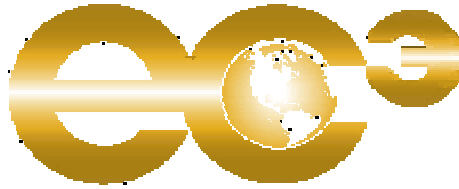


Electronic Payments Primer

**Copyright 1999
National Electronic Commerce Coordinating Council**



The National Electronic Commerce Coordinating Council is an alliance of national state government organizations dedicated to the advancement of electronic commerce within states. The alliance is comprised of the National Association of State Auditors, Comptrollers and Treasurers (NASACT), NASIRE - Representing the Chief Information Officers of the States, and the National Association of State Procurement Officials (NASPO). Affiliate members are the Information Technology Association of America (ITAA), the National Association of Secretaries of States (NASS), and the National Automated Clearing House Association (NACHA).

The NECCC is pursuing several strategies to advance electronic commerce within the states, including:

- Helping to coordinate electronic commerce adoption in the states through various means, such as participation in pilot projects and the dissemination of best practices in state electronic commerce
- Holding its Annual Conference on Electronic Commerce in the States to study innovations in technology and review successful electronic commerce projects
- Conducting a number of surveys on electronic commerce practices in state government
- Maintaining and expanding its Web site (<http://www.ec3.org>) for the promotion and distribution of association materials.

The two standing committees are Program and Communications. In addition, the following six issues-related work groups were formed in 1999:

- Electronic Payments
- Electronic Commerce Transactions & Service Delivery
- Electronic Procurement Systems
- Financial Electronic Data Interchange
- Funding Issues
- Planning Issues

The Electronic Payments work group developed this primer. It also conducted an extensive survey of state credit card acceptance practices, the results of which are available on the Web site.

- 1. Introduction**
- 2. Credit Cards**
- 3. Emerging Payment Mechanisms**
- 4. Privacy & Security Issues**
- 5. Electronic Benefits Transfer**

Introduction

Purpose

The intent of this primer is to help government managers learn more about electronic payment. It will provide an overview of current practice, cutting-edge technology, and privacy and security problems and solutions; it also will suggest resources for further information. Government managers face unique barriers to developing online service-delivery applications and choosing appropriate payment mechanisms. This document highlights some of those barriers and suggests the means to overcome them. In addition, Web site citations offer more direction and resources.

Currently, credit cards are the primary electronic payment vehicle. They present a number of related acceptance issues, including fee allocation, contracting for services and risk management. A thorough understanding of how acceptance works and where costs accrue in processing can aid governments in negotiating for services.

Meanwhile, new payment mechanisms are developing for online transactions.

Electronic checks, automated teller machine (ATM) and automated clearinghouse (ACH) network-based payments and electronic wallets are options for jurisdictions that are unable or unwilling to accept credit cards, or looking for alternative ways to facilitate online business.

When government establishes a channel for electronic payments, regardless of the means, significant issues of privacy and security arise. An overview of major security considerations and corresponding protocols is provided, and key issues in protecting individual data privacy are raised.

For several years, electronic benefits transfer (EBT) has been a delivery method for government payments, primarily for cash and cash-equivalent payments (food stamps and welfare). Now it is evolving as a platform for other services. EBT used commercial networks and infrastructure to achieve a government electronic payment objective.

Credit Card Acceptance Issues

Public sector entities grapple with many issues when deciding whether and how to accept credit cards for payment. While credit cards are a commonly held, easy-to-use payment mechanism for citizens and companies, a question that often arises is who pays the processing fees – the merchant (agency or state) or the cardholder (citizen or company). Each state has to answer that question for itself, based on its laws and political climate, but learning more about the credit card acceptance procedure can help public officials make educated choices.

A cost/benefit/risk analysis should be performed to help determine what applications are appropriate for credit card use. True transaction costs for current payment processing should be measured and benchmarked against new transaction types. Governments face an additional challenge of integrating new payment methods into existing legacy systems and processes. This section of the primer contains documents from First Data Merchant Services and MasterCard International, which explore the following issues of credit card acceptance for public sector entities:

- 1. Purchasing over the Internet**
 - 2. The Cost of Card Acceptance, and**
 - 3. Banking Terms You Need to Know**
- (please refer to this section as you encounter new terminology)

Purchasing over the Internet

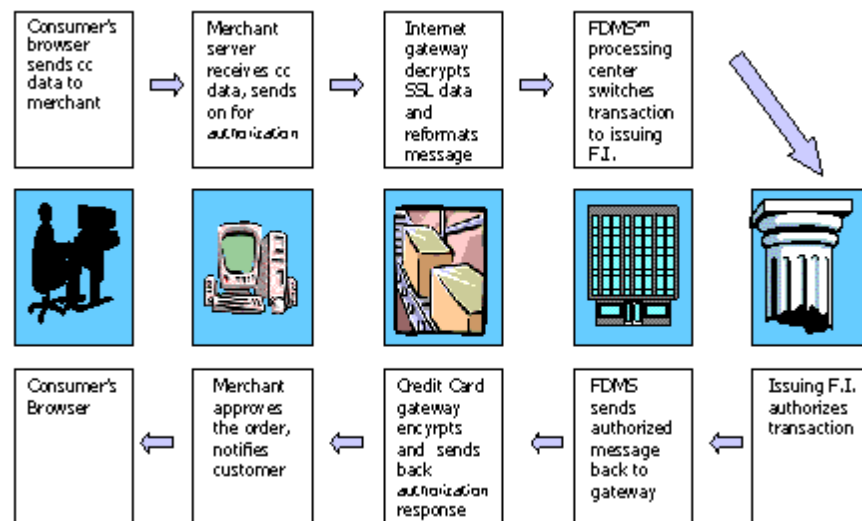
Making purchases over the Internet involves four main parties: the consumer or credit card holder; the government (merchant) offering products or services for sale; the merchant bank that has contracted with the government to enable it to accept credit cards over the Internet; and the company that processes credit card payments for the merchant bank, known as the acquiring processor. (The acquiring processor processes government credit card transactions through the financial network on behalf of merchant banks.) One other party is involved: the bank that issued the consumer's bank card.

The consumer interacts with the government's Web site by using a Web browser. The government's commerce application makes goods and services available for sale over the Internet by payment-enabling the government's Web server application. To accept credit card payments over the Internet, the government must have an account with a bank that offers Internet credit card processing. The bank may also function as the acquiring processor to move the credit card transaction through the financial networks; or it may designate another company to function as acquiring processor on its behalf.

Diagram #1

Steps In An Internet Credit Card Authorization

The diagram shows an Internet credit card authorization using an Internet gateway. (FDMS is the acquiring processor, government is in the role of merchant.)



When a consumer decides to buy something, the commerce application prompts the consumer for credit card information, usually along with other data such as a bill-to address and a shipping address. The consumer enters payment information into a form secured by the Secure Sockets layer (SSL) protocol (see the privacy and security section for more on SSL). With the secured form, the payment information is encrypted by SSL as it is sent over the Internet to the government.

Using payment software incorporated in the Web server, the government sends the encrypted transaction to the acquiring processor for authorization. The authorization is a request to hold funds for purchase. If the government uses an Internet gateway service (as shown in diagram above), the transaction will be encrypted while in transit to the Internet gateway. Otherwise, the transaction can be sent to the acquiring processor via a private dial or leased line.

The issuing financial institution (FI) both authorizes a certain amount of money and issues an authorization code or declines the transaction. An authorization reduces the available credit limit but does not actually put a charge on the customer's bill or move money to the government. This message is transported to the issuing bank and then to the government by the acquiring processor.

If the transaction is authorized, a "capture" takes the information from the authorization and charges the authorized amount of money to the consumer's credit card. In line with bankcard association rules, the government is not allowed to capture transactions until the ordered goods can be shipped or the service is provided, so there may be a time lag between the authorization

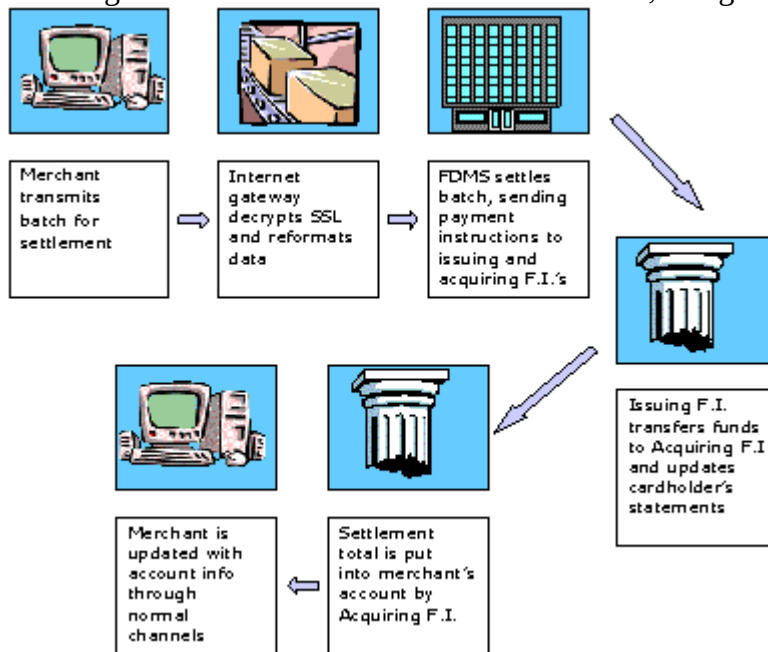
and the capture. If the consumer returns goods after the transaction has been captured, a credit is generated.

The final step is to settle the transaction between the government and the acquiring processor. “Captures” and credits usually accumulate into a batch and are settled as a group. When a batch is submitted, the government’s payment-enabled Web server connects with the acquiring processor to finalize the transactions; money is subsequently transferred to the government’s bank account. (See diagram 2.)

Diagram #2

Steps In An Internet Credit Card Settlement

The diagram shows Internet credit card settlement, using an Internet gateway.



The Cost of Card Acceptance

Discount Rate

The Discount Rate is a rate established by your Acquirer/Processor that compensates the acquirer for accepting bankcards as a form of payment and paid by the government agency. Acquirers set discount rates based primarily on the expenses they incur in serving bankcard customers' needs. These expenses typically include authorization, draft capture and settlement, administrative and operating expenses and interchange fees.

What is Interchange?

Issuers incur costs in processing card transactions and maintaining cardholder accounts. To reimburse them, acquirers pay issuers a fee for each transaction they process - the interchange reimbursement fee, commonly referred to as "interchange." Interchange specifically reimburses issuers for certain costs of card issuance, e.g., risk, processing and financial carrying costs.

The interchange fee for which transactions qualify is a critical factor in determining discount rate. MasterCard, for example, offers several categories of interchange fees. The rates vary, primarily depending on such factors as:

- The authorization method used
- Whether electronic draft capture is employed
- Whether the card is presented face-to-face (and the magnetic stripe read) at the time of payment
- The amount of transaction information captured
- Whether the card is a consumer or corporate card
- The merchant industry segment (government in this case)

Generally, the faster and more automated (i.e., electronic) the transaction, the lower the interchange fee. The interchange fee for which your transactions qualify is a critical factor in determining your discount rate. Your Acquirer can review in more detail the various interchange options available to you.

Administrative and Operating Expenses

Several other factors also affect the discount rate. These factors include whether the acquirer's ancillary services are bundled or unbundled (broken out separately from the discount) and the amount of exception processing required of the acquiring bank. Exception processing includes any special requirements in reporting, accounting, programming or other areas that necessitate additional work by the processor or acquiring bank. Also calculated into the discount rate are the costs of merchant customer service, operations, overhead and bankcard association assessment fees.

The following are fees that are often unbundled:

Authorization Fees: Per item fees for electronic authorizations (on-line or voice).

Set-Up (or Sign-Up) Fees: Costs to technically and administratively set up account or outlet.

Imprinter Fees: Monthly charge for the lease or rental of imprinter.

POS Terminal Fees: Monthly charge for the lease or rental of terminal.

Maintenance Fees: Monthly or annual fees for the maintenance of your account.

Batch Fees: A charge for every batch processed including sales, credit and batch header tickets.

Chargeback Fees: A charge for handling each charged-back transaction.

In evaluating Acquirer proposals, it is critical that all costs, the discount rate, as well as any unbundled fees be taken into account for comparative purposes.

© 1998 MasterCard International Incorporated

Banking Terms You Need to Know

Acquiring Bank/Merchant Bank - The bank that does business with merchants enabling them to accept credit cards. A merchant has an account with this bank and each day deposits the value of the day's credit card sales. Acquirers buy (acquire) the merchant's sales slips and credit the tickets' value to the merchant's account.

Acquiring Processor - The processor provides credit card processing, billing, reporting and settlement and operational services to acquiring banks. Many financial institutions don't do their own bankcard processing because it's more cost-effective to let someone like First Data invest in the equipment and people and do it for them.

Authorization - The act of insuring that the cardholder has adequate funds available against their line of credit. A positive authorization results in an authorization code being generated, and those funds being set aside. The cardholder's available credit limit is reduced by the authorized amount.

Batch - The accumulation of captured (sale) transactions waiting to be settled. Multiple batches may be settled throughout the day.

Capture - Converting the authorization amount into a billable transaction record within a Batch. Transactions cannot be captured unless previously authorized, and the goods or services have been shipped or transmitted to the consumer.

Cardholder - Any person who opens a credit card account and makes purchases using a credit card.

Credit Deposit - The value of a merchant's credit card purchases that are credited to its bank account after the acquiring bank buys the merchant's sales slips. The deposit is credited. It is not funded until the acquiring bank gets the monetary value from the issuer during settlement.

Discount Rate - The fee a merchant pays its acquiring bank/merchant bank for the privilege to deposit the value of each day's credit purchases. The fee is usually a small percentage of the purchase value.

Interchange - The exchange of information, transaction data and money among banks. Interchange systems are managed by Visa and MasterCard associations and are very standardized so banks and merchants worldwide can use them.

Interchange Fee - A fee paid by the acquiring bank/merchant bank to the issuing bank. The fee compensates the issuer for the time after settlement with the acquiring bank/merchant bank and before it recoups the settlement value from the cardholder.

Issuer - The bank that extends credit to customers through bankcard accounts. The bank issues the credit card and receives the cardholder's payment at the end of the billing period. Also call the issuing bank or the cardholder bank.

Settlement - As the sales transaction value moves from the merchant to the acquiring bank, to the issuer, each party buys and sells the sales ticket. Settlement is what occurs when the acquiring bank and the issuer exchange data or funds during that function.

Ticket - Another name for the sales slip or its monetary value that results when a credit card purchase is made.

Transaction - One example of a transaction is the process that takes place when a cardholder makes a purchase with a credit card.

© 1998 First Data Merchant Services Corporation all rights reserved. "FDMS" is a service mark of First Data Merchant Services Corporation.

Emerging Payment Mechanisms

Many sectors, including government, have expressed great interest in alternatives to using credit cards to enable online transactions. So far, though, there has been limited penetration of new electronic payment mechanisms. Recent developments in the industry have given hope to the expansion of these offerings, however, both in numbers and acceptance.

As governments explore these methods, they need to carefully analyze comparative costs. A cost/benefit/risk analysis of possible payment mechanisms - such as digital cash, electronic checks and ATM and ACH network alternatives - should be performed and compared against the true costs for current processes. It is important to expand the range of payment options so citizens can interact with government through whatever mechanisms they choose.

Digital Cash and Electronic Wallets

Most current payment mechanisms are activated by an account relationship: an individual or company gains access to a form of digital currency by means of an existing credit card or bank account. This usually entails transferring a limited sum of money from the bank or credit card to an electronic wallet mechanism, which then is debited to pay online merchants that accept this form of payment.

No single medium for electronic wallet mechanisms has gained dominance, however, and due to their proprietary nature, many merchants have chosen to stay largely with credit cards. However, a new standard has recently been endorsed by several major payments and technology companies (including American Express, AOL, IBM, MasterCard, Microsoft and Visa) that may help open up more digital wallets: the Electronic Commerce Modeling Language (ECML). According to its sponsors, ECML uses a set of uniform field names that streamlines the process by which merchants electronically collect data for shipping, billing and payment. It provides a set of simple guidelines, making it easier to use digital wallets.

If the ECML standards become widely adopted, it could substantially increase the ease of use and utility of wallets, making it efficient for governments to accept the payment vehicles they offer.

Electronic Checks

An electronic check is any check that is electronically encoded for the purposes of automated transmission through the payment-processing stream. An electronic check may originate through the conversion of a paper check to an electronic transaction as early as possible in the check collection process. Conversion may take place at the point of sale (POS), the lockbox, or the point of deposit. In its more recent manifestation, an all-electronic check never takes form as a paper check; instead, it originates from the payer's computer and is digitally signed.

Government agencies that accept paper checks at the point of sale should consider the benefits of converting them into electronic funds transfers and returning the paper check to the customer.

These systems are designed to improve the payments collection time, reduce fraud and error and eliminate the need to bundle and deposit paper items.

The process of converting a paper check to an electronic funds transfer begins when the customer presents a paper check at the point of sale. It is scanned through a check reader, which captures the customer's account information and an image of the check. The amount is then hand-entered on a terminal keypad at the POS. Checking account information is automatically verified against a check database. If no negative information is found, an authorization slip is printed for the check writer to sign. This slip allows the paper check to be converted into an electronic one through the ACH system. The paper check is stamped VOID/EFT PROCESSED and returned to the customer. Settlement is made to the government entity with an ACH credit transaction that deposits the purchase amount into the entity's account.

This process offers government enormous benefits. Due to the compressed processing time, check fraud can be detected days earlier than with conventional paper-based methods. Information on non-sufficient-funds transactions is available as many as 10 days earlier, allowing the collection process to be expedited and check databases to be updated sooner. This reduces loss from such accounts. In addition, fewer individuals view the customer's account information. Approximately 10 people normally handle a paper check before it gets to the receiving depository financial institution. With electronic check conversion, only the check writer and the cashier view the customer's account information. Federal agencies are deploying these POS check conversion systems today with the help of the Federal Reserve Banks.

An electronic check is an electronic version of a paper check. It contains and transmits the same basic information as a paper check and is bound by the same regulatory requirements. It works much like a paper check, too. The check writer, or payer, originates the check from a computer or other electronic device. It appears on-screen exactly like a paper check and, when completed, leaves a representation of a manual signature as an indicator that it has been digitally signed. The check is sent through a network such as the Internet to the payee, where the information it contains creates a virtual check. The payee deposits the check with its financial institution, which clears the check to the payer's financial institution. The payer's financial institution validates the check and debits the payer's account for the amount. Digital signatures, using a combination of software and hardware technologies secure the entire process. To encode data, an electronic check uses Financial Services Markup Language/Extensible Markup Language (FSML/XML), an industry standard.

There are advantages to using electronic checks. For example, an electronic check can carry enhanced information that cannot be transmitted with a paper check, such as an original invoice that includes line-item details. In addition, electronic checks are useful to business customers that wish to receive payment and remittance data directly from the government and have flexibility in where payments are deposited. All-electronic checks also avoid the handling, sorting, imaging and storage costs of their paper counterparts. Appreciating these benefits, the federal government and the Federal Reserve Banks are using electronic checks to pay Department of Defense vendors.

ACH Network Alternatives

Most people are familiar with a traditional ACH debit transaction, where a consumer provides account information to the merchant, which then debits the individual's account. The National Automated Clearing House Association (NACHA) has proposed piloting an ACH credit application known as the Credit Push Internet Payment Model. Here the merchant provides its account information to the consumer in encrypted form, which the consumer electronically forwards to his bank. The bank initiates an ACH credit to the merchant's account.

In this model, both the merchant and the consumer receive digital signatures issued by their respective banks. The consumer initiates a transaction at a merchant Web site, and the merchant sends a digitally signed invoice to the consumer. The consumer has the option of asking his bank to validate the merchant's digital signature to ensure that he is doing business with the intended merchant. He digitally signs the invoice and sends it to his bank for processing. The bank validates the consumer's digital signature to verify that it is dealing with its customer and account owner. The bank then processes the credit through the ACH Network.

NACHA cites the following advantages for this model:

- Unlike with debits, consumers do not have a 60-day window to rescind the payment when they initiate credits
- Costs for ACH Network transactions are much lower than credit card fees
- The consumer never sees the merchant account information
- Many consumers do not have credit cards, are not permitted to make certain purchases with credit cards or prefer to make purchases directly from their checking accounts
- The consumer is not required to understand the certificate processing underlying the transaction
- The model preserves the consumer's privacy: the consumer is fairly anonymous to the merchant and does not have to supply the merchant with an account number

ATM Network Alternatives

The Star System ATM network has proposed allowing consumers to make payments over the Internet using their ATM cards. The model requires banks to create a secure environment for their consumers to generate private keys to create digital signatures, and then corresponds the public key to the consumer's DDA account to validate those signatures. The consumer then initiates a transaction on a merchant web site and chooses ATM as the payment method. The consumer enters their ATM card number and uses a digital signature to sign and authorize transactions instead of a PIN number.

Advantages of using an ATM card instead of a credit card include:

- Costs for ATM network transactions are significantly lower than credit card fees
- Many consumers do not have credit cards, are not permitted to make certain purchases with credit cards, or prefer to make purchases directly from their checking accounts
- Funds are guaranteed via a debit or memo posting to account

- The Star Network already permits PIN-less ATM transactions that allow consumers to pay their utility companies by phone using their ATM cards. This means that the rules and infrastructure already are basically in place to support this model
- Consumers are familiar with the technology

Sources:

[Http://www.ecml.org](http://www.ecml.org)

<http://www.echeck.org>

<http://internetcouncil.nacha.org>

Privacy & Security Issues

INTRODUCTION

State government has an obligation to the people it serves to protect the *privacy* of confidential information it collects. This includes the expectation that transaction data will be *secure* from unauthorized users. The state has an obligation to make sure that the transaction is *authentic* and cannot be repudiated. The state is also obliged to warrant to the citizen that the information represented on the web is *accurate, timely* and a bona fide representation by the state. Enforcing aggressive policies, paying constant attention and wisely using technology insure that all these obligations are met.

The Risk Chain

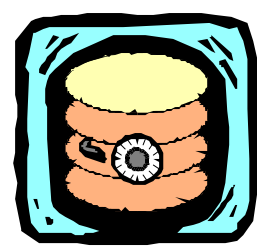
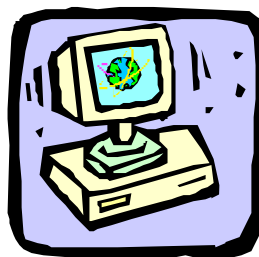
The chart below describes the chain of risk--the points where states should focus their efforts to protect security, privacy and authenticity--beginning with the person wishing to do business on a government Web site, who is known as the transactor.

Authenticate ID of Transactor The transactor should be authenticated if the transaction is limited to certain users so it cannot be repudiated at a later date. The chart lists some technologies used for authentication.

Protect Data in Transit The data transmitted should be secure from manipulation and secure from unauthorized users.

Authenticate Web Site Content The transactor has a right to expect that the web site visited is a true representation of the state.

Protect Data in Repose Finally, data collected by the state through any means should be secure from unauthorized users.



Security Policies

Privacy Policies

Open Records Policies

AUTHENTICATE ID OF TRANSACTION

Password, PIN
Electronic ID's
Intrusion Detection

PROTECT DATA IN TRANSIT

Encryption
Secure Socket Layer
(includes encryption)
S/MIME

AUTHENTICATE WEB SITE CONTENT

Maintenance
Branding

PROTECT DATA IN REPOSE

Firewalls

Evaluating Risk Levels

Demand from the public for interactive Web access to government information and services is on the increase. Any organization contemplating permitting electronic transactions should first assess the risks and then put appropriate privacy and security measures in place: Different kinds of transactions will require different levels of security and privacy. The three questions below help appraise the level of risk inherent in a transaction.

1. What is the consequence if a transactor repudiates the claim? Say that a citizen seeks information available through the Freedom of Information Act and accessible on the Web. In this case, the state has an obligation to make sure the data is accurate, but the consequence of the transactor denying that he sought the information is negligible. This type of transaction represents a low risk to security and privacy. However, what if a prospective licensee warrants his criminal status through an online application? The consequence of awarding a license based on an affirmation that is later repudiated could be serious.
2. What is the likelihood that a transactor would provide a false identity? For instance, a citizen voluntarily makes a payment for taxes owed. It is unlikely that someone would pay the tax bill other than the citizen who owes the money. On the other hand, someone could be motivated to assume the identity of a political foe in order to file an inaccurate ethics report.
3. What is the consequence if the information that is traded falls into the wrong hands? The consequences would be minor if it became known that a citizen sought information available through FOIA. But financial data or medical records that fell into the wrong hands could have seriously adverse affects.

Often, the risk associated with a transaction can be quantified by some measure, like cost. Then the state can select security measures with the rigor and expense appropriate to the risk.

Connecting to the Internet improves citizen access to government information and services and also provides the government entity access to the vast resources available on the Internet. However, connecting to the Internet includes risks from hackers and other outside sources, as demonstrated by the recent attacks on federal government Web sites. Every government entity needs to develop a comprehensive *security policy*. A good starting point is the Site Security Handbook, published as Request for Comments (RFC) 2196 (www.ietf.org/rfc/rfc2196.txt). The handbook provides guidelines for developing computer security policies and procedures for sites that have systems on the Internet. One key element of any good policy is to define access permissions--who can access what information or resources.

When they collect personal information, federal agencies must protect an individual's right to privacy as required by the Privacy Act, 5 U.S.C. 552a and the federal Office of Management and Budget's Circular No. A-130, "Management of Federal Information Resources." State and local laws vary; some protect certain kinds of data (e.g., social security numbers) while viewing other information collected as open records. State and local government organizations need to consult with their legal counsel to ensure that they can appropriately protect information collected over the Internet. Any government entity also should provide a link to its *privacy policy* on every Web page.

Associations and business are also addressing the issue of privacy. Sites on the topic include <http://www.truste.org>, <http://www.cpawebtrust.org/> and <http://www.bbbonline.org/>.

The latter two are sponsored by the American Institute of Certified Public Accountants and the Council of Better Business Bureaus, respectively.

The Technologies

Encryption: Through the application of an algorithm to electronic data, the content can be disguised to all except those who know the algorithm or a complementary one. Any transaction that involves the transmission of personal information, or requires a user ID and password, should be encrypted.

Intrusion Detection and Firewalls

One of the first steps in securing web transactions is to assess the risk associated with the data and system resources and to identify the level of protection necessary to prevent unauthorized access, i.e., intrusion. An intrusion is any attempt to compromise the integrity, confidentiality or availability of a resource. Intrusions can be categorized into two main areas: well-defined attacks and deviations from normal system usage patterns. Intrusion detection is a growing concern for everyone connected to the Internet.

A firewall is a mechanism used to control and watch access to and from a network for the purpose of protection. It acts as a gateway through which all traffic to and from the protected network passes. At the same time, it provides a wall between one part of a network--the Internet, for example--and the agency's internal systems. A firewall consists of one or many computer devices and lets traffic flow between network components only as the security manager intends.

Intrusion detection has for many years been considered part of the firewall system. Nowadays, system advances, increased risk of attacks and the technology employed by hackers make it critical to have an intelligent application that builds a profile of the system and can detect deviations from the profile.

Electronic ID's

Listed below are several devices categorized as electronic identification. They can be used in combination to exploit their special strengths.

Passwords, ID, and Personal Identification Numbers (PIN's)

These techniques are the most commonly used and may be sufficient for many low risk web-based transactions. The user login session should be encrypted.

Digital Signatures/Certificates

Digital signatures and certificates offer authentication of the transactor's identity and ensure that the transaction can't be repudiated later. The underlying technology for digital signatures is public key infrastructure (PKI). It relies on encryption and a network of trusted third parties to act as intermediaries between the transactor and government. Confidence in a digital signature depends on which trusted third party issues the certificate, how the identity of the transactor is established and how the certificate is issued, i.e., remotely via software or mail or in person.

In determining whether an electronic signature is required, agencies should consider the relationships between the parties, the value of the transaction and the likely need for accessible, persuasive information regarding the transaction at some later date (e.g., audit or legal evidence). For a thorough discussion of digital signatures and the trust relationships, please see <http://internetcouncil.nacha.org/> for the Certification Authority Rating and Trust (CARAT) guidelines. CARAT is a NACHA work group.

Biometrics

The term "signature" has long been understood to include "any symbol executed or adopted by a party with present intention to authenticate a writing" (Uniform Commercial Code, 1-201(39)(1970)). This flexible definition permits the use of other electronic signature technologies, such as digitized signatures (encoding the characteristics of a handwritten signature presented on a special input device) or biometrics. Biometrics relies on a scan of some physical characteristic, such as fingerprints, that is matched to a stored scan to confirm identity.

Smart Cards

Plastic cards with embedded computer chips are called smart cards. The chips frequently contain information about the cardholder's identity. It may be a digitized record of his fingerprint that can be validated against a scan, or the cardholder's digital signature.

Secure Socket Layer (SSL)

The most common form of securing online transactions is the Secure Socket Layer (SSL) session. SSL is the predominant Internet security protocol that provides protection against eavesdropping or tampering with information being transmitted. The SSL protocol includes provisions for server authentication (verifying the server's identity to the user); version 3 allows server-to-server authentication. Currently, two levels of security are available for the SSL transmission of information. The more common one uses a 40-bit key; the other, employed for financial transactions and other sensitive information because it is more difficult to compromise, uses 128-bit encryption keys. Depending on the application, government entities should plan on using 128-bit encryption on their Web sites and provide a warning to the user if they use 40-bit encryption.

Secure Multipurpose Internet Mail Extensions (S/MIME)

Secure Multipurpose Internet Mail Extensions (S/MIME) is a set of standards for the secure exchange of electronic messages on the Internet. It provides privacy and authenticity. S/MIME uses public-key encryption technology to protect messages from unauthorized interception and

forgery. While SSL secures a transaction between a user and a Web site over the Internet, S/MIME secures messages between users, applications and computers.

A special note about Server Logs and Cookies

Server log software and cookies are used to track visitors to web sites. The information collected for analysis can include where the request came from, time and pages visited. They collect identifiable information about the visitor such as:

- The hostname (or IP address) of the client requesting access;
- The user-agent information including the type of browser, its version, and the operating system it's running on;
- Where and when the visit originated; and
- The pages visited.

Cookies are small data files written to the visitor's hard drive by the Web site. A cookie file contains unique information such as passwords, lists of pages visited and the last date of a session at a particular web site. A cookie is often used in commercial sites to identify the items selected for a specific shopping cart application, or to customize a web presentation to a particular user.

The information collected through server logs and cookies may be very valuable to a commercial enterprise and be sought under Freedom of Information Act, but citizens may expect confidentiality.

Government organizations' planing to provide Internet accesses to services need to assess what technology is appropriate for a given transaction. This would include a risk assessment, and establishing appropriate policies and implementing appropriate technologies to protect the public. Organizations must strike a balance, recognizing that achieving absolute security is in most cases highly improbable and prohibitively expensive.

Electronic Benefits Transfer

Electronic benefits transfer (EBT) is electronic access to government benefits or payments via card technology at an ATM or Point of Sale (POS) terminal. Most frequently, EBT is used to provide food stamp and cash assistance benefits.

How EBT Works

EBT recipients do not have their own bank accounts. Instead, an EBT contractor maintains a database that contains information about benefit levels for each recipient. This Cardholder Authorization System (CAS) is credited when the government deposits benefits and is debited when the recipient makes a purchase or withdraws cash.

Means-tested benefits are benefits, such as food stamps, that a person or household receives because income is below a certain level. Recipients can access their food stamp benefits only at merchants authorized by the federal Food and Nutrition Services to participate in EBT. Food stamp benefits cannot be accessed at ATMs since food stamps must be used to purchase approved food items and cannot be converted to cash.

Most EBT projects use magnetic stripe cards. Newer systems strive to piggyback on commercial ATM and debit card systems, so that existing POS and ATM terminals can be used. The appearance of a card does not indicate whether it can be used to access food stamps and cash benefits, just as the appearance of an ATM card does not show whether it accesses a checking or savings account.

Like other debit card transactions, an EBT transaction is initiated by swiping the card through a POS or ATM terminal. The recipient must then enter a PIN. At a merchant terminal, the recipient pushes a button to choose a cash or food stamp transaction. A recipient can usually access both food stamp and cash benefits using the same card but must indicate which benefit is being used.

The terminal transmits the transaction to the CAS. If the transaction is a purchase or cash withdrawal, the CAS verifies that there is a sufficient balance and approves the transaction. If the balance is too low, the transaction is denied. For a food stamp transaction, the reason for the denial will be printed on the receipt, along with a balance, so that the cardholder might be able to make a transaction involving a lesser amount. EBT transactions are online (real-time) transactions. Once a recipient has made a purchase or withdrawal, the balance is updated automatically.

The Future of EBT

As EBT evolves, stakeholders are looking to utilize the infrastructure as a vehicle for delivering additional government services. Current initiatives include the addition of Women, Infants and Children (WIC) and childcare benefits.

WIC differs from traditional food stamp benefits in that a specific list of items and their exact quantities are prescribed to participants. This and other “prescription” programs, which are more

complex and specific than food stamps, are more amenable to smart card technology than to traditional magnetic stripe cards. Smart cards require a special reader to access the information on the chip; many newer POS devices are equipped to handle both technologies, and other readers are emerging in the marketplace. There are still numerous issues to sort through concerning standards, however, which - in addition to the cost of the readers - has slowed the spread of this technology.

Still, other human service programs are beginning to look to card-based delivery.

One example is the Health Passport Project of the Western Governors' Association. The HPP uses a smart card for health records and insurance information for recipients of Medicaid and other government-sponsored health services. It contains important data, such as child immunization records and allergies to medication, in addition to billing information. HPP is being piloted in Bismarck, North Dakota; Cheyenne, Wyoming; and Reno, Nevada.

The following Web sites offer additional information about EBT:

NACHA: <http://www.nacha.org>

U.S. Department of Agriculture, Food and Nutrition Service:

<http://www.usda.gov>

Western Governors' Association: <http://www.westgov.org/hpp/>