Cross-Industry Working Team

The needs of commerce have been a primary factor in the evolution of information technology throughout history. The purpose of this paper is to explore how, on tomorrow's networks, universal, fast, and secure payments can be made and received for services, physical goods and information.

"ELECTRONIC CASH, TOKENS AND PAYMENTS IN THE NATIONAL INFORMATION INFRASTRUCTURE"

Table of Contents

1.0 Introduction

2.0 Fundamental Properties

3.0 Required System Features

4.0 Optional Features and Functions

5.0 System Management and Control

6.0 Summary

Glossary

1.0 Introduction

The needs of commerce have been a primary factor in the evolution of information technology throughout history. Records of economic transactions on clay tablets, pictographic expressions of value, and physical tokens in media ranging from stone to plastic illustrate available technologies and states of economic development. Many of today's information infrastructure activities also deal with billing and payment. Most bills are mailed, faxed, and with decreasing frequency, presented in person; payments are generally made by cash, check, credit card, or money order. None of these methods, however, fully addresses the unique constraints or opportunities of doing business in an advanced networked environment. The purpose of this paper is to explore how, on tomorrow's networks, universal, fast, and secure payments can be made and received for services, physical goods and information.

1.1 Considerations in Electronic Payments Over the NII

Numerous payment mechanisms are presently available to meet individual preferences. These include cash, checks (including certified checks), charge cards, credit cards, debit cards, traveler's checks, prepaid cards, physical tokens and scrip, bank notes, banker acceptances, letters of credit, and barter (e.g., the exchange of gold, Treasury bills, etc.). Each of these mechanisms has a different set of attributes that makes it more or less desirable for different types of electronic commerce transactions. None is completely adequate in its present form for the distributed networked environment of the National Information Infrastructure (NII). This is because existing payment mechanisns either assume that the parties will at some time be in each other's physical presence or that there will be a sufficient delay in the payment process for frauds, overdrafts, and other undesirable conditions to be identified and corrected.

Many of these payment mechanisms have already begun to adapt in response to the conduct of business over networks. But more remains to be done. Further, to ensure universal availability and acceptability, entirely new forms of electronic payment are needed.

Presently, for example, credit card charge information can be entered into a device screen and sent securely over the network from buyer to seller as an encrypted message (e.g., privacy-enhanced mail message). This practice, however, does not meet important requirements for an adequate financial system, such as nonrefutability, speed, safety, privacy, and security. To make a credit card transaction truly secure and nonrefutable, (1) a customer must present his or her credit card information (along with an authenticity signature) securely to the merchant; (2) which must validate that it is dealing with the true owner of the credit card account; then (3) relay the credit card charge information and signature to its bank; which (4) must relay the information to the customer's bank for authorization approval; and (5) the bank must return the credit card data, charge authentication, and authorization to the merchant. Then, and only then, can the actual goods, services, and funds flow.

If there can be a lapse in time between the charging for and the delivery of goods or services -- for example when an airline ticket is purchased well in advance of the date of travel -- the customer verification process can be simpler. In fact, all the relaying and authorizations can take place after the customer-merchant transaction is completed, unless the authorization request is denied. On the other hand, if the customer wants a `digital` airline ticket, which would be downloaded into a PC or other information appliance immediately at the time of purchase, many message relays and authorizations must take place in realtime while the customer waits. Such exchanges may require many sequence-specific operations such as staged encryption and decrypting and exchanges of cryptographic keys.

If this process is extended to all of the small-dollar services that may ultimately be available over the NII (e.g., $3 pay-per-view movies and $1 video game rentals), the overall processing load on key system components will likely become unmanageable or nonviable. Providing this processing service for numerous $1 and $3 transactions may not be as financially attractive as it is now, when the average credit card transaction is about $60.

Today's electronic transactions systems can be modified and refined to work over the NII. They can also be extended to take advantage of new technological capabilities. For this reason, alternative mechanisms for managing digital cash are to be expected. Some requirements are illustrated in the following scenario set in the NII.

1.2 Scenario

A student is doing research in the electronic library. Using a public communications port on the NII's equivalent of today's pay phone, she launches an inquiry using a knowledge-gathering software agent which roams the world's networks and identifies relevant studies. Some are located through a commercial archival research service with which she has never before dealt. She would like to retrieve copies of these studies to review on her portable knowledge appliance. The archive service informs her that there will be an $8 charge for the copies. The student can't buy on credit since she doesn't have an account with this service and the service doesn't accept credit cards for charges under $10. So she places her university's student smart card containing electronic cash provided as part of a scholarship into her appliance. She transfers $8 worth of these electronic tokens to the research service. The service validates the tokens as authentic and sends the reports to the student. Upon receipt of the requested reports, the student in turn completes the transaction by transferring ownership of $8 in tokens to the service. Later, browsing on an entertainment network, the student sees an advertisement about a movie. She sends a request to the advertising distributor to have the movie presented on her appliance. The distributor notifies her that the charge will be $3.99. She places her university card into her knowledge appliance and transfers $3.99 in electronic tokens. The movie service attempts to validate these tokens and discovers that they are earmarked for specific scholarship purposes, which do not include purchasing entertainment movies. The service returns the tokens to the student with an explanation.

1.3 Digital Cash (Electronic Tokens)

Digital cash, also called electronic money or electronic cash, offers some features that should make it an attractive alternative for payment over the NII. But is it the equivalent of paper cash, or are there important differences? As demonstrated in the scenario, digital cash does not have to be designed to faithfully emulate all the properties of paper cash. It can be implemented to preclude some features of paper cash, such as complete anonymity, while including other desirable attributes not possible with paper cash, such as full divisibility, assignment of limits and constraints, and links to the current owner.

This paper focuses on the concept of *electronic tokens*. Digital cash is one form of electronic tokens. However, electronic tokens can also be designed as electronic analogues of other forms of payment as well, including checks and credit backed by a bank or financial institution. These latter alternatives are designed to accommodate the many individuals and entities that might prefer to pay on credit or through some mechanism other than cash. The availability of credit is an important stimulant to commerce.

In an electronic token system, tokens can be stored on a user's card or computer, and can be exchanged directly between remote transacting parties. This exchange does not require a fixed network infrastructure, and can be accomplished through an intermittent network connection, e.g., via mobile appliances that use wireless networks. Other electronic payment mechanisms have been proposed that require on-line third-party payment servers to process transactions. These mechanisms can be designed with any of the attributes of electronic tokens, including anonymity. They differ from electronic token systems in that (1) they depend on a network infrastructure and (2) they require the on-line involvement of at least one additional party and, in some cases, multiple parties. Because requiring an on-line third-party connection for each transaction could lead to processing bottlenecks and potentially undermine the goal of reliable use, this paper does not discuss third-party systems in any detail.

1.4 Structure of This Document

This report examines issues; design alternatives; and legal, regulatory and ethical considerations surrounding digital cash and related electronic payment mechanisms (notably electronic tokens representing credit and bank check functions). The next two sections describe the key requirements of electronic tokens and the system in which they must function. Section 4.0 considers various issues related to representing, storing, and retrieving electronic tokens. The rules by which the electronic token system should operate, and its management and control, are discussed in section 5.0.

2.0 Fundamental Properties

There are many ways to implement an electronic token system. All must incorporate a few fundamental features. Specifically, electronic tokens must have the following four properties.

Monetary value -- Electronic tokens must have a monetary value; they must represent either cash (currency), a bank-authorized credit, or a bank-certified electronic check. An electronic check without bank certification would also have monetary value, but it would carry the risk that the check, when deposited, might be returned for insufficient funds. Electronic tokens thus can comprise the electronic analogue of virtually all currently used forms of payment, including cash.

Exchangeability -- Electronic tokens must be interoperable, that is, exchangeable as payment for other electronic tokens, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations, electronic benefits transfers, and the like.

Retrievability -- Electronic tokens must be able to be stored and retrieved. Remote storage and retrieval (e.g., from a telephone or personal communications device) would allow users to exchange electronic tokens (e.g., withdraw from and deposit into banking accounts) from home or office or while traveling. The tokens could be stored on a remote computer's memory, in smart cards or other easily transported standard or special-purpose devices. Because it might be easy to create counterfeit tokens if they are stored in a computer or on a card that must be read into a computer, it might be preferable to store tokens on a dedicated device that cannot be altered. This device should have a suitable interface to facilitate personal authentication using personal identification numbers (PINs) or other means, and a display so that the user can view the card's contents. One example of a device that can store electronic cash is the Mondex card and pocket-sized electronic wallet recently announced by financial institutions and telecommunications suppliers in Britain.

Tamper-resistance -- Throughout their life cycle, electronic tokens should be difficult to tamper with, copy, or forge. Tokens should not be easy to copy or tamper with while being exchanged; this includes preventing or detecting duplication and double-spending. Counterfeiting poses a particular problem, since a counterfeiter may, in network applications, be anywhere in the world and consequently be difficult to catch without appropriate international agreements. Detection is essential in order to audit whether prevention is working.

3.0 Required System Features

To be accepted by the user, an electronic token system must contain certain controls that allow transactions to be verified and authenticated. The system also must be convenient, reliable, private, and protected. Descriptions and implications of these requisite system features follow.

Authentication -- Users must be assured that electronic tokens and their storage device (e.g., a smart card or PCMCIA) cannot be easily forged or altered, and that, if they are altered, evidence of this tampering will be immediately apparent upon inspection of the token or storage device. When electronic tokens are exchanged, the receiving party must be able to obtain certification that the tokens are authentic. This authentication may require on-line connection to some third-party authority, or it could be handled directly by the transacting parties. If the transacting parties are co-located, the authentication could be done off-line.

Nonrefutable -- Users must also be able to verify that exchanges have taken place between the intended parties. This verification could be provided by a receipt and/or proof-of-payment mechanism. Such mechanisms could include a record attached to the electronic token itself; a separate receipt; or a means by which a transaction could be traced, reconstructed, and verified upon request. Receipt and payment information must be nonrefutable, despite any complications that may result from delivery of services over long periods of time, interruptions in service, or differences in billing and collection policies of various service providers. Distribution and disclosure of receipts and proofs may be particularly complicated to achieve for services that are delivered over a long period of time.

Different services may have different policies. For example, a music provider might charge for partial delivery of an album (since the user may have abandoned the session once the favorite track arrived), while a movie producer might charge (or not charge) depending on how much of the movie had been delivered. The cause of interrupted delivery might also be considered; e.g., intentional customer action versus a problem in the network or provider's equipment. In general, implementing payment policies will be simpler when payment is made by credit rather than with cash.

Accessible -- Users must find the exchange process to be accessible, easy to effect, and quick. Speed in particular will have design and cost implications, being a function of network capabilities, computing power available at every locale, and the specific form of the electronic token.

Reliable -- The infrastructure supporting the exchange must be reliable. The user must feel confident that the NII and the supporting payment infrastructure can be counted on to be available on demand. The user must be assured that the electronic token system will operate reasonably well regardless of component failures or system load conditions.

Private -- The electronic token system must ensure and maintain privacy. Users must be assured that knowledge of transactions will be confidential, limited only to the parties involved and their designated agents (if any). Privacy must be maintained against eavesdroppers on the network and against unauthorized insiders.

Protected -- The users must be assured that they cannot be easily duped, swindled, or falsely implicated in a fraudulent transaction. The user must be protected against eavesdroppers, imposters, and counterfeiters. This protection must apply throughout the whole transaction protocol by which a good or service is purchased and delivered. This implies that, for many types of transactions, trusted third-party agents will be needed that can vouch for the authenticity and good faith of the involved parties.

4.0 Optional Features and Functions

There are several additional features and functions that should be considered in designing an electronic token system. These provide added safety, convenience, and value to the user. Although they are not required for a working electronic token system, most of these features have, in fact, been included in various proposed token systems.

4.1 Accounting

Features to be considered from an accounting and recordkeeping standpoint include the following.

Divisibility -- Electronic tokens could either be designed so they can be subdivided into arbitrary small units or available only in discrete increments. If change from a large-denomination token can be obtained remotely, token divisibility may not be necessary.

Receipts -- Purchasers seek refunds for any number of reasons. Regardless of whether their purchase was made via paper cash, debit or credit card, or electronic tokens, they will need a receipt or proof of purchase. New electronic analogues must be developed to replace physical receipts.

4.2 Conversions

Various features and functions involve the user's ability to convert electronic tokens into paper money and vice-versa.

Cash purchase of tokens -- Some users might prefer to purchase electronic tokens with paper cash. This practice would allow them to maintain anonymity. It would also let people without bank accounts purchase tokens.

Fungibility -- Users' ability to convert electronic tokens to paper cash and/or other monetary equivalents would increase the value and utility of the electronic token, particularly during the transition period when the NII is evolving and not yet universally used. On the other hand, this conversion capability could make the token a more attractive target for crime because of its increased fungibility (i.e., interchangeability).

International use and multi-currency -- People in the United States should be able to access and pay for foreign services as well as U.S.-based services from abroad. To support this access, electronic tokens would need to be available in multiple currencies. A service provider in one country could then accept tokens of various currencies from users in many different countries, redeem them with their issuers, and have the funds transferred back to banks in the local country. This ability to transport currency electronically across borders could have repercussions on trade and international banking laws.

4.3 Limits and Constraints

Many system requirements can be loosened and risk mitigated by imposing operational constraints, such as limits on (1) how much can be stored on and transferred by electronic tokens, (2) the time over which a given electronic token is valid, (3) the number of exchanges that can take place before a token needs to be redeposited with a bank or financial institution, (4) the number of such transactions that can be made during a given period of time, or other conditions. These and similar constraints and limits, however, introduce a whole set of implementation issues all their own.

Time limits -- Time limits could be imposed beyond which the electronic token would expire, worthless. The user would have to redeem or exchange the token prior to the expiration deadline. For this feature to work, electronic tokens would have to be date/time-stamped, and time would have to be synchronized across the network to some degree of precision.

Maximum amount and rate limits -- An upper limit could be imposed on the allowable value that could be assigned to any single electronic token device or that could be transferred to the same device within a given period of time. Imposing this maximum limit, however, could limit the issuer's liability. Additionally, since the user's terminal could be programmed to execute small transactions continuously at a high rate over the network, a strategy of reporting transactions over a certain amount will be ineffective for law enforcement. However, a tamper-resistant unit could enforce a policy involving both transaction size and value with time. For example, an "anonymous coin-purse" feature of the unit might be capable of receiving or spending no more than $500 in any 24-hour period. Alternatively, the "rate ceiling" for the next 24 hours could be made dependent on the rate of use or on the number of exchanges that could be permitted before a token would have to be redeposited in a bank or financial institution and reissued. Exchanges could also be restricted to a class of services or goods (e.g., electronic benefits could only be used for food, clothing, shelter, or educational purposes).

Conditional payment and post-dating -- The exchange process should allow payment to be withheld from the seller upon the buyer's instructions until delivery of purchases, goods, or services within a specified time in the future. Conversely, it should allow delivery to be withheld upon the seller's instructions until payment is received.

4.4 Traceability

The ability to trace transactions made in an electronic token system involves the following features.

Token registration -- It might be useful for all electronic tokens issued to be uniquely identified and registered. Just as physical coin and paper currency is identified with a unique serial number, so too could electronic tokens be similarly protected. It would then be easier to spot copies or tokens with duplicate or unregistered numbers.

Anonymity -- The issue of anonymity involves a spectrum of positions. Many users may want their transactions to be completely anonymous, with the identity of either the buyer or seller unknown. However, when a court order or warrant is presented, it might be in everyone's best interests to be able to reveal user identities and transaction details. In some cases, too, users might want to give up their anonymity in exchange for detailed reports of transactions, to improve their management information system, or to sell details of transactions to marketing organizations. The best resolution of these various concerns might be "almost anonymous" transactions, in which the transactor's anonymity is maintained unless either the transactor gives permission and/or a government warrant is issued. From a technical standpoint, additional encryption techniques will be needed to help achieve the desired level of anonymity, along with the relaxation of certain accounting features, constraints, and limitations.

4.5 Safety

An electronic token system raises a new set of safety issues. The anonymity, convenience, and privacy offered by electronic transfers over the NII can be turned against a user. For example, a criminal could force a victim to transfer tokens withdrawn from the victim's account to the criminal's electronic token device over the network. The criminal could then transfer the account to an accomplice (possibly in another country) and flee. This scenario is less risky for the criminal than kidnapping and forcing someone to make a withdrawal from an automated teller machine (ATM), since the robbery can be done in the privacy of the victim's residence or at a place of the robber's choice. It is also more lucrative, since the victim can be forced to execute a number of transactions of a high value. Moreover, if the transfer session is anonymous, the criminal could be very hard to trace. These possibilities give rise to various safety-related features and functions related to the following.

Ownership -- To ensure authentic ownership of a given token, the token could be linked to the current owner. This feature would require authentication of the owner as well as of the electronic token (requiring, for example, passwords, shared secrets, or biometrics such as verbal verification, dynamic handwritten signature recognition, fingerprints, hand geometry, or retinal scan). The advantage of such a feature is that lost or stolen electronic tokens would be worthless to anyone but the owner. Digital signatures ensure only that the electronic token is authentic, not the holder of the electronic token. The use of PINs or other secrets ensures that the holder of the electronic token is in possession of some knowledge believed to be known only by the legitimate owner. It is, however, possible for this knowledge to be compromised and used without the owner's awareness.

Biometric authentication cannot be duplicated by anyone but the owner, but may be coerced. If an electronic token is linked to either an owner's secrets or biometrics, the transfer of tokens to new owners would require altering this linkage. Alternatively, the owner could be identified only with the device that is storing/producing the token. It may be useful for the electronic token system to feature a false positive password/secret that provides a seemingly legitimate response, but in reality tags the transaction as invalid, renders the electronic token useless if used by anyone but the rightful owner, or notifies the authorities that a crime is in progress.

Co-located applications and data -- The relationship between electronic tokens used as payment mechanisms and other security-sensitive information objects that might be stored with electronic tokens needs to be carefully defined, especially when these are co-located in a single multipurpose device. Driving license information, health care-related information, buying preferences, biometrics, and other personal profile data as well as monetary units of value may all need to be stored in the same computer, card, or device in a private and secure fashion. Monetary electronic tokens should be able to be logically and/or physically isolated from other co-located data, lest linkages offer new opportunities for unauthorized misuse.

5.0 System Management and Control

Ease of implementation and enforcement will depend on the specific features and functions that make up an electronic token system. For example, if electronic tokens can be exchanged and their ownership transferred off-line without links to the previous owners or transaction records, it will be more difficult to audit and enforce government and commerce regulations; counterfeiting and tampering will also be more difficult to prevent.

However, the mere selection of features is not sufficient to ensure a safe and secure system. Meeting the goals of system safety and security will require careful consideration of the entire system including user behavior and financial transaction processes as well as hardware and software. Any electronic token system encompasses many vulnerabilities that are not fully addressed by encryption and digital signature technologies alone, but that are often attacked through faulty or negligent people and processes.

System implementation should make money-laundering, black market activities, and insider fraud difficult to effect and easy to detect. Some important system management controls, policies, and procedures in meeting this goal are discussed below.

5.1 Legal Measures

Laws can be passed with strict penalties. These laws can help deter potential criminals who would knowingly evade legal business practices. However, if the prize is tempting enough, evasion simple enough, and the probability of detection low enough, laws will not be sufficient to prevent crime. The system must be designed with crime prevention as a key consideration. After-the-fact attempts at law enforcement will be ineffective and will further overload the courts and penal institutions.

5.2 Technological and Administrative Controls

A mix of technologies can be used to ensure security and privacy and prevent fraud. These technological controls include tamper-proofing cards, circuits, and tokens and making them tamper-evident; encryption; digital signatures; key management schemes, including dynamic key exchange; threat and vulnerability analysis; biometrics; and exchange of shared secrets. The choice of technologies made will affect costs, performance, and the degree to which the required and desired features can be attained.

Administrative controls can also be applied. For example, when electronic tokens are withdrawn or deposited remotely into an account, institutions could authenticate themselves to customers, as well as have the customers authenticated to the bank. Smart cards could require methods for the point-of-sale terminal device or computer to authenticate itself to the smart card. These techniques should not accidentally result in service denial to legitimate users. Additionally, "watch lists" of bad cards or tokens could be maintained to facilitate early interception of known fraudulent activities.

5.3 Audits

The system could be designed to provide an audit trail of the exact path an electronic token has traveled. This audit trail would account for each electronic token issuance and exchange, and could be used to detect double-spending and to prove that payment was sent, received and accepted, or deal with other things as specified.

5.4 Policy and Practice Issues

Several important issues associated with how electronic tokens are to be implemented are presented below.

Certification authorities (CAs) -- Most implementations of electronic tokens will require a certifying authority, some trusted third party that vouches for the authenticity of a transacting party or identifying information such as the public key used for encryption and digital signature schemes. Consider, for example, public key digital signature mechanisms. In this case, the signing party encrypts a message with his/her private key and distributes his/her public key to the receiving party. The receiving party can decrypt the signed message with the public key and knows that only the person with the private key could have encrypted the message. But how does the receiving party know that the correct public key was sent? The public key could be included in a certificate signed with the private key of a well-known trusted third party.

Trusted third-party organizations are needed that can (1) vouch for the legitimacy of the distributed public keys and (2) certify and register ownership of the associated transaction devices. An electronic token system will probably require a hierarchy of such CAs, whose functions, policies, procedures, and interrelationships will need to be determined. For example, the following certification functions are needed: CAs who set policies for how their certificates are issued and distributed and who run the cryptographic systems, agents of the CAs who actually verify identities and/or issue certificates, and directories that publish certificates, certificate revocation lists, etc.

Issuers -- The issuers of electronic tokens must be willing to exchange the tokens they create/issue for actual money. Who should issue electronic tokens? Will each bank/government agency issue its own, individually identified electronic tokens? If so, must each entity honor and accept each other's tokens? Alternatively, will organizations issue tokens from a common pool? If so, should there be a central issuing organization? Should this be a governmental body like the U.S. Treasury or the Federal Reserve?

Should there be restrictions on who can issue electronic tokens? Should issuing organizations be licensed and/or regulated? Are international agreements and regulations required? Without sufficient controls and safeguards, a wide variety of official and unofficial currencies could be created and circulated via the NII.

Obligations -- Paper cash is obligated (backed) by the U.S. Government. Who should be obligated to honor electronic tokens? If a bank issues an electronic token, should the bank be obligated to accept it as long as it is certifiably authentic?

Liability -- Who is liable (i.e., suffers the loss) when an electronic token is lost or stolen? Should lost or stolen tokens be traced and/or replaced by the issuer as are traveler's checks, or treated like cash (i.e., not replaced)? If counterfeit electronic tokens are accepted in payment, who is liable? Is it the merchant or service provider accepting the electronic tokens, the bank or financial institution issuing the tokens, the bank or financial institution accepting the tokens, or the last person found holding the tokens when they were discovered to be counterfeit?

Escheatment -- State escheatment laws presently require accounts with unclaimed balances and unused traveler's checks to revert to the state after a specified period of time. Should electronic tokens representing digital cash similarly revert to the state if they remain unused after a specified period of time? If this practice is adopted, the electronic tokens system must be able to uniquely account for all issued and outstanding electronic tokens, and be able to determine which state is eligible to receive the funds.

Universality -- Universal service is a fundamental requirement of an electronic payment system. Anyone who wants to use electronic tokens should be able to obtain them, even if an individual does not have a bank account or a line of credit with a bank. Thus, people should be able to purchase electronic tokens with paper cash or government credits. Users should not need to be prequalified to obtain and use electronic tokens. However, since universal service should not necessarily imply anonymity, should users be required to identify themselves when purchasing tokens?

Regulation -- An electronic token system will need to support the enforcement of international, national, and state regulations preventing monetary fraud and abuse (e.g., tax evasion and money laundering). Simply setting a maximum allowable transaction size will not work because in a totally electronic world, computers could tirelessly exchange electronic tokens at the speed of light, effectively substituting one large transaction with many small ones. Rather, constraints are needed on the rate at which an individual user or device transfers money over the NII. Additionally, transaction amounts (e.g., the total amount transferred over a given period by a given user or device) should be monitored. The ability to perform this monitoring raises questions about how the electronic token system is implemented. Should tokens be tagged so that flows (perhaps of a given minimum value) of electronic currencies across geographic boundaries (e.g., states and countries) can be reliably reported? Monitoring transborder information flows without state and international cooperation will not work. A uniform international electronic commercial code and cooperation between law enforcement organizations are required.

Fees, float, and redemption -- Will users be assessed a fee (issuance charge) when purchasing electronic tokens? If so, will this charge be exacted at the time of issuance or billed for later payment? Are redemption charges appropriate? Between the time the token has been purchased and its redemption (float), the unclaimed money could be invested and could collect interest or could be treated like a cash withdrawal. Who keeps the float and for how long? Should there be any special reports or checks made at redemption, for example, to determine if the sum of payments made equals initial withdrawals?

Accounting -- There are various design alternatives regarding the extent to which electronic tokens are accounted for and by whom, and the way in which accounting records are stored. These various alternatives affect both the privacy and integrity of the transaction, often in opposing ways. Will user decrements, increments, balances, and entire transaction histories be recorded? Will records be maintained on user cards or devices, or in a control bank's or issuer's database? For how long will records be maintained? Should there be any federal, state, or local government requirements regarding accounting and recordkeeping?

6.0 Summary

Although alternative payment mechanisms for use over the NII exist, electronic tokens offer several particularly attractive features. Electronic tokens can duplicate many of the conveniences and benefits of real cash when used in financial transactions over the NII. Furthermore, they can be used even over unreliable networks or networks with only intermittent connectivity. Also, electronic tokens require minimal communication and processing resources.

Certain choices must be made regarding how electronic tokens are to be implemented in the NII. A broad implementation could extend electronic tokens beyond serving as a simple (albeit secure and protected) analogue to paper cash to serving as analogues to such payment mechanisms as checks, credit charges, and electronic benefits transfers. Or, electronic tokens could be implemented with all the features of paper cash, including anonymity, and allow an unlimited number of "inaudible" off-line person-to-person exchanges. Such an implementation could be extremely difficult to manage and control. Alternatively, electronic tokens could be restricted to certain limits and features. For example, the number of off-line person-to-person exchanges allowed could be limited, or there could be a limited time period during which the token is valid before it must be redeemed by the issuer or a bank.

Numerous other implementation issues will need to be addressed, including liability, identifying valid issuers of electronic tokens, the need for a multi-currency capability, and the need to establish international rules and regulations regarding the use of electronic tokens before a truly secure, convenient, safe and private electronic token system can be developed and accepted.

The decisions and collective wisdom not just of financial and technology experts, but of public policymakers and ultimately of ordinary consumers will be needed to realize the potential benefits of this emerging technology. The Cross-Industry Working Team will promote the exploration and diffusion of technical solutions to meet new opportunities for electronic commerce afforded by the NII.

Glossary

Automated teller machine (ATM): A self-service unit that lets a user with appropriate identification and account relations carry out financial transactions such as cash withdrawal.

Biometrics: Methods of personal authentication that rely on electronic sensing of a unique personal characteristic such as a fingerprint.

Dedicated network: A communications facility established for a specific purpose. Each remote terminal on the network is assigned to a specific termination point.

Electronic funds transfer: Any funds transfer that is sent electronically, either by telecommunication or written on magnetic media such as tape, cassette, or disk.

Encryption: Using ciphers to alter information before it is transmitted over a network. Encryption ensures, to the greatest extent possible, that messages cannot be read or altered during transmission.

Float: The value of funds tied up in the payments process. Also, funds that become available to an account holder before a related payment has cleared; this may occur with a funds deposit or withdrawal.

Hand geometry: A method of personal authentication based on the characteristics of an individual's hand (e.g., its shape, dimensions, etc.).

Issuer: A financial institution or other organization responsible for supplying credit cards, debit accounts, checks, electronic tokens, etc. An issuer sets the card or account holder's credit limit, pays for his/her purchases, and funds the free credit period and any extended credit.

Handwritten signature recognition: A personal authentication technique based on pen acceleration and pressure during signature writing.

Key: A secret value used in an encrypting algorithm known by one or both of the communicating parties; it is similar to a combination number for a vault. A symmetric key is used to control both the encryption and decryption processes. Public key encryption uses a pair of different values to control a related encryption and decryption process: the sender encrypts with the receiver's public key, and the receiver decrypts with his/her private key. A session key uses a unique key for a simple data exchange or set of data exchanges.

Key management: The process by which keys are distributed to usage points while kept in a protected form by encryption.

Off-line: A mode of operation that does not require a network and/or third-party authentication.

On-line: A mode of operation that does require a network and/or third-party authentication.

Paper cash: Bank notes and coins.

Personal authentication: Techniques used to authenticate an individual (i.e., validate an individual's unique identity) by testing for knowledge of secret codes or unique physical traits.

Personal identification number (PIN): A unique number used to identify a customer when using credit and debit cards in ATMs, etc. PINs are normally four- to six-digits long and are to be kept secret by the user.

Protocol: A specified procedure or process used to achieve a specific and common result, such as a network communications message format.

Remote: A transfer mode that, among other things, allows payment transactions to be conducted over public networks between two or more parties that are physically separated.

Retinal scan: A personal authentication technique based on infrared scan of the eye retina.

Smart card: A card form device containing a microprocessor.

Validate: Substantiate that the elements of a financial transaction are correct, appropriate, and acceptable.

Rank & file

Last update: 7/12/08