This document was produced by
System Development Corporation in performance of IRAD 983-7760

series base no./vol./reissue
TM- 5616 /000/ 00

author
D. Kaufman & K. Auerbach
technical

release
for C. Weissman
date
12/10/75 page 1 of 27 pages

TM a working paper

System Development Corporation
2500 Colorado Avenue • Santa Monica, California 90406
Telephone: 213-829-7511

A SECURE, NATIONAL SYSTEM FOR ELECTRONIC FUNDS TRANSFER

ABSTRACT

This paper presents guidelines for development of a secure national network for electronic funds transfer. Six security principles are developed. These principles, together with certain important networking notions, are utilized to evolve a system level design of a secure localized system for electronic funds transfer. This design is then further defined in order to address the various problems involved when local systems are linked to form a national network. It is concluded that national standards are needed in order to prevent proliferation of incompatible local systems.

Keywords:
Banking, Cryptography, EFTS, Internetting, Network Privacy, Security, Standards.

1.0 INTRODUCTION

As the computerization of bank functions continues its rapid advance, electronic funds transfer is becoming a reality. Independently developed local systems are evolving -- but the emergence of a system national in scope is inevitable. Unless planning for security and for operation on a national scale begins now, development of an efficient and secure future system may be impossible.

This paper presents guidelines for development of a secure national network for electronic funds transfer. Six security principles are developed. These principles, together with certain important networking notions, are utilized to evolve a system level design of a secure localized system for electronic funds transfer. This design is then further defined in order to address the various problems involved when local systems are linked to form a national network.

We believe that a secure, national network for electronic funds transfer (EFTS) can be built with currently available technology. We do not suggest that the monumental task of interconnecting all the various financial institutions in the United States be undertaken, rather we contend that pilot EFTS networks being planned today could and should provide a high degree of security assurance. Furthermore, these pilot systems could be built so that as they inevitably grow, proliferate, and interconnect, they can be linked together to form a national network without major impact on either local system structure or local system security and privacy.

2.0 EFTS SECURITY PRINCIPLES

As a basis for this discussion of EFTS security principles, several basic assumptions must be made about EFTS schemata. These include:

1. All funds transfer transactions are initiated by a cardholder (possibly assisted by a teller or a merchant) at any of a variety of Point of Sale or Automated Teller devices. These devices are commonly referred

to as Remote Service Units (RSUs). Although other transactions not involving a transfer of funds may be handled by an EFTS system, they are not addressed in this discussion to avoid distraction from the major issues addressed.

2. Each bank card has imprinted or recorded on it a personal account number (PAN), institution identification information, and other data such as the expiration date of the card. A cardholder initiating a transaction must supply a value not on the card. This value is called a Personal Identification Number (PIN). The PIN was conceived as an aid in verifying the identity of the user of the card (i.e., the PIN is a password).

3. All funds transfer transactions must be authorized. An authorization, or transaction approval, is based upon a verification of the cardholder's identity and an examination of his account. If the cardholder has supplied the appropriate PIN and if his balance or credit limit is sufficient to allow the transaction, then an authorization is generated. A Host Processing Center (HPC), the computer facility of a financial institution, will typically authorize transactions.

4. Financial institutions may require that the EFTS network provide backup support for the HPC authorization function. For instance, the network may have to provide an alternate site to perform transaction authorizations when the primary HPC is down. Similarly, the EFTS network may be required to log all transactions.

These assumptions must be considered in the development of any EFTS network design.

Security Principle #1: The PIN should be known only by the cardholder.

It is important to realize that the PIN is potentially a powerful tool for providing EFTS security, and apparently the only currently viable means for positive identification of the cardholder.

The authentication process is important since cards can easily fall into the wrong hands. Cards can, of course, be stolen or lost. Furthermore, any card which can be easily produced can also be easily forged. Electronic funds transfer will provide a powerful incentive to illegally produce and distribute fraudulent bank cards. The identity of cardholders must, therefore, be authenticated.

The PIN, therefore, plays a critical role in EFTS security, and PIN distribution must be carefully controlled. It has been suggested that PINs be stored at the computing facility of the cardholder's financial institution. It may also be desired to store PINs at the network's backup sites. Unfortunately, the greater the distribution of the PIN, the greater is the risk of illegitimate PIN acquisition. For example, if PINs are stored at the bank, they are potentially exposed to dishonest bank employees. And more distressing, if PINs are stored at a backup site, they are potentially exposed to personnel who may not even be under the control of the cardholder's bank.

Only the cardholder need know the PIN if, at the time of issue and within the network, it is transformed by a one-way process to create a unique new value, and if only the transformed version is used to authenticate cardholders. The new value could then be used for cardholder authentication, but the original PIN could not be determined from this new value. Thus, neither the HPC nor the backup sites have access to the original PIN. PIN transformation is discussed in more detail in the system level design portion of this paper.

Security Principle #2: There should be no way to derive the PIN from information on the card.

The importance of PIN security to EFTS security is recognized in both the banking and the security communities. Oddly enough, however, many PIN schemes currently being discussed are based upon the notion of deriving the PIN from the information on the card (and primarily from the PAN). Such schemes do reduce the need for PIN storage in the system since PINs can simply be derived when needed, but such schemes risk PIN exposure.

Schemes in which the PIN can be derived from information on the card are inherently weak. Once the algorithm used to convert card information into PINs becomes exposed, any person who obtains the card must be assumed to have obtained the PIN as well. This observation has two important implications in general PIN systems. First, the secrecy of the PIN depends entirely upon the secrecy of the algorithm used to generate the PIN. Second, the incentive for theft of an algorithm is high, since that algorithm is utilized to generate all PINs for a particular institution's cards. The means for determining such algorithms exists. The algorithms may be exposed by bank personnel who, by the nature of their jobs have access to it, or given sufficient cards with known PINs, it may be possible to synthesize the algorithm. Once the means of deriving PINs is known, production of apparently valid but unauthorized cards is a simple matter. The system level design section of this paper will describe a method of PIN verification which does not require that the PIN be derivable from information on the card.

A rough analogy may be drawn to the security problem of telephone credit accounts. Credit identification numbers are based on the account holder's telephone number, and the time lag between the development of new methods of deriving credit card numbers and the fraudulent use of them has always been short indeed. The potential rewards of defrauding an EFTS system are incalculably greater.

Security Principle #3: Exposure of PINs should be minimized during a transaction.

This principle stresses once again the importance of the PIN in EFTS security. A transaction will involve many devices and probably more than one financial institution. PINs should, therefore, be transformed or otherwise protected at the earliest possible stage in the transaction.

Security Principle #4: Sensitive or private transaction data should not be subject to unauthorized exposure.

During the course of a transaction, sensitive data passes through a variety of devices and may be transmitted over public communications lines. Not all EFTS devices may be "trustworthy." Communications lines can be easily tapped. Obviously any sensitive data such as the PIN should not be exposed unnecessarily. Furthermore, because privacy statutes are likely to be enacted in the near future, the network must exercise strict control over all personal information involved in transactions. The PAN, for example, may be regarded as private information and not all devices will need to have access to the PAN.

Security Principle #5: Transaction data should not be subject to unauthorized alteration.

As transaction processing is performed, alteration of certain data could result in authorization of otherwise illegitimate transactions. For example, transactions may be diverted to the wrong institution or the amount of the transaction might be changed during a transaction, fooling the HPC into authorizing an improper transfer. Protection via an encrypted error detection field is a simple technique to prevent such unauthorized alteration. This technique is detailed later in this paper.

Security Principle #6: All transaction requests and transaction authorizations should be authenticated at their destination.

RSUs, where all transaction requests originate, and HPCs, where processing of the transaction occur, may be physically remote from one another. However, each must act on information received from the other. It is essential that the

identity of the source of information be authenticated by the receiver of the information. An HPC must know that the request it receives actually comes from an RSU and not an outside source,such as a penetrator tapping onto the line. An RSU must know that a transaction authorization actually came from the appropriate HPC. Otherwise a physical transfer of funds or merchandise may occur when the necessary authorization was denied or simply did not take place.

An example will illustrate this point. A grocer rings up a bill for a customer's purchase. The customer wishes to use his card to pay the bill, and wishes to receive an additional $50.00 cash. The grocer enters the transaction request on his RSU and the customer inserts his card and enters his PIN. When the grocer receives an authorization on his RSU, he accepts the transfer as payment and gives his customer $50.00 in cash. A penetrator could have injected a false authorization message somewhere along the line. The grocer would then assume that his account has been credited in the amount of the cash disbursement plus the cost of the groceries, but the "authorization" is fraudulent and the grocer has been cheated. A direct, positive identification of the source of messages in the system must be incorporated to prevent such fraud.

3.0 SYSTEM LEVEL DESIGN

The six security principles may now be combined with basic intercomputer network concepts to formulate a general design for a local EFTS system. The following paragraphs describe a design that has the potential to provide a high degree of security assurance.

The design incorporates cryptographic devices. These devices encipher data (i.e., transform data in order to conceal its meaning) and decipher data (i.e., reverse the encipher process in order to render data once again intelligible). Proper use of cryptographic techniques can greatly enhance network security. However, in order to simplify presentation of the design, the system is first presented and analyzed without cryptographic devices. The cryptographic devices

are then introduced and discussed in detail. It is important to note, though, that security is an integral part of the entire design.

An EFTS system configuration without cryptographic devices is illustrated in Figure 1. This structure includes four major types of devices or processors. Two of these, RSUs and HPCs, were discussed previously. A third type of device, the transaction processor (TP), interfaces RSUs to the rest of the EFTS system, manages funds transfer requests initiated at RSUs, and performs the one-way PIN transformations. The fourth device type, the switch, interconnects HPCs and TPs.

An example (see Figure 2) may help to clarify the function of these devices and the relationship between them. Using the example of the customer at a grocery store, we will assume that the customer maintains his card account at institution X and that the grocer maintains his account at institution Y. The customer desires to use his card to pay his grocery bill of $35.00 and wishes to receive an additional $50.00 cash. The customer inserts his card into the RSU and enters his PIN. The grocer enters a request for a transfer of $85.00 (i.e., $35.00 for the groceries plus $50.00 for the cash the grocer will give the customer) from the customer's card account to the merchant's account. The RSU collects all this information and forwards it to the TP.

The transaction request is then received by the transaction processor. The TP isolates the customer's PIN from the transaction request and derives two new values, PIN' and PIN'', by performing two successive transformations on the PIN. PIN'' is compared with a set of digits, called cryptographic check digits (CCDs), recorded on the customer's card. If PIN'' is not equal to the CCDs, the PIN is invalid. The funds transfer would not occur and a transaction denial would be sent to the grocer at the RSU. In this example we will assume that the CCDs and PIN'' are equivalent and that transaction processing continues.

The TP then sends a debit request message destined for HPC X, the computer facility of the institution at which the customer has his account. The debit

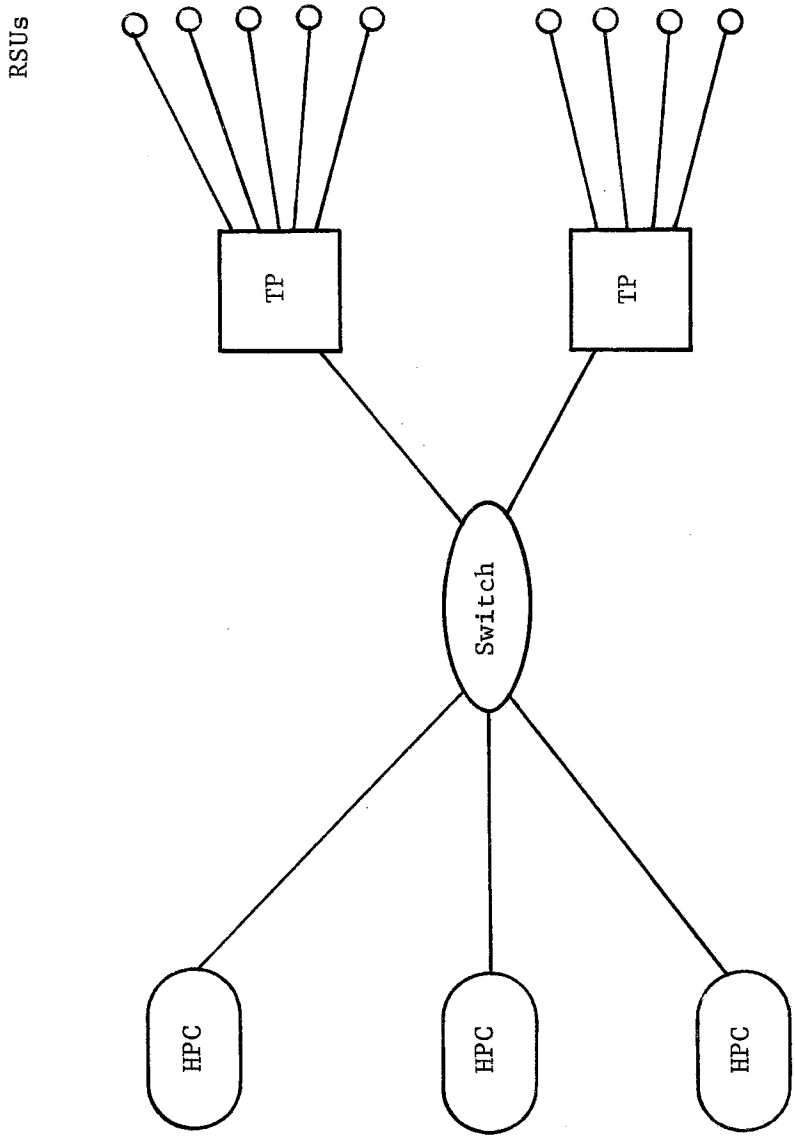


Figure 1. Local EFTS Network (without Cryptographic Devices)

RSU	TP	HPC X	HPC Y
1. Grocer enters transaction 2. Customer inserts card into RSU and enters his PIN 3. Transaction data is forwarded to TP	4. Transaction data is received from RSU 5. PIN' and PIN'' are generated 6. PIN'' is checked against CCDs 7. PIN'' check succeeds (If check fails, transaction is aborted at this point.) 8. Debit Approval Message is created and sent to HPC X	9. Debit Request Message is received from TP 10. PIN' is checked 11. PIN' check succeeds (If check fails, rejection is sent to TP and transaction is aborted at this point.) 12. Customer's account balance is checked for sufficiency. (If check fails, rejection is sent to TP and transaction is aborted at this point.) 13. Customer's account balance is found sufficient and $85.00 (i.e., the transaction amount) is deducted. 14. Debit Approval Message is created and sent to TP.	
	15. Debit Approval Message is received from HPC X 16. Credit Message is created and sent to HPC Y, Transaction Approval Message is created and sent to RSU.		17. Credit Message is received from TP 18. Grocer's account is credited with $85.00
17'. Transaction Approval is received from TP 18'. Customer receives groceries and $50.00 in cash			

Figure 2. An EFTS Transaction

message is addressed to HPC X and transmitted via the switch. It should be noted that the customer's PIN is not transmitted, instead PIN' is sent along with additional transaction information.

Upon receiving the debit request, HPC X verifies that PIN' correlates properly with the customer's PAN and that the customer's account balance is sufficient to cover the $85.00 request. If either test were to fail, the debit request would be denied and a debit refusal sent to the TP.

Assuming the debit is approved, HPC X records the debit request, reduces the customer's account balance by $85.00, addresses a debit authorization to the TP and transmits the authorization via the switch.

The TP sends two messages upon receiving the debit authorization. One message is sent to the grocer's RSU, indicating to the grocer that the funds transfer has been approved. The second message is a credit message sent to the HPC Y via the switch. At this point the transaction is completed.

The transaction scenario outlined above demonstrates some basic functions of an EFTS system. Several simplifying assumptions were made to clarify the presentation. Neither backup support for HPCs nor cryptographic devices were included, and logging of transaction data for auditing and accounting was not discussed. Furthermore, message acknowledgements and retransmissions were ignored. Each time a network message is transmitted, an explicit acknowledgement is expected. If an acknowledgement is not received promptly, the message should be retransmitted. Throughout this design presentation we will assume that an acknowledgement/retransmission mechanism exists where appropriate.

In the subsequent, detailed discussion of the local EFTS design, the issues of HPC backup, logging and auditing will be considered. The security of the EFTS system will be analyzed after the full presentation of the system level design.

3.1 THE SWITCH

The switch interconnects HPCs and TPs. The exact nature of the switch is of no concern here -- any switch which is capable of carrying messages to a specified destination in a timely manner is acceptable. In a centralized system the switch may consist of a single message switching computer. On the other hand, the switch may consist of a geographically distributed network of message or packet switching mini-computers. The term "distributed networks" as used in this paper means those networks where messages, or pieces of messages -- packets -- are carried from source to destination by being relayed from one switching computer to another until the destination is reached. Currently such distributed networks can relay a message across the United States in less than one-half second.

The distributed approach (which is used in the ARPANET) offers many advantages over the centralized approach. Distributed networks have the potential to provide alternate message pathways when one of the switching centers fails. When a centralized switch fails, the entire EFTS system halts. Distributed approaches, besides having a great potential for reliability, may be designed to adaptively route traffic through the various communications paths in order to reduce communications delays.

Unfortunately, distributed systems are not necessarily the most cost effective approach for a local EFTS system. Distributed systems generally require a much higher initial investment than centralized systems. It should be noted, though, that either a centralized or a distributed switch can be incorporated into a local EFTS system without impacting other system components.

3.2 HOST PROCESSING CENTERS

Each HPC is the computer facility for a specific financial institution and as such is subject to the particular policies of that institution. A large and varied population of HPCs now exists. The manner in which accounts are maintained and PINs are handled will undoubtedly vary.

Each HPC must adhere to the message formats and protocols developed for the local EFTS system. All communication between HPCs and TPs must conform to these standards. For instance, HPCs will receive only transformed PINs. The precise manner in which transaction messages are generated, transaction data interpreted, and transformed PINs verified can be determined by each institution.

Functions may be desired in the EFTS system other than those illustrated in the simple transaction scenario presented above. For example, a facility to back up HPCs or to log data on all transactions is likely to be included in most EFTS system requirements. In this EFTS system design these functions are provided by one or more special-purpose HPCs (see Figure 3). The switch need not distinguish between such special-function HPCs and transaction HPCs.

Only TPs and HPCs need to recognize the functions of these special HPCs. It is expected that a TP would transmit a message to the logging HPC at the start and end of each transaction. Similarly, the debit and credit HPCs would transmit log messages to the logging HPC each time they either authorize or refuse a request.

Whenever a primary HPC is not operating, it is expected that TPs would interact with a backup HPC. The backup HPC would partially determine the validity of debit requests based upon information collected from HPCs when they are operating. Transaction information would be stored at the backup HPC until the primary HPC is again operating.

3.3 TRANSACTION PROCESSOR

The TP manages all transactions in the EFTS system. The TP interprets each transaction request received from an RSU. A set of actions is associated with each type of transaction. These actions include a sequence of messages to be sent to HPCs and the RSU initiating the request.

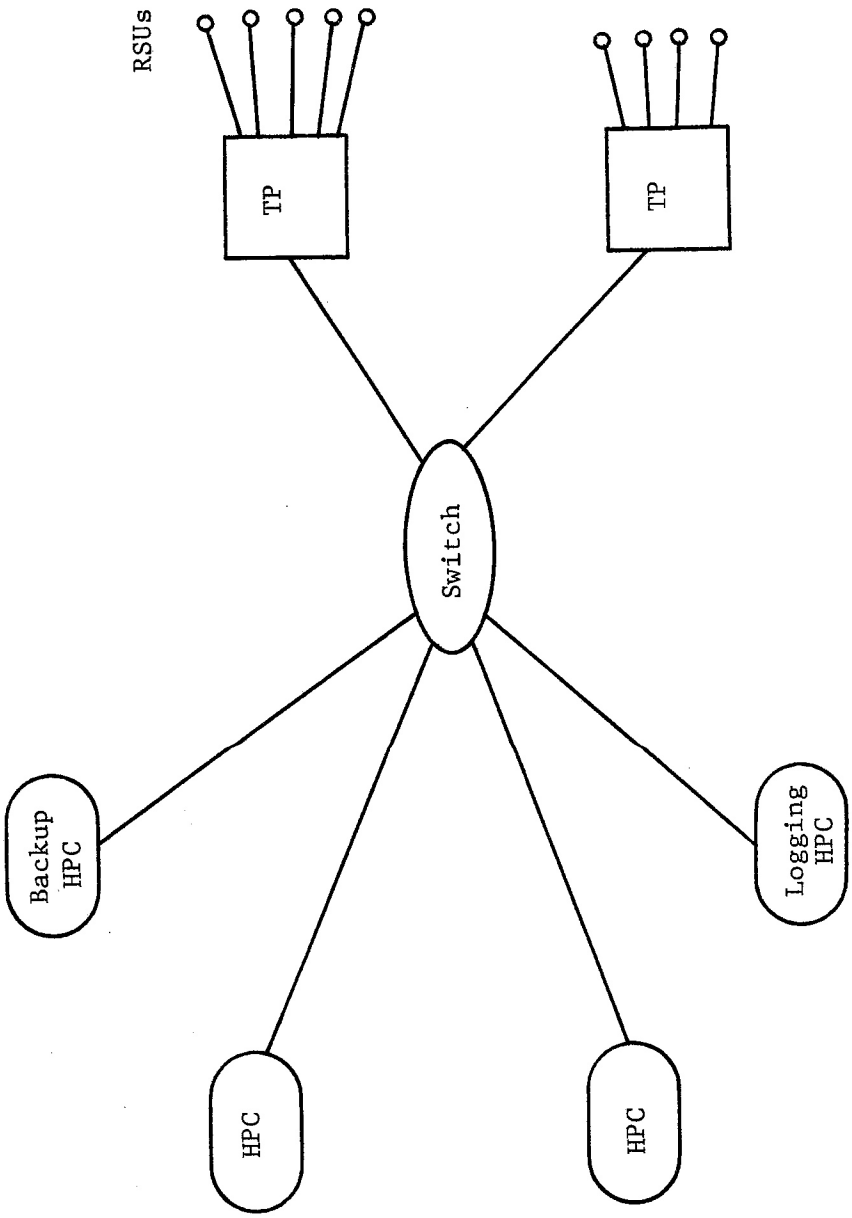


Figure 3. Local EFTS Network with Special-Purpose HPCs.

The TP must determine to whom the various transaction messages should be sent. Thus the TP must maintain tables indicating where messages should be routed.

The TP manipulates PINs. Upon receiving a transaction request, the TP creates two transformed PINs, PIN' and PIN''. Both transformations should be PIN dependent (i.e., they should vary with the value of the PIN) and should be resistant to attempts to determine original PINs from transformed values.

Transformations of this type can be performed in many ways. One such technique employs the NBS standard algorithm for data encryption. This algorithm has two inputs, a text string and a key. The output is a scrambled version of the input text string. The algorithm has the desirable property that even if both a sample input text string and the output are known, the key can only be determined by testing all 76×10^{15} possible keys. (This protects future cyphers from sophisticated penetration attacks.)

The transformation process is illustrated in Figure 4. In this method the PAN is the first text input to the NBS algorithm and the PIN is the key input. The output of the first application of the algorithm is PIN'. PIN' is then input to the algorithm as the text and a predetermined but secret value is input as the key. The resulting output is PIN''. Thus both PIN' and the "secret value" must be known to determine PIN'' and both the PIN and the PAN must be known to determine PIN'. The important security implications of this approach are discussed later.

3.4 CRYPTOGRAPHIC DEVICES

Two types of cryptographic devices are included in the EFTS system design. These devices are referred to as Network Cryptographic Devices (NCDs) and Serial Cryptographic Devices (SCDs). An EFTS network incorporating cryptographic devices is illustrated in Figures 5 and 6.

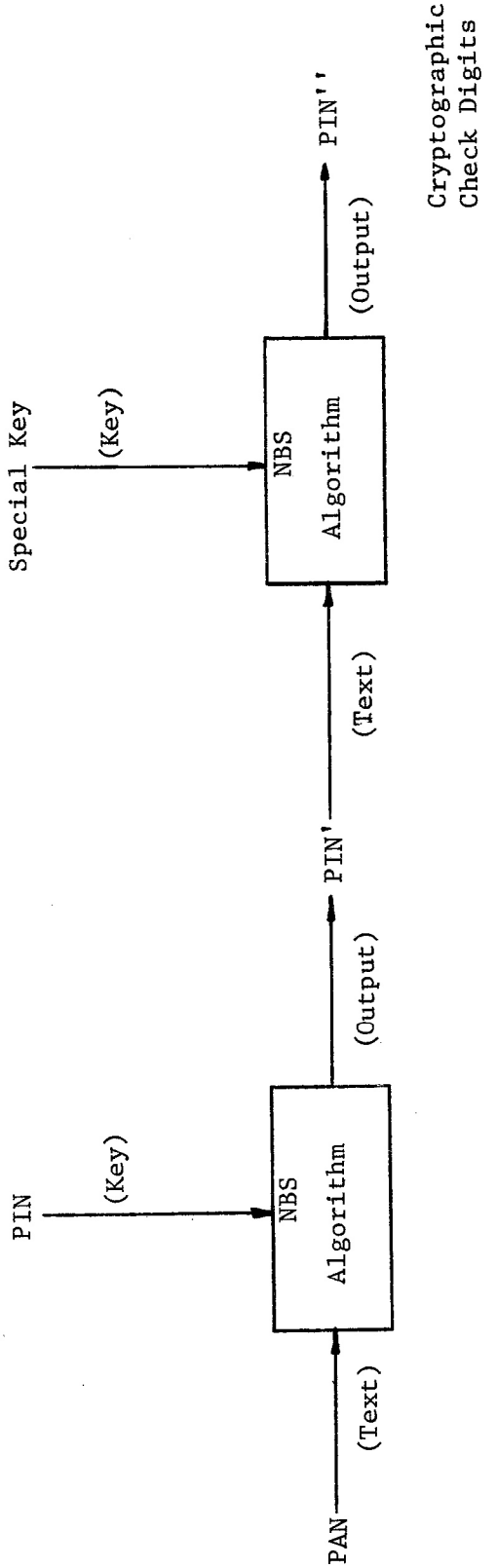


Figure 4. PIN Transformation Using National Bureau of Standards Data Encryption Algorithm

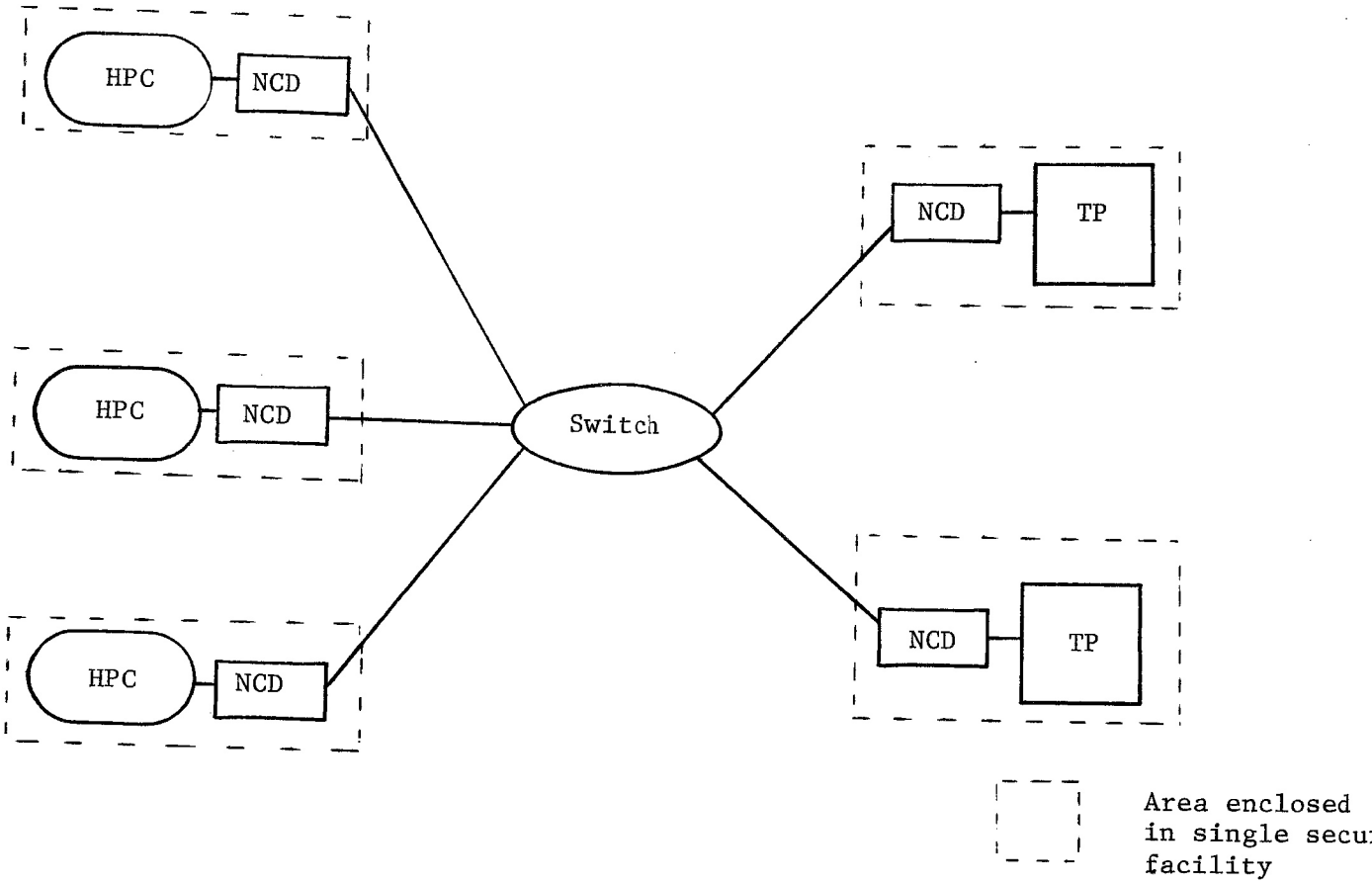
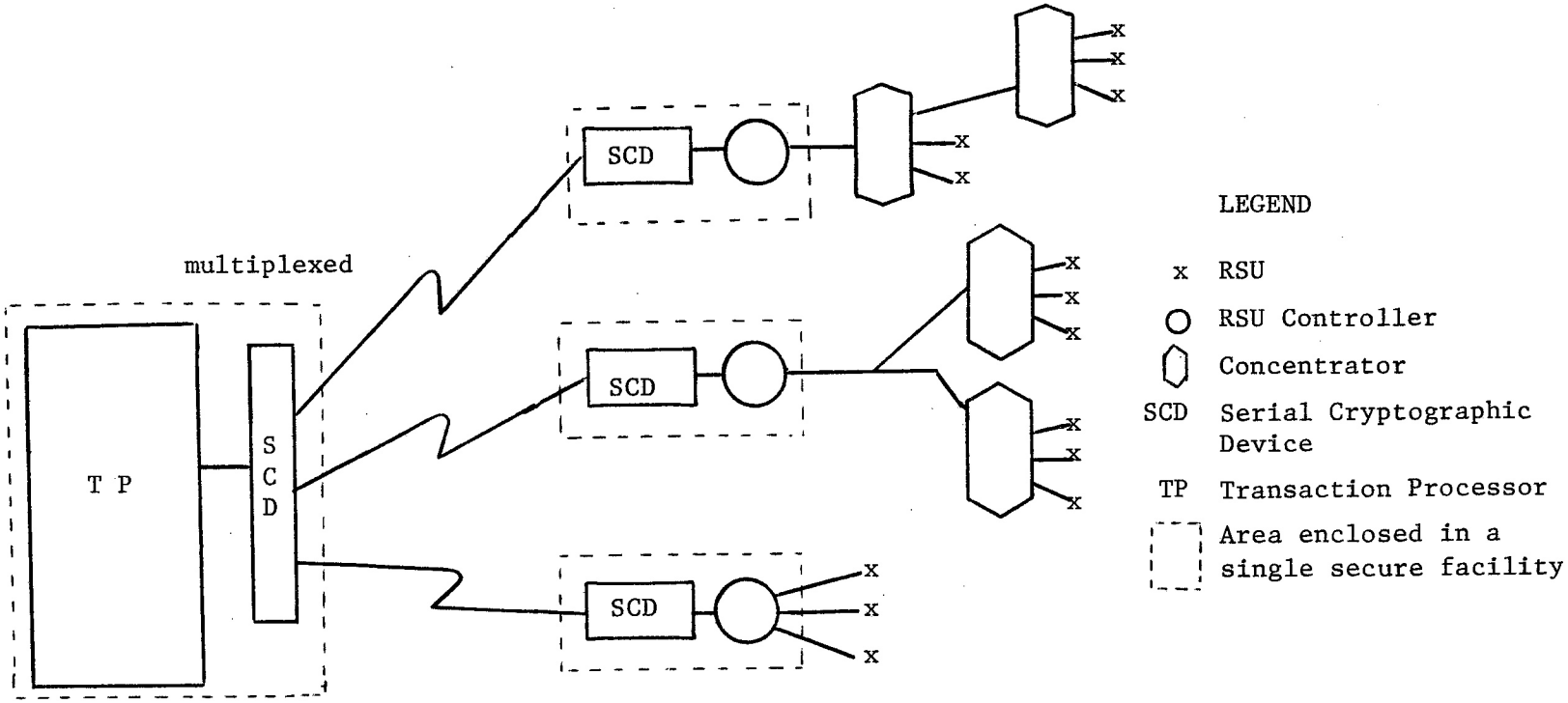


Figure 5. Portion of EFTS Network with Cryptographic Devices



As shown above, RSUs are not directly connected to TPs or SCDs. RSUs are directly connected to an RSU controller. Several RSUs may be attached to a single controller. This may be accomplished by concentrators, multidrop lines, etc. Communications security between RSU controllers and RSUs is, of necessity, the responsibility of the RSU manufacturer.

Figure 6. Transaction Processor - RSU portion of EFTS network

The National Bureau of Standards (NBS) Data Encryption Algorithm should be utilized in the SCDs and NCDs. The algorithm has many desirable features for use in such devices (see reference 1). Furthermore, it is rapidly being accepted as a standard for use in EFTS networks.

SCDs are similar to standard cryptographic devices now available. An SCD protects a single telecommunications line. Multiplexed SCDs can simultaneously handle several such lines. NCDs, on the other hand, are quite unlike anything now produced. NCDs maintain a fully interconnected network. By using a unique key, each NCD can protect the communications path to any other NCD in the network. This technique is described in Section 4. It is assumed that an automatic key update mechanism in the NCDs and SCDs changes keys after a given amount of use.

4.0 EFTS SYSTEM SECURITY ANALYSIS

The EFTS system described above should provide substantial security assurance. The following few paragraphs analyze the system's security based upon the six EFTS security principles previously presented.

Security Principle #1: The PIN should be known only by the cardholder.

In the system presented above, the PIN is not stored anywhere in the system. All processing beyond the TP is based upon transformed versions of the PIN. HPCs perform authorization checks on transformed PINs only and it is virtually impossible to derive the actual PIN from the transformed PIN.

Security Principle #2: There should be no way to derive the PIN from information on the card.

This principle can simply be restated as a system requirement. There is certainly no need in the system presented in this paper to generate PINs from information on the card. The use of cryptographic check digits derived from the PIN illustrates that the PIN can be verified without being implicitly exposed on the card.

Security Principle #3: Exposure of PINs should be minimized during a transmission.

PINs entered at RSUs are in the clear until enciphered by SCDs. PINs are again exposed in TPs. Thereafter, PINs are discarded and only transformed PINs are utilized.

If PINs were transformed at the RSU, only transformed PINs would appear in the network. Unfortunately, many RSUs already exist and none perform the transformation described in the system design. Exposure of the PIN can be reduced further if new RSUs adopt the transformation design proposed herein.

Security Principle #4: Sensitive or private transaction data should not be subject to unauthorized exposure.

When data is enciphered, it is considered safe from exposure. Thus, sensitive or private transaction data is safe as it flows between SCDs and as it flows between NCDs. There is, however, a potential weak link between RSUs and their controller Because RSUs and RSU controllers are built to operate as an integrated unit, the burden of providing communication security between these devices must fall on the manufacturers. Manufacturers should be required to provide this security.

Data is necessarily in clear (non-enciphered) form while in RSUs, RSU controllers, TPs, and HPCs. Consequently these devices will require procedural and physical protection.

Security Principle #5: Transaction data should not be subject to unauthorized alteration.

Cryptographic techniques can be used in conjunction with error detection techniques to prevent unauthorized alteration of transaction data. An error detection field is calculated on each message and appended to the message before it is enciphered. Encipherment of data based on the National Bureau of Standards encryption algorithm makes it virtually impossible to alter enciphered

data with predictable impact on the data once it is deciphered. Thus, when a message is deciphered and the error detection field recalculated and compared to the value in the message, it is extremely unlikely that any changes made to the enciphered message will not be detected. This technique does not directly prevent unauthorized alteration. It does, however, eliminate any threat due to such alteration since virtually all unauthorized changes to messages can be easily detected. If encipherment is coupled with a procedure for retransmitting messages, incentive for altering data without authorization is eliminated. Thus, SCDs and NCDs combined with appropriate protection of the RSU-RSU controller link prevent unauthorized alteration of transaction data.

Security Principle #6: All transaction requests and transaction authorizations should be authenticated at their destination.

NCDs are utilized in this design to authenticate the source of HPC and TP messages. Encipherment and decipherment of messages by NCDs is based upon secret values called keys. An NCD cannot decipher a message unless it knows the key used to encipher the message.

Each NCD will maintain a unique key for communicating with each of the other NCDs in the system. Thus, if TP_1 attached to NCD_1 sends a message to HPC_2 attached to NCD_2, the key used by NCD_1 to encipher the message is known only by NCD_1 and NCD_2. When NCD_2 receives the message, NCD_2 can be assured that the message came from NCD_1. The source of the message which arrives at HPC_2 must therefore be TP_1.

Similarly, SCDs will maintain pairwise-unique keys. This technique provides a means for mutual authentication of TPs and RSU controllers. RSU controllers should be required to have a mechanism for authenticating messages sent between RSU controllers and RSUs. However, RSU to RSU-controller communications are the domain of the manufacturers of these devices.

In this system PINs are known only by cardholders and during a transaction are in the clear only in the TP. A transaction can only be initiated at an RSU since the various cryptographic devices prevent unauthorized insertion of messages into the system. Thus the PIN must be known to initiate a transaction and only a legitimate cardholder can initiate a transaction.

5.0 A NATIONAL SYSTEM

The local EFTS system previously described conforms to the six EFTS security principles. That system would provide a high degree of security assurance. By linking several of these local systems it is possible to create a secure national EFTS network. Such a national EFTS network design is illustrated in Figures 7 and 8.

Three major components --a nationwide message switching network, gateways, and NCDs--are needed to link the local systems. The nationwide message switching network carries messages between the local systems. NCDs (like NCDs in the local system) protect messages which flow through the nationwide message switching network. Gateways interface local EFTS systems to the message switching network.

An example may clarify the function of these internetwork devices. We will assume that TP_1 finds it necessary to send a debit request to HPC_2. We further assume that TP_1 and HPC_2 are not in the same local system.

TP_1, recognizing that HCP_2 is not local, generates a debit request message addressed to HPC_2. That request is enclosed in a message addressed to a local gateway, G_3. The message is transmitted, via the local switch, to G_3. G_3 receives the message and extracts the debit request. The gateway inspects the debit request to determine which local system contains HPC_2. G_3 then encloses the debit request in an internetwork message. The internetwork message is addressed to a gateway, G_4, which is part of the same local system as HPC_2.

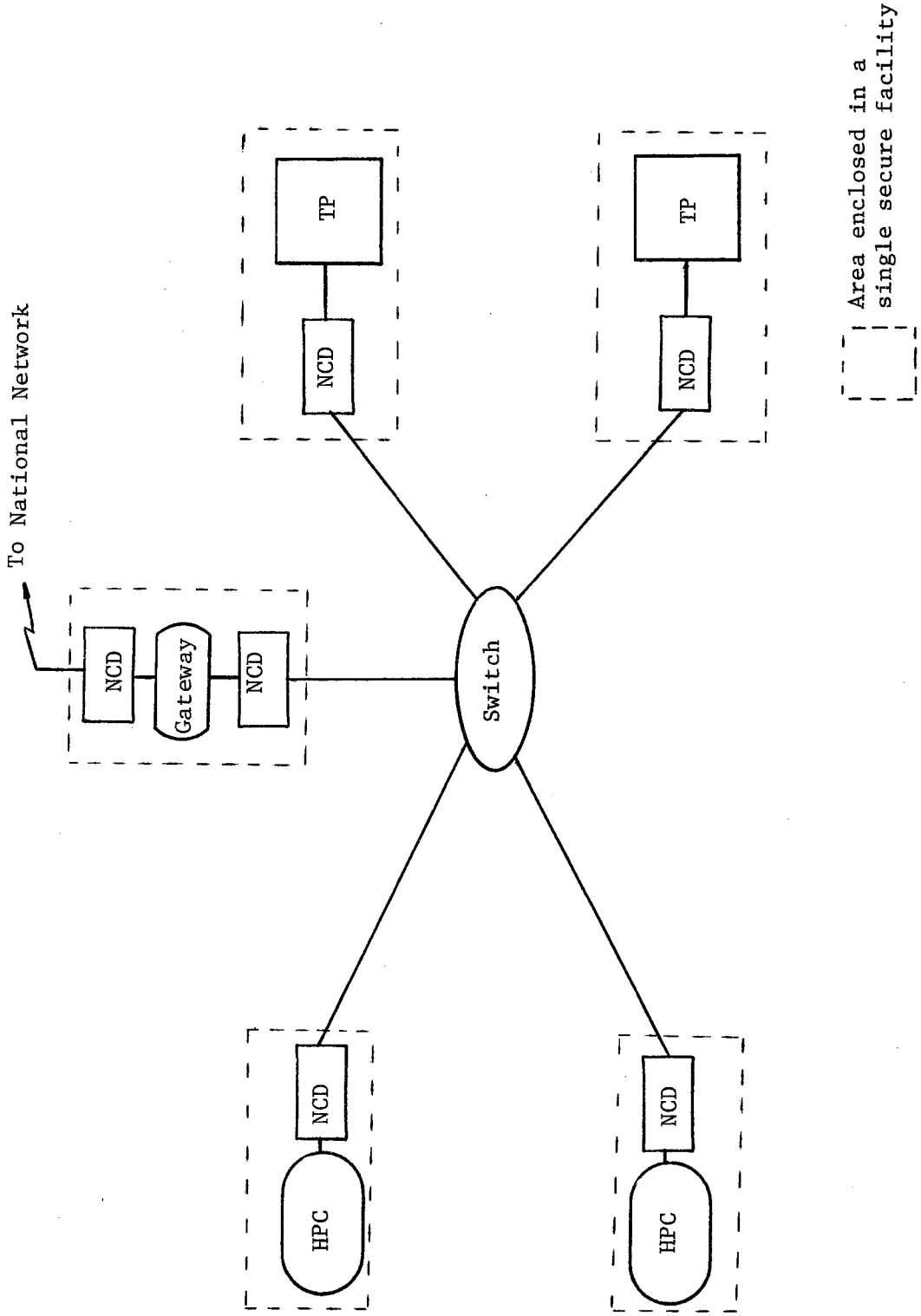


Figure 7. Local EFTS System Attached To National Network

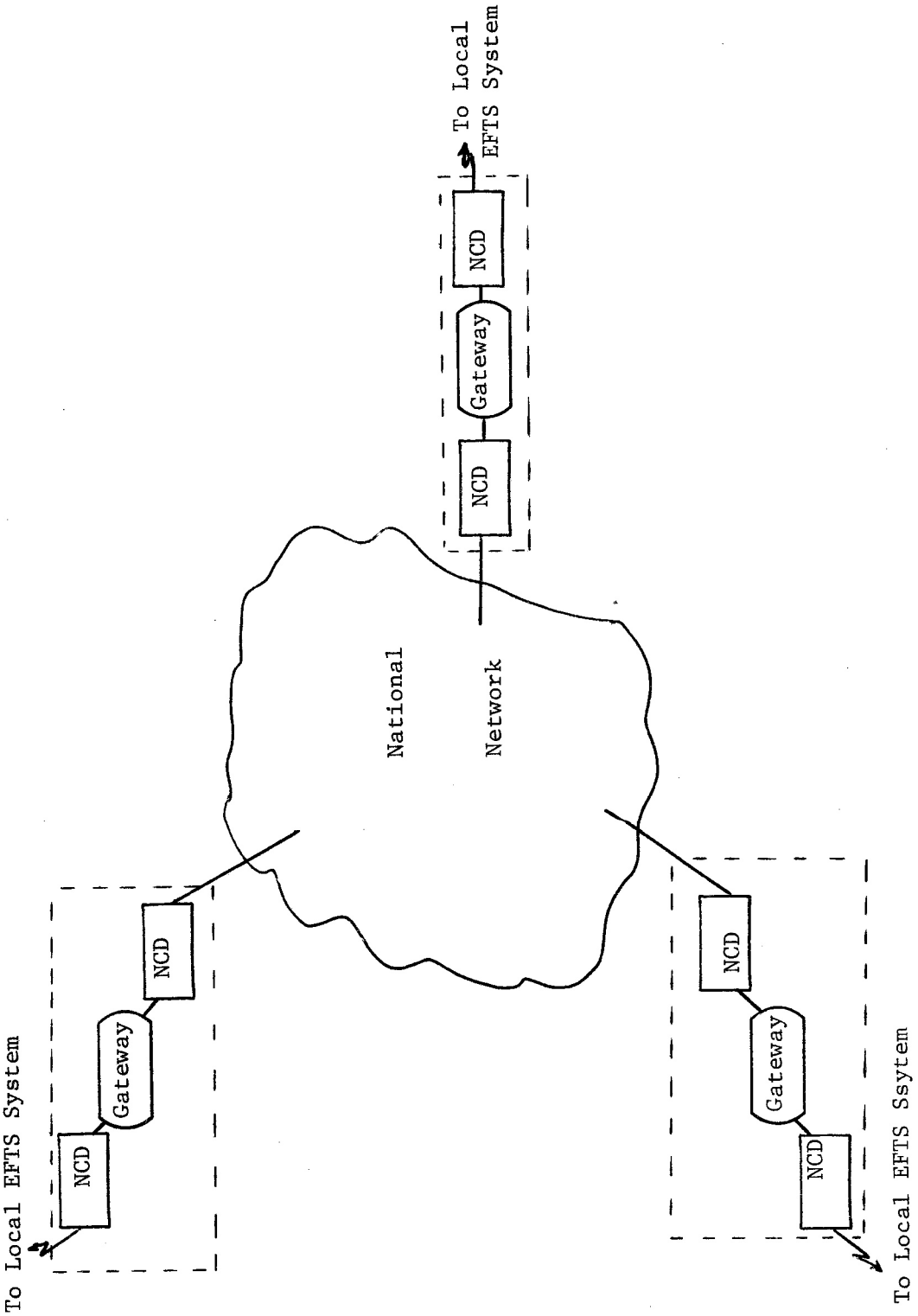


Figure 8. A National EFTS Network

The internetwork message, cryptographically protected by NCDs, is routed by the nationwide message switching system to G_4. G_4 receives the internetwork message and extracts the debit request. G_4 then routes the debit request to HPC_2 via the local switch. The resulting debit authorization or denial follows the reverse path from HPC_2 to TP_1.

5.1 THE NATIONAL NETWORK

Like the local system's switch, the nationwide message switching network may take many forms. Any network capable of carrying messages between gateways in a timely manner is acceptable. The national networks will span large distances and, when compared to local switches, will carry a relatively light EFTS message load. Hence, a distributed shared, public network seems appropriate. Because NCDs protect messages sent through the national network, it is possible to utilize a commercial, value-added network.

5.2 GATEWAYS

A TP views a gateway as a special HPC which represents all HPCs not found in the local system. An HPC views a gateway as a special TP.

The national system design presented above assumed that the local systems to be linked were identical. Unfortunately, such standardization is unlikely. Where little commonality exists between local systems, a national system will be effectively precluded. If the only differences are message formats, gateways can be used to translate the message formats utilized by different local systems. It cannot be stated too strongly--a national EFTS system requires standardization of at least transaction protocols and message information content.

To simplify the format translation task, all messages travelling through the national network will conform to a single, standard protocol and format. If a local system does not conform to the national standard, the gateway to that system must translate messages to and from the national standard. In this way

neither HPCs nor TPs are impacted by the differences between the local system and the national system. However, it must be reiterated that gateways can only reformat messages. In all other respects (protocol and information content) local messages must conform to the national standard. The more the local system resembles the national standard, the less complex the gateway becomes.

5.3 SECURITY ANALYSIS OF THE NATIONAL SYSTEM

The extent to which the national system design adheres to the six EFTS security principles is presented in a two part analysis. First, the protection of the PIN is examined. Second, the protection of transaction communications is examined.

A national network can be built in which all PINs are handled in the same manner as described earlier (see Section 3.3) whether the transaction occurs totally within the local system or whether other local systems are involved. If the national network is built in that way, security principles #1, #2, and #3 are satisfied by the national system design just as they were in the local system design. If, in some local systems a non-standard PIN transformation is used, or if the PIN is not transformed at all, PINs may be exposed. Furthermore, non-standard PIN handling mechanisms may require ad hoc processing in gateways. Such ad hoc mechanisms would increase cost and decrease security, integrity, and reliability.

The extent to which EFTS security principles #4, #5, and #6 are followed depends entirely upon the local systems. If a local system is built according to the design presented in this paper, then messages are not subject to unauthorized alteration or exposure until they enter a local system not adhering to the security principles. This result occurs because the NCDs of the national system protect against unauthorized exposure and alteration of messages sent between gateways. Furthermore, because the NCDs of the national network prevent mis-delivery, a gateway may trust that a message it receives actually originated

in the remote local network from which that message appears to have come. If both the source and destination local systems adhere to the security principles, then mutual authentication of the ultimate source and destination of a message is possible.

6. CONCLUSION

Security must be an integral part of any EFTS system design. Adherence to the six EFTS security principles will provide a high degree of system security. Through the proper use of the NBS algorithm, a system for local electronic funds transfer can be built which conforms to these guidelines for handling PINs and transaction data. Although the devices to implement such systems may not be currently available, the technology to build these devices does exist.

National systems for electronic funds transfer can be created by linking local systems. It is necessary, however, that the local systems be designed to operate as part of a national system--effective and secure after-the-fact linking of heterogeneous local systems may be virtually impossible. National standards must be developed to permit interconnection of local systems and to insure a high level of security.

BIBLIOGRAPHY

1. Branstad, D. K., "Encryption Protection in Computer Data Communications," Fourth Data Communications Symposium, Quebec City, Canada, October 1975.

2. Branstad, D. K., "Security Aspects of Computer Networks," Paper Number 73-427, AIAA Computer Network Conference, Huntsville, Alabama, April 1973.

3. Cerf, V. and R. E. Kahn, "A Protocol for Packet Network Intercommunication," IEEE Transactions on Communications, Vol. COM-22, No. 5, May 1974.

4. Ferdman, M. D., D. W. Lambert and D. W. Snow, "Security Aspects of Bank Card Systems," MITRE Technical Report MTR-2971, Vols. 1 and 2 and Executive Summary, September 1975.

5. National Bureau of Standards Data Encryption Algorithm, Federal Register, March 1975.

6. "Security and Reliability in Electronic Systems for Payments," Study Group on Electronic Systems for International Payments of the Group of Computer Experts of the Central Banks of the Group of Ten Countries and Switzerland, April 1975.