Global Information Assurance Certification Paper

Visa's 3-D Secure™: Secure Online Payment Authentication

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option -1 Research on Topics in
Information Security

Submitted by: Dominique Singer, February 20, 2005
Location: SANS Conference – Seattle, WA -November, 2004

Abstract

Most credit card purchases on the Internet today are unauthenticated purchases; the cardholder enters the card number, and then completes the purchase. These purchases are known as "card-not-present" [1] purchases, where the merchant, Issuer, and cardholder are potentially exposed to fraud because the identity of the cardholder cannot be confirmed. An e-consumer only needs to know some easily obtainable personal information (e.g. address of residence) and possess the credit card, in order to make an online purchase. In such potential cases of fraud, charges to the card usually have to be reimbursed to the cardholder. Coupled with this profit loss, a decreased consumer confidence in online shopping also occurs.

3-D Secure™, developed solely by Visa, aspires to reduce online fraud and increase consumer confidence, by requiring identity verification of the cardholder before every online purchase. The verification of the identity involves challenging the cardholder with a pre-arranged 'shared secret,' and a correct response from the cardholder, before the purchase is authorized. The 'shared secret' is something the cardholder must have personally registered with the Issuer (i.e. of the credit card), and the Issuer must confirm registration of the 'shared secret' back to the cardholder.

3-D Secure delivers assurance to the cardholder and the Issuer that the use of the credit card can only be used for an online purchase by the approved cardholder. This is possible because it can be safely assumed that only the cardholder and the Issuer know the 'shared secret.' Finally, since Visa requires the use of encrypted network communications for all 3-D Secure™ transmissions, 3-D Secure provides a secure, trustworthy, layered approach to verifying the identity of a cardholder before an online purchase can be completed.

The Model

3-D Secure™ defines a model of roles and responsibilities for all parties involved in online credit card payment purchases. 3-D Secure™ literally means "3-Domains," wherein distinct domains of responsibility are assigned: the Issuer Domain, the Interoperability Domain, and the Acquirer Domain. Each Domain has a certain level of obligation which they must fulfill, verified and certified by Visa, in order to participate in 3-D Secure™ transactions, also known as "Verified by Visa." [2]

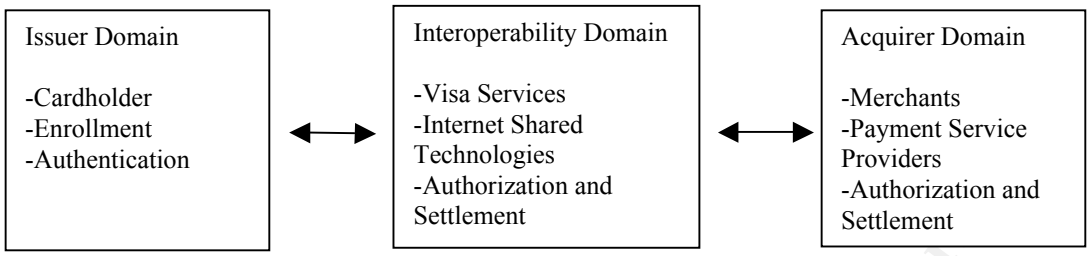

Figure 1 – The Domains and their responsibilities

The model prescribes bundling 3-D Secure™ application data within existing, secure Internet communication protocols. It also mandates the use of digital certificates to verify the identity of each participant. Embedding the application data, or 'shared secret,' within secure protocols, provides a reliable, encrypted, identity-affirmed, and layered approach to securing the use of a credit card on the Internet.

"Visa has developed the Three-Domain Secure (3-D Secure™) protocol to improve transaction performance online and to accelerate growth of electronic commerce. The objective is to benefit all participants by providing Issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of Visa cards and improving transaction performance." [3]

In order to achieve this objective of consumer and Issuer confidence in the security of online transactions, the cardholder and the Issuer must have mutual assurance of each other's identity. Both parties must also be assured that the purchase was intended to be made solely by the cardholder. Finally, there must also be certainty that the data communications for the purchase will not be prone to eavesdropping.

General Overview

The **Issuer Domain** includes the cardholder, and the traditional Issuer of a Visa credit card. This can be any qualified company that is authorized by Visa to issue Visa credit cards. This domain is responsible for the enrollment of cardholders into 3-D Secure™. The Issuer is also responsible for authenticating cardholders during every online transaction, after enrollment. Next, we have the **Interoperability Domain.** This domain entails the Internet, and all associated systems, technologies, and protocols responsible for transporting data between the Issuer, Acquirer, and into the VisaNet. The VisaNet, among other things, provides services for 3-D Secure™; such as authentication history, and enrollment directory services. The **Acquirer Domain** includes the merchants and traditional Acquirers. Merchants provide items for sale online, and Acquirers provide payment authorization and settlement services, known as 'payment service providers.' The Acquirer domain also involves defining procedures to

ensure that 3-D Secure™ merchants' transactions are operating within compliance of Visa standards.

Issuer Domain: Enrollment Process

The Issuer is entirely responsible for the enrollment process, which includes enrolling the cardholder and registering the 3-D Secure ™ cards with Visa. The Issuer must first reserve a range of numbers, to be used exclusively for 3-D Secure™, and then register that range of numbers with Visa, as 3-D Secure™ cards. The Issuer must decide for which cardholders, and in which regions, 3-D Secure™ will be implemented. The Issuer must build an infrastructure to support enrollment, and then deliver the card to the cardholder, along with instructions for how to enroll in 3-D Secure™. Finally, the Issuer also provides Customer Support for enrollment.

To enroll the cardholder, the card may be issued with instructions to visit a website, in order to enter personal information that identifies them, and only them. This may be a password, a PIN, or a Personal Assurance Message. It is something which only the cardholder knows, and then submits to the Issuer on the enrollment website. The Issuer validates this 'shared secret,' and notifies the cardholder that the authentication information has been received, and securely stored. At this point, cardholder enrollment in 3-D Secure™ is complete.

Every time a cardholder attempts an online purchase, the Issuer verifies this 'shared secret;' provided the merchant is participating in 3-D Secure™. To authenticate the cardholder, a secure, mutually authenticated request is generated from the e-merchant's software to the Access Control Server, which securely displays the 'shared secret' web page to the Cardholder, for proof of identity.

Access Control Server

The **Access Control Server** (**ACS),** also within the realm of the Issuer, comprises the systems which store and validate the 'shared secret.' During enrollment, a record of the cardholder's card number, as well as the 'shared secret,' is stored in the ACS. If the online merchant is participating in 3-D Secure™, the ACS is contacted by special merchant software when the cardholder attempts an e-purchase, and the ACS delivers the secure challenge page. If the merchant is not participating in 3-D Secure™, the online transaction will proceed as a normal credit card transaction, without challenging the cardholder for the identifying information.

The Issuer can buy, build, or outsource the hardware and software needed to perform this function. But in order to activate the ACS, Issuers must pass compliance tests performed by Visa. These compliance tests certify a level of

trust in these critical systems, and their data communications, which is required, in order to become a 3-D Secure™ participant. [4]

Interoperability Domain

The **Interoperability Domain** encompasses the Internet, underlying systems of data transport communications, common protocols, and shared services; such as VisaNet, Visa Directory Server (VDS), and the Authentication History Server (AHS). Operated by Visa, the VDS receives queries from an e-merchant's software and determines if a card number is within a valid range for 3-D Secure™ authentication. If the number is within the appropriate range, the VDS will then reply to the merchant with an address for the appropriate Access Control Server (ACS).

Regardless of authentication success or failure, the ACS forwards a duplicate record of its response to the Authentication History Server (AHS), for every 3-D Secure™ authentication attempt. This information is then stored in the AHS, for archival purposes. A copy of any authentication record is available to Acquirers and Issuers, upon request, for dispute resolution.

Finally, VisaNet is also within the Interoperability Domain. After a successful payment authentication, the VisaNet receives the authorization from the Acquirer, forwards this to the Issuer, and provides traditional settlement and clearing between the Issuer and the Acquirer. VisaNet also involves the systems which deliver the Directory Service and the Authentication History Service.

Acquirer Domain

The **Acquirer Domain** encompasses the merchant and the Acquirer. The merchant provides the Internet e-commerce storefront, and accepts Visa credit cards for purchases. Essentially, the Acquirer is a "Visa member financial institution that enters into a contractual relationship with merchants for the purpose of accepting Visa cards" for payment. [5]

After successful authentication, the Acquirer receives authorization (for funds available) requests from the merchant, and forwards the request to the traditional authorization and settlement system (i.e. VisaNet, or the Issuer). The Acquirer delivers the authorization response to the merchant, and submits the completed transaction to the settlement system. Acquirers are also responsible for ensuring that merchants are compliant with Visa's Cardholder Information Security Programs (CISP/AISP). [6]

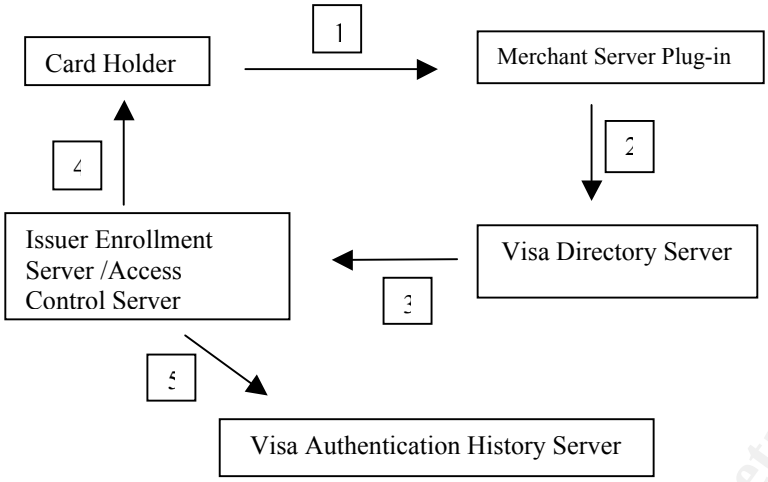

Figure 2 - Simplified Flow of 3-D Secure™ authentication requests

Visa Requirements

In order to participate in 3-D Secure™, Issuers, merchants, and Acquirers must pass Visa compliance tests. In addition to the requirements for 3-D Secure™, participants must also fulfill general Visa credit card data handling agreements before participation. This adds an additional layer of security, by requiring all parties to handle cardholder data in accordance with prescribed security procedures and methodologies. Visa certifies compliance with these standards by performing regular audits of all businesses managing credit cardholder data. [7]

Cardholder Information Security Program (CISP)

One such requirement is Visa's Cardholder Information Security Program (CISP), mandated by Visa in 2001. This is a requirement for all Issuers, merchants, and Acquirers involved in managing Visa cardholder data and transactions. Essentially, the CISP ensures that Issuers, merchants, Acquirers, and all inter-related systems operate at the highest possible levels of system security.

The CISP is a program containing documents and a series of specific, technical guidelines to implementing secure electronic systems. Additionally, Visa Merchants are required to pass annual audits, quarterly network scans, and other CISP compliant tests. Their risk and importance is determined by their total number of annual transactions. Finally, by their agreement, Visa members are held liable for all problems arising from non-compliance with CISP guidelines.[8] [9]

Account Information Security Program (AIS)

The Account Information Security Program (AIS) is another testing criterion which must be passed by the Merchants, Issuers, and Acquirers (payment service providers). This program outlines 15 areas of security which must be addressed before being validated and certified compliant. [10]

Product Integration Testing (PIT)

The PIT is a testing environment which Visa provides, to test and certify implementations of 3-D Secure™ components. All 3-D Secure™ components are required to pass certification before they become 'activated,' which means they will be able to participate in 3-D Secure™ online transactions. This is achieved primarily within the PIT, where rigorous application testing against established Visa standards occurs. [11]

3-D Secure™: Application Details, Authentication Flow

To Begin the exploration of 3-D Secure™, an understanding of the applications and their functions is essential. Each piece performs a specific function, and resides within a clearly defined Domain of responsibility. It is this application data which provides the first layer of security; in this case, the challenging and transmission of the cardholder's 'shared secret.' This application information must then be transmitted over encrypted, authenticated network channels.

Merchant Server Plug-in (MPI)

The 3-D Secure™ e-merchant incorporates a Merchant Server Plug-In (MPI) into their e-commerce website. The MPI can be developed in-house, contracted to a 3rd Party, or purchased as a service provided by Visa. The MPI determines if a given transaction requires 3-D Secure™ authentication, and if required, sends an eligibility request to the Visa Directory Server (VDS) for verification of enrollment.

Visa Directory Server

The Visa Directory Server maintains a database of all active 3-D Secure™ card accounts. If the card is eligible, the VDS will parse the record of the card number; and reply with the URL for the appropriate Access Control Server (ACS). The MPI then invokes a secure 'inline' Internet browser page on the cardholder's computer, displaying the ACS authentication challenge page from that URL. This page is only transmitted over secure, encrypted communication channels (HTTPS).

The cardholder enters the 'shared secret,' and submits this authentication response to the ACS challenge page. Once the authentication response is

submitted to the Access Control Server, the ACS reports the results back to the MPI, and then returns control of the 'shopping experience' back to the merchant software. At that point, the 3-D Secure authentication process is complete, and the transaction then proceeds normally for authorization and settling of the purchase.

Authentication History Server

When the ACS responds to the MPI, it also sends a duplicate transmission of the response to the Authentication History Server (AHS), regardless of success or failure of the authentication. The purpose of the AHS is historical recording, for use in dispute resolutions. The Authentication History Server is also administered and maintained by Visa.

Secure Network Communications

3-D Secure™ requires confidentiality, assurance of message delivery without being changed (integrity), and assurance of the identity of the message source and destination. SSL/TLS and a Public Key Infrastructure (PKI) deliver these requirements. To provide confidentiality, SSL/TLS delivers encryption; but it is very important to note, however, that simply implementing a strong encryption algorithm (key strength) doesn't mean that the 3-D Secure™ systems, or communication channels, ought to be considered secure. Layered security must be implemented, where a strong focus upon security in all areas from applications, network connections, to key storage, is of paramount importance. 3-D Secure™ provides this layered security in many areas: Visa certifications and audits of 3-D systems' implementation, 'shared secrets,' and the use of digital certificates to authenticate the identity, encrypt the traffic, and provide message integrity for all data communications.

The Shopping Details

Visa requires that all 'shopping cart' data communications travel over existing, well-known, secure protocols such as Transport Layer Security (TLS), and SSL (Secure Sockets Layer). These protocols provide the framework for what is known as a Public Key Infrastructure (PKI). Compliant implementations of PKI are a fundamental requirement by Visa for 3-D Secure™. In order to appreciate the contribution which these layers of security provide, it is first important to understand some of the working details of these protocols.

Secure Transport Protocols

The Secure Sockets Layer (SSL) protocol delivers reliability and security between two communicating applications, by providing encrypted network

channels of communication. SSL consists of two layers, the "Handshake Protocol and the Record Protocol." Among other responsibilities, such as maintaining state for a reliable connection, the Handshake Layer negotiates keys to use for session encryption, encryption strength, and the algorithm for Message Digests. The Record Layer is primarily responsible for encrypting the application data, and then delivering it to the transport communications protocol (TCP) for reliable network transmission. [12]

The Transport Layer Security protocol is an enhanced replacement of SSL. It is often referred to interchangeably with SSL, but this is technically incorrect. TLS provides enhancements and more encryption options, and is referred to as TLS version 1.0, or SSL version 3.1. For purposes of discussing 3-D Secure™, however, these secure transport protocols will also be referred to as SSL/TLS.

"TLS specifies a private end-to-end connection, optionally including strong mutual authentication, using a variety of cryptosystems. Initially, a handshake uses three subprotocols [SIC] to set up a record layer, authenticate endpoints, set parameters, as well as report errors. Then, there is an ongoing layered record protocol that handles encryption, compression, and reassembly for the remainder of the connection." [13]

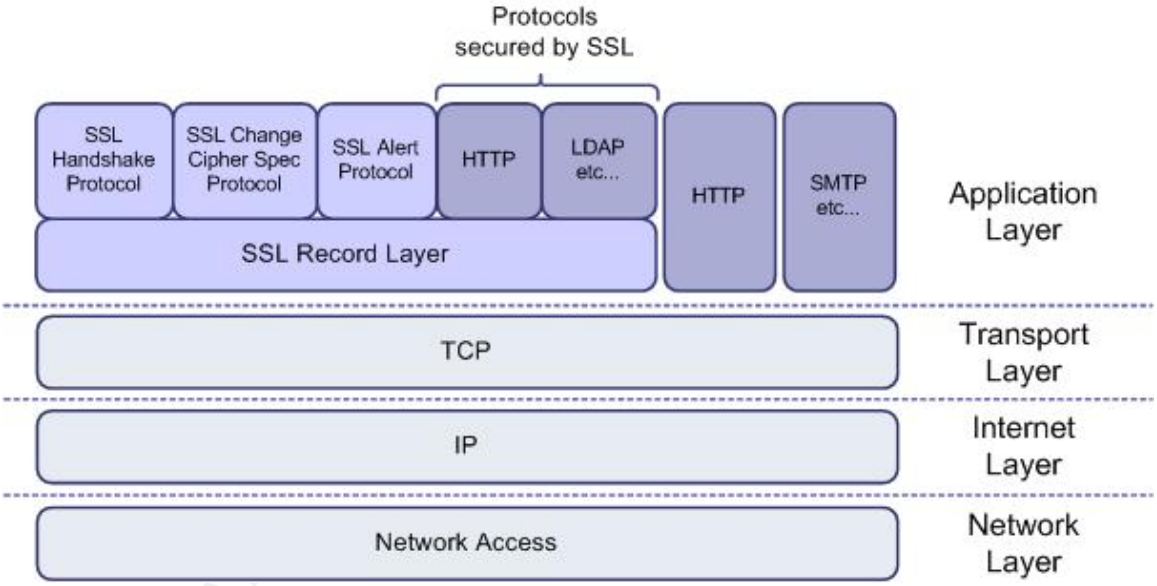

Figure 3 - SSL sub-protocols in the TCP/IP model (Artur Maj, used by permission)[14]

The SSL/TLS protocols provide encryption, message authentication, and integrity assurance for application data communications. For 3-D Secure™, SSL/TLS is required to exchange the 'shared secret,' and the credit card information. As Figure 3 depicts, the HTTP application data can be embedded within the SSL/TLS protocols, becoming an HTTPS (HTTP + SSL/TLS) data communication. This is the most common type of e-commerce transaction on the Internet today.

The Secure Socket Layers: In Brief

As mentioned, the SSL/TLS Handshake Protocol establishes criteria between both network endpoints, negotiating parameters to secure the session. This involves key strength and type negotiation, possible digital certificate exchange, agreement upon the algorithms for message authentication, and the optional agreement of data compression algorithms.

The SSL/TLS Record Layer is responsible for receiving the bulk data from the application (HTTP), breaking it into single-bit (stream), or fixed-length chunks (block-cipher) of data, and then applies the encryption algorithm. The Record Layer optionally compresses, and authenticates the data with a 'message digest.' The receiving network SSL/TLS layer endpoint decrypts, decompresses, and verifies every data message. It then delivers that data to the application layer. The application layers on each end are essentially oblivious to this encryption/decryption process. [15]

Symmetric and Asymmetric Encryption

To better understand the levels of security which SSL/TLS deliver for 3-D Secure™, it is also important to understand general details about encryption. There are two common methods of encryption, both of which are employed in SSL/TLS. Symmetric encryption involves using one key for both encryption and decryption. It is much faster to encrypt data with symmetric encryption, and is commonly used for application data, and bulk data transfers. Asymmetric encryption involves two keys, one for encryption and one for decryption. This type of encryption is often referred to as public/private key encryption, which entails the concept of a key ring, or key pair. The key pair is a digital file which contains the public and private key. The private key is kept private, and only the public keys are exchanged.

SSL/TLS: Symmetric Encryption

The SSL/TLS protocol's initial handshake negotiates the key strength and type, and based upon that agreement, a single key is created, exchanged, and used to encrypt the preliminary session. Using such a single key for encrypting and decrypting data defines symmetric encryption. Optionally, the negotiated SSL/TLS security parameters can also define a period of time the key will be valid, after which a key re-negotiation must be initiated.

SSL/TLS: Asymmetric Encryption

In asymmetric encryption, each party wishing to establish an encrypted network connection must exchange a portion of their key pair with which they encrypt and decrypt data communications. This portion is called the public key, and only the public keys are exchanged between the two parties. Asymmetric encryption involves using one key for encryption, and a different key for decryption.

The private key is the mathematical complement of the public key, and is therefore the only key which can decrypt messages encrypted with the corresponding public key. Each party uses the *other* party's public key to encrypt the message they wish to send. Each party uses their private key to decrypt (decipher) the encrypted messages. Only the holder of the private key, generated simultaneously with the public key, can decipher a message encrypted with the corresponding public key.

SSL/TLS provides the ability to exchange public keys with the Handshake protocol. Both network endpoints (the web browser and the e-merchant shopping cart) have software capable of communicating with the SSL protocol. The client (HTTP browser) endpoint requests a secure connection to the server (shopping cart), and this establishes the SSL/TLS protocol (HTTPS) connection.

"The elements of the handshake sequence, as used by the client and server, are listed below:

1. Negotiate the Cipher Suite to be used during data transfer
2. Establish and share a session key between client and server
3. Optionally authenticate the server to the client
4. Optionally authenticate the client to the server" [16]

Public Key Infrastructure

In addition to SSL/TLS, which encrypts the network connection with negotiated encryption methodologies, 3-D Secure™ requires the use of a Public Key Infrastructure (PKI) for data communications between the cardholder, merchant, and the VisaNet. 3-D Secure™ requires that all data communications are authenticated, i.e. all communicating parties digitally affirm their identity. Furthermore, all messages must be confirmed to have been unmodified during transmission. These requirements are delivered by a SSL/TLS and a Public Key Infrastructure (PKI). [17]

Digital Certificates

PKI entails the use of digital certificates, which are the equivalent of an electronic identity for the holder of the digital certificate. Digital certificates contain personally identifying information; such as name, business, role, and other contact information. Digital certificates also contain the public key of the party referenced in the digital certificate. The purpose of digital certificates, therefore,

is to make a public key readily available, and to authenticate the identity of that public key holder. For authenticity assurance, the digital certificate is digitally signed by an independent authority.

Certificate Authority

For 3-D Secure™ and most e-merchant storefronts, digital certificates are 'digitally signed' by what is known as a Certificate Authority (CA). There are many Certificate Authorities; two of the most common are Verisign and Thawte. These CA's perform a variety of functions, but the most important is providing ultimate authority on the validity of any given digital certificate. The purpose of a CA is to provide an independent authority, which affirms the identity and integrity of the public keys contained within a digital certificate.

All certificates issued by a Certificate Authority have a specific lifetime. If the certificate needs to be invalidated for any reason, a Certificate Revocation License (CRL) is issued by the CA to expire that certificate, while simultaneously referencing the new certificate. A CRL will alert any party attempting to encrypt data with the public key found within the certificate that the certificate is expired, and should not be trusted. A function within PKI involves the checking for this status prior to attempting encryption.

Message Digests

The encrypted data message can be sent through another mathematical algorithm, utilizing the message, and a random bit of numbers. This creates a summary of the message known as a 'message digest.' The message digest provides assurance of the integrity of the message because the encrypted (confidential) message is passed through a specific, known mathematical algorithm, and combined with a random number of unique bits (the algorithm determines the 'randomness' of the 'random bits'). This one-way function cannot be reversed, recreated, or forged, because of the randomness of the unique bits.

The receiving SSL/TLS endpoint, having negotiated this 'hash' algorithm in the Handshake, uses the algorithm to verify the message digest has not been altered. If the message were somehow decrypted, or otherwise altered, a new message digest would have to be created, and a different set of random numbers would have to be used to create the digest. If the digest is different, the algorithmic 'checksum' will not affirm the integrity of the data message, and will therefore discard the data message. This algorithm is optionally negotiated in the SSL/TLS handshake, and is one case where TLS provides more options than SSL. [18]

Digital Signatures: Proof of Authorship

Finally, to provide mutual authentication, each party checks the digital signature of the digital certificates, compared to the signature of the encrypted data message. This is merely another mathematical function involving the message digest and the private key. Once the message digest is created, it can be encrypted using a private key and an algorithm, such as the Digital Signature Algorithm (DSA), as implemented by the Digital Signature Standard (DSS).

Since the private key is only available to one entity, this function provides a unique output. That output is known as the Digital Signature, and can be used to authenticate SSL/TLS data exchanges, as well as affirm the identity within digital certificates. This is possible because the complement of that private key, the public key, is used to verify the signature. [19]

3-D Secure™: Riding the Layers of Security

Utilizing these prevalent, secure protocols and standards, 3-D Secure™ delivers a secure authentication mechanism for online payments. Not only are 3-D Secure™ transactions traversing encrypted channels, but the integrity, confidentiality, and authenticity of the data messages are ensured by means of digital certificates, message digests, and digitally signed messages. The cardholder is thoroughly protected.

Wrapping Up the Sale: 3-D Style

The cardholder visits the merchant's e-commerce storefront, and decides upon items they wish to purchase; both parties are participants in 3-D Secure™. The cardholder selects the "BUY" option, and this invokes the merchant's secure 'shopping cart.'

The Cardholder Commits

The web browser and the merchant's e-commerce server establish a secure, digitally authenticated network connection. The merchant challenges the cardholder for the credit card, the cardholder enters the card number information, and then clicks "BUY" (or some similar mechanism).

The Merchant Server Plug-In (MPI), a critical application component of 3-D Secure™, recognizes the card number to be within a range for 3-D Secure™ transactions. The MPI and the Visa Directory Server (VDS) exchange digital certificates, which are digitally signed (required) by each party, and establish a

secure, mutually authenticated network session. The MPI transmits a Verify Enrollment Request (VEReq) to the Visa Directory Server. The Directory Server then affirms or denies the enrollment status of the card number with a Verify Enrollment Response (VERes).

Authentication

If the cardholder is enrolled in 3-D Secure™, the VDS response will contain the web address of the Access Control Server (ACS). The MPI then negotiates an SSL/TLS 'inline' web browser connection, from the cardholder's computer, to the Access Control Server. The ACS replies with an HTML form to the cardholder. This form contains the Purchase Authentication Page, which challenges the cardholder for the 'shared secret.'

Embedded within the form are hidden fields which contain purchase transaction data, and merchant specific state information (application integrity checking). When the cardholder submits the 'shared secret,' the MPI then issues a Payer Authentication Request (PAReq) to the ACS. The ACS replies with a Payer Authentication Response (PARes), which affirms or denies the validity of the match between the ACS record, and the cardholder's 'shared secret' input. [20]

Validation and Archival

If the cardholder is authenticated, the Payer Authentication Response (PARes) from the ACS will include a Transaction Status message, and a Card Authentication Verification Value (CAVV). Both of these values have new message digest values, ensuring their integrity. The MPI validates the reply from the ACS, by verifying the digital signature of all communications. The ACS then initiates a secure SSL/TLS connection to the Authentication History Server, and submits a duplicate record of the transaction to the Server. This occurs regardless of the success or failure of authentication, for the purpose of archive and dispute resolution. All of these messages are digitally signed, verified, and stored on the AHS.

Once the MPI receives an affirmative response from the ACS, the merchant software will then proceed with the authorization exchange with the Acquirer. The MPI releases control of the 'shopping experience' back to the merchant's e-commerce software. The authorization request is processed by the Acquirer in the traditional manner for settlement processing of credit card transactions. This process may be encrypted as bulk data delivery to 3rd parties, known as batch processing, or it may be a secure process developed in house, and approved to meet Visa Guidelines and Regulations. If the authentication fails, the transaction will not be allowed to proceed. [21]

Implementation Considerations

Implementation covers the areas each member of 3-D Secure™ must address in order to successfully participate in 3-D Secure™ transaction processing. The responsibilities are unique to each domain; Issuer, Acquirer, and Interoperability, with minimal impact to the cardholder. Implementation publications are available only to Visa Members, from a Visa representative, and clearly outline the technical requirements.

Issuer Domain

The Issuer must develop a coherent business plan to deploy a 3-D Secure™ compliant system. Underlying technologies and initial cardholders must be chosen. An Enrollment process and Customer Service support must be developed. The Issuer must build an infrastructure upon PKI; and support, develop, or outsource the following key 3-D Secure (TM) components:

A. Enrollment Server
B. Access Control Server
C. Secure Web Server

In order to deploy these systems, the Issuer must operate an approved PKI, which includes the generation and secure storage of public/private keys, as well as digital certificates. They must actively monitor and audit these systems. Finally, they must satisfy all of Visa's security requirements, by proving functionality within the Product Integration Testing (PIT) environment. When 'server activation' is achieved, the systems are eligible to become a participant of 3-D Secure™.

Acquirer Domain

The main consideration within the Acquirer Domain is for the merchant, and involves the implementation of the Merchant Server Plug-in (MPI) into existing e-storefront software. The merchant must implement an approved 3-D Secure™ MPI system, or they can outsource it to an approved 3rd Party. The MPI provides the primary authentication functionality for 3-D Secure™ purchases, and Visa has published several documents which cover the details of the MPI. [22]

Acquirers must "determine the Merchant's eligibility to participate in the 3-D Secure service." Acquirers handle "authorization responses," and settlement between merchants and the VisaNet. As it pertains to the actual authentication mechanisms, however, the Acquirer Domain has little interaction. [23]

Interoperability Domain

The Interoperability Domain includes the Internet, VisaNet, and the underlying technologies involved in secure network communications. Operated exclusively by Visa, VisaNet requires the use of secure communications for all data exchanges. For 3-D Secure™, VisaNet includes the Visa Directory Server, the Authentication History Server, and traditional authorization and settlement services.

Visa must provide, deploy, and operate two types of services:

A. Interoperability Services
    a. Visa Directory Service
        1. provide enrollment responses to MPI requests
        2. maintain active database of Issuer enrollments and URL records for reaching the Access Control Server
    b. Authentication History Service
        1. must be able to receive history messages from the ACS
        2. Secure Archival
        3. Used for dispute resolution
B. Enabling Services
    a. Enrollment Service (for Issuers)
    b. Proof of Attempt Service [24]

Conclusion

Visa's 3-D Secure™ authentication system provides a definitive solution to confirm the identity of the cardholder, every time they attempt to make an online purchase with their credit card. The model defines a secure architecture, which implements secure core internet protocols, digital identity standards, and clear definitions of all participant's roles and responsibilities.

From an application perspective, 3-D Secure™ provides a reliable form of authenticating the identity of the cardholder. By requiring the cardholder to first register a 'shared secret' with the Issuer, and then challenging for that 'shared secret' during every 3-D Secure™ online purchase, the Issuer, merchant, and cardholder can be assured that the identity of the cardholder will be confirmed.

In addition to this layer of security, 3-D Secure (TM) requires encrypting the application data ('shared secret'), and implementing a Public Key Infrastructure. The PKI affirms the identity of each source and destination for all 3-D Secure™ data exchanges; between Merchants, Issuers, Acquirers, and VisaNet, ensuring that these communications occur only with intended parties, and will not be prone to eavesdropping. This layered approach to security makes 3-D Secure™ a

reliable and trustworthy mechanism to prove the identity of a Visa credit cardholder during an online purchase. Indeed, 3-D Secure directly reduces the potential for fraud, and increases consumer confidence that their credit card will only be used by the actual 'owner' of the credit card, during online, "card-not-present" purchases.

Glossary

Access Control Server (ACS): A server, or group of servers, which performs the 3-D Secure (TM) function of verifying the 'shared secret' of the cardholder
Acquirer: Visa member financial institution with a contractual relationship with a merchant for the purposes of accepting Visa cards. The Acquirer also performs the traditional role of receiving/forwarding authorization/settlement messages.
Acquirer Domain: systems and functions of the Acquirer and its customers, such as merchants.
AISP: Visa Account Information Security Program
Authentication: Process of verifying that the person making an e-commerce purchase is entitled to use the payment card.
Authentication History Server: Component within interoperability domain that archives authentication activity for user by Acquirers/Issuers for dispute resolution and other purposes.
Authorization: Process which an issuer approves transaction for payment
CRReq: Card Range Request
CRRes: Card Range Response
Interoperability Domain: Facilitates the transfer of information between Issuer and Acquirer Domains
Issuer: Visa member financial institution that issues Visa cards
Issuer Domain: systems/functions of issuer and cardholders
Merchant: Entity that contracts with Acquirer to accept Visa cards and manages online shopping experience.
Merchant Server Plug-in (MPI): A 3-D Secure (TM) software application which functions with the online merchant's existing 'shopping cart' infrastructure
PAReq: Payer Authentication Request: message from the Merchant Server Plug-in (MPI), to the Access Control Server (ACS), requests verification of cardholder's 'shared secret.'
PARes: Payer Authentication Response: message-formatted, digitally signed, application message sent from the Access Control Server (ACS) to the Merchant Server Plug-in (MPI), providing the results of the 3-D Secure (TM) cardholder authentication.
VEReq: Verify Enrollment Request: message from MPI to Visa Directory Server or from Visa Directory Server to ACS, asking whether authentication is available for particular card number.
VERes: Verify Enrollment Response: Message from ACS or Visa Directory Server, telling MPI whether authentication is available.
Visa Directory Server: Server/hardware/software entity, operated by Visa in Interoperability Domain, processes CRReq and VEReq messages and **creates** CRReq and (in some situations) VERes messages.
VisaNet: Systems, services through which Visa delivers online financial processing, authorization, and clearing and settlement services to members.

References:

Visa's overall approach to security, including their latest initiatives, can be found at this URL:

http://corporate.visa.com/md/fs/ecommerce/main.jsp

The "Visa Documents" referenced below can be retrieved from the following URL:

http://www.international.visa.com/fb/paytech/secure/main.jsp

Endnotes:

[1] "Fraud Control Basics." February, 2002. URL: http://usa.visa.com/business/accepting_visa/ops_risk_management/card_not_present.html?it=c|/business/accepting_visa/ops_risk_management/index%2Ehtml|Card-Not-Present

[2] At the time of this writing, it appears that Visa is moving from 3-D Secure terminology to "Verified by Visa," more information can be found at this URL: https://usa.visa.com/personal/security/vbv/index.html

[3] Visa Document: "3DS_70015-01_System_Overview_external_v1.0.2_May_2003." chapter 1, p.7.

[4] Visa Document: "3-D Access Control Server," chapter 2, p. 17.

[5] Visa Document: "Acquirer-Merchant_Implem_Guide," chapter 3, p. 23.

[6] "Cardholder Information Security Program." December, 2004. URL: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html?it=l2|/business/accepting_visa/ops_risk_management/vbv%2Ehtml|Cardholder%20Information%20Security%20Program#anchor_2

[7] Visa Document: "3DS_70015-01_System_Overview_external_v1.0.2_May_2003," chapter 10, p. 62.

[8] "Payment Card Industry Data Security Standard." URL: http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

[9] "Cardholder Information Security Program." December, 2004. URL: http://www.visa.com/cisp

[10] Visa Document: "3DS_70016-01_Security_Requirements," chapter 2, p. 14.

[11] Visa Document: "Acquirer-Merchant_Implem_Guide," chapter 1, p. 10.

[12] Thomas, Stephen. SSL and TLS Essentials. New York: Wiley Computer Publishing, 2000.

[13] "Upgrading to TLS Within HTTP/1.1." May, 2000. URL: http://www.ietf.org/rfc/rfc2817.txt

[14] "Apache 2 with SSL/TLS: Step-by-Step, Part 1." January, 2005. URL: http://securityfocus.com/infocus/1818 (used by permission)

[15] Thomas, Stephen. SSL and TLS Essentials. New York: Wiley Computer Publishing, 2000.

[16] "Mod_SSL: Session Establishment" January, 1998-2001. URL: http://www.modssl.org/docs/2.8/ssl_intro.html

[17] PKI involves many more interesting details beyond the scope of PKI within 3-D Secure ™. Austin, Tom. PKI. New York: Wiley Computer Publishing, 2001.

[18] Davis, Carlton. IPSEC, Securing VPN's, New York: McGraw-Hill (RSA Press), 2001.

[19] "Digital Signature Standard (DSS)." May, 1994. URL: http://www.itl.nist.gov/fipspubs/fip186.htm

[20] Visa Document, "3DS_70000-01_PS_Core_Functions," chapter 6, p. 74.

[21] Visa Document, "3DS_70000-01_PS_Core_Functions," chapter 5, p. 39

[22] "Visa Authenticated Payment Program, 3-D Secure™." January, 2003-2004. URL: http://www.international.visa.com/fb/paytech/secure/main.jsp

[23] Visa Document: "Acquirer-Merchant_Implem_Guide." chapter 23, p. 23.

[24] Visa Document: "3DS_70015-01_System_Overview_external_v1.0.2_May_2003," chapter 6, p. 41.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS