 3DAS™ Reader logic will exist that makes sure that the card is not changed when the 3DAS™ plug-in is requesting multiple reads of the same consumer's card.

Appendix 7 - Merchant Enrollment in E*MERGE®

The way that the E*MERGE® payment method is defined suggests that the most efficient way to operate the E*MERGE® is to allow the operators of the E*MERGE® MP Server to establish binary relationships with merchants. Therefore, the model assumes that accredited operators of the E*MERGE® Payment Servers will establish relationships with the merchant's banks working as an agent of that particular merchant.

Merchant Enrolment Flowchart



A) Register with an E*MERGE® MP Server

The first step in the establishment of a seller as 3DAS™ E*MERGE® capable is for the operator of the E*MERGE® MP Server to contact the seller and convince them of the value of the E*MERGE® service. Two items make this proposition most attractive to a seller. First, E*MERGE® authenticated transactions are card present transactions. Second, the only risk to an honest seller is that they do not meet their own terms; the terms they propose and agree with their customers. Buyers claiming that they did not purchase those goods will have to prove that the card was not in their possession at the time of the transaction.

Once the seller has agreed to join the E*MERGE® system, the operator will request from the seller a list of payment options that they would like to employ. The list the seller can select from will be restricted to those methods that the E*MERGE® system has operational.

If these are all payment methods the seller currently employs, each will be associated with a particular banking relationship and have a set of technical characteristics and seller parameters. These must be inventoried, and as appropriate, replicated on the EFTPOS side of the E*MERGE® MP Server. As an agent of the seller, the operator will contact the appropriate banks and proceed accordingly (see **The Merchant and Consumer Payment** Servers**)**.

E*MERGE® Merchant Profile

Name	Description	Source	Size
Seller Pseudonym	Randomly generated and changed on a random cycle	MP server	12 bytes
Card Pseudonym	Randomly generated and changed on a random cycle	MP server	12 bytes
3DAS™ Card Key	Data Table of 3DAS™ Marker	Operator	80 bytes
Card Pseudonym	Randomly generated and changed on a random cycle	MP server	12 bytes
3DAS™ Card Key	Data Table of 3DAS™ Marker	Operator	80 bytes
Card Pseudonym 3DAS™ Card Key	Randomly generated and changed on a random cycle As many as maybe required to meet merchant Volume		
Payment Method Type	E*MERGE® wide standard used to define if the method is MasterCard, Visa, Check, Micro-payment …	Merchant	4 Bytes
Payment Method Pseudonym	Randomly generated and changed on a random cycle	MP server	12 bytes
EFTPOS Interface	Internal pointer to the appropriate EFTPOS Interface	Acquirer and operator	As necessary
Payment Details	Static Information required to complete EFTPOS Message	Acquiring Bank	Variable - based on Acquiring Bank EFTPOS specifications
Payment Method Type	E*MERGE® wide standard used to define if the method is MasterCard, Visa, Check, Micro-payment …	Merchant	4 Bytes
Payment Method Pseudonym	Randomly generated and changed on a random cycle	MP server	12 bytes
EFTPOS Interface	Internal pointer to the appropriate EFTPOS Interface	Acquirer and operator	As necessary
Payment Details	Static Information required to complete EFTPOS Message	Acquiring Bank	Variable - based on Acquiring Bank EFTPOS specifications
Payment Method	As many as required		

B) Set up and Maintain Merchant Payment Details

Based on the interfaces and procedures that were agreed between the Acquiring Banks and the E*MERGE® MP Server operator, the necessary details will be defined and input into the E*MERGE® Merchant Profile.

Within this record the operator will define the payment methods that this seller will be allowed to accept as a means of payment utilizing the E*MERGE® mechanism. Based on the capabilities of E*MERGE® and its associated secure characteristics, the seller can achieve similar terms to those now associated with card present transactions, now also over the Internet.

In defining the content of the data element "payment details" of this record, the static information described in the underlining specification of the EFTPOS interface will be employed. This static information will allow the E*MERGE® MP Server to complete the requisite EFTPOS message as agreed by the associated Acquiring Bank.

At regular intervals and as agreed between the Acquiring Banks and the operator there is data held in these records that might need to be updated. Simultaneously, the seller may elect to add new payment methods to the list or change its Acquiring Bank.

C) Implement E*MERGE® Merchant OLTP Server

After the seller has agreed to join the E*MERGE® system the seller must organize to upgrade its existing Internet on line transaction processing system to employ E*MERGE® as its preferred mechanism for effecting payments over the Internet.

It is assumed that several software suppliers will develop standard software capable of supporting the E*MERGE® solution and that the seller will simply select the version that best meets the needs of their particular environment and requirements.

The software will require integration at three points in the seller's environment.

- During the shopping experience when the seller’s system believes that the buyer is going to purchase something the E*MERGE® Merchant OLTP control software pings the buyer’s PC to ascertain if an E*MERGE® Browser Plug-in exists. The E*MERGE® Browser Plug-in can display to the buyer that the seller uses E*MERGE®. Assuming a positive acknowledgement, the next step in the E*MERGE® process would take place or the seller would default to another less protected payment mechanism.
- At the stage that the buyer has agreed to purchase goods and after the seller prepares the final invoice the E*MERGE® Merchant OLTP control program takes control. It prepares the 2) Seller’s Invoice, and sends it to the buyer, it then waits message 3) Buyer Commits to Purchase from the buyer and finally receives message 7) Notify Seller of Acceptance confirming the banks approval.
- The final module goes into the seller's goods delivery infrastructure. In the case of soft goods delivered via the Internet, this module acts immediately following positive acknowledgement to the request for payment authorization. In the case of physical goods, this module acts immediately after the seller has delivered the goods. The purpose of this module is to format the request for payment on delivery and handle the submission of these records to the E*MERGE® MP Server. Links from this module to existing exception processing modules and cash management systems would also be introduced to assure reconciliation and appropriate error handling procedures.

D) Purchase 3DAS™ Reader

One of the key functions of this control software is the management of the E*MERGE® Merchant OLTP Merchant Profile and the generation of the requisite 3DAS™ Signatures that are used to assure transaction integrity and merchant authenticity.

The next step in the merchant implementation process is to acquire the appropriate number of 3DAS™ Readers and install them within the merchant's Internet environment. These readers will come with a set of software drivers and software that must be inserted into the environment being built to integrate E*MERGE® into the merchant's eCommerce set-up.

The 3DAS™ Readers that will be employed on the seller side of the E*MERGE® system can be identical to those employed on the buyer side. For larger sellers where volumes of purchases require several 3DAS™ Readers to sign the seller invoice it is anticipated that a rack mounted version of the reader will be required. This rack-mounted version will probably include a server responsible for handling communications with the 3DAS™ Readers and performing certain functions of the E*MERGE® process, as are efficient.

E) Issue 3DAS™ Cards

When the E*MERGE® MP Server operator is comfortable that the seller is ready to go into operation, a number of 3DAS™ Cards must be registered in the E*MERGE® Merchant Profile and delivered to the seller. The number of cards that will be required is a function of the peak volume of purchasing activity that can be expected to occur on a seller site and the delays that the seller considers acceptable in the creation and delivery of the invoice to a buyer.

At the time that the card is produced and personalized a read of the 3DAS™ Marker must take place. The data table created during the personalization process is the 3DAS™ Key and in fact will be the result of two or more reads of the marker that are used to derive the 3DAS™ Key. This information is registered in the E*MERGE® Merchant Profile within the database held by the MP server and created during the step **B) Set up and Maintain Merchant Payment Details** on page 67.

F) Register 3DAS™ Cards

After the 3DAS™ Keys are loaded onto the MP server a unique CD[35] or diskette is prepared for mailing to the seller simultaneous with the cards being sent.

When the seller receives the 3DAS™-enabled Card, and depending on if a diskette/CD was sent or a URL was printed, the seller will be instructed to enter some command into the E*MERGE® Merchant OLTP Control Software. This action will activate the payment profile initialization process of the E*MERGE® system.

This process will take place

- ✓ Every time the seller receives a new card.
- ✓ Whenever a new payment method is added a seller's 3DAS™-enabled Card

Any number of ways exist to facilitate these essential updates ranging form employing a CD or including as part of any communications session between the E*MERGE® Merchant OLTP Control Software and the E*MERGE® MP Server.

[35] It is also possible to save the cost of the diskette/CD by simply creating a unique URL associated with the merchant and print that on an instruction form sent out when the delivering the card to the merchant.

During this initialization process the E*MERGE® Merchant OLTP Control Software will either read from the diskette or attach to the URL and load the E*MERGE® Merchant OLTP Merchant Profile. During this registration process, the seller is to insert the 3DAS™ Cards into the readers. The E*MERGE® Merchant OLTP Control Software will ask each 3DAS™ Reader to read the 3DAS™ Marker inserted inside it and generate a 3DAS™ Signature using the seller pseudonym, a seller secret[36], the data and the time. It will then connect to the E*MERGE® MP Server and request authentication of each of the seller's cards. The MP server will locate the seller profile, perform card authentication and respond accordingly.

The Public Key of the MP server will also be loaded into the E*MERGE® system so that the E*MERGE® Merchant OLTP Control Software can be confident that it is receiving updates and confirmations of payment and buyer authentication from the legitimate E*MERGE® MP Server.

[36] Acknowledging there is a risk that a criminal may intercept the card and attempt to register it fraudulently. It is therefore prudent to employ a secret that only the E*MERGE® Merchant Payment Server and the merchant know in the fields used to generate this 3DAS™ Signature. This is identical mechanism to that described in section 5) Activate Consumer on Payment Server**.**

E*MERGE® Merchant OLTP Merchant Profile

Name	Description	Size
Seller Pseudonym	Randomly generated and changed on a random cycle	12 bytes
E*MERGE® MP Server Address	URL of MP server on the secure VPN	Variable
Card Pseudonym	Randomly generated and changed on a random cycle	12 bytes
Card Pseudonym	Randomly generated and changed on a random cycle	12 bytes
Card Pseudonym	Randomly generated and changed on a random cycle	12 Bytes
Payment Method Type	E*MERGE® wide standard used to define if the method is MasterCard, Visa, Check, Micro-payment …	4 Bytes
Payment Method Pseudonym	Randomly generated and changed on a random cycle	12 bytes
Payment Method Type	E*MERGE® scheme wide Standard used to define if the method is MasterCard, Visa, Check, Micro-payment …	4 Bytes
Payment Method Pseudonym	Randomly generated and changed on a random cycle	12 bytes
Payment Method	As many as required	

G) Activate Merchant on Payment Server

Assuming that the merchant enrolment completed successfully and the E*MERGE® Merchant OLTP Control Software and associated merchant eCommerce on line transaction processing system OLTP additions passed any tests that were defined, the E*MERGE® MP Server will identify the merchant as active.

Now that the Merchant has been activated or until the merchant or its Acquiring Bank state otherwise, the E*MERGE® MP Server will:

1. Accept requests for payment from E*MERGE® CP Servers
2. Issue appropriate merchant authentication information to the CP server
3. Handle the communications with the Acquiring Bank side of the EFTPOS network on behalf of the merchant
4. Inform the merchant of the status of each request for payment authorization

Appendix 8 - Exception Processing With E*MERGE®

In all electronic systems exists a possibility that errors will occur and that procedures must exist to assure successful resolution and continued operation.

Key to the E*MERGE® architecture is that it provides a secure interface between the insecure Internet and the secure EFTPOS networks employed to assure the shift and safe execution of payment transactions. Therefore, exceptions in the EFTPOS environment must be extended into the E*MERGE® environment and appropriate mechanisms to support them must exist.

Operational issues always occur and it is important to recognize that the Internet protocols do not have within them inherent capabilities to support transactional activity.

EFTPOS Exception Processing

The E*MERGE® system offers a mechanism that allows the consumers, merchant and banks involved to prove that the following conditions occurred.

- A seller sent a signed invoice to the buyer.
- The buyer agreed to purchase the goods based on the content of the seller's signed invoice at a particular price with a particular payment method.
- Both the seller and buyer held valid 3DAS™-enabled Cards at the time of the purchase and this card was used to sign the terms and conditions of that transaction.[37]
- The conditions they claim in respect to the transactions were as recorded by the trusted E*MERGE® Payment Server operators.
- The Issuing Bank with the support of the CP and MP Server authenticates both, the seller and the buyer and perform an on-line authorization.

Therefore, the only exception that can occur is that the merchant did not fulfill the obligations as set down in the invoice agreed by the two parties.

If either the buyer or the seller produce the original invoice the counterpart can validate that that was the original invoice sent or received. If necessary, an arbiter can perform a similar validation if a neutral party is required to intervene to arbitrate the dispute between the two parties.

In essence, the dispute is outside the payment system. It is an issue between the seller and buyer.

Assuming the seller agrees to resolve the dispute in the buyer’s favor then the only action that the E*MERGE® system must be able to handle is the reversal of the transaction. To achieve this result the MP server issues a credit against the original transaction employing normal payment system procedures. Acknowledging that the payment servers have kept a log of the original transaction, it can format a credit message by using the reference number of the transaction provided by the buyer or the seller. The actual means of effecting the transaction can be through an Internet screen using the 3DAS™ mechanism to sign the authorization of a credit or via a human interface employing some other method of authentication.

[37] Obviously, if the card was reported lost or stolen and it had been authorized by the Issuing Bank then another exception has occurred and would be handled the way those same exceptions are handled today.

In the event that the seller does not agree to the buyer's complaint then the buyer has the right to an appeal based on the conditions agreed in the invoice or the terms defined by the banking association responsible for payment method being employed. What the E*MERGE® system can do is assure the authenticity of the token employed by the seller ***and*** buyer at the time of the transaction and can assure all parties that this was a unique and irrefutable transaction.

One other mechanism used to reverse a transaction is a charge-back. In this case the financial transaction is handled outside of the E*MERGE® environment. The only reason that the E*MERGE® system would need to be aware is in the event that other value added services are included in the operators offering to either the buyer or the seller.

Other exceptions will relate to the improper maintenance of the seller and buyer profile or situations where a seller or buyer has been removed from the banks' systems before the E*MERGE® Payment Servers has been notified. In these cases, the EFTPOS system will return an error or exception message in response to the request for authorization. Based on the agreement reached with the involved banks actions will take place within the payment server to status the seller or buyer profiles and inform the involved parties accordingly. Actions that may be taken could extend to attempting to connect to the E*MERGE® Browser Plug-in or E*MERGE® Merchant OLTP Control Software. Upon connection, the plug-in or control software maybe requested to delete the related payment profile.

Each payment method may have unique requirements on how to handle exceptions. The design team will deal with each of them during the E*MERGE® detail design of each payment method. By design the E*MERGE® system interfaces with the EFTPOS on-line, therefore financial risk is always made after due electronic consultation with the seller's and buyer's bank. This, therefore, reduces the number of actions that could be required by the E*MERGE® system when attempting to react to exceptions issued by the EFTPOS systems.

Operational Issues

- There will be situations where, for some reason, one or more parties to a transaction disconnects from the Internet.
- There will be situations where the EFTPOS system does not respond.
- There are also situations where failures may occur due to an interruption of software or hardware.
- There will also be situations where the EFTPOS systems fail and require the E*MERGE® system to reverse the transaction or act according to the specifications defined for those exceptions by the authority responsible for that EFTPOS scheme.

The E*MERGE® system is designed around a series of independent components that are each individually responsible to monitor the progress of the payment transaction. They shall also be responsible to recover from abnormal conditions that may occur.

Each component will maintain a log that allows it to determine what actions it performed and the perceived state of that action. This is achieved by interrogating its logs and matching the condition recorded against the logic of the 8-step E*MERGE® transaction process. Through this process, the component will be able to ascertain what the state of every previously executed transaction is.

Examining a few specific conditions helps to articulate how this recovery mechanism will work.

- **Loss of connection to the EFTPOS environment.** Each EFTPOS environment includes means of assuring successful delivery of messages and a set of recovery procedures. As part of the design of these interfaces the operator of the E*MERGE® MP Server will have to make sure that all conditions are met and appropriate. The E*MERGE® Specification may have to be amended to include new exception messages. These exception messages will allow the E*MERGE® MP and CP Servers to communicate these exceptions to the seller and buyer. The working assumption is that if the buyer has sent message 4) Request Payment Authorization to the payment server or the seller has sent message A) Request for Payment on Delivery then both, the seller and the buyer, are expecting completion and the banks and the payment servers shall pursue within the confines of the EFTPOS specifications to effect completion.

- **Buyer loses the Internet Connection**. For any number of reasons the connection to the Internet will fail.

If this was to occur after the seller receives message **3) Buyer Commits to Purchase** and before the E*MERGE® Browser Plug-in sends message **4) Request Payment**, the seller will assume the buyer has agreed to the purchase. In fact, the banking system has not attempted to approve the payment.

Two events will occur sometime after losing the buyer’s connection to the Internet.

The merchant server will not receive message **7) Notify Seller of Acceptance** from his MP server. The seller should not begin delivery of goods and record an exception.

The buyer reconnects to the Internet. At this stage the E*MERGE® Browser Plug-in becomes active again and notes that message 4 had not been sent. The E*MERGE® Browser Plug-in could automatically decide to submit message 4. If some proscribed time limit has not passed or it could notify the buyer and ask the buyer to contact the seller and request status on transaction with reference number

If the connection is lost before the buyer plug-in has sent message **3) Buyer Commits to Purchase** to the seller, the E*MERGE Plug-in closes with an invoice awaiting buyer's agreement. When buyer reconnects to the Internet, the plug-in restarts and can display the pending invoice restarting at step i) Select Payment Method. Assuming the buyer confirms positively, the plug-in can attempt to send message 3 to the seller. If the seller has not timed out the transaction all is well. Otherwise, the seller’s server will reject the message and the buyer will have to connect to the seller and restart shopping process.

- **Loss of a message from the E*MERGE® Browser Plug-in to the CP server**. Assume that message **4) Request Payment** successfully left the buyer's computer but was not received by the E*MERGE® CP Server. In this case both the seller and the E*MERGE® Browser Plug-in thinks that the payment will be completed. Two events will occur after this Internet failure.

The E*MERGE® Browser Plug-in is awaiting the receipt of message 8) Notify Buyer of Seller Authentication & Payment Approval, which should be received in a period proscribed by the payment method. After this time limit has expired the plug-in, if the Internet connection is available, can send an exception message to the CP server requesting the status of transaction Ref#. If the CP server is unaware of the Ref# then an appropriate response is returned and the plug-in can re-send message 4. The merchant server is awaiting receipt of message **7) Notify Seller of Acceptance** from his MP server. If it is not received in the proscribed time-scale then merchant should stop delivery of goods and record an exception. Given that plug-in has in-built recovery log the merchant server should hold this commit to purchase as pending for some acceptable period.

In both cases the E*MERGE® scheme will have to define lower and upper time limits for each payment type.

- **Loss of a message from the Merchant OLTP Server to the E*MERGE® Browser Plug-in.** If the buyer does not receive the invoice from the merchant server the E*MERGE® Browser Plug-in has not started processing the transaction. In this case, it is up to the buyer to notice that the seller has not responded and re-issue the request to purchase.

The merchant server will notice that the same buyer has requested a repeat of the send of the invoice and re-send the last transaction with the same Ref# and 3DAS™ Signature. In the event that the seller's system has timed out the transaction it may have to prompt the buyer to reconfirm the content of the shopping basket and process the transaction through the 3DAS™ process again.

The previous transaction that was logged under a unique Ref# will remain pending in the merchant log. At some point in time the merchant E*MERGE® Merchant OLTP Control Software will note that neither message 3 nor message 7 was received and will void the transaction.

- **Loss of a message from the buyer plug-in to the merchant server.** If the seller does not receive message 3 but eventually receives message 7[38], an exception has occurred. If the seller only logs message 3 and does not act then, from the merchant server's point of view, the only requirement is to make sure that all data elements, normally received in message 3, are included in the merchant server's log. If the seller normally acts on message 3 then the seller must cause the actions that occur on receipt of message 3 to take place first, then continue processing as normal.

- **In the event the buyer's Internet connect is lost before delivery of soft goods.**

If the seller's download procedure requires that the buyer remained connected to the Internet until the seller receives 7) Notify Seller of Acceptance and the buyer receives 8) Notify Buyer of Seller Authentication & Payment Approval and the buyer prematurely disconnect, then the seller must assume that the buyer is not going to receive the soft goods. Therefore, the seller will have to credit the buyer based on the requirement of the payment method employed.

For example, if the payment method employed is a debit card and employs the ISO 8583 1200[39] messages the seller will have to submit a request to credit the buyer's account. This will operate in a manner similar to the process employed in the event of a buyer dispute. The merchant would use the reference number to ask the MP server to reverse the transaction. The MP server would format an appropriate message as defined by the EFTPOS system.

If conversely the seller has an e-mail address for the buyer, they can send e-mail to the buyer instructing them on how to download the product, or, the seller could include the file in the download.

If the seller was to employ the E*MERGE® Browser Plug-in soft good download initiation capability, the seller would simply status the matching download receiver to await a request for download from the buyer's 3DAS™ plug-in.

[38] Within message *7) Notify Seller of Acceptance* are all of the data elements that the merchant will require to assure an irrefutable transaction.

[39] The ISO 8583 1200 series of messages are used to post to the consumer's account at the time the transaction was approved and do not utilize a further clearing message as is typical in credit card transactions.

- **Loss of messages from the E*MERGE® MP Server to the merchant server**. The establishment of the technical interface between the MP server and the merchant server will be, due to volume considerations, much more robust and may in fact employ other communications channels than the Internet. At this stage in the design of the E*MERGE® system the assumption is that there will be a transaction type that allows the merchant server to request the status of transactions by submitting the Ref#. The payment server would then respond by sending a copy of message 7, if previously sent, or a new message 7.

- **Loss of messages from the merchant server to the E*MERGE® MP Server.** If a request for status message is sent and a response is not received within a proscribed period, the merchant server would simply re-send the request. In the case of message A) Request for Payment on Delivery the seller will wish assurance that these messages have been received and properly processed. During the technical design, it will be necessary to define a response message that is sent periodically to the seller confirming receipt of a series of message A(s).

During the technical design, further situations will be identified. The guiding principle is that one of the E*MERGE® components will identify what should have occurred and either assume failure and await the buyer to restart the shopping experience or attempt to identify which message did not complete and restart the transaction at the stage when it failed.

Given the simplicity of the 3DAS™ E*MERGE® process, maintaining the state of the transactions is straightforward. The only known event that will result in the buyer having to intervene is if the E*MERGE® Browser Plug-in is unable to reconnect to the Internet before the seller times out the transaction. In this case, the buyer still wishes to buy the goods and restart the shopping process or the seller simply does not make a sale and purges the invoice from the system.

Hardware and Software Issues

The other set of operational issues that can create problems is the interruption of any element of the software or hardware associated with the buyers, sellers or payment servers' configuration.

Consumer Hardware of Software Interruption

As is often the case, situations arise within the hardware or operating system that might damage the E*MERGE® Browser Plug-in, its environment or the E*MERGE® Browser Consumer Profile.

Obviously, the easiest means of recovering the machine is by using the standard backup and recover procedures. Unicate accepts that this is not a judicious assumption and that no user backs up their machine frequently enough to totally re-establish a damaged E*MERGE® environment.

The working assumption of E*MERGE® is the KISS principle "Keep It Simply Simple".

The recover should simply require the consumer to insert the installation CD (received with the 3DAS™ Reader). The installation CD would determine the extent of the damage and reload those elements. Assuming it can locate and validate the logs and consumer profiles, the consumer is ready to purchase over the Internet again secure in E*MERGE®.

In the event of damage to the consumer profile or the log, the plug-in simply needs to connect to the appropriate E*MERGE® CP Servers and initiate the log and/or profile recovery mechanism. Each payment server operator is responsible to maintain logs and operate recovery mechanisms designed to support such a situation.

If the E*MERGE® Browser Plug determines that the log or profile is corrupt it will ask the consumer to insert the first of their 3DAS™-enabled Cards.

In the event that the consumer profile is corrupted there might be just enough information in the PC to identify the address of the E*MERGE® CP Server and the Consumer Pseudonym.

If the E*MERGE® Browser Plug-in is unable to determine the address of the CP server or the Pseudonym, several methods exist to assure successful recovery.

- It could locate the E*MERGE® Mobility File if a protected memory chip is present.
- It could ask the consumer to insert the CD the Issuing Bank sent with the card.
- It could default to prompting the consumer to enter the Issuer Id as found printed on face of the card. It would then prompt the consumer to enter their ID (e.g. name and sequence number) exactly as printed on the card. The E*MERGE® Browser Plug-in can now derive the address of the payment server; www.issuerID.3DAS.org.

Independent of how the address is determined the plug-in formats a recovery message and connect to the E*MERGE™® CP Server to the URL with the extension /recovery and initiates the recovery procedure. The payment server will prepare the necessary recovery files and instruct the plug-in to continue[40].

Identical to the process described in 4) Initialize and Authenticate Buyer and Card on page 61 the payment server will authenticate the 3DAS™ enabled card[41]. Once the card and consumer are authenticated the plug-in will download the files required to restore this card's E*MERGE® Browser Consumer Profile.

If the log file was also corrupted, with the exceptions of those messages not received by the payment server, the CP server will prepare a download of the log allowing the plug-in to complete the rebuild of that card's environment. In order to protect consumer privacy the only element that the CP server will not be able to reconstruct is the detailed content of the invoices[42].

The browser will request the consumer to enter the next card and attempt to recover that cards profile and log.

In the event that the failure was to occur during a transaction, after the above outlined re-initialization is complete, the E*MERGE® Browser Plug-in should be able, with the assistance of the E*MERGE® CP Servers, to reconstruct exactly where it was, using the process described in the section Operational Issues on page 72.

[40] If a criminal steals the card, he might fake out the system making it believe that the consumer's PC is damaged. Therefore, it is prudent for the operator of the consumer payment server to validate that it is the rightful consumer. How, is left to the discretion of the Issuing Bank and the payment server operators involved?

[41] The one problem Unicate recognizes is that the consumer has misplaced the secret distributed to them with the 3DAS™ enabled Card. In this event, a customer service representative through an on-line dialogue can request the consumer enters other privileged information

[42] With the exception of situations where the consumer wishes to dispute a transaction, their loss would have no effect. In the event of a dispute, the consumer would have to rely on the merchant to provide a valid copy of the invoice. In any event the consumer will be able to validate that the invoice presented by the merchant was the same one that the consumer originally received and signed with his 3DAS™ Card.

Using the same logic already discussed, the plug-in should be able to successfully complete all transactions that reached the stage where message **4) Request Payment** had been sent. If a major failure occurred between the transmission of message 3 and before message 4, then the working assumption must be that the merchant will not receive a confirmation of payment approval and will assume the consumer aborted the transaction.

Merchant OLTP Server Interruption

The situation with the interruption or corruption of the merchant server is much more complex and their loss of E*MERGE® functionality will be the least of the merchant's problems. It is also assumed that the merchants will be much more prudent in making back-ups of their systems and the architecture of the environment will include RAID databases, operating system restoration procedures and application level recovery.

All transactions that were executed up until the time of interruption are still in process and therefore if delivery is not to happen then the MP server operator will have to identify and effect a reversal of these transactions.

The operator of the E*MERGE® MP Server, as part of their right to operate will have to demonstrate the ability to successfully handle such merchant failures without causing the consumer any harm or effecting the financial integrity of the consumers, merchants or banks involved.

E*MERGE® Payment Server or Secure VPN Interruption

The design of this trusted environment assumes these systems are 100% reliable and have build in mirroring capabilities and employ robust data base management systems and communications protocols designed to assure 100% reliability and uptime.

Working with these assumptions the only situation that can be foreseen is a complete failure of a payment server or the VPN. In this event the parties that are associated with the failed component will lose the ability to effect E*MERGE® payments until the system is restored.

The integrity of the E*MERGE® system is the fact that the payment servers can be trusted. Built into the E*MERGE® specifications will be performance criteria that defines the obligations of the operators and a standard process to assure adherence to the minimum performance and quality standards.

Appendix 9 - SET Clear Motivations & Technically Complex

Quoting from SET Secure Electronic Transaction Specification Book 1: Business Description it provides a clear description of the role of an Internet payment mechanism

> *" The development of electronic commerce is at a critical juncture.*

- *Buyer’s demand for secure access to electronic shopping and other services is very high.*

- *Sellers want simple, cost-effective methods for conducting electronic transactions.*

- *Financial institutions want a level playing field for software suppliers to ensure quality products at competitive prices.*

- *Payment card brands must be able to differentiate electronic commerce transactions without significant impact to the existing infrastructure.*

- *The next step toward achieving secure, cost-effective, on-line transactions to satisfy market demand is the development of a single, open industry specification."*

Unicate is in full agreement with these principles but is concerned that the expense of SET will in fact hold back the forecasted growth of business to consumer-based eCommerce. Quoting from an article published by the Shroud Partnership stated in 1997, 1998:

> *"All the technical and organizational elements seemed to be in place, but from the news that has been emerging about the various pilot schemes it would seem that all is not well. Many of the problems seem to be caused by the complexity of the SET process."*

They go on to say:

> *"In an effort to ensure that consumers are satisfied that their credit card transactions are safe it seems that the whole process has been over-engineered. The huge collective marketing clout of the SET members will be needed to overcome consumer resistance to the complexity of the transaction and the reluctance of merchants to invest in the necessary IT services and equipment to enable it to be used."*

SET embeds digital certificates and private keys in the buyer's insecure PC. This creates obstacles to the buyer's ability to shop using a diverse array of devices such as those found at home, in the office, in a cyber cafe or at a friend’s house. The owners of SETco and its advocates see the solution to this need for buyer mobility as the integration of smart cards "EMV" with SET. Yet, if the United States is a sample of how quickly smart card adoption will occur, it will be years before buyers have the freedom they demand.

After reviewing the status of SET implementations and visiting shops on the Internet, it is clear that there is little or no progress in SET becoming a globally accepted standard. Many banks have explored the idea of implementing SET but with the exception of limited trials no one has begun a full scale roll-out. Simultaneously, when talking with vendors of SET software interoperability between different vendor implementations is a major concern. Plans exist to alleviate this problem by the introduction of a cumbersome certification process and as of July 1999 only one vendor can successful state that it has a compliant implementation.

In parallel, there is a ground swell of negative opinion and publicity surrounding SET and several major telecommunications vendors are saying they will not implement SET because of its inherent technical complexity and their belief that this complexity was intentional.

Numerous critics of SET argue that it is overly complicated and demands excessive computation power. Numerous merchants have expressed concern at the cost of implementing SET and cannot countenance the computational burden resulting from SET's public key implementation. Everyone has expressed frustration with the complexity of the SET protocol. Systems integrators, frustrated by the fact they cannot guarantee their clients that the SET implementations will be interoperable, are antagonistic towards SET. Many wonder why SET bears no resemblance to ISO 8583, the familiar payment architecture that is employed to process payment transactions. Finally, there are industry experts that ponder if SET is yet another attempt by the payment associations to guarantee themselves revenue.

With SET's slow move from pilot into commercial deployment, many merchants have adopted SSL. They embraced SSL since it is capable of securing (within the limits of the law) the content of messages traveling between two points on the Internet. SSL is also capable of providing and performing PKi based authentication services. SSL does not secure sensitive information held inside Personal Computers and Merchant Servers. These computers are the obvious and profitable weak point for hackers to attack. All this being said SSL does not meet the security requirements of the financial institutions. Moreover, with SET being the banking systems agreed approach this complicates using SSL as a means of authentication.

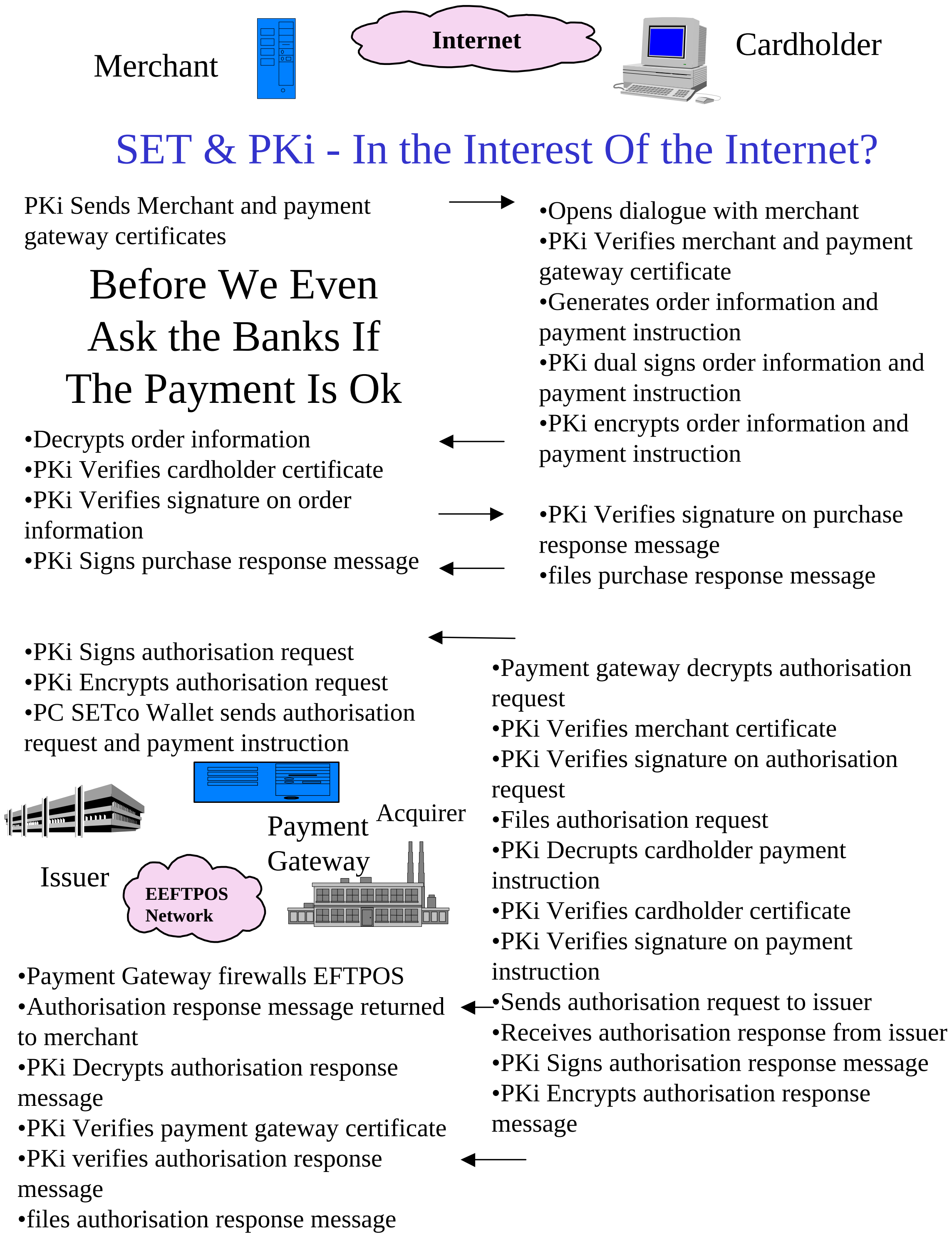
Many are looking to alternate solutions that in many cases resemble the solution Unicate is proposing but they forget two very important factors. First, they require the existence of a complex public key architecture, which the banks must agree to support. Second, they do not have a clear solution to the issue of mobility without requiring the introduction of expensive EMV like smart cards.

To complicate matters, there is work underway to merge SET and EMV. Many believe this merging will require that one or both specification will have to relinquish its objective of backward compatibility. - Net result many existing implementations will become obsolete.

Furthermore, if EMV is to dictate the technical specifications of smart card readers associated with personal computers and other Internet access devices the cost to the buyer will be staggering.

Not to put to fine a point on it, Microsoft has recently announced its Windows for Smart Card operating system. It is now discussing with hardware vendors the integration of inexpensive smart card readers into every Personal Computer. This begs an interesting question; will this Microsoft Smart Card Compatible reader also be EMV compliant? - At this time, the answer is NO!

SET PKi flow chart as explained at a conference by Racal Security Systems



SET & PKi - In the Interest Of the Internet?

PKi Sends Merchant and payment gateway certificates

- •Opens dialogue with merchant
- •PKi Verifies merchant and payment gateway certificate
- •Generates order information and payment instruction
- •PKi dual signs order information and payment instruction
- •PKi encrypts order information and payment instruction

Before We Even Ask the Banks If The Payment Is Ok

- •Decrypts order information
- •PKi Verifies cardholder certificate
- •PKi Verifies signature on order information
- •PKi Signs purchase response message

- •PKi Verifies signature on purchase response message
- •files purchase response message

- •PKi Signs authorisation request
- •PKi Encrypts authorisation request
- •PC SETco Wallet sends authorisation request and payment instruction

- •Payment gateway decrypts authorisation request
- •PKi Verifies merchant certificate
- •PKi Verifies signature on authorisation request
- •Files authorisation request
- •PKi Decrupts cardholder payment instruction
- •PKi Verifies cardholder certificate
- •PKi Verifies signature on payment instruction
- •Sends authorisation request to issuer
- •Receives authorisation response from issuer
- •PKi Signs authorisation response message
- •PKi Encrypts authorisation response message

- •Payment Gateway firewalls EFTPOS
- •Authorisation response message returned to merchant
- •PKi Decrypts authorisation response message
- •PKi Verifies payment gateway certificate
- •PKi verifies authorisation response message
- •files authorisation response message