PN-ACU-504

MSH MANAGEMENT SCIENCES FOR HEALTH, INC.

Health Sector Reform Technical Assistance Project (HSRTAP)

United States Agency for International Development USAID

This report was made possible through support provided by the U.S. Agency for International Development, under the terms of Contract No. HRN-I-00-98-00033-00, Delivery Order No. 804

Rm. 502, 5/F, Ma. Natividad Bldg., 470 T.M. Kalaw St. cor. Cortada St.,
1000 Ermita, Manila, Philippines
Tel: (632) 400-2914 • 400-2894 • 400-2933 Telefax: (632) 522-6243

A

PN-ACU-504

IDENTIFYING AND ADDRESSING OPERATIONAL, TECHNOLOGICAL, AND LEGAL ISSUES IN PRESENT AND POTENTIAL WEB-ENABLED TRANSACTIONS OF THE NATIONAL HEALTH INSURANCE PROGRAM

FINAL REPORT

This report was made possible through support provided by the U. S. Agency for International Development, under the terms of Contract No. HRN-I-00-98-00033-00. The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of the U. S. Agency for International Development.

IDENTIFYING AND ADDRESSING OPERATIONAL, TECHNOLOGICAL AND LEGAL ISSUES IN PRESENT AND POTENTIAL WEB-ENABLED TRANSACTIONS OF THE NATIONAL HEALTH INSURANCE PROGRAM

TABLE OF CONTENTS

PART I:	Executive Summary
PART II:	Legal and Policy Issues for Potential Web-enabled Transactions of the National Health Insurance Program
PART III:	HealthWeb (PhilHealth Online Transaction System)

c

PART I

EXECUTIVE SUMMARY

d

Republic Act 7875, also known as the National Health Insurance Act of 1995, mandated the Philippine Health Insurance Corporation (PhilHealth) to implement the National Health Insurance Program (NHIP), a social program designed to make the delivery of health care services more affordable. Pursuant to this mandate, PhilHealth now seeks to begin implementation of its proposed Information System Development Plan (ISDP). Through the ISDP, PhilHealth intends to take full advantage of new technologies that will allow it to conduct business and deliver services over information networks such as the Internet. ISDP is expected to include online membership and benefit profiling, online posting of premium contribution, web-enabled and text-enabled electronic eligibility checking, and online claims processing.

This paper identifies the potential legal and policy issues that need to be considered in relation to potential web-enabled transactions of the National Health Insurance Program (NIHP) of the Philippines and at the same time identify technology that will allow PhilHealth to offer services directly and securely to members and providers via the web. The authors utilized desk review, key personnel interview, research and inter-agency link up to identify possible issues and determine possible tie ups with other government agencies. The terms PhilHealth Online Transaction System (POTS) and Health Web are used interchangeably between the two documents: Legal and Policy Issues for Potential Web-enabled Transactions of the National Health Insurance Program (NHIP) done by Atty. Gigo Alampay and HealthWeb (PhilHealth Online Transaction System) done by Mr. Ruben Canlas, Jr.

The paper on the "Legal and Policy Issues for Potential Web-enabled Transactions of the National Health Insurance Program" identified five key findings that have important implications for PhilHealth's initiative to implement the ISDP:

1. **Two laws provide the legal basis and authority for PhilHealth to implement and to issue new rules and procedures to govern its envisioned online transactions.**

   (a) The National Health Insurance Act of 1995 (R.A. 7875)

   The Implementing Rules for the National Health Insurance Act were adopted through a Board Resolution issued by PhilHealth pursuant to the provisions of the NHIA. They can therefore be amended by PhilHealth to reflect new rules and procedures that will apply to online transactions.

   (b) The E-Commerce Act of 2000 (R.A. 8792)
   This law recognizes the legal validity of online transactions such as those contemplated by PhilHealth. Further, it authorizes government agencies, such as PhilHealth to adopt and promulgate, after appropriate public hearing and with due publication in newspapers of general circulation, the appropriate rules, regulations, or guidelines that would govern its online/electronic transactions.

2. **To be legally binding, electronic messages and transactions received by PhilHealth should meet three basic requirements.**

(a) *Data Origin Authentication*. The message really did come from the person or entity with whom PhilHealth was transacting.
(b) *Message Integrity*. The message received by PhilHealth is the exact message that was actually sent and was not intentionally or accidentally altered during transmission.
(c) *Non-Repudiation*. The sender cannot later deny that he or she did in fact send the message, and PhilHealth should have the means to prove it unequivocally.

3. **Most of PhilHealth's online transactions will be in a "closed" system, or with parties whose identities are known to or can be verified by it.**
Implications:
(a) PhilHealth does not need to deal with a third party such as certification authorities.
(b) PhilHealth and the parties with whom it will transact can therefore agree in advance on their respective rights and duties.
(c) The terms of transacting with PhilHealth can, in fact, are part of new implementing rules and regulations.

4. **Under the E-Commerce Act, the Commission on Audit cannot deny the validity of, or reject documents solely on the ground that these are in electronic form.**

(a) COA does not yet have any specific rules to govern the electronic transactions. But, it has consistently manifested its support for and compliance with the letter and spirit of the E-Commerce Act.
(b) In practice, it has supported various initiatives to bring government services and transactions online, including the SEC, Department of Health and GSIS.

(c) COA would have to be assured that the technology chosen by PhilHealth enables the secure transmission of documents, as well as undeniable identification of the parties involved.

5. **The importance of adequately securing the PhilHealth Online Transactions System cannot be overemphasized.**

Hacking or other unauthorized entry into the system would not only cause problems in terms of access to sensitive information, but PhilHealth could also be exposed to liability (e.g., from members whose private information is compromised) if it cannot show that it exercised the diligence required to reasonably ensure the security of its computer system.

Technology that will ensure acceptability of data. In accordance with legal findings and recommendations, the paper that discussed technology for web-enabled transactions that may be used by PhilHealth emphasized the three basic requirements for electronic data to be acceptable by any corporation, namely; authenticity of data origin, message integrity, and non-repudiation. The use of encryption and digital signatures using a

Virtual Private Network (VPN) were recommended to ensure authenticity and integrity of data being received by PhilHealth.

The study then discussed choices that PhilHealth could consider specifically in the type of web platform. A choice of three major platforms for web services was given. These three are: Microsoft.NET, SunONE, and Open Source systems. PhilHealth must decide which platform is best, given (a) the existing setup, (b) the reliability, speed, and cost of the platform that will be built. A brief survey of reliability, speed, and cost factors are outlined in the paper made. Moreover, the use of eXtensible Markup Language (XML) is encouraged because POTS or HealthWeb intends to set an initiative for interoperability with other agencies and entities (both government and otherwise).

Given the different choices of web platforms, the basic setup for HealthWeb would be the following:

(a) A HeathWeb server which includes a Web server and a Web database server which replicates relevant information from the OMIS databases (eg, Membership, Contributions, and Claims information systems).
(b) A reliable connection between the HealthWeb server and the Web, including a reliable and reasonably fast network connection between PHIC-OMIS and HealthWeb server.
(c) A "bridge" that may be composed of both software and hardware to allow HealthWeb to efficiently link up with PHIC-OMIS.

And finally, the last consideration would be the hosting setup for HealthWeb: inhouse, co-located, offshore. The advantages and disadvantages of these options are summarized in order for PhilHealth to evaluate an appropriate hosting option for HealthWeb.

This study provided PhilHealth a macrocospic view for web-enabled transactions. Further study needs to be undertaken to have a more comprehensive study on how to map out the process and flow of online activities and transactions. This follow-up study should also determine how PhilHealth could link up with other government agencies.

A more detailed discussion of each aspect for web-enable transactions are found in the succeeding documents.

G

PART II

LEGAL & POLICY ISSUES FOR POTENTIAL WEB-ENABLED TRANSACTIONS OF THE NATIONAL HEALTH INSURANCE PROGRAM (NIHP)

by

Gigo Alampay

Submitted to

Management Sciences for Health
Health Sector Reform Technical Assistance Project (HSRTAP)

15 November 2002

h

LEGAL & POLICY ISSUES FOR POTENTIAL WEB-ENABLED TRANSACTIONS OF THE NATIONAL HEALTH INSURANCE PROGRAM (NIHP)

by

Gigo Alampay

********** ********** ********** ********** ********** **********

Table of Contents

I. Executive Summary 1

II. The Legal Framework for ISDP: The National Health Insurance Act of 1995 & the E-Commerce Act of 2000 3

III. Legal & Policy Issues 4

- A. Authority of PhilHealth to prescribe rules and procedures to govern its online transactions 4
- B. Ensuring Legal Validity of Electronic Transactions and Documents 5
- C. The Limited Scope and "Closed" Nature of PhilHealth's Proposed ISDP 6
- D. Ensuring Compliance with COA Requirements 9
- E. Privacy and Data Protection 9
- F. Security of the System Itself 10

IV. Conclusion & Recommendations 10

APPENDICES 13

The E-Commerce Act of 2000 (R.A. 8792) 14

An Introduction to Digital Signatures and Electronic Authentication 26

LEGAL & POLICY ISSUES FOR POTENTIAL WEB-ENABLED TRANSACTIONS OF THE NATIONAL HEALTH INSURANCE PROGRAM (NIHP)

I. EXECUTIVE SUMMARY

Republic Act 7875, also known as the National Health Insurance Act of 1995, mandated the Philippine Health Insurance Corporation (PhilHealth) to implement the National Health Insurance Program (NHIP), a social program designed to make the delivery of health care services more affordable.

Pursuant to this mandate, PhilHealth now seeks to begin implementation of its proposed Information System Development Plan (ISDP). Through the ISDP, or more precisely, through a subcomponent of the plan known as the PhilHealth Online Transaction System (POTS), PhilHealth intends to take full advantage of new technologies that will allow it to conduct business and deliver services over information networks such as the Internet. ISDP is expected to include online membership and benefit profiling, online posting of premium contribution, web-enabled and text-enabled electronic eligibility checking, and online claims processing.

This paper identifies the potential legal and policy issues that need to be considered in relation to potential web-enabled transactions of the National Health Insurance Program (NIHP) of the Philippines.

Summary of Key Findings:

In brief, five key findings have important implications for PhilHealth's initiative to implement the ISDP:

1. **Two laws provide the legal basis and authority for PhilHealth to implement and to issue new rules and procedures to govern its envisioned online transactions.**

   (a) **The National Health Insurance Act of 1995 (R.A. 7875)**
   The Implementing Rules for the National Health Insurance Act were adopted through a Board Resolution issued by PhilHealth pursuant to the provisions of the NHIA. They can therefore be amended by PhilHealth to reflect new rules and procedures that will apply to online transactions.

   (b) **The E-Commerce Act of 2000 (R.A. 8792)**
   This law recognizes the legal validity of online transactions such as those contemplated by PhilHealth. Further, it authorizes government agencies, such as PhilHealth to adopt and promulgate, after appropriate public hearing and with due publication in newspapers of general circulation, the appropriate rules, regulations, or guidelines that would govern its online/electronic transactions.

2. **To be legally binding, electronic messages and transactions received by PhilHealth should meet three basic requirements.**

   (a) ***Data Origin Authentication***. The message really did come from the person or entity with whom PhilHealth was transacting.

   (b) ***Message Integrity***. The message received by PhilHealth is the exact message that was actually sent and was not intentionally or accidentally altered during transmission.

   (c) ***Non-Repudiation***. The sender cannot later deny that he or she did in fact send the message, and PhilHealth should have the means to prove it unequivocally.

3. **Most of PhilHealth's online transactions will be in a "closed" system, or with parties whose identities are known to or can be verified by it.**

   Implications:
   (a) PhilHealth does not need to deal with a third party such as certification authorities.
   (b) PhilHealth and the parties with whom it will transact can therefore agree in advance on their respective rights and duties.
   (c) The terms of transacting with PhilHealth can, in fact, are part of new implementing rules and regulations.

4. **Under the E-Commerce Act, the Commission on Audit cannot deny the validity of, or reject documents solely on the ground that these are in electronic form.**

   (a) COA does not yet have any specific rules to govern the electronic transactions. But, it has consistently manifested its support for and compliance with the letter and spirit of the E-Commerce Act.
   (b) In practice, it has supported various initiatives to bring government services and transactions online, including the SEC, Department of Health and GSIS.
   (c) COA would have to be assured that the technology chosen by PhilHealth enables the secure transmission of documents, as well as undeniable identification of the parties involved.

5. **The importance of adequately securing the PhilHealth Online Transactions System cannot be overemphasized.**

   Hacking or other unauthorized entry into the system would not only cause problems in terms of access to sensitive information, but PhilHealth could also be exposed to liability (e.g., from members whose private information is compromised) if it cannot show that it exercised the diligence required to reasonably ensure the security of its computer system.

Summary of Recommendations:

Finally, this paper concludes with recommendations for future action, which are condensed and outlined below:

1. Allocate resources and manpower for a comprehensive activity to identify and map out the process and flow of online activities and transactions. Questions to be answered include:

   - What particular activities will be web-enabled and which, if any, will not be allowed to be conducted online?
   - What level of security is warranted for a given transaction?
   - What legal documents or other information are needed in each activity, and which of these can be submitted online, and which cannot and therefore would have to actually be presented in its hard copy format?
   - Who would be authorized to make the transaction? Who will have access to collected data?
   - Does PhilHealth need the cooperation of, or connection with other government agencies?

2. Revise the Implementing Rules and Regulations of the National Health Insurance Act to reflect the requirements and procedures that will define the proposed ISDP, outlining, among others:

- the manner and format in which electronic messages or electronic documents shall be filed, created, retained or issued;
- when, where and how electronic messages or electronic documents are to be signed;
- the format of an electronic data message or electronic document;
- the technology, control processes and/or procedures that PhilHealth has chosen to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents; and
- other attributes required of electronic data messages or electronic documents or payments.

3. Draft and issue appropriate guidelines or rules on who will be able to use, amend and access its information online, and draw up the appropriate contracts for the same.

4. Appropriate templates of legal contracts that will govern PhilHealth's relations with health service providers and other entities/persons who will be allowed to transact online with PhilHealth should subsquently be drafted.

5. Comply with due process requirements in the drafting and issuance of rules:

   - Conduct public hearings
   - Publish new rules and/or guidelines.

6. Choose the appropriate technology that will be adopted to ensure the security and reliability of POTS

7. Conduct a cost-benefit analysis to determine the best way of implementing the chosen technology.

8. If the system is opened to "unknown" persons or entities, formulate the policy for choosing or accrediting information certifiers, who would verify the identities of such unknown persons or entities.

9. Draft and issue the rules and guidelines to ensure privacy and data protection, as well as on sharing or release of collected data.

10. Ensure COA participation and involvement in all levels of planning and implementation of the ISDP.

II. THE LEGAL FRAMEWORK FOR ISDP: THE NATIONAL HEALTH INSURANCE ACT OF 1995 & THE E-COMMERCE ACT OF 2000

The National Health Insurance Act of 1995 (R.A. 7875), was passed pursuant to Sec. II of Article XIII of the Philippine Constitution which mandates the adoption of an integrated and comprehensive approach to health development which shall make essential goods, health and other social services available to all the people at affordable cost. It mandates the Philippine Health Insurance Corporation (PhilHealth) to implement the National Health Insurance Program (NHIP).

The NHIP is a social program, and helps people to pay for health care services. It is a mechanism for those who can afford medical care to subsidize those who cannot. The program includes a sustainable system of funds constitution, collection, management, and disbursement for financing the availment of a basic minimum package and other supplementary packages of health insurance benefits by a progressively expanding proportion of the population. The program is limited to paying for the utilization of health

services by covered beneficiaries or to purchasing health services in behalf of the beneficiaries.

In its effort to make the NHIP continuously responsive to the needs of its clientele, PhilHealth now seeks to take full advantage of new technologies that now allow it to conduct business and deliver services over information networks such as the Internet and begin implementation of its Information System Development Plan (ISDP). A critical component of the ISDP, the PhilHealth Online Transaction System (POTS) is expected to include online membership and benefit profiling, online posting of premium contribution, web-enabled and text-enabled electronic eligibility checking, and online claims processing.

The legal validity and effect of online transactions such as those contemplated under the ISDP and POTS would be governed by the provisions of the **E-Commerce Act of 2000 (R.A. 8792).**[1] Note that this Act is intended to have universal application so as to cover both commercial and non-commercial acts, which includes the performance of government functions, and transactions by and with government.

The following features of the E-Commerce Act are particularly relevant to the ISDP and will facilitate PhilHealth's transactions, particularly in connection with membership registration, database updates, and claims processing:

(a) legal recognition of electronic documents;
(b) formation of electronic contracts;
(c) recognition of electronic signatures; and
(d) government use of electronic records and signatures.

III. LEGAL & POLICY ISSUES

Authority of PhilHealth to prescribe rules and procedures to govern its online transactions

The Implementing Rules for the National Health Insurance Act were adopted through a Board Resolution issued by PhilHealth pursuant to the provisions of the NHIA.[2] They can therefore be amended by PhilHealth to provide for the rules to govern electronic transactions, including the terms to which parties electronically transacting with PhilHealth would have to agree to be bound.

The E-Commerce Act further details the mandate for and authority of PhilHealth to implement its ISDP. Among others, the E-Commerce Act calls on PhilHealth to:

(a) Determine the type and level of electronic data message and electronic document security needed, and to select and use or implement appropriate technological methods that suit its (and the parties with whom it is dealing) needs;[3] and

(b) Transact its business and functions using electronic data messages or electronic documents, and for the purpose, PhilHealth is authorized to adopt and promulgate, after appropriate public hearing and with due publication in newspapers of general circulation, the appropriate rules, regulations, or guidelines, to, among others, specify –

[1] For full text, see Appendix A.
[2] R.A. 7875, sec. 49.
[3] ECA, Sec. 24.

(1) the manner and format in which such electronic data messages or electronic documents shall be filed, created, retained or issued;

(2) where and when such electronic data messages or electronic documents have to be signed, the use of a electronic signature, the type of electronic signature required;

(3) the format of an electronic data message or electronic document and the manner the electronic signature shall be affixed to the electronic data message or electronic document;

(4) the control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records or payments;

(5) other attributes required of electronic data messages or electronic documents or payments; and

(6) the full or limited use of the documents and papers for compliance with the government requirements.[4]

Ensuring Legal Validity of Electronic Transactions and Documents

The principal legal issue to be addressed in the implementation of ISDP is the legal validity of electronic transactions and documents involved in the same.

PhilHealth, then, must select the technology that it will use to reliably and securely prove the origin, receipt and integrity of electronic documents and/or signatures; to identify the parties it is transacting with; and to associate those parties with the contents of such electronic documents.[5]

While the selection of the technology itself is a technical task, from a legal viewpoint, such selected technology must meet with the requirements for electronic authentication outlined under Sections 8 and 9 of the E-Commerce Act of 2000.[6]

---

[4] ECA, Sec. 27.

[5] For an introduction to digital signatures and electronic authentication, see Appendix B.

[6] Sec. 8. Legal Recognition of Electronic Signatures

An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which:

(a) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;

(b) Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in light of all the circumstances, including any relevant agreement;

(c) It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and

(d) The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.

Under these provisions, any electronic message or information received by PhilHealth as a result of the proposed ISDP should be assured of the following:

(a) *Data Origin Authentication*. First, that the message really did come from the person or entity with whom PhilHealth was transacting.

(b) *Message Integrity*. Second, that the message received by PhilHealth is the exact message that was actually sent. PhilHealth should be able to verify that the message was not intentionally or accidentally altered during transmission.

(c) *Non-Repudiation*. And finally, that the sender cannot later deny that he or she did in fact send the message, and the PhilHealth would have the means to prove it unequivocally.

The adoption of the technology or mechanism that can assure those concerns is important because it will allow PhilHealth and the party it is electronically transacting with to assess any associated risks, such as whether there is a likelihood of the transaction being able to be successfully completed; or whether its validity can be challenged.

The Limited Scope and "Closed" Nature of PhilHealth's Proposed ISDP

The type of electronic documents and transactions that will be involved in the ISDP will depend on how extensive or web-enabled PhilHealth decides to be.

One possibility is for PhilHealth to be as fully web-enabled as it can be. In this case, all its transactions, from membership registration to data updates to claims processing and to accreditation, would be possible online. Ideally, for example, persons who wish to register with PhilHealth would not need to physically present their birth certificates because PhilHealth would be able to electronically verify and obtain authentic digital copies of the same from the National Statistics Office.

The number of electronic documents that could be processed on any given day by the system would be enormous and would require electronic verification from a number of government agencies. (See table below.)

A fully web-enabled PhilHealth presumes that all other agencies of the government are similarly web-enabled. While certainly PhilHealth can connect its network and databases to other government agencies and vice-versa, as they gain the required capability, this vision of e-governance is still several years away.

The scope of the ISDP would therefore be limited. Certain activities, like initial applications or requests for status updates, can be conducted online. But some requirements, such as documentary requisites, might still need physical or hard copy presentation to PhilHealth.

Sec. 9. Presumption Relating to Electronic Signatures

"In any proceeding involving an electronic signature, it shall be presumed that
(a) The electronic signature is the signature of the person to whom it correlates; and
(b) The electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows or has notice of defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances."

Table 1. Documents Required in Selected Transactions with PhilHealth

Type of Transaction	Document/Signature Needed	Agency Involved
Membership Registration	• Birth Certificate • Baptismal Certificate • GSIS/SSS Member's card • Passport • Any other ID/Document acceptable to PhilHealth	NSO GSIS / SSS DFA
Registration of Dependents	• Marriage Contract • Birth Certificate/Baptismal Certificate of dependents • Adoption papers/Court resolution • Marriage contract • Affidavit from disinterested persons • Other ID/document	Civil Register / City Hall NSO Civil Register City Hall
Updates / Revisions	• Birth Certificate (correction/change of name) • Marriage Contract (change of status) • Additional dependents (birth certificate) • Change of address (written notice)	NSO Civil Register NSO Post Office
Employer Registration / Data Amendment / Revision	• Business name • Suspension of operation • Termination • Merger • Change of Ownership- Deed of Sale • Resumption of Operation (PhilHealth forms for rehired/new employees)	DTI/SEC
Report of New Hires by Employer	• Notice to PhilHealth	
Enrollment of Indigent Members	• Community-Based Information System	LGUs
Privately sponsored members	• Application to PhilHealth	
Individually paying member	• Enrollment with PhilHealth	
Claims Payment	• Prescribed PhilHealth forms	

Accreditation	• Initial Business Permit • LGU/DND Certification	SEC DTI LGU DND
Accreditation	•	
Accreditation	• Depends on person/institution being accredited	DOH PRC Nat'l Assn.
Monitoring and verification vis quality assurance of health care providers	• submission of periodic reports	

Source: Implementing Rules and Regulations of R.A. 7875 (July 2000)

It is important to note that most, if not all PhilHealth transactions in the proposed ISDP can be expected to be conducted as a "closed system." That is, the parties that PhilHealth will be dealing with in any given transaction are likely to be "known" parties, i.e., people or entities that PhilHealth knows or already have prior experience with, such as, professional health service institutions, hospitals, LGUs and even individual members. PhilHealth would not be dealing with persons that it cannot or would have no way of reliably identifying.

This is in contrast to "open" systems where the parties involved may not know each other, and therefore usually rely on third parties such as certification authorities to verify each other's identity and messages.[7]

In other words, PhilHealth can limit the number of parties it will transact with, possibly leaving the process of verifying "unknown persons" (e.g. individual claimants or registrants) to those parties.

For example, the October 1999 version of the ISDP states that applications for memberships would be validated and screened by Regional Health Insurance Offices which would receive and process the application for membership. Similarly, claims and receipts can hypothetically be verified and assessed by accredited hospitals or health service providers. Assuming secure systems are in place, online transactions by these "known" parties with PhilHealth can then be presumed by it to be valid.[8]

From a legal and policy standpoint, the distinction is important because under a closed system:

(a) PhilHealth does not need to deal with a third party such as certification authorities.

(b) PhilHealth and the parties with whom it will transact can therefore agree in advance on their respective rights and duties.

(c) Indeed, PhilHealth can prescribe or even define the terms that would govern ISDP transactions pursuant to the National Health Insurance Act which gives it the power to, among others, formulate and promulgate policies for the sound administration of the National Health Insurance Program, as well as to set standards, rules and regulations

[7] For background information on digital signatures and certification authorities, please see Appendix B.

[8] Note that in any event, hard copies of documents and receipts can still be kept by the hospitals and would be available for actual presentation if necessary.

necessary to ensure quality of care, appropriate utilization of services, and overall accomplishment of Program objectives.[9]

Ensuring Compliance with COA Requirements

To date, the Commission on Audit has not promulgated any specific rules to govern the electronic transactions of government agencies and GOCCs.

Nonetheless, it is clear that under the E-Commerce Act, the COA cannot deny or reject submitted supporting documents solely on the ground that these are in electronic form.

Indeed, COA has consistently manifested its support for and compliance with the letter and spirit of the E-Commerce Act:

- It has issued COMMISSION ON AUDIT MEMORANDUM NO. 2000-090 (August 11, 2000) which disseminated copies of the E-Commerce Act to all its officers, department heads and staff.
- In practice, it has participated and supported various efforts by other government agencies to bring their services and transactions online, including the SEC, Department of Health and GSIS, among others.

It is important to remember that under the E-Commerce Act, the technology or mechanism chosen should be "as reliable and appropriate for the purpose for which the electronic document involved is generated or communicated, in light of all the circumstances."[10] In practical terms, for example, the procedure allowing for the electronic amendment or revision of members' data may be less sophisticated (e.g., mere assignment of passwords to persons/entities accredited to make minor corrections or updates) than procedures involving claims reimbursements which also require electronic transmission of private information such as medical records.

It is with these latter cases that COA is likely to be more concerned with, and COA would have to be assured that the technology chosen by PhilHealth enables the secure transmission of documents, as well as undeniable identification of the parties involved. Thus, PhilHealth would have to choose more secure authentication procedures. It can, for example, choose to adopt a technology involving cryptography and issue digital signatures to accredited parties. PhilHealth's and the other parties' rights and duties under such an arrangement would then be established by a series of contracts.

Where for whatever reason the authenticity and/or integrity of electronic documents cannot be guaranteed, physical or hard copy documents would then be required by COA.

It is critical, therefore, that COA be involved in all stages of developing and implementing the ISDP, in order to avoid unnecessary delay or complication. But, as long as COA is duly informed and involved, given its avowed commitment to the spirit and language of the E-Commerce Act, there should be no insurmountable problems as far as addressing any and all COA issues in the implementation of ISDP is concerned.

Privacy and Data Protection

Policies regarding privacy and data protection need to be clearly stated and publicly disclosed.

---

[9] R.A. 7875, sec. 16 (b) and (c).
[10] ECA, Sec. 8.

This is important not only to ensure that the right to privacy of members and providers will be protected, but also to gain the trust of PhilHealth partners and members in the use and reliability of the ISDP.

Clear guidelines need to be in place to detail and/or limit how data and records provided by health care providers and PhilHealth members are to be used, shared (with other government agencies or possibly private sector entities/persons), collected and kept.

Questions that will have to be addressed, include:

- Who will have access to collected data and information?
- What does having access mean? What sort of controls will they have?
- How much access should they have? Are there different levels of access and authority?
- What use can they legally have for the data or information shared or given to them by PhilHealth?

Security of the System Itself.

Although the security of the PhilHealth information system itself is largely a technological issue, there are legal and policy aspects involved as well. Note that only recently, the PhilHealth email server was hacked.[11] While it appears that there was no significant damage, an attack on the ISDP, given the sensitive and private nature of information that could be compromised, would have more serious consequences.

It would not only cause problems in terms of unauthorized access to sensitive information, but PhilHealth could likewise be exposed to liability (e.g., from members whose private information is compromised) if it cannot show that it exercised the diligence required to reasonably ensure the security of its computer system.

IV. CONCLUSION & RECOMMENDATIONS

The specific legal steps and measures that must be taken by PhilHealth will depend in large measure on the type and scope of activities and transactions that will and will not be enabled under POTS. **A comprehensive project to identify and map out the process and flow of such activities and transactions is therefore recommended.**

Such identification of the particular activities or transactions to be covered should be made in order to determine and implement specific legal measures to protect or enable PhilHealth, including, among others, the following:

- What particular activities will be web-enabled and which, if any, will not be allowed to be conducted online?
- What level of security is warranted for a given transaction? As previously stated, the technology or mechanism chosen for purposes of identity authentication should be reliable and appropriate for the purpose for which it is used. More sensitive information or correspondence deserve more sophisticated and secure measures, than those involving minor details or corrections.

[11] "Gov't site, e-mail server breached; budget blamed," by Erwin Oliva INQ7.net, July 24, 2001.

- What legal documents or other information are needed in each activity, and which of these can be submitted online, and which cannot and therefore would have to actually be presented in its hard copy format? What legal templates are necessary or doable in each case?

- Who would be authorized to make the transaction? Again, what measures or technologies are appropriate to ensure reliable online identification of such authorized person?

- Who will have access to collected data?

- For each identified activity or transaction, does PhilHealth need the cooperation of, or connection with other government agencies, and which government agencies are these? What legal document is necessary to bind PhilHealth and the government agency involved?

Once this is done, several steps to address the broad legal and policy issues identified earlier will follow:

(a) **The Implementing Rules and Regulations of the National Health Insurance Act would have to be revised to reflect the requirements and procedures that will define the proposed ISDP.** Pursuant to the E-Commerce Act, this will include, but is not necessarily limited to the following:

- the manner and format in which electronic data messages or electronic documents shall be filed, created, retained or issued;

- where and when such electronic data messages or electronic documents have to be signed, the use of a electronic signature, the type of electronic signature required;

- the format of an electronic data message or electronic document and the manner the electronic signature shall be affixed to the electronic data message or electronic document;

- the control processes and procedures that PhilHealth has chosen to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records or payments;

- other attributes required of electronic data messages or electronic documents or payments; and

- the full or limited use of the documents and papers for compliance with the government requirements.[12]

(b) **PhilHealth must also decide and issue appropriate guidelines or rules on who will be able to use, amend and access its information online**, and draw up the appropriate contracts for the same. Appropriate templates of legal contracts that will govern PhilHealth's relations with health service providers and other entities/persons who will be allowed to transact online with PhilHealth should be drafted.

[12] ECA, Sec. 27.

(c) **Public consultation through public hearings, as well as due publication of any new rules, regulations or guidelines are legal requisites** and must be complied with by PhilHealth in its initiatives relating to the implementation of the ISDP.

(d) For the most part, given the closed nature of ISDP, **PhilHealth must decide on and implement the technology or measures it will put in place to reliably and securely identify the parties involved in online transactions.** PhilHealth can choose to implement the system itself, or else, it can choose to outsource the implementation to the private sector. Each has its advantages and disadvantages, and **a detailed cost-benefit analysis to determine the best option would be advisable.**

(e) If and when the choice is made to open the system even to people or entities who are unknown to PhilHealth, appropriate contracts would have to be entered into with information certifiers, such as certification authorities, who will issue the appropriate identity certificates and verify the identities of such unknown people or entities.

(d) Regardless of whether the ISDP is an open or closed system, **the technology chosen must be evaluated on the basis of whether it can reliably assure:**

i. **That the message really did come from the person or entity with whom PhilHealth was transacting.**

ii. That the message received by PhilHealth is the exact message that was actually sent and PhilHealth should be able to verify **that the message was not intentionally or accidentally altered during transmission.**

iii. **And finally, that the sender cannot later deny that he or she did in fact send the message,** and the PhilHealth would have the means to prove it unequivocally.

(f) **Rules and guidelines to ensure privacy and data protection, as well as rules on sharing or release of collected data need to be put in place.** These rules and guidelines should also be publicly disclosed, and efforts made to ensure that all concerned parties are aware of the same.

(g) It cannot be overemphasized that **COA involvement in all levels of planning and implementation is critical.**

APPENDICES

A. The E-Commerce Act of 1995 (R.A. 8792)

B. An Introduction to Digital Signatures and Electronic Authentication

Republic of the Philippines

Congress of the Philippines

Metro Manila

Eleventh Congress

Second Regular Session

Begun and held in Metro Manila, on Monday, the fourteenth June, two thousand.

Republic Act No. 8792

AN ACT PROVIDING FOR THE RECOGNITION AND USE OF ELECTRONIC COMMERCIAL AND NON -COMMERCIAL TRANSACTIONS AND DOCUMENTS, PENALTIES FOR UNLAWFUL USE THEREOF AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Republic of the Philippines in Congress assembled:

PART I
SHORT TITLE AND DECLARATION OF POLICY

Sec. 1. Short Title. - This Act shall be known as the "Electronic Commerce Act of 2000".

Sec. 2. Declaration of Policy. - The State recognizes the vital role of information and communications technology (ICT) in nation-building; the need to create an information-friendly environment which supports and ensures the availability, diversity and affordability of ICT products and services; the primary responsibility of the private sector in contributing investments and services in telecommunications and information technology; the need to develop, with appropriate training programs and institutional policy changes, human resources for the information technology age, a labor force skilled in the use of ICT and a population capable of operating and utilizing electronic appliances and computers; its obligation to facilitate the transfer and promotion of adaptation technology, to ensure network security, connectivity and neutrality of technology for the national benefit; and the need to marshal, organize and deploy national information infrastructures, comprising in both telecommunications network and strategic information services, including their interconnection to the global information networks, with the necessary and appropriate legal, financial, diplomatic and technical framework, systems and facilities.

PART II
ELECTRONIC COMMERCE IN GENERAL

Sec. 3. Objective. - This Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and reliability of electronic documents related to such activities and to promote the universal use of electronic transaction in the government and general public.

Sec. 4. Sphere of Application. This Act shall apply to any kind of data message and electronic document used in the context of commercial and non-commercial activities to include domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information.

Sec. 5. Definition of Terms. For the purposes of this Act, the following terms are defined, as follows:

a. **"Addressee"** refers to a person who is intended by the originator to receive the electronic data message or electronic document. The term does not include a person acting as an intermediary with respect to that electronic data message or electronic document.

b. **"Computer"** refers to any device or apparatus which, by electronic, electro-mechanical or magnetic impulse, or by other means, is capable of receiving, recording, transmitting, storing, processing, retrieving, or producing information, data, figures, symbols or other modes of written expression according to mathematical and logical rules or of performing any one or more of those functions.

c. **"Electronic Data message"** refers to information generated, sent, received or stored by electronic, optical or similar means.

d. **"Information and communication system"** refers to a system intended for and capable of generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document.

e. **"Electronic signature"** refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.

f. **"Electronic document"** refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

g. **"Electronic key"** refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.

h. **"Intermediary"** refers to a person who in behalf of another person and with respect to a particular electronic document sends, receives and/or stores or provides other services in respect of that electronic document.

i. **"Originator"** refers to a person by whom, or on whose behalf, the electronic document purports to have been created, generated and/or sent . The term does not include a person acting as an intermediary with respect to that electronic document.

j. **"Service provider"** refers to a provider of -

(i) On-line services or network access, or the operator of facilities therefor, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing; or

(ii) The necessary technical means by which electronic documents of an originator may be stored and made accessible to a designated or undesignated third party;

Such service providers shall have no authority to modify or alter the content of the electronic data message or electronic document received or to make any entry therein on behalf of the originator, addressee or any third party unless specifically authorized to do so, and who shall retain the electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.

CHAPTER II
LEGAL RECOGNITION OF ELECTRONIC WRITING OR DOCUMENT AND DATA MESSAGES

Sec. 6. Legal Recognition of Data Messages. - Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data message purporting to give rise to such legal effect, or that it is merely referred to in that electronic data message.

Sec. 7. Legal Recognition of Electronic Documents. – Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing, and -

(a) Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that -

(i) The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and

(ii) The electronic document is reliable in the light of the purpose for which it was generated and in the light of all the relevant circumstances.

(b) Paragraph (a) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the document not being presented or retained in its original form.

(c) Where the law requires that a document be presented or retained in its original form, that requirement is met by an electronic document if -

(i) There exists a reliable assurance as to the integrity of the document from the time when it was first generated in its final form; and

(ii) That document is capable of being displayed to the person to whom it is to be presented: *Provided*, That no provision of this Act shall apply to vary any and all requirements of existing laws on formalities required in the execution of documents for their validity.

For evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.

This Act does not modify any statutory rule relating to the admissibility of electronic data messages or electronic documents, except the rules relating to authentication and best evidence.

Sec. 8. Legal Recognition of Electronic Signatures. An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which -

a.) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;

b.) Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all the circumstances, including any relevant agreement;

c.) It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and

d.) The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.

Sec. 9. Presumption Relating to Electronic Signatures. - In any proceedings involving an electronic signature, it shall be presumed that -

a.) The electronic signature is the signature of the person to whom it correlates; and

b.) The electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows or has notice of defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances.

Sec. 10. Original Documents. - (1) Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if:

(a) the integrity of the information from the time when it was first generated in its final form, as an electronic data message or electronic document is shown by evidence aliunde or otherwise; and

(b) where it is required that information be presented, that the information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all relevant circumstances.

Sec. 11. Authentication of Electronic Data Messages and Electronic Documents. - Until the Supreme Court by appropriate rules shall have so provided, electronic documents, electronic data messages and electronic signatures, shall be authenticated by demonstrating, substantiating and validating a claimed identity of a user, device, or another entity in an information or communication system, among other ways, as follows:

(a) The electronic signature shall be authenticated by proof that a letter, character, number or other symbol in electronic form representing the persons named in and attached to or logically associated with an electronic data message, electronic document, or that the appropriate methodology or security procedures, when applicable, were employed or adopted by a person and executed or adopted by such person, with the intention of authenticating or approving an electronic data message or electronic document;

(b) The electronic data message and electronic document shall be authenticated by proof that an appropriate security procedure, when applicable was adopted and employed for the purpose of verifying the originator of an electronic data message and/or electronic document, or detecting error or alteration in the communication, content or storage of an electronic document or electronic data message from a specific point, which, using algorithm or codes, identifying words or numbers, encryptions, answers back or acknowledgement procedures, or similar security devices.

The Supreme Court may adopt such other authentication procedures, including the use of electronic notarization systems as necessary and advisable, as well as the certificate of authentication on printed or hard copies of the electronic document or electronic data messages by electronic notaries, service providers and other duly recognized or appointed certification authorities.

The person seeking to introduce an electronic data message and electronic document in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic data message and electronic document is what the person claims it to be.

In the absence of evidence to the contrary, the integrity of the information and communication system in which an electronic data message or electronic document is recorded or stored may be established in any legal proceeding -

(a) By evidence that at all material times the information and communication system or other similar device was operating in a manner that did not affect the integrity of the electronic data message and/or electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;

(b) By showing that the electronic data message and/or electronic document was recorded or stored by a party to the proceedings who is adverse in interest to the party using it; or

(c) By showing that the electronic data message and/or electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using the record.

Sec. 12. Admissibility and Evidential Weight of Electronic Data Message and Electronic Documents. - In any legal proceedings, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence -

a. On the sole ground that it is in electronic form; or

b. On the ground that it is not in the standard written form and electronic data message or electronic document meeting, and complying with the requirements under Sections 6 or 7 hereof shall be the best evidence of the agreement and transaction contained therein.

In assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, stored or communicated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard.

Sec. 13. Retention of Electronic Data Message and Electronic Document. - Notwithstanding any provision of law, rule or regulation to the contrary - (a) The requirement in any provision of law that certain documents be retained in their original form is satisfied by retaining them in the form of an electronic data message or electronic document which -

i. Remains accessible so as to be usable for subsequent reference;

ii. Is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to accurately represent the electronic data message or electronic document generated, sent or received;

iii. Enables the identification of its originator and addressee, as well as the determination of the date and the time it was sent or received.

(b) The requirement referred to in paragraph (a) is satisfied by using the services of a third party, provided that the conditions set forth in subparagraphs (i), (ii) and (iii) of paragraph (a) are met.

Sec. 14. Proof By Affidavit. - The matters referred to in Section 12, on admissibility and Section 9, on the presumption of integrity, may be presumed to have been established by an affidavit given to the best of the deponent's knowledge subject to the rights of parties in interest as defined in the following section.

Sec. 15. Cross-Examination. - (1) A deponent of an affidavit referred to in Section 14 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings has the right to cross-examine a person referred to in Section 11, paragraph 4, sub-paragraph c.

CHAPTER III

COMMUNICATION OF ELECTRONIC DATA MESSAGES AND ELECTRONIC DOCUMENTS

Sec. 16. Formation and Validity of Electronic Contracts. - (1) Except as otherwise agreed by the parties, an offer, the acceptance of an offer and such other elements required under existing laws for the formation of contracts may be expressed in, demonstrated and proved by means of electronic data message or electronic documents and no contract shall be denied validity or enforceability on the sole ground that it is in the form of an electronic data message or electronic document, or that any or all of the elements required under existing laws for the formation of the contracts is expressed, demonstrated and proved by means of electronic documents.

(2) Electronic transactions made through networking among banks, or linkages thereof with other entities or networks, and vice versa, shall be deemed consummated upon the actual dispensing of cash or the debit of one account and the corresponding credit to another, whether such transaction is initiated by the depositor or by an authorized collecting party: *Provided*, that the obligation of one bank, entity, or person similarly situated to another arising therefrom shall be considered absolute and shall not be subjected to the process of preference of credits.

Sec. 17. Recognition by Parties of Electronic Data Message or Electronic Document. - As between the originator and the addressee of a electronic data message or electronic document, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of a electronic data message.

Sec. 18. Attribution of Electronic Data Message. - (1) An electronic data message or electronic document is that of the originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic data message or electronic document is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator with respect to that electronic data message or electronic document; or

(b) by an information system programmed by, or on behalf of the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard an electronic data message or electronic document as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the electronic data message or electronic document was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the electronic data message or electronic document as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify electronic data messages as his own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the electronic data message or electronic document is not that of the originator, and has reasonable time to act accordingly; or

(b) in a case within paragraph (3) sub-paragraph (b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic data message or electronic document was not that of the originator.

(5) Where an electronic data message or electronic document is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic data message or electronic document as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the electronic data message or electronic document as received.

(6) The addressee is entitled to regard each electronic data message or electronic document received as a separate electronic data message or electronic document and to act on that assumption, except to the extent that it duplicates another electronic data message or electronic document and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic data message or electronic document was a duplicate.

Sec. 19. Error on Electronic Data Message or Electronic Document. - The addressee is entitled to regard the electronic data message or electronic document received as that which the originator intended to send, and to act on that assumption, unless the addressee knew or should have known, had the addressee exercised reasonable care or used the appropriate procedure -

(a) That the transmission resulted in any error therein or in the electronic document when the electronic data message or electronic document enters the designated information system, or

(b) That electronic data message or electronic document is sent to an information system which is not so designated by the addressee for the purpose.

Sec. 20. Agreement on Acknowledgment of Receipt of Electronic Data Messages or Electronic Documents. - The following rules shall apply where, on or before sending an electronic data message or electronic document, the originator and the addressee have agreed, or in that electronic document or electronic data message, the originator has requested, that receipt of the electronic document or electronic data message be acknowledged:

(a) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by or through any communication by the addressee, automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the electronic data message or electronic document has been received.

(b) Where the originator has stated that the effect or significance of the electronic data message or electronic document is conditional on receipt of the acknowledgment thereof, the electronic data message or electronic document is treated as though it has never been sent, until the acknowledgment is received.

(c) Where the originator has not stated that the effect or significance of the electronic data message or electronic document is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and if the acknowledgment is not received within the time specified in subparagraph (c), the originator may, upon notice to the addressee, treat the electronic document or electronic data message as though it had never been sent, or exercise any other rights it may have.

Sec. 21. Time of Dispatch of Electronic Data Messages or Electronic Documents. - Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic data message or electronic document occurs when it enters an information system outside the control of the originator or of the person who sent the electronic data message or electronic document on behalf of the originator.

Sec. 22. Time of Receipt of Electronic Data Messages or Electronic Documents. - Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic data message or electronic document is as follows:

(a.) If the addressee has designated an information system for the purpose of receiving electronic data message or electronic document, receipt occurs at the time when the electronic data message or electronic document enters the designated information system: Provided, however, that if the originator and the addressee are both participants in the designated information system, receipt occurs at the time when the electronic data message or electronic document is retrieved by the addressee.

(b.) If the electronic data message or electronic document is sent to an information system of the addressee that is not the designated information system, receipt occurs at the time when the electronic data message or electronic document is retrieved by the addressee;

(c.) If the addressee has not designated an information system, receipt occurs when the electronic data message or electronic document enters an information system of the addressee.

These rules apply notwithstanding that the place where the information system is located may be different from the place where the electronic data message or electronic document is deemed to be received.

Sec. 23. Place of Dispatch and Receipt of Electronic Data Messages or Electronic Documents. - Unless otherwise agreed between the originator and the addressee, an electronic data message or electronic document is deemed to be dispatched at the place where the originator has its place of business and received at the place where the addressee has its place of business. This rule shall apply even if the originator or addressee had used a laptop or other portable

device to transmit or receive his electronic data message or electronic document. This rule shall also apply to determine the tax situs of such transaction.

For the purpose hereof -

a. If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business.

b. If the originator of the addressee does not have a place of business, reference is to be made to its habitual residence; or

c. The "usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

Sec. 24. Choice of Security Methods. - Subject to applicable laws and/or rules and guidelines promulgated by the Department of Trade and Industry with other appropriate government agencies, parties to any electronic transaction shall be free to determine the type and level of electronic data message and electronic document security needed, and to select and use or implement appropriate technological methods that suit their needs.

PART III
ELECTRONIC COMMERCE IN SPECIFIC AREAS

CHAPTER I. CARRIAGE OF GOODS

Sec. 25. Actions Related to Contracts of Carriage of Goods. - Without derogating from the provisions of part two of this law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

(a) (i) furnishing the marks, number, quantity or weight of goods;

(ii) stating or declaring the nature or value of goods;

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notice of loss of, or damage to, goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(g) acquiring or transferring rights and obligations under the contract.

Sec. 26. Transport Documents. - (1) Where the law requires that any action referred to contract of carriage of goods be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages or electronic documents.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more electronic data messages or electronic documents unique;

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of Section 25, no paper document used to effect any such action is valid unless the use of electronic data message or electronic document has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of electronic data messages or electronic documents by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more electronic data messages or electronic documents by reason of the fact that the contract is evidenced by such electronic data messages or electronic documents instead of by a paper document.

PART IV
ELECTRONIC TRANSACTIONS IN GOVERNMENT

Sec. 27. Government Use of Electronic Data Messages, Electronic Documents and Electronic Signatures. - Notwithstanding any law to the contrary, within two (2) years from the date of the effectivity of this Act, all departments, bureaus, offices and agencies of the government, as well as all government-owned and-controlled corporations, that pursuant to law require or accept the filing of documents, require that documents be created, or retained and/or submitted, issue permits, licenses or certificates of registration or approval, or provide for the method and manner of payment or settlement of fees and other obligations to the government, shall -

(a) accept the creation, filing or retention of such documents in the form of electronic data messages or electronic documents;

(b) issue permits, licenses, or approval in the form of electronic data messages or electronic documents;

(c) require and/or accept payments, and issue receipts acknowledging such payments, through systems using electronic data messages or electronic documents; or

(d) transact the government business and/or perform governmental functions using electronic data messages or electronic documents, and for the purpose, are authorized to adopt and promulgate, after appropriate public hearing and with due publication in newspapers of general circulation, the appropriate rules, regulations, or guidelines, to, among others, specify -

(1) the manner and format in which such electronic data messages or electronic documents shall be filed, created, retained or issued;

(2) where and when such electronic data messages or electronic documents have to be signed, the use of a electronic signature, the type of electronic signature required;

(3) the format of an electronic data message or electronic document and the manner the electronic signature shall be affixed to the electronic data message or electronic document;

(4) the control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records or payments;

(5) other attributes required of electronic data messages or electronic documents or payments; and

(6) the full or limited use of the documents and papers for compliance with the government requirements: Provided, That this Act shall by itself mandate any department of the government, organ of state or statutory corporation to accept or issue any document in the form of electronic data messages or electronic documents upon the adoption, promulgation and publication of the appropriate rules, regulations, or guidelines.

Sec. 28. RPWEB To Promote the Use Of Electronic Documents and Electronic Data Messages In Government and to the General Public. - Within two (2) years from the effectivity of this Act, there shall be installed an electronic online network in accordance with Administrative Order 332 and House of Representatives Resolution 890, otherwise known as RPWEB, to implement Part IV of this Act to facilitate the open, speedy and efficient electronic online transmission, conveyance and use of electronic data messages or electronic documents amongst all government departments, agencies, bureaus, offices down to the division level and to the regional and provincial offices as practicable as possible, government owned and controlled corporations, local government units, other public instrumentalities, universities, colleges and other schools, and universal access to the general public.

The RPWEB network shall serve as initial platform of the government information infrastructure (GII) to facilitate the electronic online transmission and conveyance of government services to evolve and improve by better technologies or kinds of electronic online wide area networks utilizing, but not limited to, fiber optic, satellite, wireless and other broadband telecommunication mediums or modes. To facilitate the rapid development of the GII, the Department of Transportation and Communications, National Telecommunications Commission and the National Computer Center are hereby directed to aggressively promote and implement a policy environment and regulatory or non-regulatory framework that shall lead to the substantial reduction of costs of including, but not limited to, lease lines, land, satellite and dial-up telephone access, cheap broadband and wireless accessibility by government departments, agencies, bureaus, offices, government owned and controlled corporations, local government units, other public instrumentalities and the general public, to include the establishment of a government website portal and a domestic internet exchange system to facilitate strategic access to government and amongst agencies thereof and the general public and for the speedier flow of locally generated internet traffic within the Philippines.

The physical infrastructure of cable and wireless systems for cable TV and broadcast excluding programming and content and the management thereof shall be considered as within the activity of telecommunications for the purpose of electronic commerce and to maximize the convergence of ICT in the installation of the GII.

Sec. 29. Authority of the Department of Trade and Industry and Participating Entities. - The Department of Trade and Industry (DTI) shall direct and supervise the promotion and development of electronic commerce in the country with relevant government agencies, without prejudice to the provisions of Republic Act. 7653 (Charter of Bangko Sentral ng Pilipinas) and Republic Act No. 337 (General Banking Act), as amended.

Among others, the DTI is empowered to promulgate rules and regulations, as well as provide quality standards or issue certifications, as the case may be, and perform such other functions as may be necessary for the implementation of this Act in the area of electronic commerce to include, but shall not be limited to, the installation of an online public information and quality and price monitoring system for goods and services aimed in protecting the interests of the consuming public availing of the advantages of this Act.

PART V

FINAL PROVISIONS

Sec. 30. Extent of Liability of a Service Provider. – Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of the electronic data message or electronic document for

which the person or party acting as a service provider as defined in Section 5 merely provides access if such liability is founded on -

a.) The obligations and liabilities of the parties under the electronic data message or electronic document:

b.) The making, publication, dissemination or distribution of such material or any statement made in such material, including possible infringement of any right subsisting in or in relation to such material: Provided, That

i. The service provider does not have actual knowledge, or is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes any rights subsisting in or in relation to such material;

ii. The service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and

iii. The service provider does not directly commit any infringement or other unlawful act and does not induce or cause another person or party to commit any infringement or other unlawful act and/or does not benefit financially from the infringing activity or unlawful act of another person or party: Provided, further, That nothing in this Section shall affect -

a) Any obligation founded on contract;

b) The obligation of a service provider as such under a licensing or other regulatory regime established under written law; or

c) Any obligation imposed under any written law;

d) The civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any material, or to preserve evidence of a violation of law.

Sec. 31. Lawful Access. - Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plain text, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key.

Sec. 32. Obligation of Confidentiality. - Except for the purposes authorized under this Act, any person who obtained access to any electronic key, electronic data message, or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.

Sec. 33. Penalties. - The following Acts shall be penalized by fine and/or imprisonment, as follows:

a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the

damage incurred and a mandatory imprisonment of six (6) months to three (3) years; c) Violations of the Consumer Act or Republic Act No. 7394 and other relevant or pertinent laws through transactions covered by or using electronic data messages or electronic documents, shall be penalized with the same penalties as provided in those laws; d) Other violations of the provisions of this Act, shall be penalized with a maximum penalty of one million pesos (P1,000,000.00) or six (6) years imprisonment.

Sec. 34. Implementing Rules and Regulations. - The DTI, Department of Budget and Management and the Bangko Sentral ng Pilipinas are hereby empowered to enforce the provisions of this Act and issue implementing rules and regulations necessary, in coordination with the Department of Transportation and Communications, National Telecommunications Commission, National Computer Center, National Information Technology Council, Commission on Audit, other concerned agencies and the private sector, to implement this Act within sixty (60) days after its approval.

Failure to issue rules and regulations shall not in any manner affect the executory nature of the provisions of this Act.

Sec. 35. Oversight Committee. – There shall be a Congressional Oversight Committee composed of the Committees on Trade and Industry/Commerce, Science and Technology, Finance and Appropriations of both the Senate and House of Representatives, which shall meet at least every quarter of the first two years and every semester for the third year after the approval of this Act to oversee its implementation. The DTI, DBM, Bangko Sentral ng Pilipinas, and other government agencies as may be determined by the Congressional Committee shall provide a quarterly performance report of their actions taken in the implementation of this Act for the first three (3) years.

Sec. 36. Appropriations. - The amount necessary to carry out the provisions of Secs. 27 and 28 of this Act shall be charged against any available funds and/or savings under the General Appropriations Act of 2000 in the first year of effectivity of this Act. Thereafter, the funds needed for the continued implementation shall be included in the annual General Appropriations Act.

Sec. 37. Statutory Interpretation. - Unless otherwise expressly provided for, the interpretation of this Act shall give due regard to its international origin and the need to promote uniformity in its application and the observance of good faith in international trade relations. The generally accepted principles of international law and convention on electronic commerce shall likewise be considered.

Sec. 38. Variation by Agreement. - As between parties involved in generating, sending, receiving, storing or otherwise processing electronic data message or electronic document, any provision of this Act may be varied by agreement between and among them.

Sec. 39. Reciprocity. - All benefits, privileges, advantages or statutory rules established under this Act, including those involving practice of profession, shall be enjoyed only by parties whose country of origin grants the same benefits and privileges or advantages to Filipino citizens.

Sec. 40. Separability Clause. - The provisions of this Act are hereby declared separable and in the event of any such provision is declared unconstitutional, the other provisions, which are not affected, shall remain in force and effect.

Sec. 41. Repealing Clause. - All other laws, decrees, rules and regulations or parts thereof which are inconsistent with the provisions of this Act are hereby repealed, amended or modified accordingly.

Sec. 42. Effectivity. - This Act shall take effect immediately after its publication in the Official Gazette or in at least two (2) national newspapers of general circulation.

AN INTRODUCATION TO DIGITAL SIGNATURES AND ELECTRONIC AUTHENTICATION

What are Electronic and Digital Signatures?

Under the Electronic Commerce Act of 2000, electronic signatures "refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document."[13]

There are many methods for creating an electronic signature. These methods range from simple ones--- such as typing a name at the bottom of an email message--- to more complex and secure ones--- for example, biometric technologies, such as fingerprints or retinal scans.

Still other types of authentication methods include: magnetic strip cards with personal identification numbers (PIN), user names and passwords, public key cryptography, writing tablets with electronic pens, and even smart cards that generate a unique access code every few seconds. As technology advances, the list of viable electronic signature alternatives is sure to grow.

Note that technically speaking, electronic signatures are different from digital signatures. A "digital signature" does not refer to the image of a signature in any way. Unlike both an "electronic signature" which is simply any form of mark intended to be a signature, and a "digitized signature" which refers to an electronic image of a signature, a "digital signature" is actually a term of art that refers to scrambling data in order to provide security and authentication.

Digital signatures are created and verified using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and then back into the original form.

Encryption: How Digital Signatures Work

Military communications have relied on encryption for thousands of years. In fact, Alexander the Great communicated with his generals by sending messages in which each letter was shifted a certain number of positions. This was a form of "secret key encryption," i.e., anyone who knew the secret code (or key) would be able to send and receive messages securely.

Today, commercially available encryption software creates encryption so strong that it is all but impossible to break the code and ascertain the original message without the use of the authorized software.

To be secure, a secret-key coding system requires some method of distributing the secret key to intended users, without it falling into the hands of other parties.

Now, before going further into the basics of cryptographic and digital signature technology, a few terms need to be defined first.

"Encryption" is simply the process by which information is scrambled by use of a code.

A "hash function" is a process that creates a relatively small number that represents a much larger amount of electronic data. For instance, if I had a ten-page word processing document on my computer I could use special hashing software to derive a particular number associated with that document. If even

[13] RA No. 8792, sec. 5(e).

on comma were changed on the document, the resulting hash number from the changed document would be completely different. This number is called the "message digest."

Digital signatures use a "one-way hash function," i.e., there is no way to reverse engineer or derive the content of the message based on the resulting message digest. When a digest is sent along with the message, the recipient can check to see if the message had been tampered with by using the same hashing software to make her own digest of the message and then checking to see if the two numbers match.

Public Key Cryptography

By its nature, the Internet is poorly suited for a secret-key system because it is an "open" network in which a message may make several "stops" before arriving at its final destination.

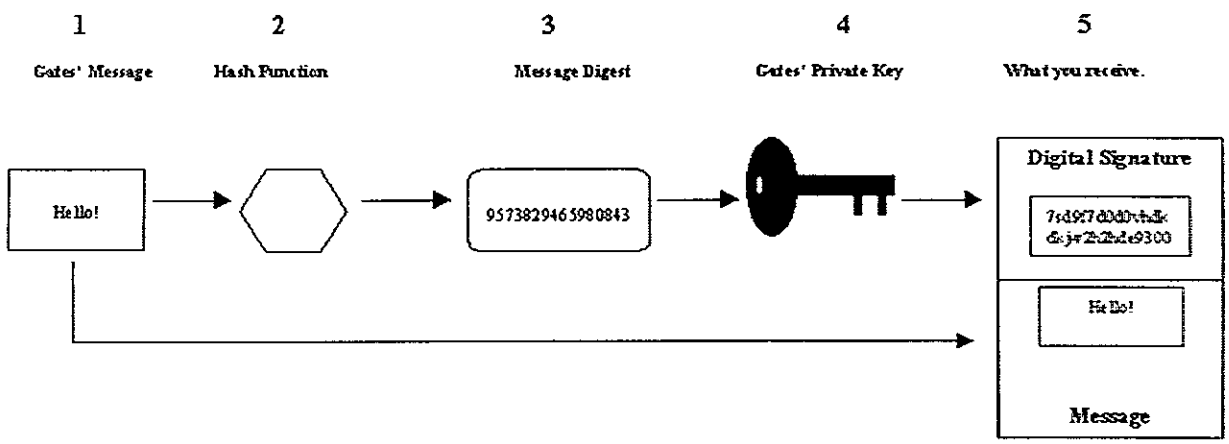
This creates a serious risk that a third party could intercept a secret key at some point along its routing, which would allow the third party to read messages, or even send encoded messages purporting to be from the authorized holder of the key.

Physically delivering a secret key to every user through a secure channel, on the other hand, would be slow, expensive and unwieldy. It would effectively rule out one-time transactions between people and firms that have not previously exchanged secret keys.

Public key cryptography eliminates the need for users to share a secret key, which makes it ideally suited for communications over open networks such as the Internet.

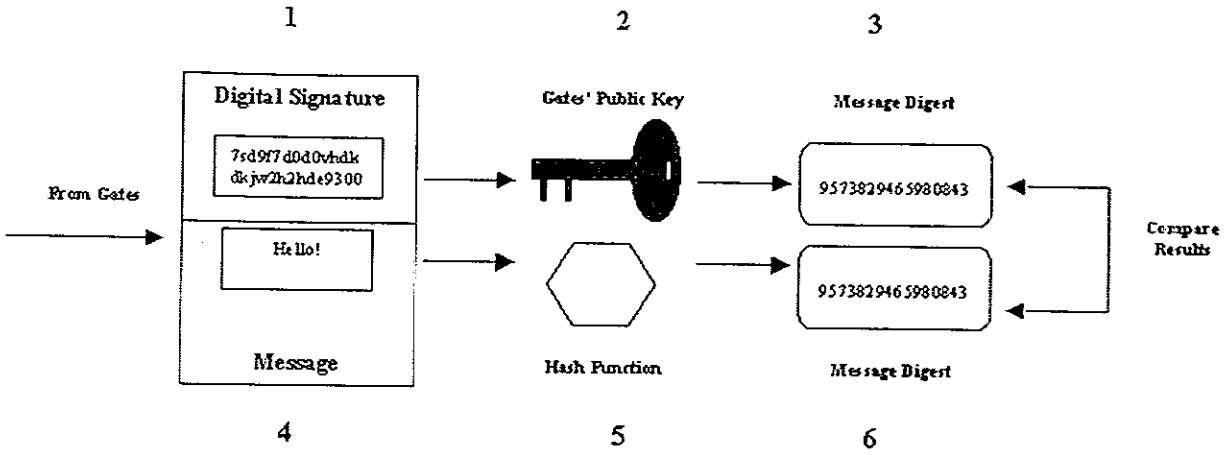
In a public key system, each user has software that generates two related keys, a public key and a private key. The fundamental characteristic of this key pair is that only this particular public key can decrypt a message encrypted with its corresponding private key. Similarly, only this particular private key can decrypt a message encrypted with its corresponding public key.

The process is illustrated in the two diagrams below.



Let us assume that (1) Bill Gates has a message that he wants to digitally sign and send to you. He would then (2) run his message through one of several standard algorithms known as a "hash function" that performs a series of mathematical operations on the original message. The hash function produces a number called a (3) "message digest" which can be thought of as a fingerprint of the message, because any change in the message, no matter how slight, will cause the hash function to produce a completely different message digest. (4) Using his private key, Bill Gates then encrypts the message digest. The

message digest encrypted with Bill Gates' private key forms the actual (5) "digital signature" for the message. Both the digital signature and the actual message are then sent to you.



Upon receipt of the message, your computer and software would then perform two separate operations to verify Bill Gates' identity and to determine if the message had been altered in-transit.

To verify Gates' identity, your system would (1) take the digital signature and (2) use Gates' public key to decrypt the digital signature, which would then (3) produce the message digest. If the operation is successful, you would then know for a fact that Bill Gates' (who alone has access to his private key) must have sent the message.

In order to ensure that Gates' message had not been altered, your system would (4) run Gates' message through the (5) same hash function that Gates' used, which would then (6) yield a message digest of Gates' message. You would then be able to (7) compare the two message digests, and if they are identical, confirm that the message has remained unaltered in transit.

Generally then, users of this system would keep their private key very safe (perhaps password-protected, or even embedded in a smartcard) but they would make their public key freely available, by sending it to all potential recipients of messages or posting it to an Internet public key directory.

In this way, the private key holder (in the example, Bill Gates) can send a message to anyone on the Internet, and, if his public key decrypts the message, the recipient knows it must have come from the private key holder. Conversely, anyone on the Internet who wants to send the private key holder a message can encrypt the message with his public key, and send the message with the knowledge that only the private key holder can read the encrypted text.

Public Key Infrastructures and Certification Authorities

The process of public key cryptography described above can work well between parties who know each other.

But what happens in transactions between parties who have never met each other before? In the example above, how would you know for certain that Bill Gates, and not someone else posing as Bill Gates, did in fact send the message?

In general terms, how can one bind the identity of a particular party to a particular public key. This need has been widely perceived in the marketplace, and several companies are stepping into the so-called "trusted third party" business. Such a company is known as a "certification authority" (CA).

The CA essentially vouches for the identity of a person who subscribes to their service. It issues a certificate in effect guarantees the identity of the person (or subscriber) associated with a given public key. The CA is responsible for undertaking certain measures to ascertain the identity of the person to whom it issues a certificate. This certificate issued by the CA

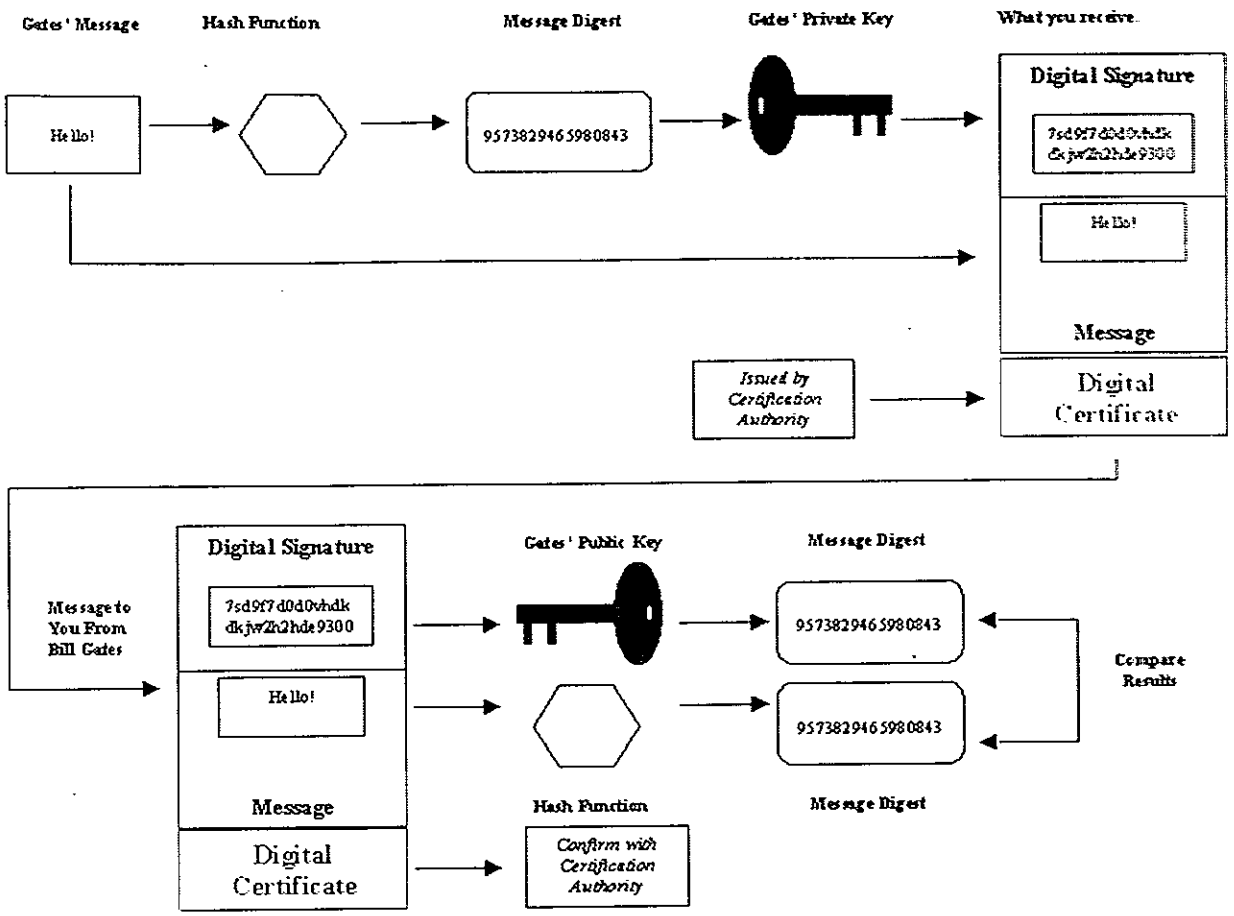
(1) identifies the CA issuing it;
(2) identifies the subscriber ;
(3) contains the subscriber's public key; and
(4) is digitally signed with the CA's private key.

The digital certificate can also contain additional information including a reliance limit, or a reference to the CA's "certification practice statement" that gives relying parties notice of the level of inquiry conducted by the CA before issuing the certificate.

Thus, if Bill Gates wished to use a CA to vouch for his identity on the Internet, he would have to present the CA with a copy of his public key along with sufficient proof of his identity (or else the CA could also issue Gates' private and public keys). Once satisfied with the identity of Bill Gates, the CA would issue Gates' a digital certificate.

Going back to our example, and as shown in the diagram below, Gates will send you, along with his digital signature, a copy of his digital certificate. And, in addition to the steps described above, upon receipt of Gates' message, you can also confirm with the CA identified in the digital certificate that Gates is who he says he is, and that his certificate has not expired or been revoked.

Note that all these activities would be transparent to you, and would happen in much the same way as occurs with online credit card validation systems.


Gates' Message
Hash Function
Message Digest
Gates' Private Key
What you receive
Hello!
9573829465980843
Digital Signature
7sd9f7d0d0vhdk
dkjw2h2hde9300
Hello!
Message
Issued by Certification Authority
Digital Certificate
Message to You From Bill Gates
Digital Signature
7sd9f7d0d0vhdk
dkjw2h2hde9300
Hello!
Message
Digital Certificate
Gates' Public Key
Hash Function
Confirm with Certification Authority
Message Digest
9573829465980843
9573829465980843
Mesage Digest
Compare Results

PART III

HealthWeb
(PhilHealth Online Transaction System)

An overview of the technology and functionality
for serving PhilHealth members
through the World Wide Web

FINAL REPORT
18 November 2002

By Ruben Canlas Jr.
Digital Solutions

Outline of Report

I. Summary *3*

II. Introduction to POTS *5*
- a. What is POTS? *5*
- b. Why is POTS/HealthWeb needed? *5*

III. Description and analysis of current system *6*
- a. Macroscopic perspective *6*
- b. Other government agencies *6*
- c. PHIC current online system *7*

IV. HealthWeb: features and functions *8*

A. MEMBERSHIP PROCESSING
1. Membership Application *9*
2. Status of Application *2*
3. Level 1 or Conditional Approval *13*
4. Level 2 or Full Member Approval *15*
5. Amendment (Edit Profile) *17*

B. CLAIMS PROCESSING
1. Claim Request *19*
2. Claim Approval *21*

C. AUXILLARY FEATURES
1. Online Registration *23*
2. Feedback/Grievance 25

V. Suggested technological solutions *26*
1. Establishing digital identity *26*
2. Basic security issues: digital signatures, keys, VPNs *29*
3. A survey of available technology *33*

VI. Conclusions and Recommendations 36

I. Summary

POTS stands for PhilHealth Online Transaction System. It is the working name for a computerized and networked system that allows PHIC members to use the WorldWide Web (or the Web) in order to process crucial requests and view the results of those requests. In technical terms, POTS is a **web-based system**. Thus a more appropriate name for the system is HealthWeb. From hereon, HealthWeb will be used in this paper to refer to the same system.

HealthWeb is the working name for a web-based system that allows PhilHealth Insurance Corporation (PHIC) to expand its reach and extend its services to members and applicants. It uses secure web technology to allow remote users to connect to computerized services, which include applications for membership, and checking the balance of contributions and status of claims.

Computerized information systems already exist within PHIC, particularly the Operations Management Information System (OMIS). However, OMIS is limited to the Central Office and only PHIC staff can use it. Parts of OMIS can be made available via the Web such that members and applicants can directly make requests and receive the results of these requests without need of PHIC staff. This can be enabled by connecting the relevant parts of OMIS to the WorldWide Web, via the Health Web.

This allows PHIC to gain the benefits of a decentralized system which frees up human resources, enabling it to serve more people and promote system transparency, which is one of the requisites for good governance.

This document presents an overview of the technology that will allow PHIC to offer services directly and securely to members and applicants via the Web. Although some crucial technologies can be discussed in detail, the time constraints given in the analysis and design stage allowed for this project only allow discussions in broad strokes.

Where issues and problems need to be discussed in more detail, this document will try to point these out in its recommendations.

The crucial issues and recommendations involved in developing HealthWeb include the following:

1. Integrity and Security of Transactions. A transaction may be considered reliable and secure if it answers the following issues:

    a. Confidentiality. Only authorized parties have access to the transaction and no eavesdropper can examine its details and contents.
    b. Provenance. The originator of the transaction is true and verifiable. No unauthorized entity can fake a transaction using another digital identity.
    c. Non-repudiation. Both the originator and receiver of the transaction cannot repudiate the transaction (ie, both parties cannot deny that the transaction between the two really transpired).
    d. Integrity. The transacted information cannot be altered during and after transmission. Any alteration can be detected.

    The use of encryption and digital signatures are proposed to be the solutions to these issues. PhilHealth may choose to develop a Virtual Private Network (VPN) either by buying an off-

the-shelf solution, by building its own, or by using a combination of both off-the-shelf and self-developed (or outsourced) systems.

2. Reliability, Speed and Cost of the Web Platform. A choice of three major platforms for web services was given. These three are: Microsoft.NET, SunONE, and Open Source systems. PhilHealth must decide which platform is best, given (a) the existing setup, (b) the reliability, speed, and cost of the platform that will be built. A brief survey of reliability, speed, and cost factors are outlined in the latter section of this paper. Moreover, the use of eXtensible Markup Language (XML) is encouraged because HealthWeb intends to set an initiative for interoperability with other agencies and entities (both government and otherwise).

3. Given the different choices of web platforms, the basic setup for HealthWeb would be the following:

    a. A HeathWeb server which includes a Web server and a Web database server which replicates relevant information from the OMIS databases (eg, Membership, Contributions, and Claims information systems).
    b. A reliable connection between the HealthWeb server and the Web, including a reliable and reasonably fast network connection between PHIC-OMIS and HealthWeb server.
    c. A "bridge" that may be composed of both software and hardware to allow HealthWeb to efficiently link up with PHIC-OMIS.

4. And finally, the last consideration would be the hosting setup for HealthWeb: inhouse, co-located, offshore. The advantages and disadvantages of these options are summarized in order for PhilHealth to evaluate an appropriate hosting option for HealthWeb.

Lastly, it is recommended that a more detailed study be conducted on how to interconnect HealthWeb with various agencies like SSS, GSIS, NSO, SEC, etc.

II. Introduction to HealthWeb

b. What is POTS/HealthWeb?

POTS stands for PhilHealth Online Transaction System. It is the working name for a computerized and networked system that allows PHIC members to use the WorldWide Web (or the Web) in order to process crucial requests and view the results of those requests. In technical terms, POTS is a **web-based system**. Thus a more appropriate name for the system is HealthWeb. From hereon, HealthWeb will be used in this paper to refer to the same system.

As earlier mentioned, HealthWeb will be able to respond to crucial but redundant requests, particularly on Membership processes, like the following:

- Filing an application to be a PHIC member;
- Checking of membership and payment status;
- Requests to change or update membership info; and
- Filing of claims.

c. Why is POTS/HealthWeb needed?

In sum, HealthWeb will:

- Free up PHIC human resources from redundant tasks like answering frequently asked questions or requests that could otherwise be passed on to a web-based system;
- Enable PHIC to reach and serve more people, as mandated by law;
- Empower PHIC members and allow PHIC to reach its goals more effectively and comprehensively in the process; and
- Create a system that encourages transparency, which is a requisite for good governance.

The core of a PhilHealth computerized system already exists, but is only operational at the PHIC Central Office (CO). Moreover, only PHIC personnel have access to the system.

HealthWeb will make some of the frequently used functions available to members and applicants via the Web. This in turn enables PHIC to reach and serve more people than is currently possible.

Moreover, frequently requested services or questions that do not necessarily need human attention can be offloaded into HealthWeb. For instance, HealthWeb will allow a member to check the status of a claim or contribution without having to speak with PHIC personnel. This frees up PHIC human resources and creates more transparency.

III. Description and analysis of current system

a. Macroscopic perspective

The characteristics and uses of the Web have been subject to much hype and misinterpretation in the past. However, removing all the hype surrounding this technology will leave one vital quality that is now being exploited by businesses and governments worldwide – the power of accessibility.

The Web allows anyone with a computer and an internet access to connect anywhere. No matter what type of computer or what software or platform is being used, the Web is available. Palmtop computers like PalmPilot can now surf the Web and Mobile phones with internet connections have already arrived, even in the Philippines.

In the field of medicine, internet/web connections have created scenarios that at first glance seem to have come from science fiction:

- A combination of digital cameras and inter-networking has allowed doctors from different parts of the globe to watch and discuss a surgery in real time.
- Add robotics to the scenario above and a surgeon has been able to conduct an operation hundreds of miles away from the actual operating room, by using robotic arms that are controlled remotely in a different location.
- Using a network of handheld computers and internet connections, doctors can now monitor their patients records even without visiting the hospital.

Businesses were the first to realize the value of the Web. Different customers from different areas often ask the same questions. Creating a list of frequently asked questions that is available on the Web has freed up staff time on the tedious task of answering redundant questions.

One popular example of status checking is FedEx, which allows users to logon to the FedEx website and track their package even without speaking to a FedEx employee.

b. Other government agencies

- In the local scene, the SSS now allows members to check their status by using the Web and online kiosks on malls.
- The Department of Trade and Industry allows various companies to register their products and services via Web in order to link them up with both local and foreign companies who may need the same products and services. DTI also publishes vital trade and industry statistics on the web, making the information more accessible to interested parties.
- Several years ago, the National Statistics Office (NSO) began publishing vital statistical information on the country. They have since then computerized their work process and it is only a matter of time when they make some of their services available on the Web.
- The Security and Exchange Commission (SEC) publishes its forms and application requirements online. They have yet to offer web-based applications.

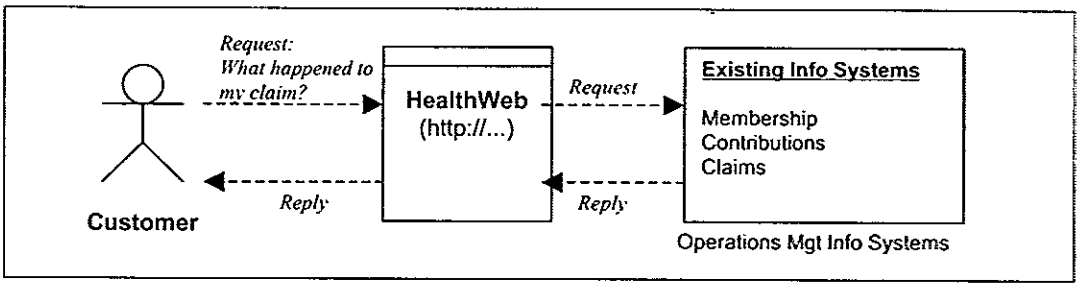
c. PHIC current online system

PHIC's Information Systems Development Plan (ISDP) identifies some of the computer systems that are already operational and some that have been slotted for development. For maximum efficiency, HealthWeb will be connecting to these systems:

1. Membership and Contribution Information System (Operational at the CO: ISDP, page 11)
2. Claims Processing (Operational at the CO: ISDP, p. 14)
3. Website (For development: ISDP, p. 17)

Except for the Website, the systems above are driven by databases that exist at the PHIC Central Office. That is, items 1 and 2 above contain the Membership, Contributions, and Claims databases.

The diagram below gives an idea of how the HealthWeb system interacts with the existing systems to provide services to a PHIC member (ie, "Customer"):



The illustration above shows how a Customer can log on to the website of HealthWeb and use an online form to ask for the status of a claim. The Customer directly accesses the data that is stored within the existing Operations Management Info Systems without having to contact PHIC staff.

IV. HealthWeb: Features and Functions

This section discusses the features and functions that the HealthWeb system needs to perform. The descriptions below were based on the reading materials provided by PHIC, and discussions with Dr. Banzon and Eugene Foz. Any mistake, however, shall only be the result of the author's misinterpretation and may be corrected accordingly.

Limitations:
Owing to the time constraints, the systems analysis was cursory at best. More detailed systems analysis is recommended. This list of features and functions also need further fleshing out in terms of detailed analysis of business processes and workflow. Furthermore, the analyses must take into consideration an earlier study conducted by the Technical Working Group on Information Management and Reporting Systems Review (IMRSR-TWG).

Design Considerations:
It is recommended that further analysis and design of HealthWeb must be take an object-oriented approach. In particular, the HealthWeb System must be independent of the other systems to which it connects. As far as HealthWeb is concerned, it will merely push data and retrieve data from any other system. For example, a change in the implementation of OMIS and other systems should ideally have no effect on HealthWeb.

DESCRIPTION OF FEATURES AND FUNCTIONS:

A. MEMBERSHIP PROCESSING

1. **Name:** Membership Application

Overview: This feature allows a user to fill up an online application form, and send it online.

Primary Actor: Applicant

Starting Point: The user requests for an application form.[1]

Ending Point: The Application is sent or canceled.

Measurable Result: The approving authority[2] receives the new online application and a hardcopy of certified true copy of proof of identity is received by mail.

Flow of Events: The process begins when the user requests for an application form. The user is reminded that s/he should have a required proof of identity onhand, like a birth certificate, a baptismal certificate, passport, etc (see, Implementing Rules and Regulations or IRR, p. 12 for a complete list). The user fills up the form, adds some vital information from the proof of identity (eg, Passport Number, in the case of Passport), and clicks the Submit button. The user is prompted to review the submitted information one final time and click the Submit button again to send the info. After this, the user is given a tracking number and is instructed to print or write it down. The user is also instructed to send a certified true copy of the proof of identity to the nearest PHIC office for verification. (See Alternative Flow of Events, below)

Alternative Flow of Events 1: The user tries to or still wishes to apply but has no certified true copy of the proof of identity onhand. In this case, the user is still given a tracking number and is instructed to save the filled up form. When the certified true copy of proof of identity has been established, the user can then log back and resume the process.

Alternative Flow of Events 2: The user opts for a courier to pickup his/her papers. This is similar to what is being done by the Department of Foreign Affairs (DFA) in processing passport applications and renewals. In brief, the user agrees to pay an additional amount to arrange for a courier to pick up the required documents and deliver them to the PHIC Approving Authority. The courier can also collect the payment for this service.

[1] The term "user" is used here in the generic sense because anyone can fill up the form for someone else. Sample cases include a secretary who is applying for the employees of her company, or a child who is filling up the online form for a parent who is not very familiar with the use of the web, or may have visual impairment.

[2] "Approving authority" here needs to be discussed further. This could be a staff from the RHIO or from accredited hospitals who can review and verify the authenticity of the hardcopy documents. However, RHIO and hospital staff may not have the capability to do this verification.

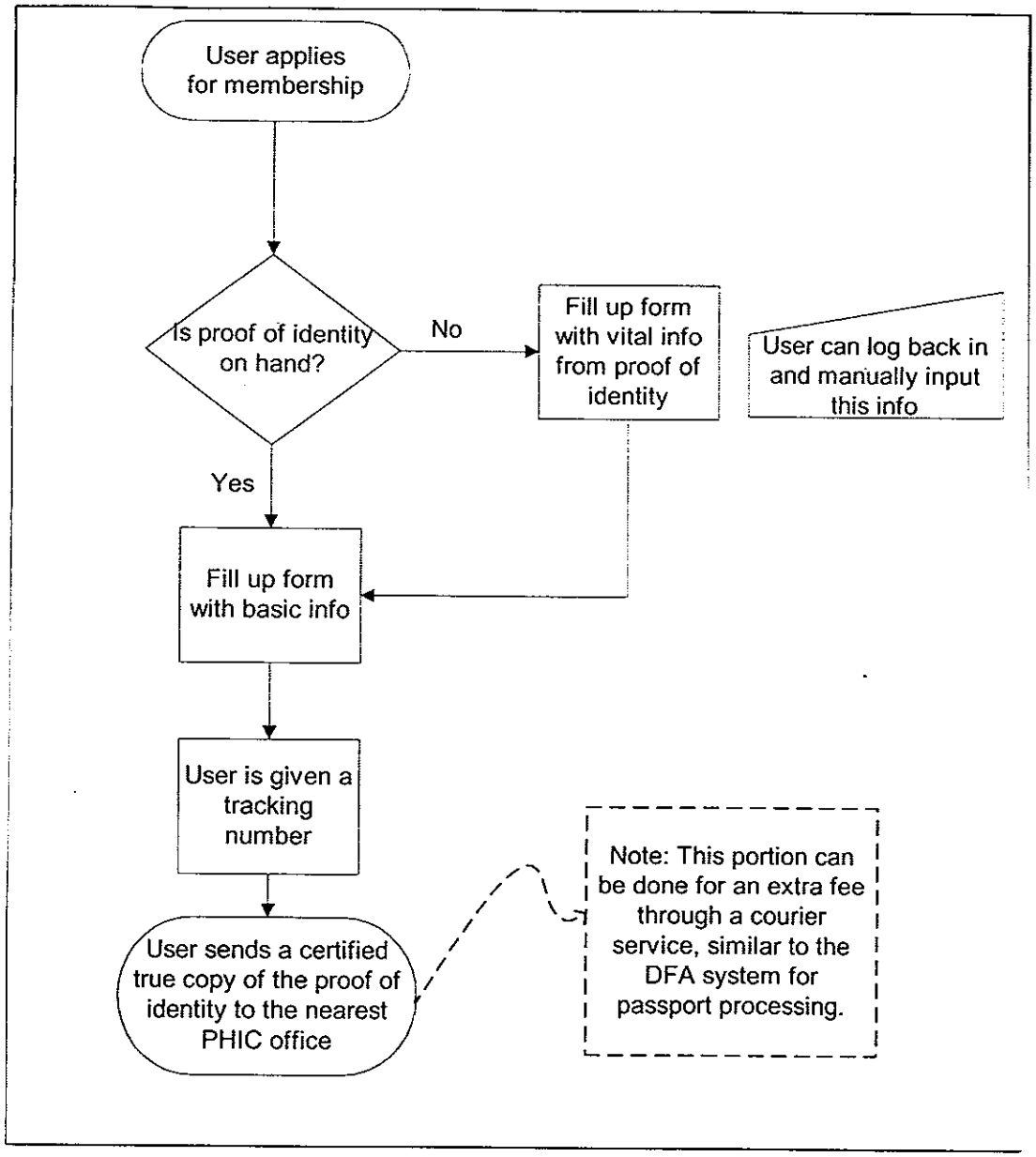


Diagram: Membership Application

40

2. **Name:** Status of Application

Overview: This feature allows a user to view the status of his/her application.

Primary Actor: Applicant

Starting Point: The user requests to view the status of an application.

Ending Point: The user reads the status.

Measurable Result: The status request is logged on to a database.

Flow of Events: The process begins when the user requests to view the status of his/her application. The user is prompted to enter a tracking number. Next, the system checks for the status of the application and displays it to the user.

Alternative Flow of Events: The user forgets or loses the tracking number. In this case, the user can request to have the number emailed back. After receipt of the tracking number, the user can resume the request.

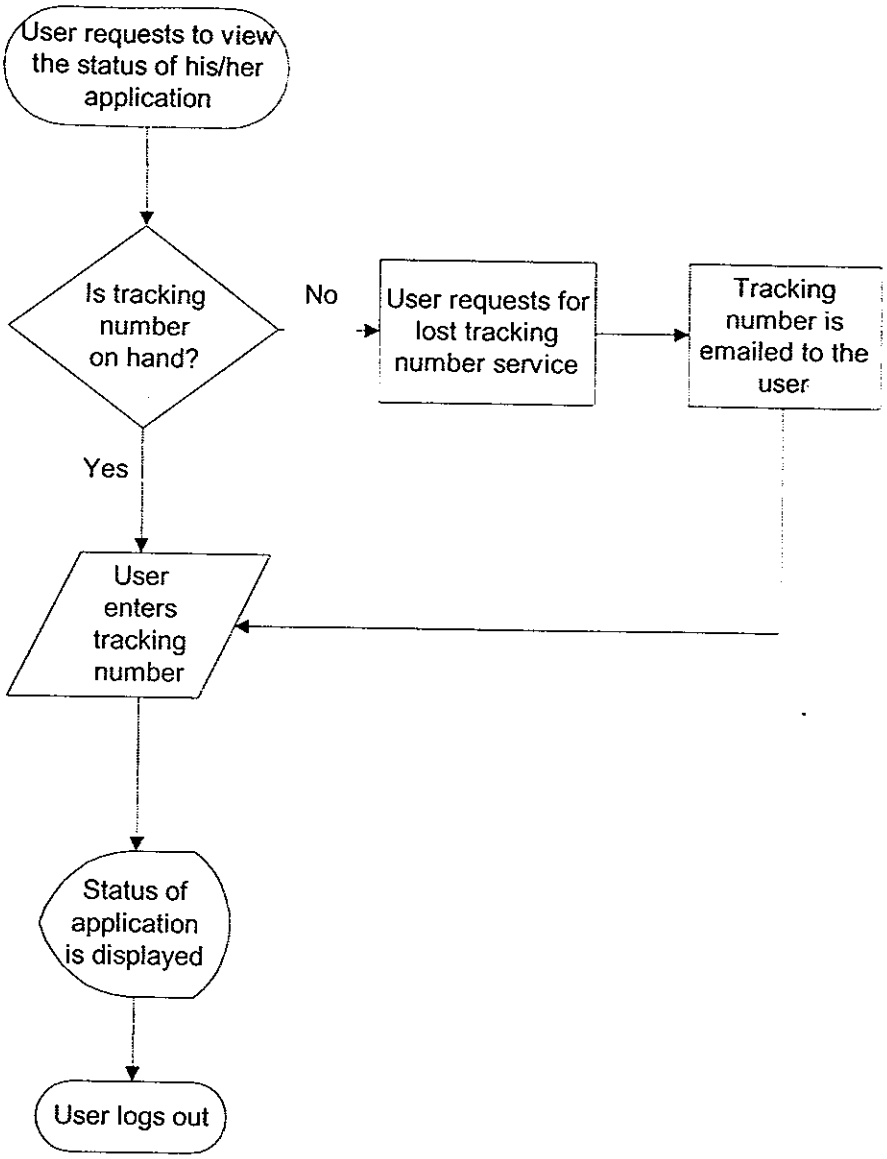


Diagram: Status of Application

3. **Name:** Level 1 or Conditional Approval (1 of 2 Approval Levels)

Overview: This feature allows a user (the Approving Authority) to review and grant Conditional Approval to an applicant.

Primary Actor: Approving Authority or AA.

Starting Point: The AA requests a list of pending applications.

Ending Point: An applicant is given a Level 1 Approval (ie, pending receipt of Proof of Identity). At this level, the Member is allowed to start making voluntary contributions.

Measurable Result: The applicant status is marked as Conditionally Approved.

Flow of Events: The process begins when the Approving Authority views a list of applications. The AA checks the eligibility of the applicant. That is, the AA sorts out applications that seem dubious. In addition, the AA can also review the application information to find duplicate identities (ie, possible fraudulent applications using existing identities that are already members), or check whether the name is included in the Black List. The process ends when an applicant has been given a Level 1 approval. The system generates a letter that can either be printed or emailed to the applicant, announcing the granting of Level 1 approval. The message can also instruct the applicant to next undergo medical evaluation, and that Level 2 or Full Approval will be granted as soon as the hardcopy documents have been received and verified by the Approving Authority.

Alternative Flow of Events: None have been determined at this point.

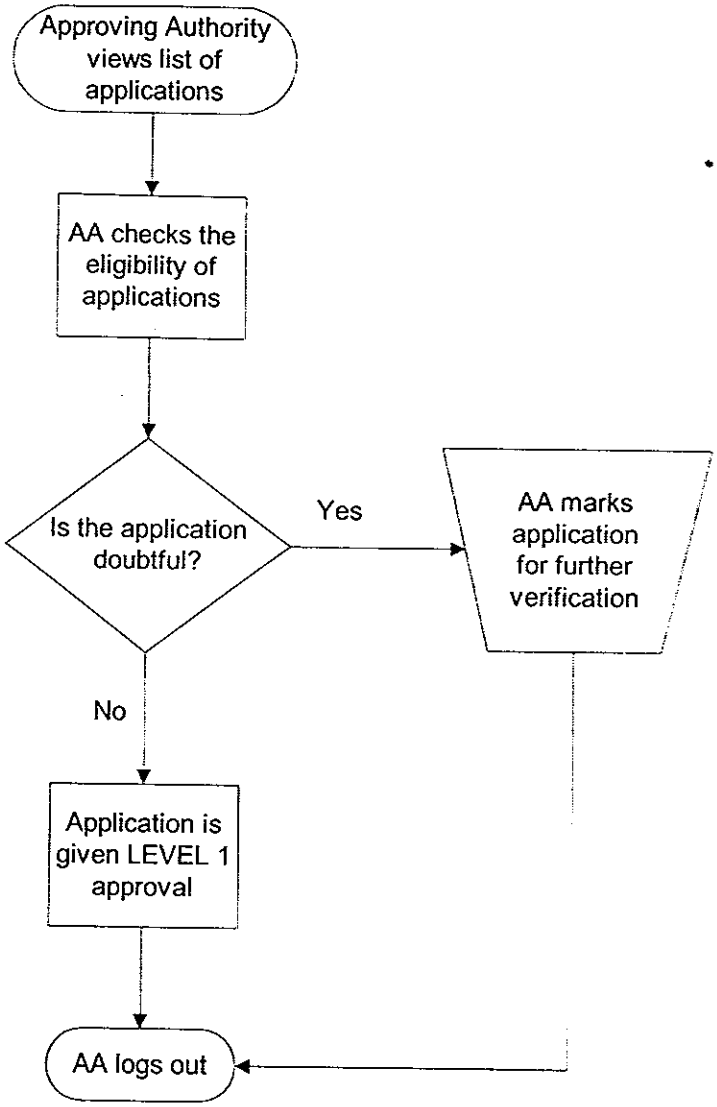


Diagram: Conditional Approval

4. **Name:** Level 2 or Full Approval

Overview: This feature allows a user (the Approving Authority) to grant full approval to an applicant.

Primary Actor: Approving Authority or AA.

Starting Point: The AA receives the certified true copy of the Proof of Identity (PoI). (Alternatively, the AA receives notice that the Proof of Identity has been verified as correct by another reviewer, which may either be from RHIO, from an accredited health care provider, or by another authority designated by PHIC).

Ending Point: An applicant becomes a member.

Measurable Result: Information about the new member is added into the Membership database.

Flow of Events: The process begins when the Approving Authority (AA) verifies – or receives verification of -- the certified true copy of the Proof of Identity. The AA then opens the file of the applicant, checks whether the applicant has fulfilled the other requirements, and grants full membership status.The system generates a letter that can either be printed or emailed to the applicant, announcing the granting of Full Membership.

Alternative Flow of Events: The applicant may have failed to undergo Medical Evaluation and thus cannot be a full member. In this case, the system can generate a letter to remind the applicant to undergo Medical Evaluation immediately before full membership is granted. Another alternative case is when the applicant's Proof of Identity may have problems, in which case the AA generates a letter that will be sent to the applicant, stating the problems. Another possible alternative flow is when the PoI has been proven false. In this case, the AA can generate a letter notifying the applicant of the disapproval, and has the option to elevate a possible case of fraud to relevant authorities (eg, the Legal Department or the Police). The disapproved member is also added to the Black List database.

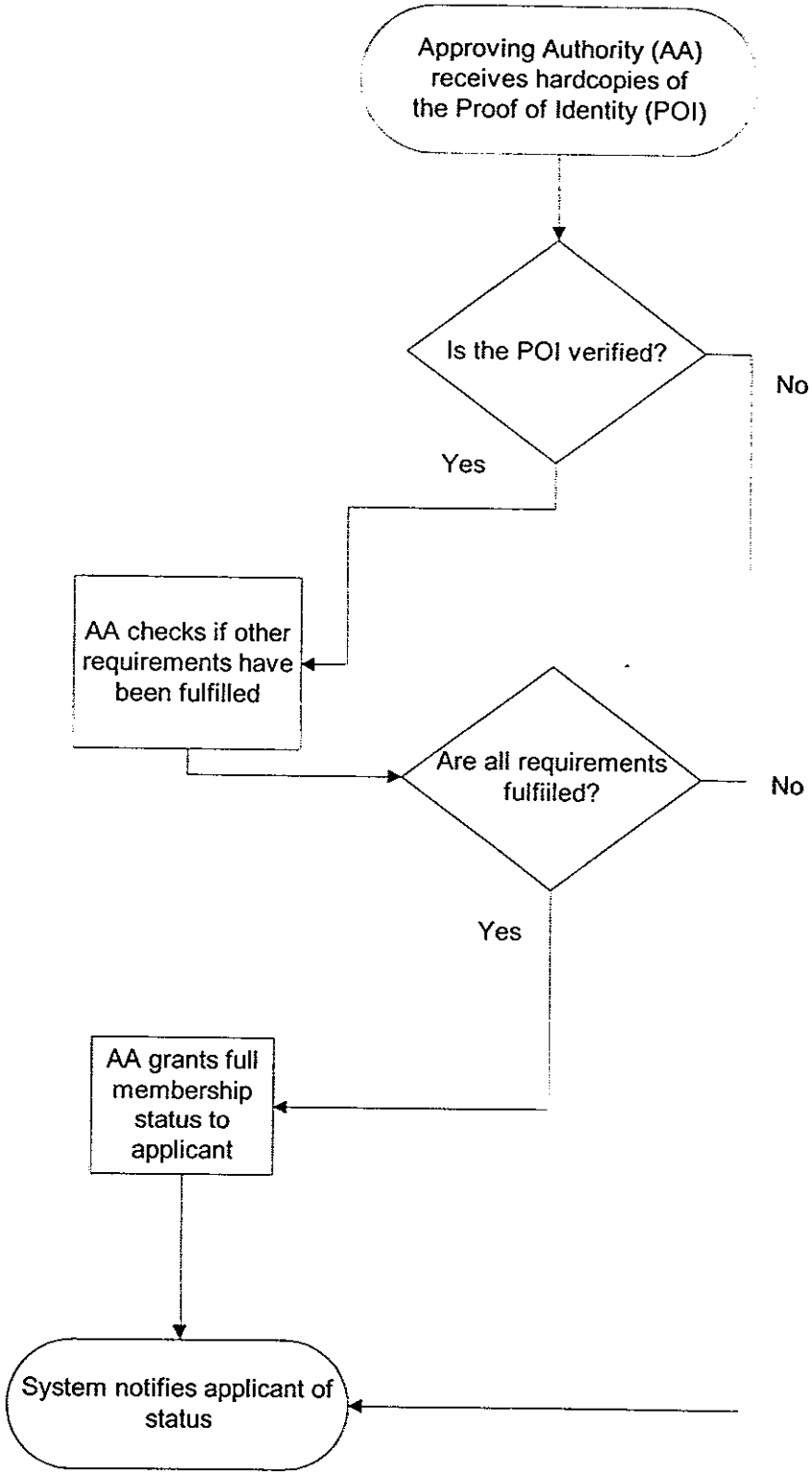


Diagram: Full Approval

46

5. **Name:** Amendment (Profile Editing)

Overview: This feature allows a user to directly make changes to his/her profile (without having to go PHIC staff).

Primary Actor: Member

Starting Point: The Member requests to update or make changes to his/her profile.

Ending Point: The member's profile is amended.

Measurable Result: The amendment is entered into the log and details of the amendment may be emailed to the member.

Flow of Events: The process begins when a member requests a form to update his/her profile. Upon successful authentication, the member's profile is shown on the screen. The member can then make the amendments and submit them. When the amendments are submitted, the system first checks for invalid entries. If now invalid entries are present, the member's profile is finally amended.

Alternative Flow of Events: The member may opt to cancel the amendment. In this case, the member may still rollback the changes by clicking on a Cancel button. NOTE: after the final submission, it would not be possible to cancel the amendment. However, the member can request for another amendment in order to change the information again.

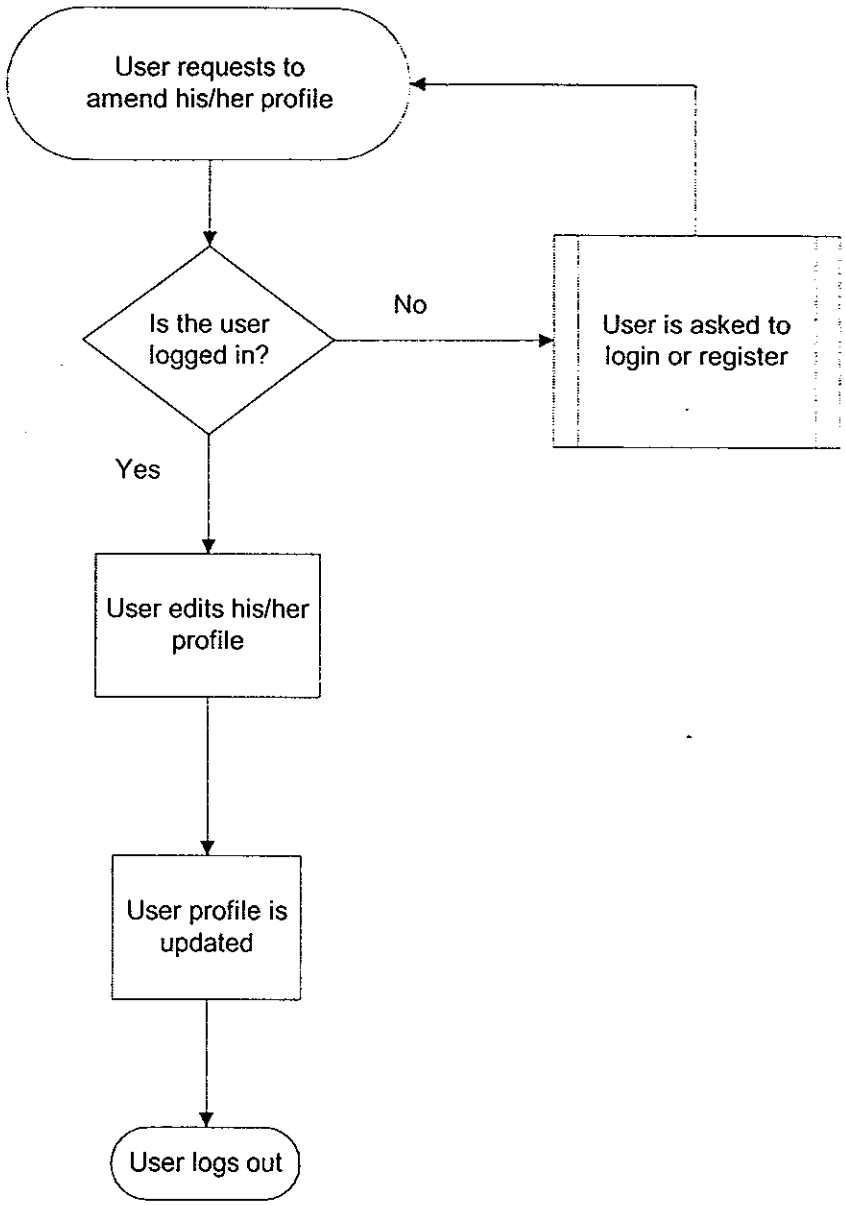


Diagram: Amendment

48

B. CLAIMS PROCESSING

1. **Name:** Claim Request

Overview: This feature allows a Member to make a claim.

Primary Actor: Member

Starting Point: The Member requests a Claim Form.

Ending Point: The Member sends the Claim Form.

Measurable Result: The claim is added to the list of pending claims.

Flow of Events: The process begins when a Member requests for an online Claim Form. The Member is first given a checklist, emphasizing that s/he should have the required documentary proof (eg, proof of hospitalization etc). After the checklist is reviewed, the Member is given the online Claim Form to accomplish. When the Member submits the Claim Form, the basic data in it is checked for validity (eg, valid email address, only numbers must be in the telephone, valid area code, etc). The Member is then asked for a final review of the data. Next, the Member can finally send the Claim Form online. After this, the Member receives instructions on where to send the documentar proofs and when to follow up. The Member is instructed to write down the instructions or print them out.

Alternative Flow of Events: Aside from hardcopy documentary proof, the Member can give a hospitalization reference number that can be cross-checked by the HealthWeb system (of course, this is only possible with computerized hospitals or health care providers).

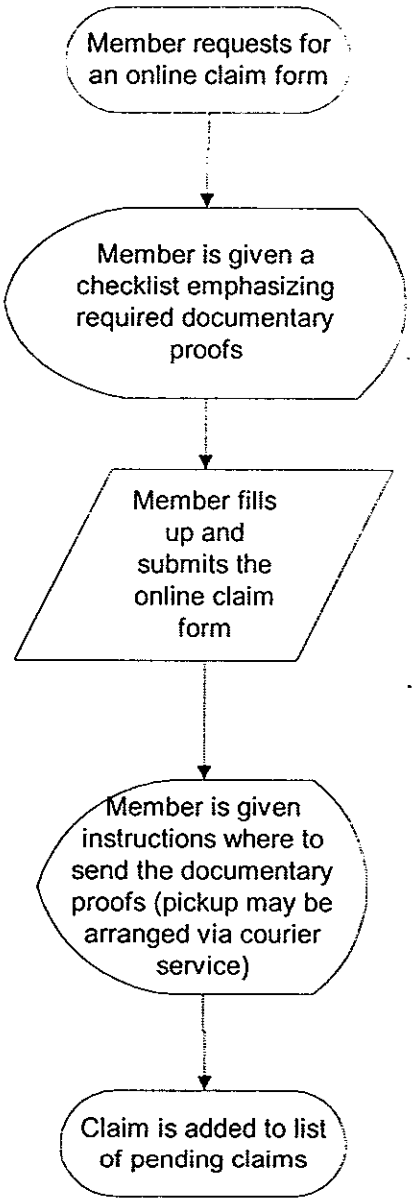


Diagram: Claim Filing

50

2. **Name:** Claim Approval

Overview: This feature allows an Approving Authority to approve a claim.

Primary Actor: AA

Starting Point: The AA receives notification that the documentary proof of a claim has been verified.

Ending Point: The AA sends a notice of approval or disapproval.

Measurable Result: The approved/disapproved claim is added or updated into the Claims database.

Flow of Events: The process begins when the Approving Authority (AA) verifies – or receives verification of -- the documentary evidence submitted by the Member-claimant. The AA then opens the claim, checks whether the claimant has met the other requirements (eg, check the Contributions database), and grants the claim.The system generates a letter that can either be printed or emailed to the applicant, announcing the granting of Full Membership. The system also then updates the relevant databases (eg, the Claims database, etc)

Alternative Flow of Events: Another alternative flow of events is when the Member's documentary proof may have problematic information, in which case the AA generates a letter that will be sent to the Member, stating the problems and the steps to take to clear it up. Another possible alternative flow is when the proof has been proven false or fraudulent. In this case, the AA can generate a letter notifying the Member of the discrepancy or disapproval, and has the option to elevate a possible case of fraud to relevant authorities (eg, the Legal Department or the Police). The disapproved claim is also added to the Black List database.

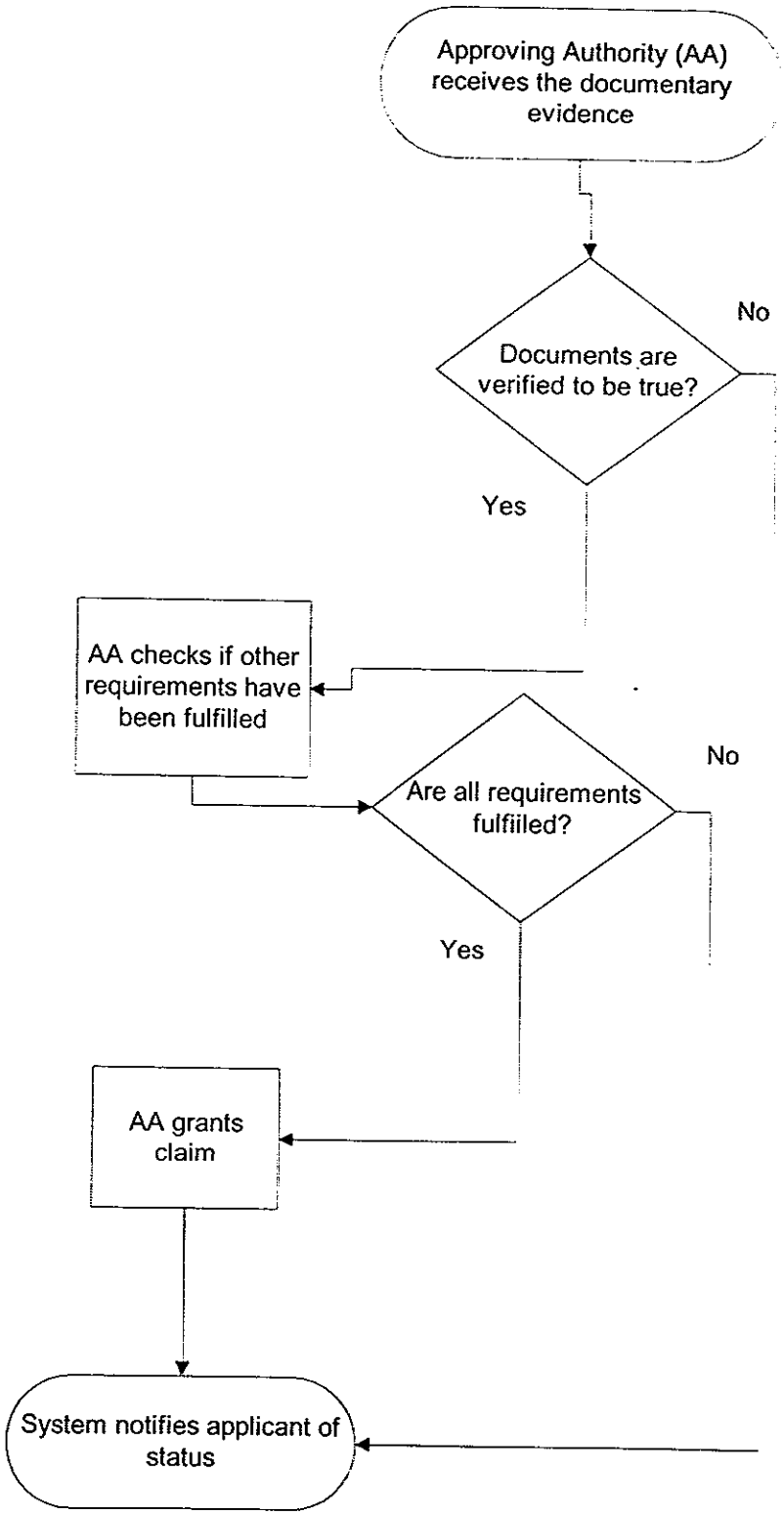


Diagram: Claim Approval

AUXILLARY FUNCTIONS

1. **Name:** Online Registration

Overview: This feature is the first step needed to use HealthWeb. It is similar to opening a web email account, and is based on the principle that if a person can access HealthWeb, then that person should have an email account. This feature is designed to establish the existence of the user's email account, and the user's ability to access that account. Email is a vital method of communication for HealthWeb. All notifications and announcements will be sent to online users via their registered email accounts.

Primary Actor: Registrant

Starting Point: The Registrant requests to register online.

Ending Point: The Registrant activates his/her online account and becomes an online user.

Measurable Result: A new online user is added into the list of online users.

Flow of Events: The process begins when the Registrant requests for online registration. The Registrant is then asked to specify a username and a working email address. The Registrant is reminded that the email address must be a true, working email because the password (and other crucial information) may only be sent through that address. After sending the online form, the Registrant is notified automatically to check his/her email for the next instructions. When the Registrant opens his/her email, the letter will contain a randomly generated activation code and password.

The user is then asked to follow a link to the activation page and input the activation code. The user is reminded that the activation code and password will expire after X amount of days, hence it is important that the account be activated ASAP. After a successful activation, the user is prompted to enter an emergency question that will be used in case the user forgets his/her password. Then, the user is prompted to logon to the system for the first time (by using the username and emailed password). Upon a successful first-time logon, the user receives a prompt that encourages him/her to change the password. The user is now added to the list of online users.

Alternative Flow of Events: The Registrant may fail to activate the account after three attempts. Another alternative flow is that the activation code and password may have expired. In this case the Registrant is prompted to re-register. If the Registrant still encounters a problem, s/he is encouraged to email tech support stating the error message.

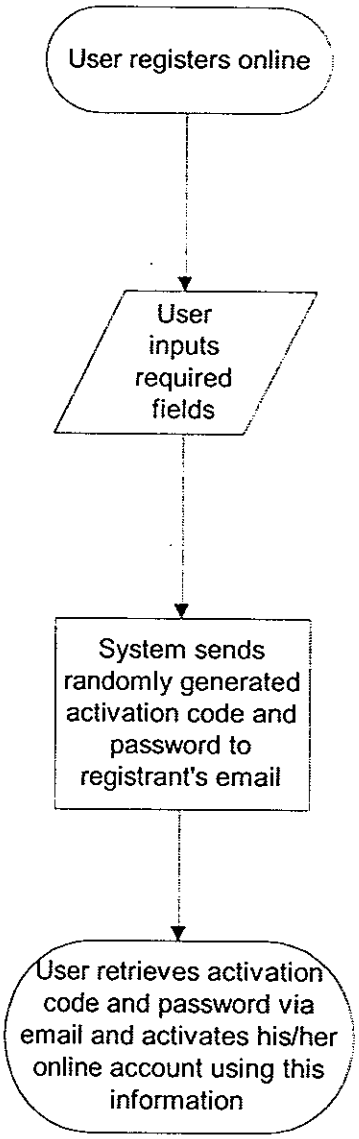


Diagram: Online Registration

2. **Name:** Feedback/Grievance Features

Overview: The Feedback/Grievance features will allow a Member to send feedback or file a grievance regarding PHIC service or a particular claim. These features will be discussed in broad strokes, since they mirror the other features outlined above. In particular, the Feedback/Grievance features are similar to the filing of membership in that they involve the filing and sending of a form with the request "pushed" to the task list of a Grievance Authority.

Flow of Events - Filing: The process begins when a member requests to file a Feedback Form. The system checks whether the member is properly logged in. The member then must specify whether the request is for a general feedback or a specific grievance (ie, against a claim). From this, the user fills up the appropriate form and submits it online. The system asks the member to make a final review of the form and click the send button. In the case of a grievance, the user is given a grievance tracking number. The feedback/grievance is entered into the Feedback database.

Flow of Events - Processing: The process begins when the GA "pulls" a list of incoming feedback and grievances. In case of good feedback, the GA can opt to circulate the commendation via email. In case of a grievance, the GA then marks the request for processing. At certain stages during processing, the GA can update the status of the grievance request. If a Member requests for grievance status, the status of the grievance is pulled out of the Grievance database. When a decision on the grievance is reached, the GA updates the database and then notifies the Member about the decision.

V. Suggested technological solutions and some important issues

1. Establishing digital identity

For a more detailed discussion of the digital signature, please refer to the Legal Framework. The discussion below outlines a simple means of establishing digital identity. More complex and secure ways can be created, but, as discussed below, will still be prone to fraud as is the case in the real world. The task then is to try to make the system as difficult to fool as possible.

Traditional method
To better understand the concept of establishing digital identity, we can begin by understanding how identity is established in the traditional sense. The traditional way of establishing the identity of, say Juan dela Cruz, was to show documentary evidence – eg, a certificate of live birth proves that a certain Juan dela Cruz was born in January 1, 1990.

This implies two things:

a. That on Juan's birth, a witness was present and later registered the birth with the Hospital or City Hall. (Alternatively, when Juan was baptized, this was recorded by the Church, including Juan's birthdate)
b. That the Hospital, City Hall, and the Church are authorities that could be trusted to keep relatively error-free documents.

From the basic event of a birth, other documents may be generated, eg, a Passport or a Driver's License. Since a birth certificate is required to get a Passport, showing a Passport is a second-degree proof of birth (and hence, of identity).

Digital equivalent (and fraud)
In the digital world, the "birth" of a digital identity can draw a parallel from an online registration. If the relevant digital world is HealthWeb, then registering for an online account in HealthWeb system is equivalent to the birth of a digital user. With this analogy, the HealthWeb system becomes the witness to the event, and the database of online users becomes the registry where the event is recorded.

Since it is difficult to establish the veracity of identity over the internet, two methods must be implemented side by side:

a. **A basic test of digital identity** is by the lateral method of checking through an email account. Let us say Pedro is trying to pose as Juan and enters realjuan@yahoo.com (Juan's email) in the field asking for the registrant's email address. This method backfires because the activation code and password will be sent to Juan's email address, which Pedro presumably cannot open.[3]

[3] Note that as emphasized, this is a simple way to establish digital identity. Email accounts can be hacked, mainly because some email users simply refuse to use more secure passwords. In any event, the degree of security can be increased by adding other security measures.

Another way is for Pedro to create a fake account like fakejuan@yahoo.com. Even if Pedro can open this email, what Pedro has succeeded to do was simply activate an online account with HealthWeb.

b. **Supplement the above with the traditional method.** The more important test of identity happens when the online user finally applies for membership, a process which involves sending and verifying traditional evidences of identity. PHIC can also find alternative means of establishing identity, as in the case of members with credit card accounts.[4]

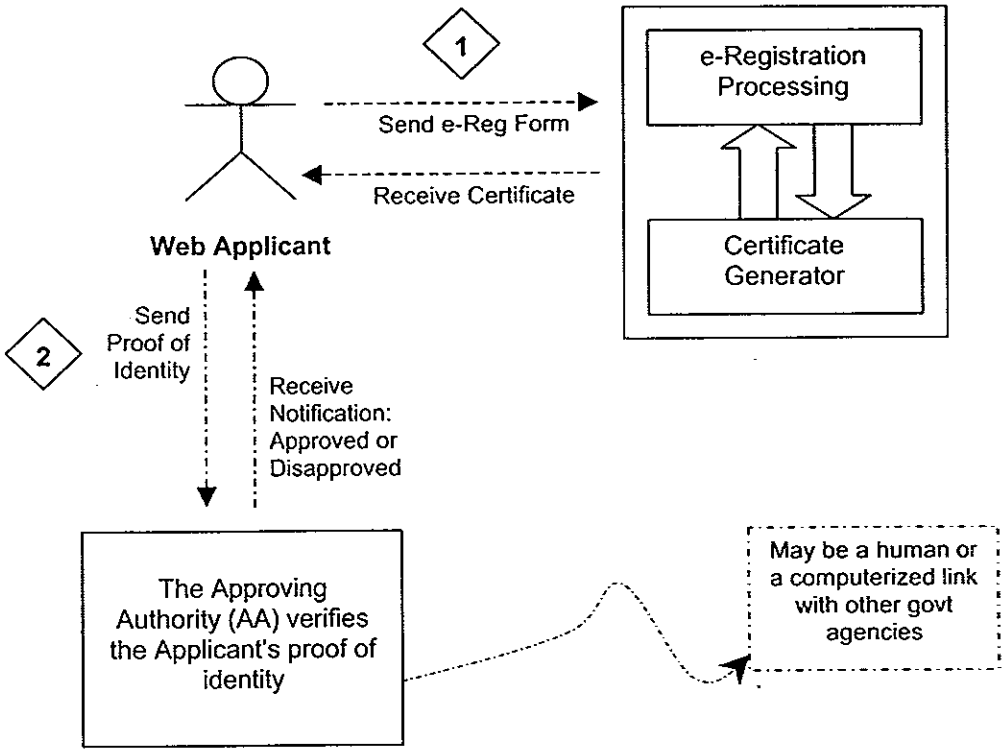
The caveat here is that the digital world, as in the real world, is prone to fraud. Someone may be able to fake any of the documents above and fool the system altogether. Fake certificates of live birth which could fool untrained people can be made using today's hi-resolution color printers. Even biometric methods like thumbprint scanners could also be fooled using simple methods, as recently reported in some journals.

The situation can be best illustrated by a cartoon featuring a paranoid home owner that put several locks on his door. The burglar simply opened the door by patienty chiseling at the hinges from outside. Hence, no matter how many locks are in the system, the point is to keep checking the door: whether it has new vulnerabilities or something has been overlooked. Or maybe the problem is not at the door but somewhere else: unlocked windows or an unsecured backdoor.

What is important to note here is that fraud can come easily from both the online and the real worlds, and that precautions must always be taken in order to make fraud more difficult.

The illustration below gives an overview of how digital identity is established:

[4] Admittedly, even the granting of credit cards can be prone to fraudulent identities.



Explanation:

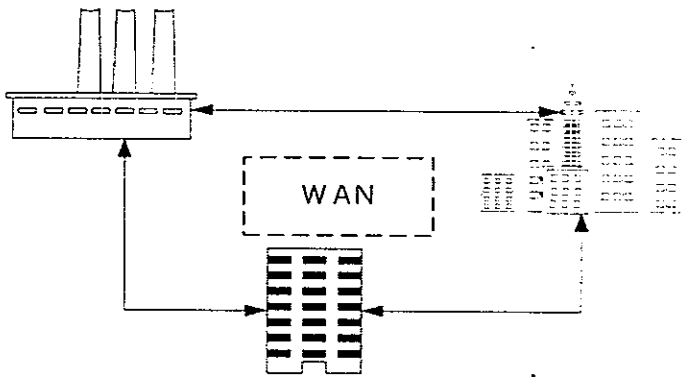
1 The Applicant establishes digital presence thru online registration. The system then verifies digital presence via email and a Digital Certificate. Note that at this point, only *digital presence* has been established, and not the applicant's identity.

(The Digital Certificate can then be combined with other Proofs of Identity like SSS/GSIS Numbers, the Members PIN and the login password in order to form a relatively good way of establishing identity. Caution must be taken to minimize giving the user too many numbers and passwords to memorize.)

2 The Applicant next sends Proof of Identity to the Approving Authority (AA). Bear in mind that AA at first can be a human. Later this can be computerized, once HealthWeb can hook up directly with SSS, GSIS, NSO, etc to establish identity.

2. Basic Security Issues during Electronic Transactions: Digital Signature, Public-Private Keys, Virtual Private Networks, and Encryption

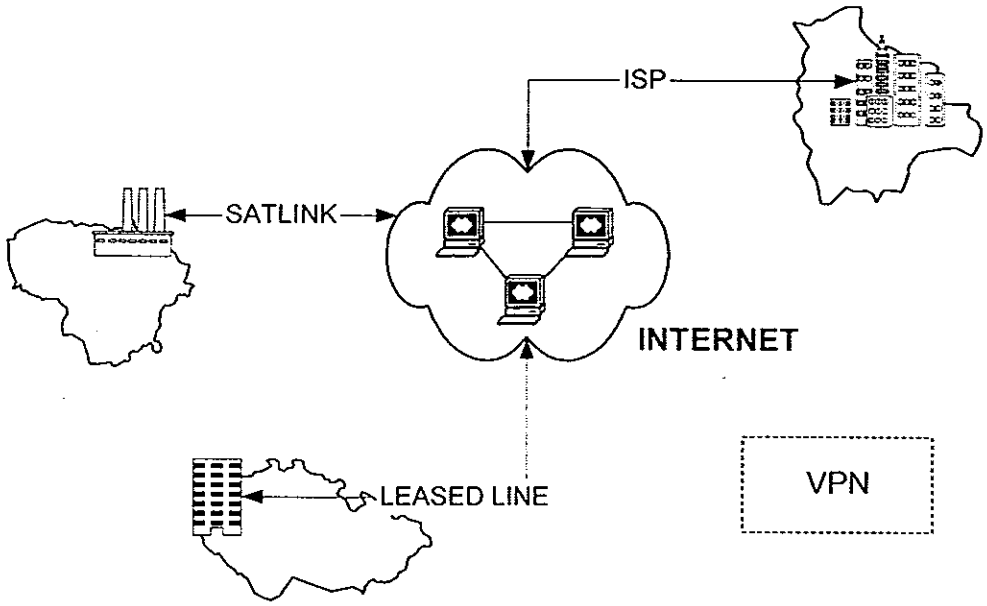
Overview: Infrastructure. In the early days of networked computing, companies used Wide-Area Networks, or WANs in order to hook up physically separated buildings and office branches.



WANs were relatively secure, since they used privately built infrastructure[5]. The problem with WANs is that they are expensive to build and maintain, owing to the infrastructure requirements.

When the internet became prevalent in mid- to early 1990s, it allowed a relatively cheaper substitute to the WAN. This substitute later became known as the Virtual Private Network or VPN. This method uses the internet to create a "virtual" private network (hence, simulating a real WAN or private network). The illustration below shows how this is done.

[5] Again, cables that interconnect WANs can still be tapped. Hence, data circulating through the WANs could be intercepted. This loophole could be solved using data encryption.



The internet poses major security loopholes. To respond to these, various methods of securing data through the internet were proposed by proponents of VPN. No matter what the system is, these VPNs use the following common components:

- Digital signatures and keys
- Data encryption and secure sockets (ie, Secure Sockets Layer or SSL)
- Firewalls to block unknown and unauthorized entities

In effect, VPN creates a secure "tunnel" through the internet which trusted and authorized entities can use to make transactions. Because VPNs use the existing internet infrastructure, implementing them is relatively inexpensive compared to building WANs.

VPN solutions can either be developed or purchased. Some brochures from "off-the-shelf" VPN solutions are attached with this report.The purpose of these VPNs will further be clarified in the next section, which discusses secure online transactions.

Overview: Transactions. In online transactions, it is vital to ensure the security and integrity of data. For instance, if Abe sends email to his bank requesting for his bank to pay Cris Php 1,000.00, this transaction will only be reliable provided that the following are ensured:

a. *Confidentiality:* Anyone can intercept the email and read its contents. Hence, the message must as much as possible be confidential.

b. *Provenance:* The bank must be able to check that Abe was indeed the person who sent the check. This is to guard against counterfeit messages.

c. *Non-repudiation:* Abe could later deny that he sent the request for payment. Hence, the bank needs to be sure that Abe could not repudiate the request.

d. *Integrity:* The information in the email could be altered or corrupted in transit (eg, the amount becomes **10**,000.00 instead of **1**,000.00). Hence the system needs to ensure that information in a transaction has not been altered or corrupted in any way.

Digital Solutions. The discussion below presents an overview of how the digital world ensures the integrity and security of a transaction.

a. *Confidentiality.* In order to keep a message secret, it can be "scrambled" or encrypted. Strong encryption will foil attempts to open the message. Although there is always news of hackers being able to break strong encryption, these efforts mostly involve a concerted effort using tremendous computing resources. [6]

b. *Provenance:* To ensure the identity of the parties involved, digital signatures can be used. In the example given, Abe can be given a digital signature. This digital signature is unique[7] and is composed of a combination of a public key and a private key.

   Abe gives the bank his public key and keeps the private key to himself. (Please see illustration below). When Abe issues his payment request, he signs it with his private key. No one else can sign the message using Abe's private key (hence guaranteeing provenance). To unlock the message, the bank must use Abe's public key. Two issues are important here:

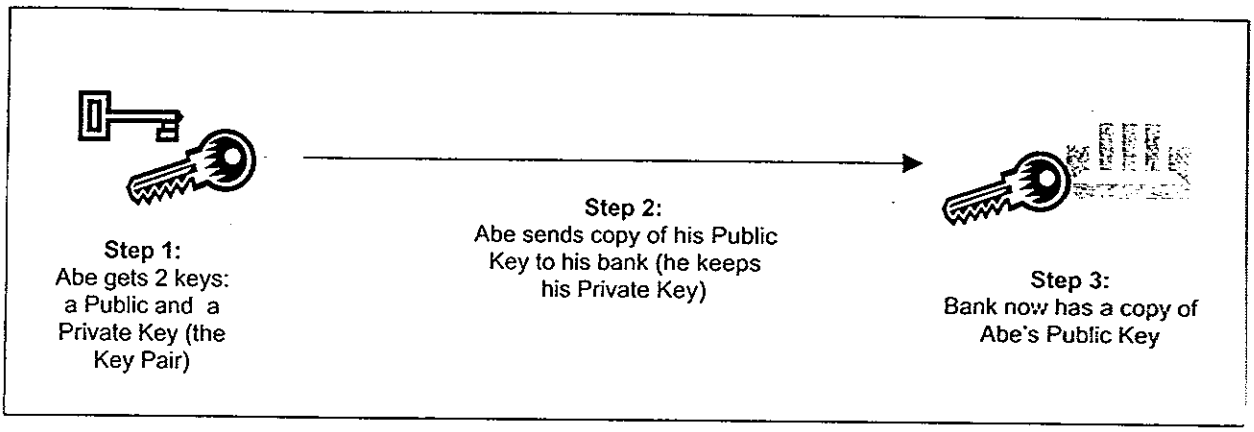
   i. Only Abe's **public** key can unlock a message that was encrypted by Abe's **private** key.

   ii. Hence, someone masquerading as Abe by using a fake private key will be foiled because the bank, using Abe's public key, can only unlock a message that was signed by Abe.

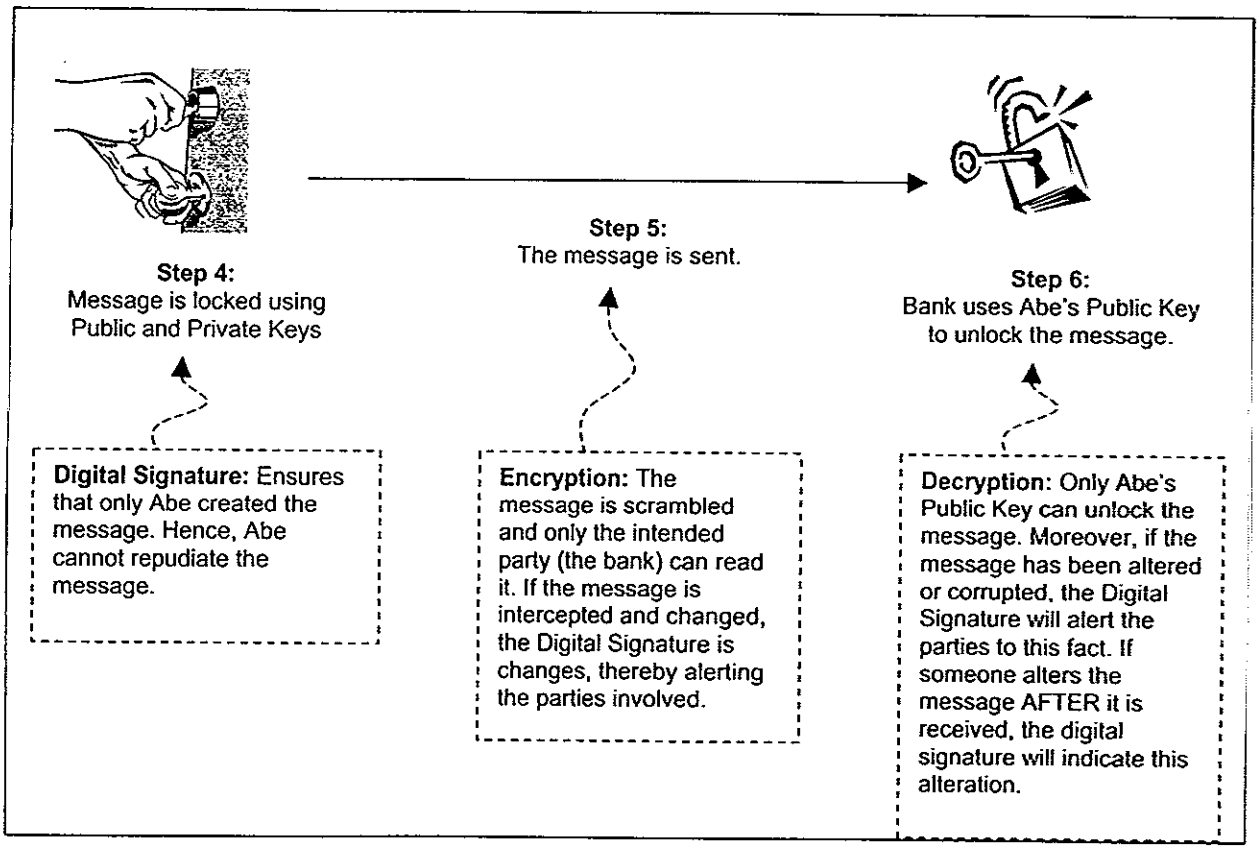
[6] Often a networked effort using various supercomputers and ordinary PCs all over the world via the internet.
[7] That is, no one else can use the same signature and masquerade as someone else.

SECURITY AND INTEGRITY IN AN ELECTRONIC TRANSACTION

A. Preparation: *Abe acquires public and private keys; he distributes the public key.*



B. Transaction: *Abe sends a payment request. Bank verifies the request.*



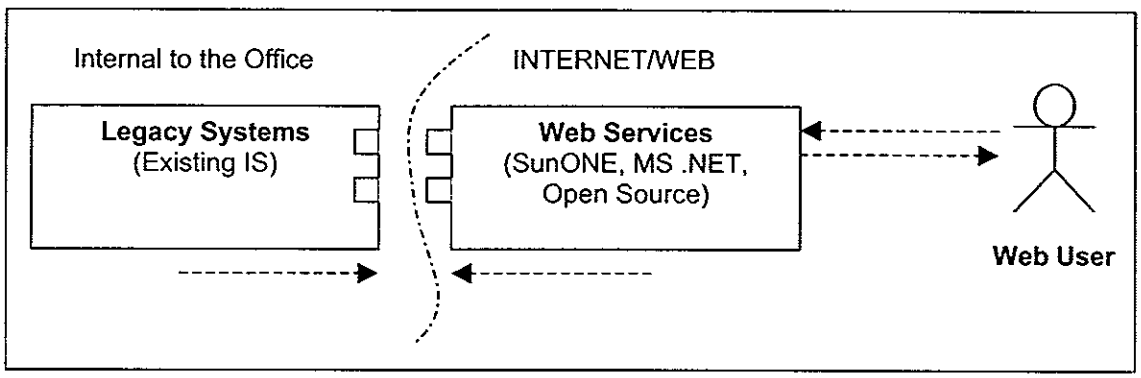
c. *Non-repudiation and integrity:* Non-repudiation relies on two main conditions:

i. Only Abe created and sent the message; and
ii. The message was not altered in transit and even after its receipt.

Hence, by using the digital signature, both conditions are satisfied. Only Abe has access to his private key and is responsible for its security. Hence, any message or transaction bearing his digital signature is cannot be denied or repudiated.[8]

3. A Survey of Available Technology

Brief Background. Web technology has matured and evolved since its simple, early use in the mid-90s into full platforms today, which are collectively known as **web services.** Web services are a comprehensive suite of solutions that allow organizations to run applications that could run over the network, which can then be connected to the internet using the Web as an interface. For organizations with existing or legacy computerized systems, web services can also provide components that could connect to these legacy systems without having to overhaul it.



The illustration above shows how Web services can provide a link that allow a user to use the Web to connect to an organization's internal information system (IS). Note that not all of the internal IS will be exposed to this link – security measures will be implented so that only public information is published on the Web.

Web Services: The Minimum Requirements. The minimum requirements for developing and running HealthWeb will be the following:

1. A web server with a backup server.

2. A database that will store dynamic content. This is apart from the existing databases like Membership, Contributions and Claims. The purpose of this database is to speed

[8] Of course, if Abe is not careful, someone can open his computer, find his digital signature, and use it to forge a transaction. But keeping his private key safe is Abe's responsibility, just as a home-owner is responsible for taking care of the house keys.

up HealthWeb by storing various replica of only the needed information to provide dynamic content.

3. A fast internet connection (eg. leased line) with backup.

4. A web services platform. The web services platform is the software backbone of HealthWeb. This connotes that programming will be done in the chosen platform. This is further explained below. Meanwhile here is a diagram that shows how these components work together.

Web Services: Choices of Platforms. The power of web technology to be accessible virtually anywhere, and its subsequent explosion, have brought about several competing platforms to deliver these web services. Deciding which platform to use is tricky, especially since the competing platforms are interoperable to some extent. As expected, each platform have their own sets of advantages and disadvantages in relation to the systems that are currently running at PHIC.

Below are given three main platforms which can be used for developing and running HealthWeb.,

1. *Microsoft .NET Web Services.* These services were designed to take advantage of systems that run on Microsoft products. They include various tools ranging from ASP, Open Database Connectivity (ODBC, a standard way of connecting to various databases), and supplementary development environments which include VisualBasic (VB) and Visual C++. The .NET platform can only run on Windows 2000 and XP. The main advantage of .NET is that development tools for this platform are plenty, and relatively easier to use than the other platforms (which can translate to faster development time). Another advantage would be that if configured properly, and if run on powerful machines, .NET is fast and can take advantage of the fact that most desktop computers today have Microsoft systems running in them. The main disadvantage is that Microsoft is often known for the instability of the systems it produces, and their susceptibility to virus and hacker attacks.

   Although .NET is a free platform, .NET itself must run on Windows 2000 or XP and supplemented by other Microsoft products like SQL Server and Visual Studio.NET – products that need to be licensed from Microsoft. It is well-known that licensing is a big issue with Microsoft, and hence this may be a decision factor for this platform.

2. *SunONE (also known as Java Web Services).* This platform was created by Sun Microsystems and is based on Java, Java Server Pages (JSP), and Java Database Connectivity (JDBC, a standard way of connecting Java applications with almost any database – Sun's answer to ODBC). SunONE can run both in UNIX and Microsoft Windows servers, using Apache Web server. The main advantages of SunONE are the stability and security of its applications. The main disadvantage is that SunONE slows down when it runs on Windows servers.

   SunONE is free but to optimize its speed, it must run on Sun machines which could command a high cost. Again this is another decision factor.

3. *Open Source Systems.* These systems mostly belong to the public domain and are often free. The best Web programming environment by far is called PHP[9] and it is often used in conjunction with a simple, free database called MySQL. Like SunOne, these will run on the Apache web server, which is a stable web server. Current surveys show that more than 60% of web servers on the internet are running Apache – the rest run Netscape and Microsoft web servers. All of these can either run on Microsoft Windows servers, or Linux servers. Again, Linux is open source and therefore free. The advantage of open source systems is that cost is much lower than the others. Open source systems have also been proven to be more secure and stable. The disadvantage of these systems is that IT workers skilled with open source systems are often few. Also, some training may be needed for IT staff that is more geared towards the more popular Microsoft solutions.

A note about XML

Although there are differences in execution among the competing platforms, all of them can speak XML, or eXtensible Markup Language. XML has become the standard format for generating and exchanging information. The main motivation behind XML is to allow one organization to connect to the content of another organization easily and conveniently.

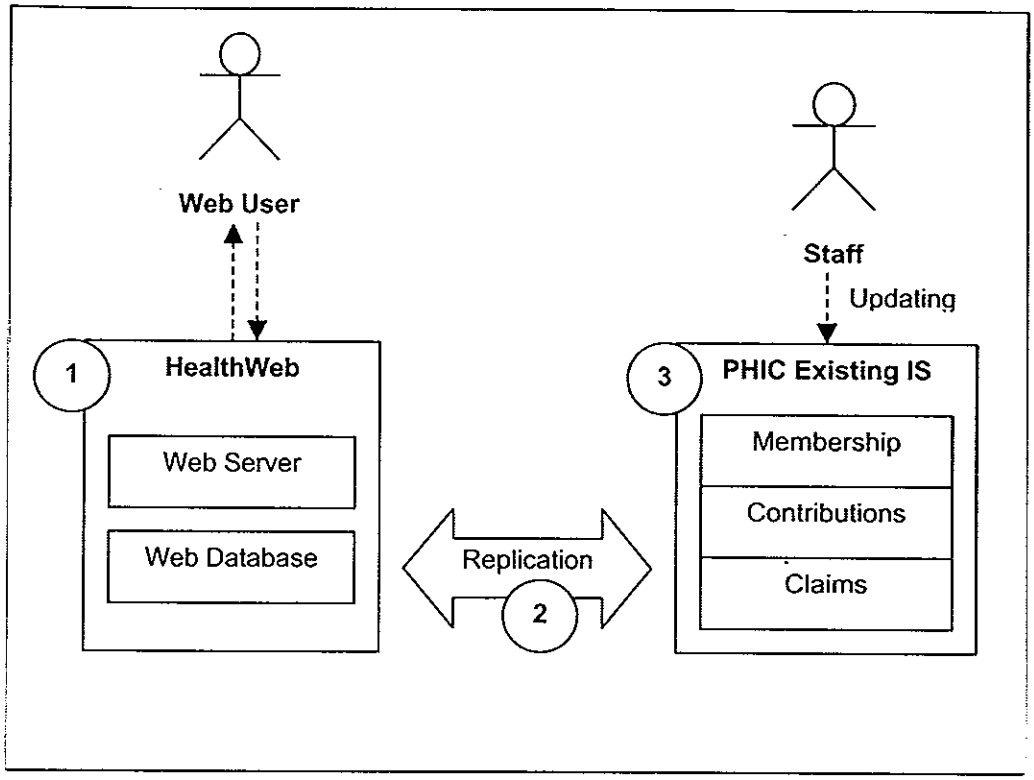
If PHIC is interested in eventually interconnecting with other online government agencies, it may be worthwhile to consider using XML to this purpose.[10]

[9] PHP was designed to be a programming environment for the Web. Hence it runs relatively faster than the other web service platforms.

[10] Information on emerging XML business standards can be read from http://www.ebxml.org/, a global standards body that aims to compile a repository of common business process and objects. Using standards will further enhance and facilitate interoperability.

VI. Conclusions and Recommendations

Suggested Web Setup



The simplified illustration above provides an overview of how the web services could be interoperated. The numbers in circles represent crucial areas that will affect the speed and stability of HealthWeb.

Area 1 (HealthWeb) is the core of the web service. It has the Web Server that accepts user requests and gives back the results of that requests. Ideally, it will extract the requested information from the Web Database that is also within Component 1.

The Web Database is an aggregate of data extracted from Area 3 (PHIC Existing IS). A regular replication can be scheduled during midnight to avoid adding to the network traffic. Any new updates may also cause an event trigger that could re-index the data in Area 3 and then "push" the new data to the Web Database in Area 1.

Area 2 points out that replication may greatly affect the speed of the database. In particular, this Area will play an important role in deciding which web hosting option to choose. These web hosting options are presented later in this section.

Factors to consider on choosing the web platform

The main factors that can help decide on the final platform are the following:

1. Total cost of development and eventually maintaining and upgrading the system, including purchasing the software, development tools and the subsequent licenses (eg annual fees that will be incurred for running such a platform).

2. Speed of the final web application. Speed here refers to three aspects:

    a. The speed of interoperability between the existing IS and the web services;
    b. The speed of the web applications themselves; and
    c. The total speed of delivering services to the web user.

3. Stability of the system. During peak hours, PHIC cannot afford for HealthWeb to break down. This implies that:

    a. HealthWeb itself is built on a stable platform;
    b. The HealthWeb applications themselves are stable; and
    c. Fault tolerance and disaster recovery must be included as major components of the system.

Web Hosting Options

The following discuss, in broad strokes, three web hosting options for HealthWeb:

Option 1. Inhouse hosting. Hosting the web server and database within PHIC CO
Advantages: Total degree of control.
Disadvantages: Cost of acquisition of equipment (servers, backup devices, leased line) and cost of maintenance and reallocating human resources to devote time on web maintenance. Another disadvantage would be the speed of the connection. If the leased line breaks down, a backup is needed.

Option 2. Collocated or dedicated hosting in a local ISP. Collocation is a term used for giving an ISP the server and letting their staff maintain it for the organization.
Advantages: Minimal overhead (ie, depending on the agreed maintenance fee), faster connection (since it is direct to ISP, ie, if ISP devotes a good bandwidth to the server). ISP will perform data backup.
Disadvantages: Very "iffy" – depends a lot on the quality of the ISP and its devotion to the PHIC server. Control may also be a problem: if modifications need to be made, they have to be done through ISP's staff.

Option 3. Offshore hosting. This may sound prohibitive at the start but some local organizations have done this option with good results. For example, the Asian Development Bank (ADB) rents a dedicated server in the United States. The advantage is that all major preventive maintenance is done by web host and will even include web statistics reporting (hence, lower maintenance cost in terms of cash out and personnel). This arrangement also makes the server enjoy fast and reliable internet connections (through the use of redundant

connections). The host will usually provide a telnet connection to control the server remotely. The disadvantage with this option is that since HealthWeb will be regularly replicating its data to and from the PHIC CO, the round trip time may be slow. On the other hand, this replication could be scheduled during the graveyard shift.

PhilHealth's vision of extending its services by using web technology can be realized properly by carefully studying the various options outlined here. Given the limitations of time to create this overview paper, a more specific recommendation in terms of which platform to choose cannot be made. The obvious next step is for PHIC to conduct a detailed assessment of and assign weights to the existing hardware, software, human resource skills, and total costs of owning the system (maintenance, license fees, upgrades, etc). The desired result is a relatively objective assessment from which further discussion can be conducted that would form the basis of a final decision.

Since this online service will represent a major leap in the business processes of PHIC, it is also highly recommended that a more comprehensive analysis of processes and workflow be conducted. As earlier stated, such a study has already been conducted, with corresponding recommendations on how to further streamline the business processes and workflow of the existing setup. Perhaps this previous study could be incorporated into the more detailed design of HealthWeb through the coordination of programmers/designers of PHIC's information systems, web developers, and business process analysts.

Another next step that could be done in parallel to the activities mentioned above is the coordination with other online government agencies in terms of establishing digital identity. A further study is recommended, detailing the possibility of this endeavor, with PhilHealth leading the way towards interoperability. This, of course, is subject to privacy issues as discussed under the Legal Framework paper.

All the activities recommended can then have as their final output a more comprehensive functional needs analysis, and functional requirements and specifications document, which would then be the blueprint of HealthWeb.

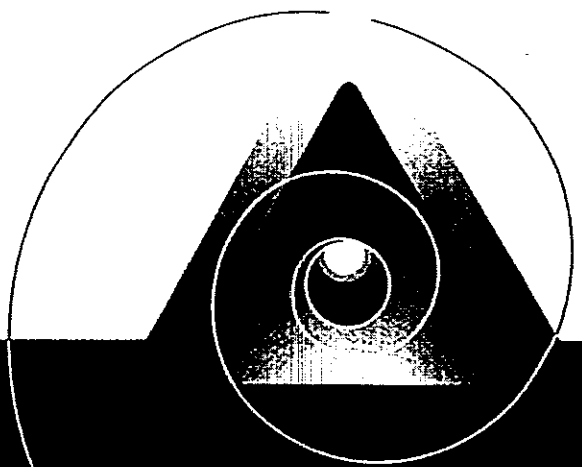
In sum, HealthWeb poses major challenges in IT innovation and government service. A well-prepared development and sound implementation methodology will allow PhilHealth to lead the way in online public service.

© Ruben Canlas Jr
Digital Solutions
benc@digitalsolutions.ph
26-F Carmel Avenue, Project 6, QC

THE TECHNOLOGY GUIDE SERIES®

www.techguide.com™

A Practical Guide to the Right VPN Solution



This Guide has been sponsored by

OpenReach

69

This **Technology Guide** is one in a series of topic-focused Guides that provides a comprehensive examination of important and emerging technologies.

This series of Guides offers objective information and practical guidance on technologies related to Communications & Networking, the Internet, Computer Telephony, Document Management, Data Warehousing, Enterprise Solutions, Software Applications, and Security.

Built upon the extensive experience and ongoing research of our writers and editorial team, these Technology Guides assist IT professionals in making informed decisions about all aspects of technology development and strategic deployment.

techguide.com is supported by a consortium of leading technology providers. OpenReach has lent its support to produce this Guide.

Visit our Web site at **www.techguide.com** to view and print this Guide, as well as all of our other Technology Guides.

This is a free service.

produced and published by

techguide.com

visit www.techguide.com™

you can't set up a Virtual Private Network, you can tell him you already did.

Here's a VPN that anyone can set up in minutes.

OpenReach's revolutionary "point and click" VPN services make it easy for you to securely connect remote offices, partners, and employees over the Internet — today — for as little as $99 per month.

With OpenReach, you can transform any PC into a powerful VPN appliance that works with any ISP, Internet access and network equipment.

No hassles. No network changes. No capital investment. Stop by our site and check it out today.

OpenReach

www.openreach.com
888-783-0383

Visit ATG's Web Site
to read, download, and print
all the Technology Guides
in this series.

www.techguide.com

"The significant problems we face cannot be solved by the same level of thinking that created them."

Albert Einstein

Table of Contents

Summary 4
Introduction 5
VPN Overview and Benefits 8
VPN Implementation Alternatives 25
Key Features and Cost Elements for a VPN Solution 30
Selecting the Right VPN Solution 35
Conclusion 37
Case Study 38
Glossary of Terms 42

About the Editor...

Jerry Ryan is a principal at ATG and the Editor-in-Chief of techguide.com. He is the author of numerous technology papers on various aspects of networking. Mr. Ryan has developed and taught many courses in network analysis and design for carriers, government agencies and private industry. He has provided consulting support in the area of WAN and LAN network design, negotiation with carriers for contract pricing and services, technology acquisition, customized software development for network administration, billing and auditing of telecommunication expenses, project management, and RFP generation. Mr. Ryan has been a member of the Networld+Interop Program Committee and the ComNet steering Committee. He holds a B.S. degree in electrical engineering

The Guide format and main text of this Guide are the property of The Applied Technologies Group, Inc. and is made available upon these terms and conditions. The Applied Technologies Group reserves all rights herein. Reproduction in whole or in part of the main text is only permitted with the written consent of The Applied Technologies Group. The main text shall be treated at all times as a proprietary document for internal use only. The main text may not be duplicated in any way, except in the form of brief excerpts or quotations for the purpose of review. In addition, the information contained herein may not be duplicated in other books, databases or any other medium. Making copies of this Guide, or any portion for any purpose other than your own, is a violation of United States Copyright Laws. The information contained in this Guide is believed to be reliable but cannot be guaranteed to be complete or correct. Any case studies or glossaries contained in this Guide or any Guide are excluded from this copyright.

Copyright © 2001 by The Applied Technologies Group, Inc., 209 West Central Street, Suite 301, Natick, MA 01760, Tel: (508) 651-1155, Fax: (508) 651-1171
E-mail: info@techguide.com Web Site: http://www.techguide.com

Summary

This Technology Guide is written for Business and for IT Managers at small to medium-sized businesses who plan and implement the network infrastructure for their businesses. The Guide is primarily for IT and networking managers who are selecting VPN solutions. It is written to help the reader navigate the VPN swamp. This Guide assumes the reader is familiar with the Internet and with the distinction between intranets and extranets. It should help readers understand VPN applications, benefits, and implementation alternatives.

After reading this Guide, the reader should be able to evaluate features of a VPN solution relative to his/her requirements. Based on least cost of ownership, the reader will be able to select a VPN solution from a set of alternatives that is most suitable for their near- and long-term needs.

Introduction

E-business, e-commerce, e-marketplace, business-to-business (B2B), and business-to-consumer (B2C), are now common business parlance. Every organization is defining and implementing its e-strategy. The question is no longer whether to migrate to an e-environment, but what is the best way to migrate to a Web and Internet-based business model.

The Internet allows businesses to reach their customers, and vice versa, anytime and anywhere in the world. A US company need not deploy any resources or infrastructure in China, for example, to engage in business in China. A mom-and-pop e-business in a non-English speaking country has as good a probability of reaching a customer in the US as an American multi-billion dollar company. A common challenge to both companies is the use of the Internet to leverage their business.

One of the key technologies for using the Internet in a secure and private manner is the virtual private network (VPN). This Technology Guide explains VPN applications, benefits, and implementation alternatives. More importantly, it provides guidelines for selecting the right VPN solution.

The Guide focuses on needs of small and medium-sized businesses that do not have the technical and management resources to deploy, to maintain, or to operate their own VPNs. Many large enterprises will find the VPN deployment model discussed here to be the most cost-effective answer to their e-business and remote office requirements.

The Business Problem

Before the popularity of the Internet, large enterprises were building multi-million dollar private data networks (now called intranets), using telecommunications services such as leased lines, Frame Relay, and Asynchronous Transfer Mode (ATM) to communicate among geographically dispersed sites. These services were often supplemented with services, such as switched analog or ISDN, to connect smaller sites and mobile users. Small and medium-sized enterprises, who could not afford the cost of long-distance leased facilities, were limited to low-speed switched services.

These intranets were expensive and required hordes of support personnel. Intranets also had long planning, design, and implementation cycles, resulting in tremendous lost-opportunity costs. As the Internet became ubiquitous and as ISPs offered high-speed Internet access, enterprises reduced the cost and the time to deploy their intranets by off-loading them to the Internet.

As enterprises dabbled in e-commerce, whether as B2B or as B2C, it became clear that the Internet was the practical and cost-effective way to connect with customers and partners. The concept of connecting with external users or organizations came to be known as extranets.

As cost-effective as the Internet is, it introduces one major challenge—security. Though the Internet has emerged as the network foundation for e-endeavors, it is paradoxically a public, shared network of networks and is not suitable, in its natural state, for secure transactions or private communications.

Enterprises have recognized that e-business is more than just Internet connectivity or the exchange of e-mails and files. E-business needs real time exchange of data. This involves all of the enterprise procurement, supply-chain management, sales and customer relationship management, online business transactions, online dealings with financial institutions, etc. These requirements make security over the Internet paramount.

Virtual Private Network—The New Solution for E-Business

VPNs have emerged as the key technology for achieving security over the Internet. While a VPN is an inherently simple concept, early VPN solutions were geared towards large organizations and their implementation required extensive technical expertise. As a consequence, small and medium-sized businesses were left out of the e-revolution. Recently, VPN solutions have become available that focus specifically on the needs of small and medium-sized businesses.

Historically, the term VPN has also been used in contexts other than the Internet, such as in the public telephone network and in the Frame Relay network. In the early days of the Internet-based VPNs, they were sometimes described as Internet-VPNs or IP-VPNs. However, that usage is archaic and VPNs are now synonymous with Internet-VPNs.

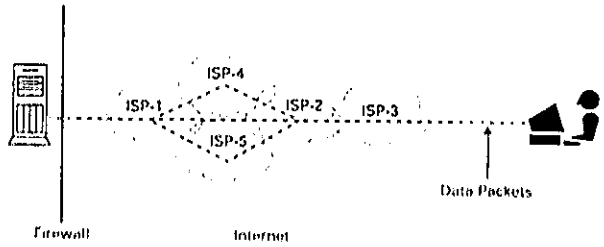


Figure 1a: Data flow through the Internet

VPN Overview and Benefits

Protection Beyond the Firewall

A firewall is an important security feature for Internet users. A firewall prevents data from leaving and entering an enterprise by unauthorized users. However, when packets pass through the firewall to the Internet, sensitive data such as user names, passwords, account numbers, financial and personal medical information, server addresses, etc. is visible to hackers and to potential e-criminals. Firewalls do not protect from threats within the Internet. This is where a VPN comes into play.

A VPN, at its core, is a fairly simple concept—the ability to use the shared, public Internet in a secure manner as if it were a private network. Figure 1a shows the flow of data between two users over the Internet when not using a VPN. As shown by the dotted lines, packets between a pair of users may go over networks run by many ISPs and may take different paths. The structure of the Internet and the different paths taken by packets are transparent to the two users. With a VPN, users encrypt their data and their identities to prevent unauthorized people or computers from looking at the data or from tampering with the data.

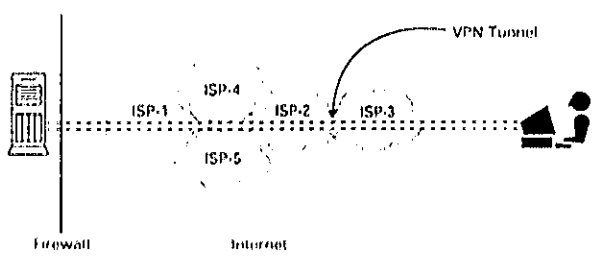


Figure 1b: VPN over the Internet

Figure 1b, shows the encrypted flow of packets—referred to as a tunnel in a VPN. The VPN tunnel is shown graphically as a line connecting the starting point and endpoint of the encryption. While the tunnel is shown in Figure 1b and in other literature as if the tunnel is a fixed path, packets associated with the tunnel may take different paths, like the ones in Figure 1a. In this example, the endpoints of the VPN tunnel are a client at the user station and a server or gateway at a central site. We need software or some other device at each end of the tunnel to initiate, authenticate, and terminate a VPN tunnel. In addition to encryption, VPN also allows for user- and data-authentication.

VPN Applications

A VPN can be used for just about any intranet and e-business (extranet) application. Examples on the following pages illustrate the use and benefits of VPN for mobile users and for remote access to enterprise resources, for communications between remote offices and headquarters, and for extranet/e-business.

Remote Access

In this application, when not using a VPN, mobile and remote users often use analog (dial-up modems) or ISDN switched services to connect to a headquarters data center. This is shown in figure 2a. These connections are used to access e-mail, to download files and to execute other transactions. This type of connection would also be used by small offices that do not have a permanent connection to the enterprise intranet.

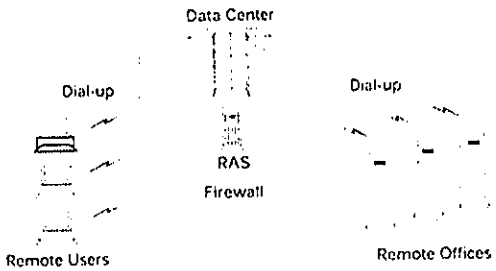


Figure 2a: Remote access using switched services

The cost elements for such an application include:

- Dial-up connection charges, especially for users making long-distance connections.
- A remote access server (RAS) at the central site to handle incoming calls.
- Technical personnel to support remote users and to configure, maintain, and support a RAS.

With a VPN, as shown in figure 2b, remote users and branch offices set up dial-up connections to local ISPs and connect via the Internet to a VPN server at headquarters.

VPN benefits include:

- Elimination of the RAS, of associated modems, and of technical support costs to install, configure, and maintain the RAS.
- Replacement of long-distance or 800-number services with local ISP connections at remote sites.
- Access to all enterprise data and applications (not just e-mail or file transfers) over the Internet.

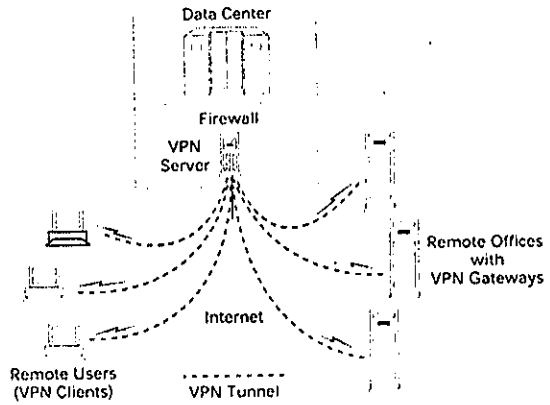


Figure 2b: Remote access using VPN

New costs for VPN include:

- Installation, support, and maintenance of a VPN server at the central site and of VPN clients for remote users.

Studies show that the cost savings in long-distance charges alone pay for the VPN setup costs within a few months, and substantial recurring savings follow.

Branch-to-Branch or Branch-to-Headquarters

In Figure 3a, a business has an intranet connecting remote locations with headquarters. Each campus has a router connecting the campus to a backbone router over a LAN or WAN link (smaller networks may not need backbone routers). A single router may be connected to both the campus LAN and to the other campuses with a WAN link. WAN routers are typically mesh-connected using leased lines or a Frame Relay service.

Primary cost elements for a branch-to-branch intranet include:

- Routers, both campus and backbone.
- Telecommunications services, in particular long distance. The cost of the intranet backbone,

depending on the traffic volume and geographical reach, can run from tens of thousands of dollars a month to hundreds of thousands of dollars a month. These costs are especially onerous for multi-national organizations.

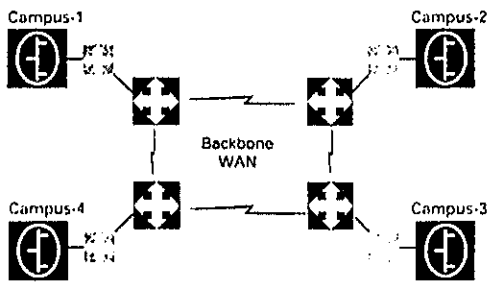


Figure 3a: Enterprise intranet without VPN

With a VPN, the intranet backbone WAN is replaced by the Internet. This is shown in Figure 3b. The new costs for this configuration include the deployment and maintenance of VPN gateways at remote campuses and the deployment and maintenance of a VPN server at the headquarters site. In addition, each location pays for an Internet connection.

VPN benefits include:

- Elimination of backbone routers.
- Elimination of system administration, configuration, and technical support for routers and elimination of the need to design and maintain routing tables.
- Elimination of long-distance services; as with the remote access case, this results in substantial savings. The amount of savings depends on the size of the intranet.
- Reduction in lost-opportunity cost due to the elimination of long provisioning cycles for long-distance service and for international telecommunications services.
- Most likely, better performance than an intranet due to higher speed facilities inside the Internet.

The migration to VPN could pay for itself in a few months. There would also be substantial recurring savings.

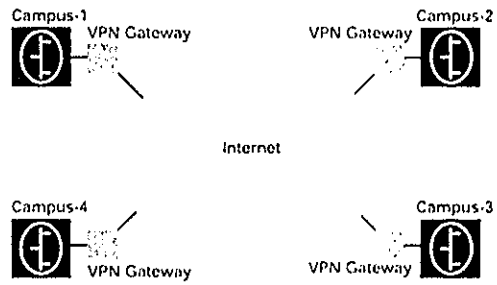


Figure 3b: Branch-to-branch and branch-to-headquarters over VPN

B2B, B2C, and Extranet

Before the availability of the Internet and VPNs, electronic transactions and communications between enterprises were particularly difficult since there was no standard or common way to enable these communications.

As shown in Figure 4a, there were numerous networks and architectures to enable inter-corporate commerce. For example, the banking industry has a long history of electronic transactions among banks and with central banks. The brokerage industry, similarly, has special systems for communicating with stock exchanges, with settlement bodies, and with depository companies. In addition, there were several custom-made networks with proprietary transaction formats for electronic data interchange (EDI). In some cases,

corporations or government agencies set up their own standards to execute transactions with their business partners and suppliers. Many organizations had to connect with multiple EDI networks because of the diverse nature of their business.

These historic approaches had numerous drawbacks:

- Very expensive to develop since everything is tailor-made for one industry.
- Long design and deployment time.
- Inability to adapt to new requirements.
- Lack of qualified personnel for narrowly used proprietary systems.
- Could not be easily extended to new locations and customers.
- High entry cost for new customers/members and lost opportunity cost for not being able to participate in e-commerce with non-members.

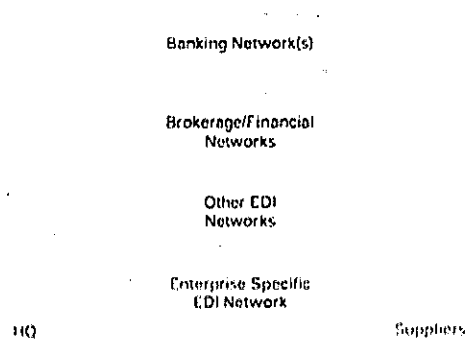


Figure 4a: E-Commerce before the Internet and VPN

The Internet, of course, has changed all that. Now, any organization or individual can engage in business transactions or other communications in a secure and private manner by using a VPN over the Internet. Figure 4b shows an example of the new environment.

VPN benefits include:

- Open interfaces; anyone can use it without a major initial investment.
- Fractional cost compared to proprietary networks.
- Worldwide ubiquity built in; reach any customer anywhere without adding infrastructure at those sites.
- Low entry cost, narrowing the opportunity gap between large and small enterprises.
- Rapid deployment, flexibility, ease of modification.
- Choice of vendors in selecting a solution.
- Extensive availability of technical personnel and expertise.

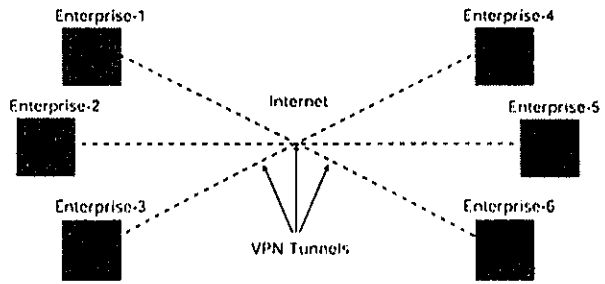


Figure 4b: E-Business and extranets with VPN

The three examples discussed in this section explain the benefits and versatility of VPNs for e-business. VPN has become a prerequisite for secure commerce or for secure communications over the Internet. In the following section, the Guide explains technologies underlying VPN and the applicable security standards for VPNs.

VPN—Technical Concepts and Enabling Technologies

A VPN is essentially a software technique to securely route private, un-routable traffic on the public Internet. Three functions form the basis of a VPN:

1. Packet encapsulation ("tunneling")
2. Encryption
3. Authentication

(This section provides an overview of encapsulation, encryption, and authentication techniques used in a VPN. Knowing some basic VPN concepts will help the reader later understand trade-offs in selecting the right solution.)

People sometimes consider network Quality of Service (QoS) as another VPN requirement. This function refers to network performance, response time, availability, packet loss, etc. However, the implementation of the network QoS is a responsibility of the ISPs, and the user will have to monitor and manage QoS for any VPN that spans multiple service providers. Attaining end-to-end QoS is a complex task for the ISPs and, besides technology, also requires agreements among ISPs on QoS parameters. While there are some VPN products that claim QoS implementation through the customer-premise equipment, these devices have no impact on the network QoS. They essentially manage traffic priorities through queuing mechanisms that control the release of packets to the network. While this may be an important consideration for some customers (with under-capacity routers and low-speed links), this QoS has nothing to do with end-to-end network level QoS. Instead, if QoS is an important criterion for VPN selection, it's often best to actually separate the QoS requirement from the VPN requirements, thus obtaining the maximum flexibility while still guaranteeing the service levels needed. For example, if QoS is important, select a single ISP that can provide an adequate SLA for network performance, and then select the most cost-effective, manageable, and flexible VPN solution separately.

The Scope of Encapsulation and Encryption

Figure 5 shows general layout of an IP packet. Each part of the IP packet has security exposures if sent in the "clear" over the Internet.

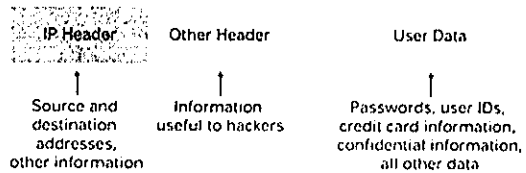


Figure 5: IP packet and security threats

1. IP Header: Among other information, it includes addresses of the source and destination of the packet. By capturing these addresses, a hacker can learn the addresses of target servers and try to set up unauthorized communications with them. A hacker can also learn the addresses of authorized users and use these addresses to act as an authorized user.

   We can encrypt the addresses but that creates a problem on the Internet because routers look at these addresses to route packets to their correct destinations. We will see how encapsulation solves this problem.

   Tunnel Mode: When the IP header above is encrypted and is encapsulated in another IP header, the mode of transmission is referred to as the tunnel mode in the IP Security (IPSec) standard.

2. Other Headers and User Data: Other headers contain information used by hackers to attack an enterprise's Web sites and, therefore, must be encrypted before traveling over the Internet.

   The User Data part of the packet, of course, contains not only all of an organization's business data but also its user IDs and passwords.

   Thus, we need to encrypt the entire packet when transmitting packets over the Internet.

Encryption Concepts

Virtual private networks ensure the privacy of information by using encryption. Encryption is a technique for scrambling and unscrambling information. The scrambled information is called cipher-text and the unscrambled information is called clear-text.

In a VPN, when information is sent from one location to another, the VPN Gateway at the sending location pulls information off the LAN and encrypts the information into cipher-text before sending the encrypted information on the Internet. The VPN Gateway at the receiving location decrypts the information into clear-text and puts the decrypted information on the LAN.

It used to be that encryption was made secure by keeping the encryption algorithm a secret. The problem with this approach is that once someone cracks the algorithm, that person has access to all the information that has ever been encrypted with that algorithm. Furthermore, since the encryption algorithm is a secret, it's hard to tell how good the algorithm is because only a few people test it.

Today, encryption algorithms are published so that everyone knows how they work. Popular published encryption algorithms include the Data Encryption Standard (DES) and Blowfish. If the algorithm isn't secret, how are secrets kept? The answer is keys.

Keys

A key is a secret code that is used by the encryption algorithm to create a unique version of the cipher-text. One way to think about it is that the encryption method is like a combination lock that is purchased at the hardware store and the key is the combination that comes with that lock. Even though many buyers each purchase the same lock, it doesn't mean that they have access to each other's tool shed.

So security is no longer dependent upon keeping the encryption algorithm a secret; it now depends on keeping the key a secret.

Key Lengths

When working with well-known encryption algorithms the security strength depends on the length of the keys used. An 8-bit key provides 256 combinations (two to the eighth power). A 16-bit key provides 65,536 combinations (two to the sixteenth power). And so on.

With a 16-bit key, someone could make 65,536 attempts before finding the combination that would unlock his/her cipher-text. With people, this would be impractical, but with computers, it wouldn't take long to run through the possible combinations. Many VPN products use 168-bit keys to encrypt data. A 168-bit key creates 374,144,419,156,711,000,000,000,000,000,000,000,000,000,000,000,000 possible combinations. Even fast computers would take years to try all these.

Still, it's not enough to use long keys. As with the encryption algorithm, once someone has the key, he/she has access to all the information that has ever been encrypted with it. Fortunately, with keys, one can routinely change the key so that even if someone has the key, it would only be useful for cipher-text encrypted with that key. The length of time a key is used is called a crypto-period.

Symmetrical or Private Keys

When the same key is used both to encrypt and to decrypt information, the key is called a symmetrical key. Symmetrical keys require users of a VPN to possess (share) the same key at each end of the connection. Because the key is shared, symmetrical keys are frequently referred to as shared secrets. As the name suggests, these keys work as long as it is only the authorized parties who know the key. These parties take the appropriate steps to keep the key secret. One of the problems with secret keys is distributing them to authorized users. Obviously, these keys cannot be sent over the Internet because of the public nature of the Internet.

Asymmetrical or Public Keys

Another class of keys allows information to be encrypted with one key and decrypted with a different key. Information encrypted with the first key cannot be decrypted with the same key and vice versa. These keypairs are called asymmetrical keys.

With asymmetrical keys, one key is called the public key and the other is called the private key. The public key is made available to anyone—it is not secret. The private key is secret and it is only known by its owner. If someone wants to send information that only an intended person can see, the information is encrypted using the target's public key. That private key has the property that only it can decrypt the cipher-text created using the public key!

On the flip side, if a user wants to be certain that a message was from a known person, the message would have been encrypted using a private key. The message is then decrypted using the public key. If the message decrypts correctly, it must have come from the originator.

Asymmetrical keys get us around having to distribute and manage secret keys.

Authentication Concepts

Authentication answers the question "Are you really who you say you are?"

There are two types of authentication: User/System authentication and data authentication.

User/System Authentication: This is the way of verifying that the person or system is indeed who the person or system claims to be. A common technique for authentication is for each side to "challenge" the other side by sending a random number. The challenged side returns a value to the challenger by encrypting the random number using a key that should only be known to the challenged side. The challenger decrypts the returned value and if the decrypted value matches the original random number, the challenged party is treated as authentic.

Data Authentication: This verifies that a packet has not been altered during its trip over the Internet. A typical technique is for the sender to calculate a number, called a hash, based on the data content and to append the hash to the data packet. This is done prior to encryption. The receiver decrypts the packet. The receiver then calculates the hash independently and compares this receiver-calculated hash with the hash appended to the data. If the two hashes do not match exactly, the data was altered and the receiver rejects it. The hash is calculated using a mathematical function called a hash function. Hash functions have the property that they spit out a unique number ("hash") for each unique bit string that is fed into them.

Encryption Algorithms

The Data Encryption Standard (DES) is a commonly used and thoroughly tested encryption algorithm. The DES system uses 56-bit symmetric keys to encrypt data in 64-bit blocks. The 56-bit key provides 72,057,594,037,927,900 possible combinations. A per-

sonal computer would take about 20 years to run through this many combinations. However, an organization with millions of dollars worth of computers could run through this many combinations in about 12 seconds. So DES makes information safe from casual attacks by hackers, but not from a focused attack by a well-funded organization.

Figure 6: DES with 56-bit key

Triple-Pass DES is a DES system that encrypts information multiple times. With triple-pass DES, the data is encrypted once using a 56-bit key. The resulting cipher-text is then decrypted using a second 56-bit key. This results in clear-text that doesn't look anything like what was originally encrypted. Finally, the data is re-encrypted using the first key. This technique of encrypting, decrypting and encrypting is referred to as EDE. It effectively increases the key length from 56-bits to 112-bits.

3DES is an encryption algorithm that provides better security than triple-pass DES. With 3DES, the data is encrypted, decrypted and encrypted again (EDE), but with three different keys. This results in an effective key-length of 168-bits.

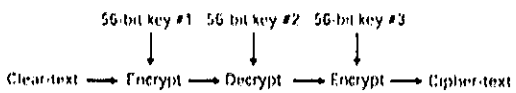


Figure 7: 3DES with 56-bit key yielding effective key length of 168-bits

VPN Protocols

This Guide has referenced the IPSec protocol as the Internet standard protocol for tunneling, encryption and authentication. IPSec is widely supported as the protocol for VPN implementations. There are two other protocols, available as alternatives to IPSec. These two protocols were developed as tactical solutions while the IPSec protocol was being developed. IPSec is widely available now but the other protocols are still used. Each of the three protocols is discussed below:

1. IP Security (IPSec)

IPSec is the security standard for the Internet. It allows for encryption and authentication. The general layout of IPSec-encoded packets is shown in Figure 8.

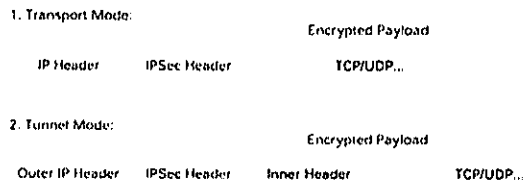


Figure 8: Encryption modes for IPSec

As shown in Figure 8, IPSec defines two modes of encryption: transport mode and tunnel mode. In transport mode, the original source and destination addresses of the header are used and are not encrypted. This makes transport mode appropriate for use over a LAN. Tunnel mode is more appropriate for use over the Internet. In particular, tunnel mode permits the routing of normally un-routable private addresses over the public Internet. In both cases, the IPSec header contains authentication information and other information needed to decrypt the packet.

2. Layer 2 Tunneling Protocol (L2TP)

L2TP was developed to merge two earlier protocols, the Layer 2 Forwarding (L2F) protocol and the Point-to-Point Tunneling Protocol (PPTP). L2TP is a protocol for putting a wrapping on non-Internet protocols such as IPX, SNA and AppleTalk, in an IP envelope, for encryption purposes. By itself, L2TP does not provide an encryption function and L2TP depends on IPSec (or some other scheme) for encryption.

3. Point to Point Tunneling Protocol (PPTP)

PPTP is a Microsoft proprietary encryption and authentication protocol. PPTP was supposed to have been replaced by L2TP, but Microsoft retains PPTP as its way of supporting VPNs in Microsoft Windows products. PPTP uses RSA instead of DES or 3DES for encryption. RSA is a weaker security algorithm than IPSec's 3DES.

Of the three protocols, IPSec, besides being the Internet standard for tunneling, encryption and authentication, has the most industry momentum and is implemented by the greatest number of vendors. There are numerous IPSec implementations available for all Windows environments. This Guide recommends IPSec as the preferred protocol for implementing VPNs.

What it all Means

While selecting and implementing a VPN solution, a user may get involved in selecting keys and encryption algorithms. At a minimum, they know the key types and encryption algorithms supported by a product. Some products require great involvement and great expertise in security details. Large businesses have complex security requirements and they benefit from the ability to customize and set every detail. Most small and medium-sized businesses do not have the need, the money, the skills, or the time to tweak every possible

VPN security setting. These businesses often prefer a solution that shields them from the internal operation of encryption algorithms and key structures.

With expanding business relationships, even smaller companies want to have e-business links with the broadest set of partners. And they want an easy way to do this. The solution these businesses pick should not require them to have certain types of network equipment (like firewalls and routers) and should not specify the type of Internet connections they use or require them to use a particular ISP.

VPN Implementation Alternatives

There are many VPN solutions available. They cover a range of price-performance, of capacity, and of installation and configuration complexity. Since VPNs are relatively new, the way of comparing products and solutions is not mature either. To provide a framework for evaluating VPNs, this Guide divides VPNs into the following categories:

1. Traditional or legacy VPN products
2. Outsourced VPNs
3. Low-end VPN/firewall products
4. Point-and-Click VPN services

Traditional or Legacy VPN Products

Most first generation VPN products fall in this category—The VPN function is typically an add-on to a router, to a LAN switch, or to a firewall. These include products from vendors such as Lucent, Cisco, Nortel, and Checkpoint. These products are optimized for

large businesses. When such a customer adds VPN functionality it often means an upgrade to a new router/switch/firewall model that supports VPN as an add-on feature. Once the customer buys the right model, the customer then physically installs and logically configures the router/switch/firewall. The customer then configures VPN configurations at central and at remote sites and for mobile and remote users.

The legacy VPN products category includes PC-based (Windows and Linux) software solutions targeted at smaller users. For these, a user installs the operating system and the networking support and then installs and configures the VPN support. Configuring the VPN support means defining security policies and key structures for VPN gateways and clients for mobile and remote users.

These VPN solutions need significant expertise to design, install, operate, support, and maintain.

Outsourced VPNs

There are three subcategories:

1. VPN service from an ISP or NSP
2. Managed VPN service from a reseller/solution provider
3. Consultant/Systems Integrators' VPN implementation services

VPN Services from an ISP or NSP

More and more ISPs and network services providers (NSPs) are providing VPNs as a service. With a managed service offering, the service components include installation of servers, installation of clients and ongoing technical support. The customer is involved with defining security policies and with the overall VPN design.

An important issue here is the availability of the managed VPN service in all the geographic areas where a customer wants to deploy their VPN. For example, regional Bell companies typically limit coverage to their operational and high-speed access providers. This may impose technological limitations. A DSL-based provider would exclude cable-users and vice versa. For example, AT&T's broadband access-services are based on cable-TV and most regional telephone companies and other providers are based on DSL. These restrictions could force one to use multiple service providers, each with its own systems administration, configuration, ordering, provisioning, and technical support. The customer would be responsible for identifying and resolving interoperability. For example, if one goes with a DSL-based ISP, how do employees with cable modems access the VPN? And with multiple ISPs one has to manage interoperability among the service providers.

Given the internal cost structure of these service providers, their services tend to be on the high end of the VPN price range and their services tend to focus on large customers. ISPs and NSPs are not known for rapidly adopting new technologies or for rapidly responding to changing customer needs.

Managed VPN Service from a Reseller/Solution Provider

These solution providers package services from multiple service providers to provide a solution covering all geographical areas. While these providers offer more flexibility than a single ISP/NSP solution, the fact remains that no single solution provider covers all possible geographic locations, covers the broad range of access technologies and maintains reasonable cost. Cost, availability in all desired locations, and technical support are the criteria for evaluating these total service solution providers.

Consultant/Systems Integrators' VPN Implementation Services

An enterprise may build their own VPN buying professional services from systems integrators and consultants. There are three phases in VPN deployment:

1. Needs-analysis, product evaluation and selection
2. Initial VPN design, configuration and rollout
3. Ongoing technical support

A business may outsource one or more of these phases. The cost of doing this and the number of new employees needed depends on the number of tasks outsourced. Small and medium-sized enterprises should contract all three phases. This could lead to high recurring charges for VPN deployment. There is also the challenge of finding the right consultant/systems integrator for the technology to be implemented.

Low-end VPN/Firewall Appliances

Low-end VPN firewall appliances are designed for small and medium-sized businesses and are purpose-built (dedicated to VPN gateway function). These appliances may use PC processors or specialized processors. Operating systems may be Microsoft Windows, Unix/Linux or a proprietary operating system. These appliances may incorporate co-processors for off-loading the encryption function to a separate chip.

These devices are called appliances due to their standalone nature. However, these appliances still have to be configured and maintained with the same level of resources as traditional VPN devices. These appliances may include additional functions such as a firewall, increasing their complexity. Appliance VPN boxes are simpler than router or firewall-based VPNs and, therefore, may be less prone to problems, easier to diagnose and require less technical support. The recurring-costs model for appliances is similar to the cost model for traditional VPN products. Many appliance designs are based on proprietary chips and could run into future scalability problems due to the high cost and long development cycles for new chips.

Point-and-Click VPN Services

This is a relatively new category among VPN solutions. This solution is independent of the ISP and allows customers to use existing equipment or generic PCs as the hardware. One example of a service provider who delivers such solutions is OpenReach.

The key characteristic of this solution is that the customer does not have to get involved in designing, configuring, and supporting the VPN.

To deploy a VPN with this approach, for example, the customer simply logs onto the service provider's Web site and registers basic information about each site that is to be part of the VPN (such as site name and IP address). The Network Operations Center then automatically creates appropriate VPN configurations based on the user-provided information and downloads this information to a floppy disk that can be installed on a PC at each location. The user simply plugs the diskette at each site in a standard PC, reboots, and now has a VPN gateway that automatically registers itself with the Network Operations Center. The VPN administrator or user can then simply use a Web browser to "point and click" the connections among the registered VPN gateways, thereby creating secure, transparent IPSec tunnels among each remote location. In addition, the solution provider uses a Web-based control center that monitors the health of VPN gateways and provides technical support for the customer. The customer data does not flow through the vendor's network control center, but directly between the remote locations as needed. The customer billing is based on

the bandwidth required for the VPN connection (i.e., cable modem, DSL, T1, etc.) Since this type of solution uses standard PCs and free software, there is essentially no up-front investment required, and thus the potential risk is significantly less than many other types of VPN solutions. In addition, unlike most outsourced VPNs, "point and click" VPNs are not tied to a single service provider, allowing customers to mix and match Internet access types and ISPs (cable modems and DSL, for example).

Key Features and Cost Elements for a VPN Solution

There are two sets of criteria for evaluating VPN solutions: basic VPN functions and total cost of ownership (TCO). The basic VPN functions are for comparing products based on current technical requirements. However, the TCO criteria show long-term cost differences of one solution over the other.

Functional Evaluation

Table 1 lists criteria for functions of a VPN solution.

Security

IPSec Support: Is IPSec the primary security protocol supported? If IPSec is not supported, there may be future difficulties interoperating with locations and businesses using Internet standard protocols. Attention should be given to future locations and e-business partners.

Ease of Key Management: Are the types of keys, authentication techniques used and their management compatible with the customer's security objectives? If a user has to deal with design and management of key distribution, the solution may require technical personnel to support it. 3DES should be considered the minimum acceptable encryption level.

Performance

Packet Throughput Capacity: This is the capacity and performance data for the device. Another number often included in product specifications is the number of tunnels handled by the device. The theoretical number of tunnels handled by a device is typically very large but is not very useful in assessing the performance of the device. Packet throughput capacity, rather than the number of tunnels, is the true measure of a device's performance.

Availability and Reliability: The device or service should be reliable enough to provide 99.9% or higher availability.

Hardware vs. Software Encryption: Encryption can be performed either through software or through hardware. While this is often considered important, it does not provide a direct measure of a product's performance. Look instead at the product's packet throughput capacity.

	Solution 1	Solution 2	Solution 3
Security			
IPSec Support			
Ease of Key Management			
Performance			
Packet Throughput Capacity			
Availability/Reliability			
Interoperability			
Access/Connectivity			
Service Coverage			

continued next page

	Solution 1	Solution 2	Solution 3
Platform Type			
Hardware/Appliance			
Add-on Feature to Firewall or Router/Switch			
Operation and Management			
Web-based Management System			
Management Reports			

Table 1: Functional criteria for selecting a VPN solution

Interoperability

Does the solution interoperate with any existing firewall that a customer might have? This will provide a secure mechanism for interoperating with current and future business partners.

Access/Connectivity: Does the solution handle a variety of connectivity choices, including dial-up, leased line, T1/E1, DSL, and cable to meet a customer's current and future needs? For many customers, wireless access is already important as well. The solution chosen must be flexible enough to support the types of Internet connectivity technology a customer needs at each location, and whatever type of connectivity technology the customer envisions deploying in the future.

Service Coverage

This issue applies to VPN as a service from ISPs/NSPs, and total service solution providers. Is the VPN service available in every location where the customer is conducting business or plans to conduct business, and in every location where the customer has partners or potential partners? The service levels and the time that it takes to make additions and changes to the service should be consistent with the customer's business objectives.

Platform Type

Hardware/Appliance: Is the internal hardware architecture transparent to the user? PC-based network appliances are not the same as an ordinary PC. Do not assume, for example, that one could employ a generic PC as a backup device for a PC-based network appliance. Also, the economies of scale of a generic PC are vastly different from that of a PC-based VPN appliance.

Add-on Feature to Router/Switch/Firewall: If VPN is an add-on feature to an existing platform, the reliability and the performance record of the platform should be known to the customer. This option allows the use of an existing device for the VPN. However, as discussed under TCO considerations, this may not be the optimal choice for a customer.

Operation and Management

The operation and management of the VPN is certainly the customer's responsibility for 'build-it-yourself' VPNs. Even for an outsourced solution, customers would certainly want to monitor the health and performance of their VPN. Certain outsourced solutions may require significant customer involvement with configuration details. This would add to the TCO of the solution.

A Web-based management and monitoring system is preferable over non-Web-based systems since it can be accessed from anywhere on the Internet. However, not all Web-based interfaces have equal ease of use. A customer certainly should go through a demonstration of the management system.

The quality of the reports from the management system is important. The reports should be easy to create, customize, and understand.

Total Cost of Ownership (TCO)

As pointed out, the functions discussed in the previous section provide a short-term view. Use TCO to

select a solution from a set of products with similar basic VPN capabilities. Table 2 lists the important elements for calculating TCO.

Basic Costs: These are calculated based on vendor fee and on equipment price. One item that warrants discussion is the additional cost of a hardware and software upgrade if the VPN is an add-on feature to an existing in-house router/switch/firewall. When an administrator adds another function to an existing platform, the complexity of maintaining that platform increases and the performance degrades. Multi-function platforms also are prone to more crashes and "glitches". Make sure you account for these costs under additional costs for personnel, flexibility, and reliability.

Additional Costs: These include indirect costs but form the major part of the TCO.

Personnel costs should include loaded salaries and infrastructure (office space, furniture, telephone, desktop, and networking) and recruitment costs for technical people and management.

	Solution 1	Solution 2	Solution 3
Basic Costs			
Annual fee			
License fee, if hardware/appliance or software solution			
Service fee, if outsourced			
Annual software license/rental fee			
Cost of additional hardware and hardware upgrade (if add-on to firewall/router/switch)			
Additional Costs			
Personnel/professional services cost for initial design and deployment			

continued next page

	Solution 1	Solution 2	Solution 3
Annual personnel/professional services cost for ongoing management and maintenance of VPN			
Interoperability and Flexibility - Opportunity cost for not being able to connect with customers and business partners in a timely manner			
Reliability and Availability—Opportunity cost for downtime (planned and unplanned)			

Table 2: Total Cost of Ownership for a VPN

Interoperability and Flexibility: These costs include the cost of lost business if one cannot connect or interoperate with customers, business partners, and their systems in a timely manner.

Reliability and Availability: These are costs of unproductive employees and of lost transactions due to system unavailability.

Selecting the Right VPN Solution

The range of VPN solutions frustrate customers trying to compare the solutions. This is especially true for customers in small and medium-sized businesses. These businesses have neither the resources nor the time for a drawn-out evaluation. By focusing on the long-term IT and networking strategy and by using a TCO framework, customers can simplify and rationalize the evaluation and can eliminate the theoretical possibilities.

Build vs. Outsource

Before developing a detailed list of technical, functional, and other requirements, a customer must decide whether they want to build their own VPN solution or they want to outsource it. This needs to be answered even when customers have in-house installed firewalls and routers for which a VPN is available as an optional feature.

A build-your-own solution has the following characteristics:

- More control and customization
- Capital investment
- In-house IT and networking personnel and resources
- Long development cycles and greater lost-opportunity cost

An outsourced solution has the following characteristics:

- No capital investment
- No in-house personnel and other resources needed to manage the technology
- Ease of expansion and changes
- Ease of migration to new technologies

For small and medium-sized businesses and, increasingly, for large businesses too, the IT trend is towards outsourced services. Businesses want to focus on the "business-of-the-business" and providing internal IT services is becoming a distraction.

For VPNs, if a customer can find an outsourced solution that meets his/her functional requirements and is flexible enough to support their future needs, outsourcing is a better solution than a build-your-own solution.

For a more specific and detailed cost/benefits analysis of implementation alternatives, a user should use Tables 1 and 2.

Conclusion

The ability to use the Internet in a secure manner is the foundation of e-commerce. A VPN is the key to attaining that objective. Not only do VPNs provide security across the Internet, they can eliminate expensive intranets and EDI networks.

There are numerous solutions available for implementing a VPN. Small and medium-sized businesses will find that, more often than not, building their own solutions, even as add-on features to existing in-house solutions, will be more expensive and less compatible with their business objectives in the long run.

For the outsourced solutions, managed VPN services from network services providers are no longer the only option for customers. Customers should compare emerging services such as point-and-click VPN services and network service provider VPN solutions. A point-and-click solution may not only cost less than the alternatives, but also provide greater flexibility and more scalability to reach customers and business partners worldwide.

Case Study: Integrating Remote Offices—How NETSCAN Used OpenReach to Become an E-Business

Overview

NETSCAN iPublishing Inc. provides legislative and regulatory news feeds to its customers and has built its business by delivering timely news via the web. With increased demand on their resources and a more complex IT infrastructure, the company was facing a number of challenges fulfilling its promise to deliver secure, timely information to its customers. As a small company with limited IT resources and offices in three states, NETSCAN was forced to use a less-than-ideal system for communicating important documents and information between offices.

NETSCAN Needs To Connect

To meet its customers' needs, NETSCAN delivers the latest news on legislative happenings within 12 hours of the activity, using a combination of people and software. This tight schedule makes it imperative for NETSCAN's data collection, creation, and delivery processes to be efficient and infallible. However, with 35 employees located in three different states (Florida, Pennsylvania, and outside Washington, DC), the company was struggling to maintain its short production time. Since providing timely information for breaking news stories is critical to the success and reputation of NETSCAN, the company realized it could no longer bet its business on email and unsecured FTP, the current methods for transferring files between separate locations.

NETSCAN was also facing a number of challenges integrating its offices. Each office uses a different service to connect to the Internet and has its own separate local area network (LAN) environment. This environment highlights a number of inherent problems that were putting NETSCAN's business at risk:

The Problem

- Separate Offices
  NETSCAN has 3 separate physical locations, each with different types of connections to the Internet, that need to communicate and collaborate
- Unreliable Existing Connections
  The existing method of sharing files and information via email and FTP is unreliable
- Limited IT Resources
  There is no dedicated IT staff at any location, so any solution has to be straightforward, easy to implement, and self-managing
- Limited IT Budget
  NETSCAN cannot afford a costly standard VPN or WAN solution
- Need for Growth
  NETSCAN needs to find an alternative to its current methods to prevent potential loss of business and to position itself as an e-business for future growth

Searching for the Right Solution

Many small companies face the same dilemma that NETSCAN did. They need to adopt a more mature and robust IT infrastructure but lack the internal resources (both money and staff) needed to implement one of the solutions on the market. The standard solution for connecting multiple locations of a company, a virtual private network (VPN), is traditionally tar-

geted at larger companies that can afford the investment required for such a solution. NETSCAN knew that it needed to solve its current file transfer issues, but it also knew that a traditional VPN was not a feasible solution. With the three different Internet connections and no internal IT staff to handle the complex technology that is part of a VPN, as well as the reality that outsourcing to a large managed service provider was far too expensive for the company, NETSCAN was left looking for some other way to meet its needs.

Once NETSCAN found OpenReach, it realized it could securely connect its multiple offices without hiring additional IT staff or purchasing expensive and proprietary equipment. With a "point-and-click" VPN solution designed for small-to-medium businesses, OpenReach provided secure and scalable LAN-to-LAN connectivity over the Internet while addressing all the problems that NETSCAN faced when considering a traditional VPN solution.

The Solution

- **Fast, hassle-free installation.**
  NETSCAN went live with OpenReach VPN services the same day that the services were downloaded onto the company's dedicated PCs.
- **Immediate secure, seamless communication.**
  Within a matter of hours, NETSCAN was transmitting files and information securely via the Internet with OpenReach's services between its Virginia and Florida offices.
- **Proactive monitoring and alerting.**
  NETSCAN has already benefited from OpenReach's monitoring services. Shortly after installation, OpenReach actually alerted NETSCAN's Virginia office to a problem with its Internet connection at the Pennsylvania office, which was unrelated to the OpenReach solution. NETSCAN's Virginia office was able to proactively resolve the issue before it caused problems for workers in Pennsylvania.

Conclusion

Without making a substantial investment or having dedicated IT staff at each location, NETSCAN has been able to create what it never thought possible: an affordable and robust VPN for its entire business. Employees at the various NETSCAN offices, especially those who travel between offices, are "delighted" at the connectivity and privacy that OpenReach provides. NETSCAN has been satisfied with the initial performance of OpenReach VPN services. The ease of installation, affordability, and immediate deployment have enabled NETSCAN to become a connected e-business.

For a complete copy of this case study, visit the OpenReach website:

www.openreach.com

OpenReach, Inc.
660 Main Street
Woburn, MA 01801
1.888.783.0383

Glossary of Terms

Asymmetrical Keys—The use of a key pair. One key is used to encrypt the information, the other is used to decrypt it.

Authentication—Verification of the identity of specific users or systems.

B2B—Business-to-Business transactions over the Internet.

B2C—Business-to-Consumer transactions over the Internet.

Certificates—A unique private key which identifies a user or system to another user or system which also holds its own unique certificate.

Crypto Period (encryption period)—Length of time for which the encryption keys are held valid.

Data Encryption Standard (DES)—A commonly used standard for encrypting data over the Internet. DES, or Standard DES, has a 56-bit key length.

3DES—A variation of the DES algorithm which uses 3 keys. One to encrypt, a second to decrypt, and a third to encrypt again. The result is effectively a 168-bit key length.

Digital Subscriber Loop (DSL)—A digital telephone link to the user premises, which allows very high speed connections, 10 to 20 times greater than the 56 Kbps modem, to the Internet.

EDE—Encrypt, Decrypt, Encrypt. Method used in the Triple-Pass DES and 3DES encryption algorithms.

Electronic Data Interchange (EDI)—A technique for exchanging transaction-related and other data between businesses based on formats and standards defined by an industry group or a corporation. Most EDI standards pre-date the Internet and are not based on the Internet standards.

Encryption—The use of a mathematical algorithm and keys to scramble and unscramble information so that it is not translatable by the naked eye.

Extranet—The extension of a private corporate network to allow connectivity with partners and customers.

Firewall—A device or piece of software which employs rules to specify that communication from a specific location or individual, or of a specific protocol, can or cannot enter the network.

Intranet—An organization's private network typically based on TCP/IP protocol.

Internet Protocol (IP)—The routing and addressing part of the TCP/IP protocol suite.

IP Security (IPSec)—The name of the standard for secure communications over the Internet. Defines framework for authentication, encryption and managing encryption keys.

ISP—Internet Service Provider

LAN—Local Area Network

Layer 2 Forwarding (L2F)—An earlier, proprietary Cisco protocol for secure communications over the Internet, replaced by L2TP.

Layer 2 Tunneling Protocol (L2TP)—An amalgamation of two proprietary protocols, L2F and L2TP, PPTP, for secure communications over the Internet. Proposed as an alternative to IPSec, but IPSec remains the dominant protocol for secure communications over the Internet.

Mesh-connected (fully meshed network)—A network whereas every entity in that network can access any other entity within that network.

Network Address Translation (NAT)—Used to convert, or translate, an address on one network to an address which will be usable on another network.

Network Services Provider (NSP)—Differs from an ISP in that it also provides services other than Internet access.

Packet Encapsulation—The placement of one packet into another packet, thereby hiding the original addressing information and data.

Point-to-Point Tunneling Protocol (PPTP)—A proprietary protocol used by Microsoft as an alternative to IPSec for secure communications over the Internet.

Public/Private Key Pair—The public key in a key pair is not kept secret. The private key, held by one individual, is kept secret.

Quality of Service (QoS)—Defines or measures the quality of expected Internet connectivity or services. QoS specifications typically include parameters such as network availability, restoration time, number of dropped packets, end-to-end delay.

Remote Access Server (RAS)—A device to support dial-in connections from remote users.

Symmetrical keys—The use of the same key to encrypt information and decrypt that same information.

Total Cost of Ownership (TCO)—Includes, in addition to initial purchase price of hardware and software, additional one-time and recurring costs such as installation, support, loss of productivity and opportunity costs. Reflects the true cost of product or service over a period of time.

Transmission Control Protocol (TCP)—A reliable protocol for application-to-application communications over the Internet.

Triple-Pass DES (Triple DES)—A variation of the DES algorithm which uses 2 keys. The first key encrypts the data, the second decrypts the data, and the first is used again to re-encrypt the data. The result is effectively a 112-bit key length.

Tunnel Mode—Mode of IPSec which enables the secure transfer of data across the wide area network inside a tunnel.

User Datagram Protocol (UDP)—An unreliable protocol for application-to-application communications over the Internet.

Virtual Private Network (VPN)—The use of the Internet as if it were a private network through the use of encryption and authentication techniques such as IPSec.

WAN—Wide Area Network

NOTES

NOTES

Look to OpenReach for the easiest VPN.

- No upfront investment
- A worldwide network built in minutes
- Centralized administration with "Point & Click" simplicity
- Any combination of ISPs and broadband services
- 24x7 monitoring, alerting and technical support
- Industry standards-based security (IPSec, digital certificates, integrated firewall)
- Scalability that grows with your business

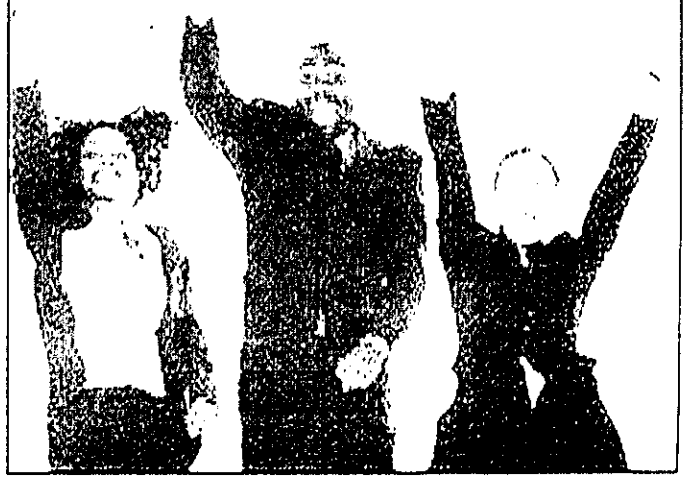
With features like this, *everyone* will be happy.

OpenReach VPN services include free software with unique features that make the solution faster, easier and less expensive than anything on the market. The OpenReach solution:

- Can be installed behind an Internet access device with a variable IP address assigned via DHCP
- Can be installed behind a NAT router or firewall
- Can be expanded almost anywhere in the world providing the strongest security anywhere you need *
- Is approximately simple, but has the performance required to support advanced applications

Plus, OpenReach offers these security measures:

- **Authentication** using Digital Signatures or alternate mechanisms
- **Data confidentiality** using 168-bit 3DES encryption
- **Protection of corporate resources** via an integrated firewall
- **Secure command and control** traffic sent via the VPN
- **Security monitoring**

OpenReach

www.openreach.com
888-783-0383