

The Advanced Payments Group



Online Debit on the Internet

Models and Guidelines

Summary Version

© *The Network Executives Council*

This document may be freely reproduced and distributed without alteration.

Prepared by Benton International

Table of Contents

Executive Summary	1
An Online Debit Transaction for Internet Purchases	4
Internet Debit: Three Models	8
Guidelines for Internet Debit	10
Table of Guidelines	15

Glossary	36
-----------------	-----------

Executive Summary

The following document is a summary of the Advanced Payments Group's (APG) activities towards developing guidelines for online debit on the Internet. The APG is a chartered sub-committee of the Network Executive's Council (NEC) of the Electronic Funds Transfer Association (EFTA). Members of the NEC include the Chief Executive Officers of the eight largest regional online debit networks.

Recent activities by established payments industry players, as well as start-ups, have demonstrated that the online debit infrastructure is the subject of ever-greater interest by those active in the new economy. Independently, the regional network industry has recognized, through the NEC, the need for a real-time, secure, and economically rational payments method for the Internet. The online debit infrastructure they represent constitutes a ready means to satisfy that need.

However, recognizing the networks' value in this situation in principle only is insufficient to make its application a reality. The values of the online debit infrastructure in the physical world, such as payments immediacy, security, and finality, are delivered today in a highly controlled environment under rules that make these values possible. Directly adapting the technology and infrastructure to the Internet, while obviously feasible, may not result in a payments mechanism that enjoys the same level of benefits. The goal of the APG, therefore, was to determine *what* needs to be controlled in the adaptation and *how* to control it to achieve at least the same level of value provided in the "physical" world.

Fortunately, technology does not appear to be a constraining factor. Many technology providers have already come forward and demonstrated techniques that, when combined into a system, should deliver the values sought. The job of the networks will be, therefore, to make clear to these providers the minimum requirements placed on the new systems employing online debit on the Internet that will utilize their technologies. In short, the development of *operating rules* that guarantee the values the networks seek.

Therefore, the regional debit networks are not dictating the technological systems that will make online debit on the Internet possible. Rather, the networks wish to establish an open framework that will encourage many solutions, within constraints that protect the networks' and their issuing financial institutions' assets.

The Advanced Payments Group, in this document, presents a summary set of recommendations, termed "guidelines", that individual networks may adopt into their

existing rules to prepare themselves to accept transactions from these new payment systems.

This document contains recommendations made by the Advanced Payments Group of the Network Executives Council to the member ATM/POS networks of that council. These recommendations are not binding upon these networks, and they are under no obligation to adopt them as part of their operating rules.

Any party who plans to develop systems for acquiring online debit transactions from the Internet and subsequently processing these transactions to the ATM/POS networks is strongly advised to contact each ATM/POS network directly for their particular implementation of these guidelines. The purpose of publishing these guidelines to the public is to prepare such parties, so that they may have useful discussions with these networks.

The guidelines are structured around three “models” of online debit on the Internet. These models represent a classification of the expected payment systems that will be presented to the networks for certification. Model 1 describes systems that attempt to adapt traditional Point-of-Sale (POS) debit, with as little modification as possible, to the Internet. It is characterized by existing card bases and self-service POS devices in the home. Model 2 recognizes the significant advances made in cryptology that make possible digital signatures and certificates, as well as chip-based and CD-ROM access devices. This model is characterized by new kinds of “authentication tokens” issued to customers by financial institutions. Model 3 recognizes the existence of payment opportunities that do not require the full extent of online debit benefits, but nonetheless find them significantly more valuable than the alternatives. Model 3 allows non-financial institution “third-parties” to issue authentication tokens to customers and validate their identity themselves. Upon validation, the third-party then launches a payment transaction to the network that does not include those authentication tokens. These third-parties carry the risk and liability for these transactions, and will not be allowed to use them in all commerce situations.

The guidelines have been developed in concert with the expertise of the networks’ technology and operating staff themselves, in conjunction with recognized industry experts. Their recommendations have been compared to the efforts of other organizations promulgating standards for the Internet payments environment. In most cases, the APG recommendations are in line with those organizations, taking departures only when a standard does not provide sufficient protection, or when it

places an unnecessarily onerous burden on the parties that will use these payment systems.

Please note: This document assumes a working knowledge of traditional online debit systems and operating rules.

An Online Debit Transaction for Internet Purchases

Before developing models for online debit on the Internet, it is important to consider whether or not there are characteristics of Internet eCommerce that conflict with the *function* of online debit. In fact, one characteristic presents a significant issue for adaptation of the “real-time” nature of online debit.

In most instances (save fuel purchases), online debit is used for buying goods that are in the possession of customers when payment is tendered. In the mail order environment, this is not the case. Goods or services are delivered after payment is tendered. Credit cards have a facility for separating the transaction authorization from the settlement, online debit does not.¹ Therefore, the APG researched a variety of options, including pre-authorization transactions (as in fuel) and the use of financial institutions as escrow agents to mitigate this problem.

The final consensus was to simply apply an online debit POS purchase transaction *as is* to Internet eCommerce. The caveat is a restriction on merchants to *promise* a shipment² date to customers before payment is tendered. Customers will also be made aware that funds are debited immediately from their account upon ordering.

Merchants must also comply with applicable rules, such as the FTC Rules on Mail Order and Telephone Order Merchandise, where applicable, that require establishment of shipment dates and refunds where shipment dates are not met.

These guidelines assume that all participants, financial institutions and non-financial institutions alike, will be protective of consumer data privacy. They will be required to adhere to statutory and regulatory principles, such as Title V of the Graham Leach Bliley Act, when applicable, and where not applicable, on consumer sensitive, voluntarily adopted and disclosed privacy policies.

Finally, a purchase transaction is only the first of several transaction products that the networks are likely to develop in conjunction with these guidelines. Examples include balance inquiries, funds transfers, point-to-point payments, etc.

¹ Strictly speaking, an online debit transaction could be initiated after the “sale” when shipment can be made. However, security principles demand that authentication tokens not be stored for later use, which would destroy the protective value of online debit for such a transaction.

² The term “shipment” should be construed to include the download of digital data.

SUMMARY



The following table summarizes these and other minor modifications to the existing POS purchase transaction:

PURCHASE TRANSACTION	
Topics	
Transaction Definition	A transaction requested by a customer for the purpose of tendering payment to a merchant where goods or services, or the title to goods or services, are not in the physical possession of the customer before the transaction is requested. Goods may be electronically fulfilled (software, access, etc) or may be shipped.
Sale and Return Policies	
Shipping	A merchant must present to the customer a "no later than" shipment/fulfillment date and/or time for the goods or services being purchased. The customer must explicitly confirm the shipment timing before the merchant may send a transaction request to the processor.
Immediate Debit	A customer must explicitly confirm to the merchant that they understand that funds will be immediately debited from their account upon confirmation of the sale.
Notification	Merchants must post all sales and return policies in a prominent and legible fashion in the shopping environment.
Disputes	
Failure to Ship	If the merchant cannot meet the agreed to no-later-than shipment date, it is highly recommended that it contact the customer or reverse the transaction.

PURCHASE TRANSACTION	
Topics	
Network Participation	<p>that it contact the customer or reverse the transaction.</p> <hr/> <p>Payment disputes are governed by network operating rules. Other disputes, such as fitness, quality or shipment of goods may or may not be governed by network operating rules and are the responsibility of the merchant and its customer as governed by applicable law.</p>

Internet Debit: Three Models

It is well known that online debit provides authentication of the customer to the issuing institution (and thus to the merchant) through a combination of the Personal Identification Number (PIN), and the card itself, with its magnetic stripe encoding of the Primary Account Number (PAN) and other data. This fundamental aspect of online debit must maintain its integrity (even if its *form* changes) when applied to the Internet. Therefore, when classifying payment systems based on online debit on the Internet, we ask: “Who authenticates what?”

In every circumstance the APG has analyzed thus far, the answer to this question can be answered in one of three ways:

- Model 1: The issuing financial institution authenticates the ATM card, PAN and PIN.
- Model 2: The issuing financial institution authenticates a “secret” and other authentication tokens.³
- Model 3: A third-party authenticates a “secret” and other authentication tokens.

The goal of the APG after establishing these models has been to develop guidelines for online debit on the Internet for each. The result has been some guidelines that are broadly applicable to all models, and others that are unique to individual models. The table below summarizes the models:

³ Secrets can be but are not necessarily PINs. The PAN must also be one of the authentication tokens, though it is recommended that an alternate PAN be issued for Internet use only, independent of the PAN associated with the customer’s ATM/POS card. If a password or other non-PIN is translated into the ATM/POS card PIN before presentation to the financial institution for verification, the payment system is still considered “model 2”.

MODEL DEFINITIONS			
Topic	Model 1	Model 2	Model 3
Description	Financial institution authenticates ATM card PAN and PIN.	Financial institution authenticates a secret and other authentication tokens.	Third-party authenticates a secret and other authentication tokens.
Authentication Tokens	ATM card and PIN.	Secret plus additional tokens that must include the PAN.	
Authenticator	Issuing Financial Institution.		Third-Party.
Device	Encrypting PIN pad with magnetic stripe reader.	Various – smart card reader, eWallet, etc.	Various – smart card reader, eWallet, browser w/ SSL, etc.

Guidelines for Internet Debit

With the establishment of the three models, it is now possible to develop detailed guidelines. As noted previously, the guidelines are meant to be adapted by the online debit networks into their operating rules.

By definition, rules are restrictions on the behavior of regulated parties. Rules control parties; they do not control technology, operations, or transactions. Traditional online debit employs rules that govern how *issuers*, *merchants*, *processors* (of various kinds), and the *network* itself are to behave. For online debit on the Internet, a set of regulated parties must also be identified.

To do this, it is helpful to expand the definition of the traditional online debit parties, and to give them some new labels. The Internet presents the normal chain of parties to a transaction in online debit with some obstacles and the models defined earlier give some parties new tasks. Therefore, the APG has settled on three new or redefined parties to online debit on the Internet that not only perform the traditional tasks associated with online debit but also new tasks that operating on the Internet require:

- **Authenticator** – This entity issues and authenticates authentication tokens. It is analogous to the issuer in traditional online debit. However, on the Internet, Authenticators may be deploying a wide variety of new digital identification technologies. In all cases, the customer's financial institution *authorizes* the debit transaction, regardless of whether this financial institution authenticates the customer's authentication tokens.
- **Processor** – This entity processes transactions to the network, the primary task of which is encryption and decryption. It is analogous to the processor in traditional online debit. However, it may have to work with a variety of new authentication token types as well as sophisticated encryption technologies.
- **Deployer** – This entity places devices into service, and by implication, is responsible for the function of these devices. Devices are for the entering and encryption of authentication tokens by consumers. This is a new role built out of responsibilities that processors, issuers and merchants have traditionally undertaken. It is important, however, as the role of the device in online debit on the Internet, especially in models 1 and 2, is heightened.

Merchants and networks are also recognized by the guidelines, but their roles are substantially similar to the ones they perform in traditional online debit.

As organizations perform the tasks identified with these roles, they will be subject to the guidelines that accompany them. Therefore, for a likely example, if a merchant also performs the responsibilities of a processor (after meeting eligibility requirements), it will then be governed as *both* a processor and a merchant. It is likely that many systems will combine the functions of the entities separately defined earlier into one entity. This entity must still meet all of the requirements for the combined functions.

Putting the model definitions together with the newly defined entities, it is possible to define two system architectures for online debit on the Internet; the first for models 1 and 2, and the second for model 3. The purpose of this architecture definition is to show the transaction flow and entity relationships assumed by the guidelines.

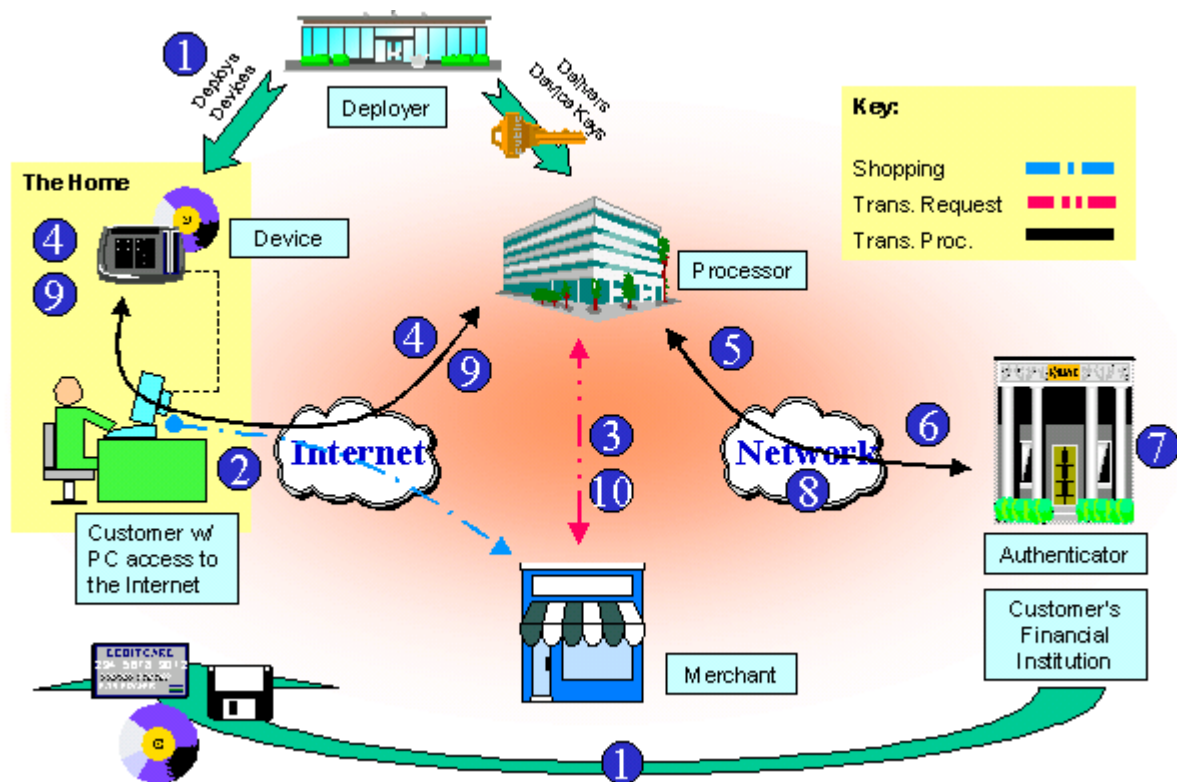


Figure 1, System Architecture for Models 1 and 2

- ① The customer is issued authentication tokens by the Authenticator. The customer also receives a device from the deployer.
- ② The customer shops for an item for purchase (or pays a bill) at a merchant's Internet site
- ③ The merchant sends a transaction request message to the Processor requesting a transaction be initiated.
- ④ The Processor effects a data connection to the customer's device attached to their PC. The customer is prompted to enter their authentication tokens. The device forms a transaction message and sends it to the Processor.
- ⑤ The Processor may re-format the transaction message into a network accepted format (e.g. ISO 8583) before routing the message to the network.
- ⑥ The network routes the message to the Authenticator.
- ⑦ The Authenticator authenticates the authentication tokens and authorizes⁴ or denies the transaction and returns the appropriate message to the network.
- ⑧ The network routes the message to the Processor.
- ⑨ The Processor routes the message to the customer's device.
- ⑩ The Processor informs the merchant of the result of the transaction request.

⁴ See the Table of Guidelines: Authenticator section for definitions of "authenticator" and "authorization".

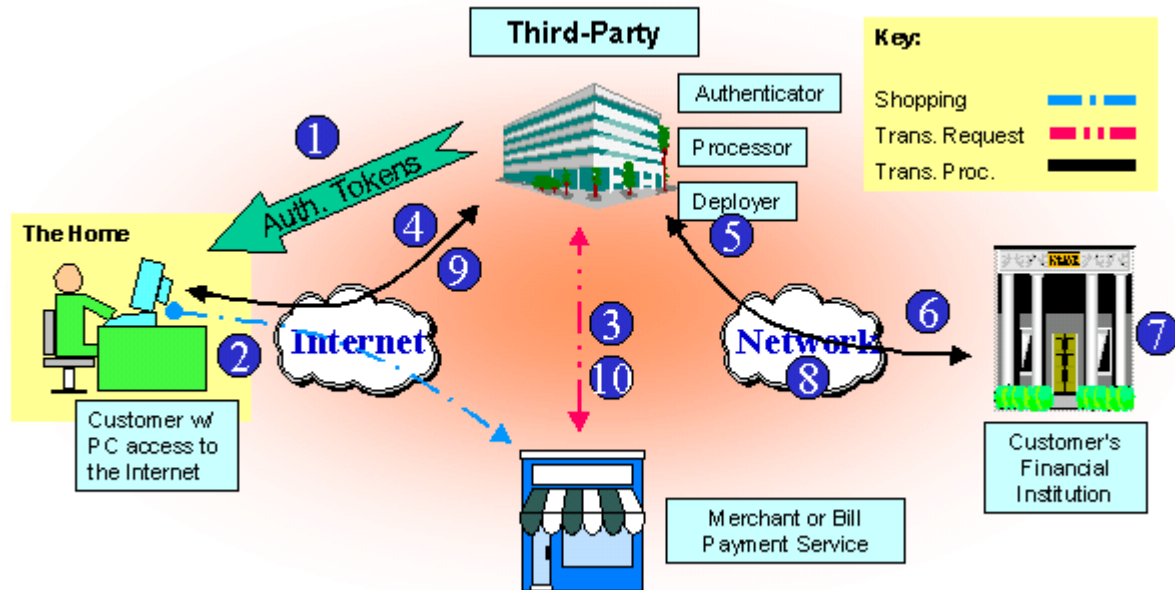


Figure 2, System Architecture for Model 3

- ① The customer is issued authentication tokens by a third-party (such as a consumer portal or a bill pay provider). The customer supplies his debit card PAN to the third-party so that it may route transactions to the network. The customer may receive a device from the third-party.
- ② The customer shops for an item for purchase (or pays a bill) at a merchant's Internet site (or at the third-party directly).
- ③ The merchant sends a transaction request message to the third-party requesting a transaction be initiated.
- ④ The Processor effects a data connection to the customer's PC (or device, if one is used). The customer is prompted to enter their authentication tokens.
- ⑤ The third-party authenticates the customer, forms the transaction message into a network accepted format (e.g. ISO 8583) and routes the transaction message to the network.
- ⑥ The network routes the message to the customer's financial institution.

- ⑦ The financial institution authorizes or denies the transaction based on funds availability *only*. The financial institution does not authenticate the customer and is not liable for the transaction.
- ⑧ The network routes the message to the third-party.
- ⑨ The third-party routes the message to the customer's PC.
- ⑩ The third-party informs the merchant of the result of the transaction request.

Table of Guidelines

The following section contains the table of guidelines developed for Online Debit on the Internet. The guidelines have been constructed under the assumption that they will be *additive* to existing online debit network POS operating rules, not in *replacement* of them. Therefore, where these guidelines are silent on certain subjects, the existing POS rules shall govern.

In addition, security requirements should be considered a minimum for compliance with these guidelines. More advanced security schemes should not be construed to be precluded.

AUTHENTICATOR			
Topic	Model 1	Model 2	Model 3
Definition	An issuing financial institution that creates, issues, and authenticates cards and Personal Identification Numbers (PIN) under the existing POS rules. All “Issuers” participating in POS under the existing rules are model 1 Authenticators.	An issuing financial institution that creates, issues, and authenticates authentication tokens to enable their customers to perform online debit on the Internet.	A network approved, financial institution sponsored third-party that creates, issues and authenticates authentication tokens to enable their customers or members to perform online debit on the Internet.
Authenticator Certification	Existing POS Rules		Third-parties must be certified by the network before they can issue authentication tokens in conjunction with network acceptance marks.
Authentication Tokens			
Specifications	Track 2 data obtained from a card and the PIN.	A financial institution (or its designated agent) issued secret and additional data that must include a PAN. It is strongly recommended that authentication token issuers	A third-party (as approved by the network) issued secret and additional data that must include a PAN or MICR. The network must approve the method the third-party uses to register

AUTHENTICATOR			
Topic	Model 1	Model 2	Model 3
Issuing		use 2-form authentication and a PAN separate from an issued ATM/POS card PAN.	customers and issue secrets.
	Customer qualification	Authentication tokens may only be issued to customers in conjunction with a depository account denominated in U.S. dollars at an insured U.S. financial institution.	The PAN or MICR used to process transactions must correspond to an account at an insured U.S. depository financial institution denominated in U.S. dollars.
	Expiry/renewal	Existing POS Rules	Require that the authentication tokens have an expiration period.
	Customer verification	Existing POS Rules	Require authentication token issuers to positively identify customers before issuing authentication tokens. Refer to "Know Your Customer" principles embodied in the Bank Secrecy Act (31 C.F.R. Part 103).

AUTHENTICATOR			
Topic	Model 1	Model 2	Model 3
<i>Fulfillment (split/activation)</i>	Existing POS Rules	Secrets (such as passwords) must be issued separately from physical authentication tokens (such as cards). Physical authentication tokens must be fulfilled inactive.	
<i>Customer selected authentication tokens</i>	Existing POS Rules	The customer must be able to change the secret.	
Authentication	Existing POS Rules	The Authenticator authenticates the authentication tokens for each transaction. If the Processor does not provide replay protection or message integrity checking, the Authenticator must perform these functions in a manner equivalent to that described in the Processor guidelines.	The third-party authenticates the authentication tokens for each transaction. The network must classify and certify the authentication method.

AUTHENTICATOR			
Topic	Model 1	Model 2	Model 3
Authorization	Transactions are authorized by the customer's Issuing financial institution. Authorization guarantees to the network that the funds represented by transactions authorized under these models will be presented to the network at time of settlement.		
Liability	Issuing financial institution as in the traditional POS rules.		Third-party in conjunction with a sponsoring financial institution. The network may establish minimum requirements for recourse and financial fitness. As sponsors, financial institutions assume financial liability for the compliance of third-parties with network rules.
Merchant Discrimination	Authenticators cannot discriminate among merchants approved to acquire transactions under the model the authenticator participates, other than industry standard practices to protect the authenticator or consumer from fraud or other risks.		
Chargebacks/Disputes	Existing POS Rules - new dispute processes and chargeback codes will be established		

PROCESSOR			
Topic	Model 1	Model 2	Model 3
Definition	The Processor may perform data content re-formatting (e.g., ISO 8583) and must provide secure translation of cryptographic content (i.e., decryption/formatting/encryption) in the transaction message.		The Authenticator
Processor Certification	Processors must be certified before they may acquire transactions under these guidelines.		
Processor Identification	Processors must provide a means by which devices are able to verify that the Processor is valid, e.g., the verification of digital certificates, keys, or other means approved by the network.		N/A
Device Processing			
Transaction Initiation	Processors initiate transaction sequences with devices in response to transaction request messages from merchants. Processors must provide devices with Processor identification information in the transaction initiation message.		N/A

PROCESSOR			
Topic	Model 1	Model 2	Model 3
Device Identification	The Processor must confirm the validity of the device and/or physical authentication token serialization before processing transactions to the network.		N/A
Replay	The Processor must provide and detect session IDs and timestamps in each message to prevent session replay.	The Processor must provide and detect session IDs and timestamps in each message to prevent session replay. The Processor is relieved from this requirement if the Authenticator provides specific protection against session replay.	N/A
Vacant Device Protection	A transaction must complete within a network-mandated number of seconds or it must be reinitiated by the Processor.		
Blocking Devices	Processors must be able to block transactions from unique, hardware-based devices at will. If the device is software-based, this restriction does not apply.		N/A
Transaction Acknowledgement	Processors must verify that transaction responses (approve/deny) are acknowledged by the device and the merchant. If they are not acknowledged the transaction must be		Third-parties must provide a method of informing the customer of the transaction

PROCESSOR			
Topic	Model 1	Model 2	Model 3
	reversed.		response (approve/deny).
Processor Security			
Protection from the Internet	<p>The Processor's network must be protected via firewalls, use a proprietary IP scheme, and implement proper facility security. The IP address of the transaction processing server and access to the server must be masked by a proxy server. All access to transaction processing systems must be logged and monitored. The Processor must have a written procedure for recovering from attacks including but not limited to secure perimeter breach and denial of service. These procedures must include plans for restoring service and for managing public perception of the attack.</p>		
No Storage of Authentication Tokens	Processors may not store authentication tokens, whether encrypted or unencrypted, except as needed to process transactions in real-time. Store-and-forward of authentication tokens is explicitly prohibited. Processors may store non-purchase transactions without authentication tokens for future processing. For these transactions, the Processor will be governed by all of the guidelines for model 3, including the Authenticator and deployer guidelines. The Primary Account Number (PAN) is exempted from this requirement.		Third-parties may store transactions for future processing for certain transaction types. Third-parties may not store purchase transactions. These transactions must be processed in real-time.

PROCESSOR			
Topic	Model 1	Model 2	Model 3
Processor Encryption			
Session	Processors must establish a Secure Sockets Layer (SSL) session between the device and the Processor, using network approved algorithms and key-lengths. The device may use the customer's PC as a proxy device to establish the Secure Sockets Layer session. The server-side certificate must be issued by a network-approved authority. All messages between the Processor and the device must be transmitted under session encryption.		
Message			
Method	All application level cryptographic processing will occur within hardware-based Tamper Resistant Security Modules (TRSM) and all cryptographic processing will use network-approved standard algorithms.	All application level cryptographic processing will occur within hardware or software-based Tamper Resistant Security Modules (TRSM) and all cryptographic processing will use network-approved standard algorithms.	N/A

PROCESSOR			
Topic	Model 1	Model 2	Model 3
<i>Data that will be encrypted</i>	The PIN. Encryption must be maintained from the device's hardware to the Processor's encryption module.	The authentication tokens. Encryption must be maintained from the device to the Processor's encryption module.	N/A
<i>Message integrity protection</i>	Integrity of critical data will be confirmed by approved industry standard cryptographic means, e.g., Message Authentication Code (MAC) or digital signature processing.		N/A
	Critical data includes the Primary Account Number, transaction amount, retrieval reference number, card acceptor name and location (Internet domain name), date and time, and session ID.		
Managing and Receiving Keys from Deployers	Keys must be received from Deployers and managed using key management practices defined by existing POS Rules: Dual control/split knowledge, secure devices containing encryption key parts, audit logging of key part usage, proper destruction of key components. Separate keys must be used for message encryption and PIN encryption. Provision must be made for periodic replacement of keys in symmetric encryption applications. Additional facility security included by reference to existing POS rules.		N/A

PROCESSOR			
Topic	Model 1	Model 2	Model 3
Transaction Receipt	Processors must provide data to merchants so that they may provide electronic transaction receipts that can be displayed and printed by the customer. The receipt must include the following: last 4 digits of the PAN only, merchant name, unique merchant ID, merchant web site address, promised shipment date, transaction type, retrieval reference number, customer name, date and time, purchase amount, authorization code, description of goods/services, and a customer service contact.		

DEPLOYER			
Topic	Model 1	Model 2	Model 3
Definition	The Deployer places “devices” into service and is responsible for their function. Devices are for entering and encrypting authentication tokens. The Deployer is responsible for the entire function of the device, as defined above, even if it includes elements that are not under the Deployer’s direct control, such as the customer’s personal computer.		The Authenticator
Deployer Certification	Deployers must be certified by the network before placing devices into service.		N/A
Device Certification	Device types must be certified by the network before use.		N/A
Device Ownership	Elements of the device that are placed into service by the Deployer must remain the property of the Deployer and must be reclaimed or disabled at will, particularly in instances of mis-use or suspected fraud.		N/A
Device - General Specifications	Devices are constructed and operate in a manner substantially similar to traditional POS.	Devices are a combination of hardware and software; designed to protect the authentication tokens and	The device must support or utilize SSL as described in the Processor section.

DEPLOYER			
Topic	Model 1	Model 2	Model 3
Device Identification	<p>traditional POS.</p> <p>The device must support or utilize SSL as described in the Processor section.</p>	<p>form/transmit transaction messages.</p> <p>The device must support or utilize SSL as described in the Processor section.</p>	
	<p>Devices must be uniquely serialized by the manufacturer. The unique serial number must be available in electronic form via a command to the device.</p> <p>It is recommended, that the serial number include a constant identifying the manufacturer and possibly the model. The unique manufacturer constant has not yet been determined by the networks, but will be determined in consultation with the manufacturers.</p>	<p>Hardware devices, and/or physical authentication tokens, must be uniquely serialized by the manufacturer. The unique serial number must be available in electronic form via a command to the device.</p> <p>It is recommended, that the serial number include a constant identifying the manufacturer and possibly the model. The unique manufacturer constant has not yet been determined by the networks, but will be determined in consultation with the</p>	N/A

DEPLOYER			
Topic	Model 1	Model 2	Model 3
Device Operation		manufacturers.	
	<i>Transaction initiation</i>	Devices must receive a transaction request message from the Processor and verify the Processor's identity through the verification of digital certificates or other means approved by the network before prompting the customer to enter the authentication tokens.	
	<i>Device identification</i>	Device and/or physical authentication token serialization data must be included in each message created by the device.	N/A
<i>Prompt</i>	Devices must prompt users for authentication token entry.		
<i>Display</i>	The device must display the dollar amount of the transaction before the user initiates the transaction.		
<i>Transaction acknowledgement</i>	The device must display the transaction response from the authentication token issuer (approve/deny) and the authorization code.		The third-party must provide the transaction response from the issuer (approve/deny) and the

DEPLOYER			
Topic	Model 1	Model 2	Model 3
<p><i>No storage of authentication tokens</i></p> <p>Device Security</p> <p><i>Tamper resistance</i></p> <p><i>Protection from viruses</i></p> <p><i>Replay</i></p>	code.		authorization code to the customer.
	Devices may not store authentication tokens, whether encrypted or unencrypted, except as needed to process transactions in real-time.		N/A
	Devices must be immune from tampering of any kind. If they are tampered with, they must cease to function or broadcast tell-tales. If device security is compromised, the deployer is responsible for any subsequent financial losses.		N/A
	Any software employed by the device must be protected from viruses.		N/A
	Devices must participate in supporting identifiers for each transaction message to be used in detecting/resisting transaction replay.		N/A

DEPLOYER			
Topic	Model 1	Model 2	Model 3
Device Encryption			
Session	The device must verify that a SSL session has been established with a recognized server by either the customer's PC or the device itself before transmitting any transaction messages.		
Message			
Method	All application level cryptographic processing will occur within hardware-based Tamper Resistant Security Modules (TRSM) and all cryptographic processing will use network-approved standard algorithms.	All application level cryptographic processing will occur within hardware or software-based Tamper Resistant Security Modules (TRSM) and all cryptographic processing will use network-approved standard algorithms.	N/A
Data to be encrypted	The PIN. Encryption must be maintained from the device's hardware to the Processor's encryption module.	The authentication tokens. If authentication tokens leave the device, then they must be encrypted within the device and encryption must be maintained from the device to the	N/A

DEPLOYER			
Topic	Model 1	Model 2	Model 3
<i>Authentication token entry</i>		Processor's encryption module.	
	(Per the existing POS rules) The PIN authentication token must be entered directly into the device, no intervening devices may be used. Authentication tokens must be encrypted in hardware immediately upon entry.	<p>Authentication tokens must be encrypted as soon as possible upon entry into the device.</p> <p>An authentication token may be used within the device to control access/use of the device when it contains private information (e.g., a private signature generation key value). The authentication token and private information must never leave the secure device in cleartext form.</p>	N/A

DEPLOYER			
Topic	Model 1	Model 2	Model 3
<i>Message integrity protection</i>	<p>Integrity of critical data will be confirmed by approved industry standard cryptographic means, e.g., Message Authentication Code (MAC) or Digital Signature processing.</p> <p>Critical data includes the Primary Account Number, transaction amount, retrieval reference number, card acceptor name and location (Internet domain name), date and time, and session ID.</p>		N/A
Key Management			
<i>Device injection and storage</i>	<p>Keys injected into devices by Deployers, including PIN encryption keys, message encryption keys, Processor identification keys and any others required to satisfy these requirements must be injected and stored in tamper-resistant hardware on the device.</p>	<p>Keys injected into devices or physical authentication tokens by Deployers, including encryption keys for the secret, message encryption keys, Processor identification keys and any others required to satisfy these requirements must be injected and stored in compliance with industry standard key management</p>	N/A

DEPLOYER			
Topic	Model 1	Model 2	Model 3
<i>Managing and delivering keys to processors</i>		practices.	
	Keys must be managed and delivered to Processors using general key management practices defined by existing POS rules and industry standards (e.g. ANS x9.24, Section 3.1).		N/A

MERCHANT			
Topic	Model 1	Model 2	Model 3
Merchant Definition	A merchant provides goods or services for sale and requests payment from customers. Merchants are also governed by guidelines developed for each transaction type.		
Merchant Sponsorship	A network member must sponsor the merchant, as in the existing POS rules, in order to display the acceptance marks of the network and process transactions through a certified Processor under these guidelines. Sponsoring institutions are financially liable for merchant activity as described in the existing POS operating rules and these guidelines.		
Merchant Certification	The merchant shall be certified by the successful completion of an audit.		
Transaction Initiation	Merchants will accept a network-branded payment from the customer by sending a transaction request message on their behalf to a Processor certified under these guidelines. The message must include all data the Processor requires to initiate a transaction with the customer, including transaction amount and the location of the customer on the Internet (IP address or other data). The transaction request message must be sent via a communication session protected, at a minimum, by Secure Sockets Layer. If the merchant performs any of the activities described in the definitions section outlined in the Authenticator, Processor, or Deployer sections of the guidelines, they will then be governed by those guidelines in addition to the merchant guidelines.		

MERCHANT			
Topic	Model 1	Model 2	Model 3
Foreign Transactions	Transactions may only be denominated and settled in U.S. dollars from customer accounts at insured U.S. depository institutions and to merchant accounts at insured U.S. depository financial institutions.		
Transaction Receipt	Processors will provide data to merchants so that they may provide electronic transaction receipts that can be displayed and printed by the customer. The receipt must include the following: last 4 digits of the PAN only, merchant name, unique merchant ID, merchant web site address, promised shipment date, transaction type, retrieval reference number, customer name, date and time, purchase amount, authorization code, description of goods/services, and a customer service contact.		

Glossary

Term	Abbr.	Definition
American Institute of Certified Public Accountants	(AICPA)	The national association of Certified Public Accountants. The AICPA promulgates practices and methods in accounting and auditing.
Certificate Authority	(CA)	An entity trusted by one or more entities to create and assign digital certificates. (ANSI)
Data Encryption Algorithm	(DEA)	A symmetric encryption method accepted as standard within ANSI commercial standards as ANS x3.92, "Data Encryption Algorithm". (Same algorithm as DES, but in commercial environment.)
Data Encryption Standard	(DES)	A symmetric encryption method accepted as standard within the U.S. government as FIPS Pub. 46.
Digital Certificate		An electronic document that represents and establishes the identity of a party on the Internet through the use of encryption.
Digital Signature		A code that cryptographically represents the identity of an entity on the Internet and its relationship to a data message, such as a transaction.
ePAN	(ePAN)	A PAN assigned to an Internet or electronic application. Generally distinct from a cardholder's PAN.
Firewall		A computer that protects a network from attacks from other networks, such as the Internet.
Internet Domain Name		A string of alphanumeric characters that labels an IP Address. The string usually contains the name of the organization represented by the IP Address.
Internet Protocol	(IP)	The networking protocol of the Internet.
Internet Service Provider	(ISP)	An organization that offers access to the Internet

Term	Abbr.	Definition
		Internet.
IP Address		The discrete identification of a location on the Internet as defined by the Internet Protocol.
Message Authentication Code	(MAC)	The result of passing a digital message through an algorithm designed to produce a unique code for every unique digital message.
Proxy Server		A server that acts on behalf of a web server, isolating it from the Internet.
Public Key Infrastructure	(PKI)	A system of employing public keys and their corresponding private keys to establish identification and authorization services for parties using a public network like the Internet.
RSA		A cryptographic method of creating and using public/private key pairs. Named for its creators: Rivest, Shamir, and Adleman.
Secure Electronic Transaction	(SET)	An open technical standard for the commerce industry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet. (SETCo)
Secure Sockets Layer	(SSL)	A security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. (Internet Engineering Task Force)
Tamper Resistant Security Module	(TRSM)	A computing device designed to protect data from revelation or modification.
Triple-DES	(3DEA)	An extension of DES that increases the practical security of the DES algorithm.