Government of Nepal

Controller of Certification Authority

Ministry of Environment, Science and Technology

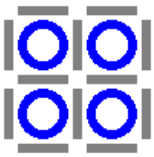
Singh Durbar, Kathmandu, Nepal

A Short Study Report

on

Government Applications and its Legal Authentication

Submitted by



IT Professional Forum

July, 2009

Executive Summary

This report covers few major government applications that are computerized in Nepal, provides details on their current status, and also looks into security measures applied and electronic authentication in practice in general. Electronic authentication is an essential component of the verification and management of identities online, and therefore, is an important element in different governmental, social and wide range of individual activities in the modern age. The report then lists Digital Signature, eSignature and some other hardware based Authentication technologies, but feels the need for establishing technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities.

This document recalls the provision of Public Key Infrastructure (PKI) for issuing and security key management in IT Policy and Electronic Transaction Act 2006 of Nepal, but still the Infrastructure is not in place to date. The document refers to OECD (Organization for Economic Co-operation and Development) guidelines on electronic authentication, and recommends following the guidelines instead of devising our own separate guidelines through a duplication of work.

The report emphasizes on the aspects of Privacy, Authenticity, Integrity, and Non-repudiation in order to ensure confidence and safety of doing business electronically. Hence it states that the government applications must ensure Cyber Security, Personal Data Security and Content Safeguards through a legal authentication system. Finally, the report also tries to conceive a noble method of authentication by assigning dedicated IP address to devices based on their unique hardware ID once IPv6 is introduced.

Due to the stipulated limited time, this report couldn't cover the security measures of Government Integrated Data Center (GIDC) being established under National Information Technology Center (NITC), but it is understandable that such a Center could play a vital role on wider security aspects than physical security alone.

Several stakeholders in the government and public sector were consulted while preparing this report, for drawing conclusion and recommendations; it is discussed amongst a wider audience of stakeholders through a workshop.

ACRONYM

CAN	Computer Association of Nepal
CCA	Controller of Certification Authority
DOR	Department of Roads
EC	Election Commission
ECS	Electronic Clearing System
e-Commerce	Electronic Commerce
eFIT	Electronic Financial Information Technology
e-Finance	Electronic Finance
EFT	Electronic Fund Transfer
eGP	Electronic Government Procurement
e-Payment	Electronic Payment
ETA	Electronic Transaction Act
GIRO	A Banking term for method of payment
HLCIT	High Level Commission for Information Technology
ICT	Information Communication Technology
IDRBT	Institute of Development and Research for Banking Technology
IRD	Inland Revenue Department
IT/ICT	Information and Communication Technology
ITC	International Trade Commission
ITPF	Information Technology Professional Forum
MOF	Ministry of Finance
MOICS	Ministry of Industry, Commerce and Supplies
NBA	Nepal Bankers Association
NCC	Nepal Chamber of Commerce
NEFT	National Electronic Funds Transfer System
NRB	Nepal Rastra Bank
NIFMIS	Nepal Integrated Financial Management Information System
NRN	Non-Resident Nepalese
OCC	Office of Controller of Certification
PAN	Permanent Accounting Number
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point of Sale
RTGS	Real-time Gross settlements
TAF	The Asia Foundation
UNCTAD	United Nations Conference on Trade and Development
VAT	Value Added Tax
VPN	Virtual Private Network

Table of Contents

1.0 Introduction

1.1 Background

This study report is an outcome of response to Request for Expression of Interest (REOI) from Office of Controller of Certification (OCC) to IT Professional Forum (ITPF) for carrying out a short study on **Government Applications and its Legal Authentication.**

IT Professional Forum (ITPF) is formally registered at the Chief District Officer's (CDO) Office, Kathmandu and Social Welfare Council as a non-government and non-profit making organization, is a team of well established IT Professionals. ITPF members represent private, semi-government, government, academic and financial institutions in Nepal. ITPF is represented in the High Level Commission for Information Technology (HLCIT) of Nepal and is an institutional member of the Computer Association of Nepal (CAN).

ITPF has conducted numerous policy researches with respect to IT policies, Electronic Transaction & Digital Signature Act & Regulations, VOIP, IPR, e-Commerce, e-Government Procurement (e-GP), e-Governance, e-Payments, business incubation, etc. and provided its assistance to Government of Nepal (GON) for the formation of Electronic Transaction Act, framework for the e-Government Masster Plan (eGMP). The Forum is also involved in academies, running M.Tech. in IT program in association with Kathmandu University. ITPF conducts various other activities such as tech talks on IT development, highly professional software / project management trainings, curriculum development and review for ICT, and other computer training programs.

The Office Controller of Certification Authority (CCA) is established under the Electronic Transaction Act 2063 (2006). OCA is in the process of setting up Public Key Infrastructure (PKI). Authentication is the essential requirement for any kind of online transaction. In absence of such authority, people cannot get confidence doing online transactions (documental or financial). In a situation of availability of other promising technologies, growing online government applications in practice and initiation of e-Government Projects by the Government through the aid support of Asian Development Bank (ADB) and other development partners, this study is considered as very timely effort.

1.2 Study Objective and Contents

Following are the objectives of the study:

- Identification of major government applications in use and up coming
- Assessment of legal authentication practice in use in selected government applications

- Identification and Assessment Authentication Technologies
- Stakeholders Consultation
- Conclusion and Recommendations

The study is divided in four sections; this introductory section gives the background on the study. The second section is devoted for identification of government applications in use and assessment of selected applications. The third section focuses on the authentication technologies assessment and the last section is devoted for preliminary conclusion and recommendations, which is planned to be discussed amongst various stakeholders through a workshop for drawing final conclusion.

1.3 Government System Security and Authentication

It will be quite easy for the Government to conduct its operations electronically through Internet. But there is a biggest problem in doing business online. Every piece of information is important from government as well as people's point of view. Neither government nor people/business wants to disclose the information to any person other than the one for whom the information is intended. As such security is the major concern for any one doing business over the Internet. The e-Government and all electronic transactions through online application require building trust so that government and public can accept such systems and feels confident working in a private, confidential and most secured environment. The security is a primary concern and is a must for carrying out government operation through Internet.

The information and communication technology (ICT) has provides various methodologies for making electronic transactions secured. Details on this will be discussed in section three of the report. In order to build confidence on transactions online, the following four major essential elements need to be considered:

Privacy: The e-Governance model must assure that privacy is maintained while exchanging documents between government and people over the web. No unauthorized person(s) can get access to them.

Authenticity: The system must promise the identity and authenticity of the sender and recipient of documents and transactions.

Integrity: The system must guarantee on the integrity of the document content when exchanged across the web.

Non-repudiation: Neither the receiver nor the sender should be in a position to deny that they had not delivered or not received.

Figure 1 illustrates the different types of securities that are required to build for the operation of secured government system. Some security measures protect the physical materials while others protect the network, logical component and databases.

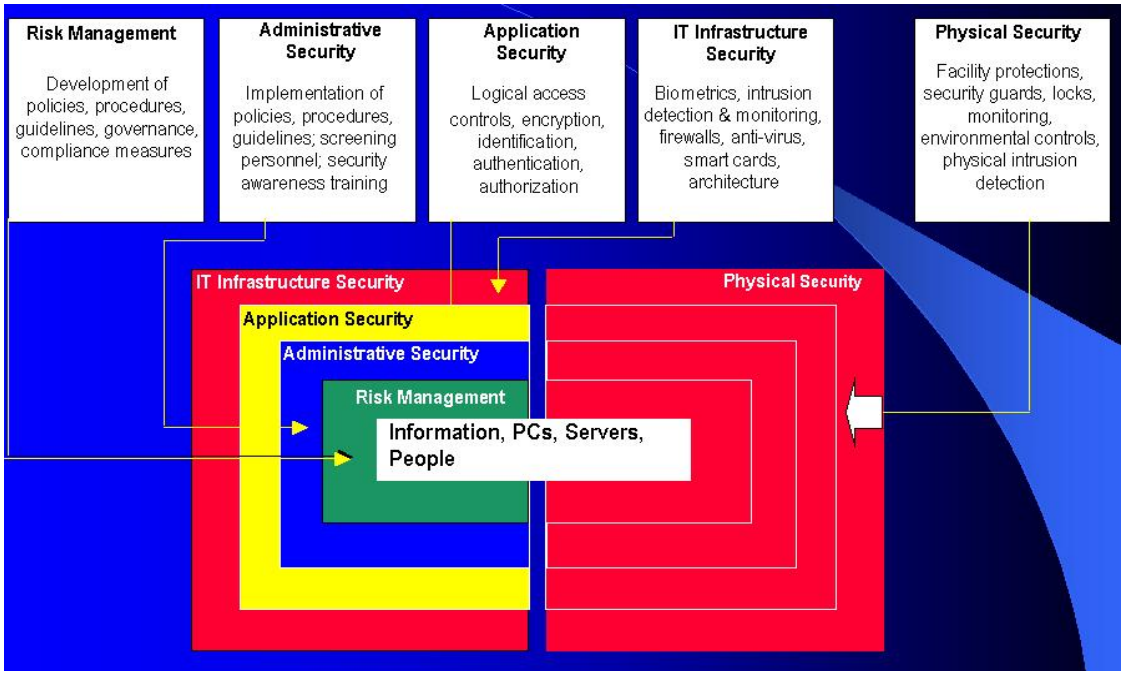


Figure 1: Security Overview

The study will be focused on application security and IT infrastructure security.

1.4 Legal Framework

The study of various Nepalese legislations was conducted and it was found that Electronic Transaction Act, Contract Act, Nepal Rastra Bank Act, Public Procurement Act, Income Tax Act, VAT Act and and regulation under these acts are more related with e-Governance system.

1.4.1 Electronic Transaction Act (ETA)

Electronic Transaction Act 2006 (ETA 2006) covers everything from legal definition of terms to the judicial systems needed to protect parties in a transaction. The ETA 2006 provides a starting place for the development of important e-readiness infrastructure. The ETA 2006 covered the following areas:

- Legal recognition of electronic records and communications: contractual framework, evidentiary aspects, digital signatures as the method of authentication, rules for determining time and place of dispatch and receipt of electronic records. The ETA addresses the use of electronic records and digital signatures in government agencies.

- Regulation of Controller of Certification Authority: appointment of a CCA, grant of licenses to Certification Authorities, duties vis-à-vis subscribers of digital signature certificates, recognition of foreign CAs.
- Cyber contraventions: civil and criminal violations, penalties, and establishment of the Adjudicating Authority etc.
- Provisions related to electronic payments, electronic funds transfers, electronic banking, intellectual property rights, including copyrights, trademarks and patents, consumer privacy, dispute management involving e-transaction, and the protection of children are not addressed by ETA.

1.4.2 Contract Act

A simple electronic transaction (e-transaction) could be a valid legal transaction based on prevailing contract law of Nepal. Like English law, Nepalese law also requires no particular form for the creation of contractual rights and obligations. A contract can be created, providing the necessary elements in place, orally or in writing. Communication of offer and acceptance using ICT could be recognised as valid contract under the provision of section 7 of the Contract Act, 2056 (2000). Moreover, parties interested to be involved in e-transaction may form a bilateral/multilateral agreement in which all of the relevant parties have agreed in advance on their respective rights and duties, and allocated any potential risks. Banks in Nepal are providing card service on the same basis.

As an example of e-transaction, structure of e-payment can be explained as below:

Intermediary could be a bank, finance company or any other company, setup to provide financial services as per the law of Nepal, Recipient of money could be any entity which needs to receive payments from clients and Payer could be any individual, organization or any other legal person which needs to pay the recipient.

Where, Recipient and Intermediary enter into an agreement for e-transaction, which outlines:

- general terms and conditions of services,
- security arrangements,
- possible risks and risk mitigation methodology and
- recipient's authority to execute agreement with Payer on behalf of Intermediary

Thus, by making two sets of agreements (a) between recipient and intermediary and (b) between recipient and payer, could create tripartite relation creating rights, liabilities and obligations for each of the parties.

In the case of global scenario, Secure Electronic Transaction specification developed by Visa, MasterCard, and other members of the payment card industry, where each of the parties to a secure electronic transaction - cardholder, merchant, and member banks that process the

transaction has a security mechanism that establishes its identity and authority within the system. As in an ordinary payment card system, the parties' rights and duties are established by a series of contracts. Similarly, SWIFT is being used by banks all over the world on the similar principle.

Neither the Secured Electronic Transaction nor the SWIFT was created by any specific dedicated legislation but by contract laws prevailing in respective countries. Such system shall at least be governed by:

- A treaty or multilateral agreement in case of transnational transactions.
- A statutory provision in case of domestic transactions.

Legally, NRB currently possess all needed authorities enabling to establish an appropriate "Payment, Clearing and Transfer System". Clearing House system is now being developed in association with private banks along with NRB. POS could be bank/financial institution itself sometime. A post office, co-operative or any other institution qualified to handle secure electronic transaction under the rules made by the NRB could be POS. Thus e-payment could be started in Nepal without any change in statutory provisions. Practical application or enforcement of 'Electronic Transaction Act' would be an added value for such transaction.

1.4.3 Nepal Rastra Bank Act

Enabling law of Nepal is Nepal Rastra Bank Act, 2058 (2002) Section 5. (1) (i) has given the NRB function:

(1) To establish and promote the system of payment, clearing and settlement and to regulate these activities;

- International Clearing and Payment Agreements: The Bank may, either for its own account or for government account and by the order of Government of Nepal, enter into clearing and payment agreements with public or private central clearing unions domiciled abroad. The Bank may, in order to implement the objectives of such agreement, enter into other necessary agreements.

- The Bank shall make necessary arrangement for the clearing and settlement of cheques, payment orders, inter bank payment security transactions made in the currencies prescribed by the Bank and any other payment instrument and carry out the functions of regulation, inspection and supervision thereof.

(2) While carrying out the functions referred to in sub-section (1), the Bank may prescribe necessary procedures.

(3) For the purpose of clearing and settlement arrangement referred to in subsection (1), the commercial bank or financial institution shall, subject to the terms and conditions prescribed by the Bank, open account in the Bank or any other financial institution prescribed by the Bank.

1.4.4 Public Procurement Act - 2006

Public Procurement Act 2006 recognizes and accepts publication of tender, exchange of information, delivery of bid document electronically. Public Procurement Regulations has specified the use of e-Procurement Portal (http://www.bolpatra.gov.np) developed by ITPF with the technical assistance of Hitechvalley iNet and financial support of the Asia Foundation for publishing the procurement related information and also procurement opportunities. The Department of Roads (DoR), Government of Nepal pioneered in e-Procurement establishing its own online e-Tendering system with tender Submission facilities in the World Bank supported projects with the technical support of Hitechvalley iNet since the last quarter of 2007. Currently the system is being extended for all the procurement of DoR. The PPA is silent on electronic payments for the purchases made by government and public enterprises.

1.4.5 Other Acts

Income Tax Act, Value Added Tax Act and regulations under them have recognized the legality of electronic transactions and Inland Revenue Department (IRD) has started accepting data received electronically. Nepalese Citizens and Businesses are practicing to register under VAT and PAN, submitting tax return and receiving acknowledgement and information electronically. The Inland Revenue Department and the Income Tax Department are happy on the response to the online facilities they have offered through their website. The transactions are being carried our smoothly on receiving tax, VAT and information and delivering the service by the departments.

E-Payment and other financial transactions online can be started with the parliamentary enactment. Statute may not be required to establish and promote system of clearing, payment and settlement. Sets of required rules, regulations and directives could be made by the NRB itself. E-Payment system has to be designed to make electronic transaction more secure, reliable and economic and practical. Enforcement of Electronic Transaction Act is a must for the confidence of its all actors. Currently businesses are using electronic form of payment under the agreement governed by Contract Act, between service providers and service seekers.

So far government has not come-up with e-Payment Policy or legislation and but in 2007 with the financial assistance of the Asia Foundation, ITPF had carried out the study on the e-Payment system for Nepal together with the NRB, Bankers' Association of Nepal, Ministry of

Finance, SCT and other stakeholders and prepared its comprehensive report with policy recommendations and architecture options.

2.0 Government Application in Use and Authentication

Government agencies of Nepal are in different stages of using ICT. Some of the software systems are running from many years and many new software systems, Internet based and LAN based, are being introduced. Most of the new systems are web based.

Government of Nepal has initiated a ICT development project with the Grant from ADB for the introduction of government services through a comprehensive set of e-Government Applications, providing wireless Internet connectivity in rural areas of Nepal complying with the e-Government Master Plan (eGMP) approved by the Government. The ICT development Project (e-Government Project) includes the following e-Government applications:

1. Government Enterprise Architecture (GEA)
2. National Identification Database (NID)
3. Introduction to Public Service Commission
4. Land Information Management System
5. Electronic Driving License and Vehicle Registration System
6. Village Network Portal

All of the government e-Services applications will be hosted in Government Information Data Center (GIDC) as provisioned in eGMP, so the authentication and security requirements in the application, data, network, data center and transactions are very crucial and should be carefully taken care.

Few of the major government agencies have been identified for the purpose of this study, where major computer application systems are in use. The list also includes the institutions where government holds the majority of shares.

I. Constitutional Bodies
Election Commission
Public Service Commission Examination System

II. Ministries and Departments
National Planning Commission
    Central Bureau of Statistics
Ministry of Finance
    Financial Comptroller General's Office (FCGO)
    Inland Revenue Department
    Department of Customs
Ministry of Education
    Office of Controller of Examination (SLC)

Office of Controller of Higher Secondary Examination
Institute of Engineering (IOE) Entrance Examination
Institute of Medicine (IOM) Entrance Examination
Ministry of Home Affairs
Nepal Police
Department of Immigration
CDO Offices
Ministry of Land Reform & Management
Department of Land Reform & Management
Department of Survey
Department of Land Information & Archive (DoLIA)
Ministry of General Administration
Ministry of Environment, Science and Technology
National Information Technology Center

Department of Transport Management
Department of Roads

III. Financial and Service Sector
Nepal Rastra Bank
Nepal Bank Limited
Rastriya Banijya Bank
Employment Provident Fund
Nepal Telecom

IV. Local Governments
Municipalities

V. Judiciary
Supreme Court / Other Court

The following section provides the briefs about the selected applications and then discusses its security and authentication aspects.

2.1 Inland Revenue Department (IRD)

The Inland Revenue Department (IRD) is the government department established in B.S. 2058 and is responsible to collect the Value Added Tax, Income Tax, Excise and some other taxes such as Rental Tax, other revenues for the country. Twenty one Inland Revenue Offices (IRO) and one Large Taxpayer Office (LTO) under IRD, all around the country; are the executing units for the assessments of tax and their collections. IROs & LTO have computer system in a network and which are connected to the computer system in the center.

2.1.1 Historical ICT Initiatives

The VAT Accounting System, the Integrated Tax Registration System and Income Tax Collection systems are in operation currently in a Wide Area Network with Distributed System Architecture. It has a central database in the IT Section of IRD. VAT Accounting System was designed, developed and implemented by Professional Computer System with the support from DANIDA.

GTZ/RAS Project had developed the system for Income Tax Collection System in the Oracle platform initially and it has been reengineered again by Professional Computer System (PCS) and is undergoing implementation.

The application software, which presently handles all aspects of revenue administration, is named “ProTax”. ProTax presently covers the following main modules:

- Taxpayer registration
- VAT assessment
- VAT collection
- Income Tax assessment
- Income Tax collection

ProTax is client server based and uses Oracle RDBMS 8i. There is one large central production database in the IRD and each of the 22 IROs & one LTO has a separate production database. Servers operate on Microsoft Windows NT Server 4.0 and Windows 2000 Server; clients operate Windows NT Workstation 4.0, Windows 2000 and Windows XP.

ProTax was developed using the Structured System Analysis and Design Methodology (SSADM) for system analysis and logical design. Oracle Designer and Oracle Developer were used for the physical design and development.

IRD has developed and implemented several online applications like e-PAN, e-TDS, e-IN, e-VAT in the next stage of the tax automation system. In these systems taxpayers enter their data and generate reports themselves and the data come to IRD via internet. e-PAN system has been developed and implemented to enter taxpayers registration data, verify it and generate the PAN card electronically. e-TDS system has been developed and implemented

for TDS data entry , verification and consolidation. e-Installment system has been developed and implemented for the installment return filers. e-PAN and e-Installment system is integrated with existing Income Tax System. Similarly there is another system called e–VAT which is integrated with existing VAT system which is developed and implemented for the VAT return filers. All these systems have been developed in PHP with Oracle backend.

More over, mobile technology enabled SMS system is launched for the effective service delivery to the taxpayers and concerned group of people. The SMS System is developed and implemented in IRD to make the information about the tax filing status to the taxpayers from the IRD database.

Likewise, IRD has developed some other online systems like Check Point entry System (not in use any more) and IRD Intranet portal for the effective tax administration.

The DANIDA – RAS Project has been supporting the Inland Revenue Department in the areas of Information & Communication Technology since the inception of the Department. The Department has been using Oracle 8i - RDBMS (Relational Data-Base Management System) as the main database since 1998. The current application of Pro-Tax was developed using the Oracle Developer tools, mainly Forms 5.0 and Reports 3.0

It was felt essential to upgrade this system and accordingly, Oracle Database 10g (Enterprise and Standard Editions) with Partitioning Options was procured by the DANIDA – RAS Project and handed over to IRD on February 12, 2009. It is now ready to provide support for data and forms migration so that the new DBMS is compatible with the Pro-Tax application.

Summary of Historical Initiatives

- 1993: VAT System Study and design started
- 1997: Computerized VAT System implemented
- 2000/01: System re-designed, developed and implemented
- 1998: Income Tax System requirement study
- 1999: KTSC established for PAN Registration
- 2001: Joint Registration for Income tax and VAT implemented
- 2001: Complete Registration, VAT, and Certain Modules of Income Tax system are running smoothly, Department Website www.ird.gov.np
- 2006: Electronic Tax Deduction at Source (E-TDS), Electronic Tax Registration System (E-PAN), Modern Revenue Accounting System (MRAS), Check Point Entry Systems (CES)
- 2007: E-Filing of VAT Returns, Completion of Income Tax Modules, SMS services and establishment of intranet with IROs, MOF, FCGO, DOC, COs, DRI
- 2008: Implementation of Income Tax, Upgrading of RAS and implementation in all IROs, IRD Portal, Redesigning of IRD Web Site, Internal Monitoring Software
- 2009: Excise automation and E-filing of Income Tax Returns to be completed; Oracle database and all its related applications are being upgraded to Oracle 10g.

The following are some other e-government initiatives by Inland Revenue Department (IRD) under Ministry of Finance, Government of Nepal:

e-PAN (Electronic Permanent Account Number) System: PAN (Permanent Account Number) is a unique number, which is issued to the taxpayers by the Inland Revenue Department to do any types of business in Nepal. e-PAN System is an Internet based system which allows to apply online for PAN registration by any taxpayers. Effort has been made to simplify the system so that the system can be operated without any training. Only requirement will be an access to Internet and skill to operate an Internet browser. In this system, intermediary organizations assigned by IRD are allowed to enter and verify the PAN registration information into the e-PAN System. After verifying the registration information the system generated the PAN Card which intermediary organizations hands over to the concerned taxpayer with their seal and signature. All the registration information of taxpayers is registered in this system and the system prints the PAN registration certificate for taxpayers.

e-TDS (Electronic Tax Deduction at Source) System: e-TDS system is an Internet based system. This allows withholders, withholdees and tax officers to access system from anywhere with Internet connection. The main objective of the system is to do away with the necessity of collecting TDS certificates from the withholders so that withholdees can submit the TDS as credit in their tax returns. System is also expected to reduce the error in TDS information thus helping taxpayer with correct TDS information on time. In this system, the withholder enters the TDS and Voucher information into the system and system generates a report, which the withholder sends to the concerned Inland Revenue Office with their seal and signature. The concerned tax officer checks that information and verifies into the system. The withholdees can see their TDS information by logging into the system with their username and password. Tax officer can also issue the tax clearance certificate to the withholdees by checking the information into the e-TDS System. Effort has been made to simplify the system so that the system can be operated without any training. Only requirement will be access to Internet and skill to operate Internet.

e-Estimated Income Tax Returns System (e-IN): e-Estimated Income Tax Returns System is an Internet based system through which taxpayers can insert estimated tax Returns information and sends the report to the tax office with seal and signature. Effort has been made to simplify the system so that the system can be operated without any training. All the verified records of e-Estimated Returns System are finally transferred into the central Income Tax Database by IT Section in IRD.

e-VAT Returns: e-VAT Returns System is also an Internet based system in which a taxpayer enters the VAT Returns and payments data into the system and sends the report to the tax office with seal and signature. Effort has been made to simplify the system so that the system can be operated without any training. All the verified records of e-VAT Returns System are finally transferred into the central VAT Database by IT Section in IRD.

SMS System: IRD has implemented a new SMS system to make queries about taxpayers instantly using the cellular phones. Functionalities such as, taxpayer's registration information, returns filing status can be instantly accessed by the taxpayers using this service.

Web Site: IRD website is in operation since the merger of the then two departments, Income Tax Department and VAT Department and has been serving its customers primarily the taxpayers. Currently the site is maintained and updated by the ICT section. All the information, notices, downloadable items are stored in this web site. Similarly, all the online systems- e-PAN, e-TDS, e-Returns and checkpoint systems are also accessed through this web site. http://www.ird.gov.np

2.1.2 Security procedure and authentication in IRD Systems

With the perspective of system securities, there are two types of system in place in IRD:

- One which is a closed group system which is only available within the Local Area Network (LAN) system for a particular IRO or LTO or IRD and is updated at IRD's Central Server and distributed again to the concerned IROs or LTO through a secured and validated process within the scope of proprietary Wide Area Network (WAN) system.

  This is the main system in operation and does not provide any physical access from users outside the network. The system comes with three layers of security systems:
  - Network Access Security
  - Application Security
  - Database Security

  The system is fully secure as long as any possible intruder has physical access to the computers in the network and knows username & password for the network and the application or the database. The database keeps track of complete audit trail of the transactions. Also these systems in the Department at the central level (in Kathmandu) have backup servers for failsafe operations and have plan for disaster recovery site at Bhairahawa.

- Second is the new group of e-government (e-GMP) applications (such as e-PAN, e-TDS, e-IN, e-VAT) that is annexed to the existing closed group applications. In order to protect central database general public is given access to a dirty database (dirty in the sense that taxpayers can try around any data during their learning process) only verified data is then transferred to the clean database and then to central database. Officers are granted only execution right on a transfer process from central database.

  For verification either user comes with printed copy to IRO which is then verified by IRO officers or for auto verification user must request physically register email address. Then for each document a one time use key is sent to registered email address as second channel upon demand from user. User will then use this key and some other data which only user is supposed to know (Such as previous period due) for verification of the document identified by transaction number. The user with the same PAN and Transaction number can edit or delete the transactions that he/she has created. The transaction created by its online users is validated by respective revenue officer and then only it will create appropriate transaction in the back office system.

Securities levels in different applications that are in operation within IRD are depicted by the following table as well:

S.No	Product	Database Level Security	Application Level Security	Database Architecture
1	Registration	Yes	Yes	Distributed
2	VAT Assessment/Collection System	Yes	Yes	Distributed
3	Income Tax	Yes	Yes	Distributed
4	Revenue Accounting System (RAS)	Yes	Yes	Distributed
5	e-PAN	Yes	Yes	Centralized
6	e-TDS	Yes	Yes	Centralized
7	e-IN (Installment)	Yes	Yes	Centralized
8	e-VAT	Yes	Yes	Centralized
9	e-SA (Income Tax return)	Yes	Yes	Centralized

In addition to the above security, some sort of security like logical security (Windows group policy), system user level security and Linux firewall as a gateway are also being provided.

2.1.3 Impression on Security Infrastructure in IRD

IRD is the largest user of ICT in Government sector. IRD has incorporated ICT in all its operation and is getting more serious with the recent e-government tools being provided to its taxpayers for easy access to the system and reduce corruption by minimizing physical contacts between the taxpayer and the officials in IROs or LTO as much as possible.

The present system for user authentication makes use of Transaction Number and authenticated email in the absence of any better ways of authentication such as digital certificates, e-signatures etc. It is for certain that Taxpayers of IRD and its officials can be one of the most serious users of any PKI infrastructures that will be set up in the country. Also, the present e-GMP systems can be improved further with the use of such infrastructure making it easy further for the taxpayers without getting in the hassles of Transaction Number etc. Also, in the absence of Payment Gateway system, IRD has not been able to adopt a better means of tax collection system and taxpayers are not able to pay their tax online.

More in depth study will be required for security status of systems in operation in IRD in further detail.

2.2 Election Commission (EC)

2.2.1 Historical ICT Initiatives

Election Results Information System (ERIS) – General Elections & Constituent Assembly Election

- Used by Election Commission in 1994, 1999, 2008(CA)
- Data reception by fax at the control centre
- Data reception by web from district counting stations in 2008
- Information dissemination through
- Media centre (Scroll display, Ad hoc query, Intranet)
- Access to electronic media (TV, Radio)
- Access to paper media (Gorkhapatra, RSS)
- Intranet/Internet in 1999
- Strong database platform (IBM DB2) in use for CA election in 2008
- Printed reports later published in books

Local Election Results Information System

- Used by Election Commission in 2054, 2062
- Data reception by fax at the control centre 2054
- Data reception also by email from districts 2062
- Information dissemination through
- Media centre (Scroll display, Ad hoc query, Intranet)
- Intranet/Internet during 2062
- Printed reports

Integrated Voters Registration System

- Voter information collection and voters list preparation
- Devnagari Voters List Solution using IBM compatible computers
- A distributed system with centralized database at the centre and information collection, entry and voter list print from district election offices.
- Backend central database on IBM's DB2 on IBM Servers
- Client Server Architecture
- Previous user interface used Foxpro
- Later upgraded in 2004 using Visual VB

Voter's ID Card Printing & Distribution

- Voter's photograph capture
- Integrating with Voters Database
- Printing of Voter's ID card
- Distribution of ID cards through District Election Office
- 13 Constituencies including Sunsari , Baitadi and districts of Kathmandu valley in 2002

- Family Card Printing
- Invitation Card Printing for CA

2.2.2 Election Commission System Security and Authentication

With the perspective of system securities, there are two types of system in place in EC

- One which is a closed group system which is only available within the Local Area Network (LAN) system for a particular District Election Office (DEO) or EC Head Quarter (HQ) and is updated at EC HQs Central Server and distributed again to the concerned DEOs through a secured and validated process within the scope of proprietary Wide Area Network (WAN) system.

  This is the main system in operation and does not provide any physical access from users outside the network. The system comes with three layers of security systems:
  - Network Access Security
  - Application Security
  - Database Security

  The system is fully secure as long as any possible intruder has physical access to the computers in the network and knows username & password for the network and the application or the database. The database keeps track of complete audit trail of the transactions. Also these systems in the EC HQ at the central level (in Kathmandu) have backup servers. They adopt proper backup procedures for its Voters Database.

- Second is for public access through its website http://www.election.gov.np . The website is for view only purpose and hence is not interactive in the sense that it cannot be updated by public. Only during the time of Constituency Assembly Election Results, a system was setup such that an authenticated user of DEO could have access to vote count entry of the candidates to CA Election in the particular constituency for which he/she was responsible. The enter vote count was later validated and verified again at the center on the basis of fax received from the DEO separately.

2.2.3 Impression on Security Infrastructure in EC

EC is one of the first users of ICT in Government sector since 1985. Most of the existing systems in EC do not require any public interaction to the system. Its current systems are less sensitive to security concerns.

However in future, going towards e-democracy, where it may be envisaged for online application for being a registered voter of Nepal or casting of votes through Internet, Mobile, there may be sophisticated requirements for a secured infrastructure in Nepal. For example, an online voting may be possible by using PKI and some additional hardware.

More in depth study will be required for security status of systems in operation in EC in further detail.

2.3 Security System at e-Procurement System of Department of Roads (DoR)

Electronic procurement system for government was initiated by ITPF since early 2003. The public procurement portal, http://www.bolpatra.com.np. was handed over to HLCIT by ITPF in 2006 and has been changed to new URL http://www.bolpatra.gov.np. The generic eProcurement system for government is not in use due to various reasons. However, department of Roads (DOR) has started its own eProcurement system. The electronic procurement system does not use ePayment and also does not use PKI since there is no infrastructure built in Nepal so far. The eProcurement system is used for the tender publication, download, submission, opening, evaluation and its management. The system compatible with the requirements set for e-Tendering by Multi-lateral Development Banks (MDB) and PPA-2006 & regulations. The system was audited by the World Bank and has highly praised the system for its compliance to MDB requirements. DoR is successfully using the system and the response and participation of Bidders are increasing in each tender. The e-Procurement System was developed by Hitechvalley iNet.

The e-Procurement System is hosed in Linux server with firewall, Intrusion detection and server based virus verification. The system uses MySQL as database system.

The e-procurement system offers the following security features:

- Only one authorized Site Administrator shall be responsible for assigning the Buyer and administer the site.
- Site Administrator can not access individual buyer's and bidder's site.
- Site Administrator can not access the bidding information except the information on home page.
- All users, whether they are Site administrator, Bidders or Buyers, must be registered with email id and password authentication in the database of e-procurement application for access to the corresponding workspace. Passwords are stored in encrypted form (as a hash) in database. Even the Site Administrator is not able to reveal the password.
- Publishing of tender, amendments, viewing the bids, and downloading of electronically submitted bids could be done only by the Buyer who creates the notice.
  - A buyer could view the list of electronically submitted bids only after the dead line for submission of bid.
  - A buyer could download the electronically submitted bids only after the dead line for opening of bid.
- Due to the absence of PKI in Nepal, a special arrangement has been made for the confidence of bidder. A buyer could open the downloaded bids only after the dead line for opening of bid and that too, with the password from the bidder and in presence of Bidder's representatives and other officials. Buyer shall collect the bidder's Password from Auditor general's office.

- A bidder has to first register to this site to submit the bid, electronically.
- Bidding documents that submitted by the Bidders in electronic form is stored in database table in binary form and not available in web server file system. Data and documents can be accessed and opened only by the e-Procurement application.
- Bidders have to use their own password for the bidding files and separately submit their password to the Auditor General's Office.
- All time stamps used in e-procurement web application is based on the DoR server system time.

It may be possible to make the system more secured with the use of digital signature and/or eSignature.

2.4 Nepalese Banking Sector

2.4.1 Background

The history of banking in Nepal goes back to many years. With establishment of Nepal Bank Limited (NBL) in 1937 (A.D); (1994 B.S.) marks the beginning of formal banking in Nepal. Currently, NBL has 98 branches spread across the country with most probably second largest customer base. To further strengthen the financial sector and to streamline financial policies and process Nepal Rastra Bank (NRB) was established in 1956 under the Nepal Rastra Bank Act. 1955. Subsequent to this, Rastriya Banijya Bank was established in 1966 under the RBB act, the largest commercial bank in Nepal. Currently, the bank enjoys 113 branches spread across the country delivering all kinds of products and services that is available in the market. The bank has highest number of customer base in the country.

With the main objective of providing institutional credit for enhancing the production and productivity of the agricultural sector in the country, the Agricultural Development Bank (ADBN) was established in 1968 under the ADBN Act 1967, as successor to the cooperative Bank.

Since inception of Nepal Rastra Bank there has been a significant growth in both the numbers and activities of financial institutions. The rate of growth of financial institutions has increased further after open economy policy. Nepal Arab Bank Limited, currently known as NABIL Bank, was the first private sector bank established. Later, Nepal Investment Bank, previously known as Nepal Indosuez Bank was established in partner with Credit Agricole Indosuez, France. Currently, there are 27 commercial banks currently operating in Nepal.

Ever since emergence of private sector banks, information technology has been in use from the day first. This is the only sector where each and every area is being automated. The banks are more equipped and are able to cater and deliver their products and services to customers more easily, quickly and reliably. The banks are able to provide different value added products for the customer's convenient and comforts. At the same rate customers are more lured and attracted towards modern banking. With evolvement of online banking through internet which is available for 24*7 from any part of the word the people of Nepal is more comfort with modern banking. Similar is the case of Automatic Teller Machine. The use of plastic card was felt more secured. Plastic card can be used to purchase any goods or services using Point of Sale (POS) terminals.

With help of information technology this sector is most probably the only one that has maintained transparency, well regulated and pays highest tax.

Emergence of private sector banks with computerized system has forced government sector bank to reform. Not just for automation and new products and services this was very needed for accountability and transparency since all government sector banks were operated manually. World Bank, DFID and Asian Development Bank are regularly involved to

reform banking service and activities in Nepal. As part of financial reform both Nepal Bank Limited and Rastriya Banijya Bank are in the process of privatization.

Good governance, strong credit restructuring, modernization, foster competition and develop capital markets are some of the needs of banking sector for today and future growth. It is only possible through computerization current era. However, computerization possesses new threats on security and authentication. This is equally important to follow Basel II and compliances.

2.4.2 Security and Authentication in Banking System

Evolvement of networked system possesses increasing threat from internal and external system. Better computer knowledge amongst both internal staff and outside public has further raised alarm on security and authentication. The on-line real-time system further demanded enhanced secured system. The banking industry is almost fully dependent on computerized environment. One cannot think of running banking operation manually. Right from the day first it has to be on-line real-time based.

Along with banking operation many other areas are automated on the same infrastructure in order to minimize cost of ownership. It could not have been justifiable just to invest for banking operation. Introduction of email system, internet browsing, file sharing system, automation of back office areas such as attendance, payroll, inventory, asset management, remittance, SWIFT, video conferencing, CCTV monitoring and recording, etc. further raises alarm for stringent security and authentication system in banking industry's IT system.

Some of the common security and authentication system implemented in banking industries are:

1. **Network security and authentication for internal users**
   Each user is given unique user-id and password to enter into network system. Only the valid user-id and with correct password can access services available in the network system such as banking software, email, internet access, network printer, etc. For more than 3 wrong attempts to login, the user-id will be tagged as intruder. User-id will be denied access even with correct password if it is tagged as intruder. Only the higher authority can remove such tag. The system forces users to change their network password in every ninety days. The password must be of minimum six characters long. The security system is governed by **IT Security Policy** of the bank. Majority of them have implemented primary domain controller to control every end-user authority.

2. **Banking application security and authentication**
   Only those users who can access network are eligible to access banking application. These users are given unique user-id and password to access banking application. Hence, there are two layer of securities to access banking application.

As in the case of network, if more than 3 wrong attempts are made the user will be tagged as Intruder and will not be allowed to login even with correct password. This can be removed only by higher authority. In some cases, each user can only use designated terminal to access banking application despite having valid user-id and password.

Within the banking application each users belongs to a group. According to their group they can access only the specified functions and features. This also depends on the level that user belongs. According to functional level of the staff, the approving authority varies.

For each transaction or change in any data, there is maker and checker concept. The user-id with approving authority is denied with transaction rights. Calendar is maintained to allow only authorized user to access the banking operations, this includes time table. The banking application data is well secured in database. The data is accessible only from application. No one is allowed to change any data from back-end. Integrity testing confirms data consistency and validity.

3. **E-Mail security and authentication**

   Those who have access to network can access email system. Each qualified users are given unique user-id and password to access emails. They are given limited email box size. There is limitation on file size while sending as an attachment. Only the designated file extensions are allowed through email. All other extension of files are blocked from both sending and receiving. In some cases, the emails are filtered against its content using email content filtering system.

4. **Internet security and authentication**

   In order to access internet, every bank has placed firewall system to protect it from external threats. Only the designated ports are opened to safe guard the networks. To protect from hackers, NATing is used to hide bank's IP. The network is accessible only from designated IP (mostly the ISP's routers port). Along with firewall some bank also uses spam filtering. The system blocks auto generated spam mails.

   Different zones are created; the access to each zone varies depending upon the department the user belongs to. Even though the user has an access to network, the user can entertain only the valid services. The servers are protected in each zone. Depending upon requirement the sites are open to end-users. Only the specific users are given full Internet access. The proxy server controls the required sites. There is only one Internet gateway for whole organization on security ground. Gateway anti-virus along with anti-virus in each workstation, gateway Anti-spam, intrusion prevention system (IPS) and web category (URL) filtering to prevent users to visit filtered sites, system are implemented in firewall. Some of parameters that are activated are:

   a. Full routing capabilities including OSPF, BGP and Policy-routing for redundancy and load balancing.
   b. IPSec VPN with 3DES and AES/256 to connect branch office for secure banking and communication.

c. Controlling, Monitoring and blocking of Instant messaging (IM) such as Yahoo Messengers, MSN, etc. and P2P applications such as Kazaa, eDonkey, etc.

d. The firewall secures all traffic from internet as well as from branch office.

e. Separation of Internet, Demilitarized Zone (DMZ), Internal and branch office network and traffic.

f. Detection and prevention for intrusions and attacks, anti-spyware, anti-malware and anti-worm protection.

g. Hub and spoke IPSec VPN: to secure all traffics from branch office using IPSec VPNs

5. Back Office system security and authentication

As in the case of banking front office application system, only the qualified users are given unique user-id and password to access back office application. The users are tagged as intruder for attempting more than three wrong passwords.

Each branch, ATM and other interface are connected through IPSec virtual private network (VPN) to protect from external intruder access or tapping. For secured internet based transaction through eBanking and remittance site. VeriSign SSL certificate is being used for data encryption on transmission transactions. Private key and public key security is being used for Remittance application. All free USB ports are blocked including floppy disk drive and other drives.

The audit trails of internet access, its usage, etc. are on secured electronic format, which can be used for security audit or investigation in case of any problem.

2.4.3 Security and Authentication at Government Owned Banks

Brief assessment of security systems in Government owned banks are made as follows

1. Nepal Rastra Bank (NRB)

NRB is using Cisco PIX firewall with basic configuration and parameters. It is being used only to allow specific port. The security in its gateway is not at par with standard setup in other banks. Anti-virus is being used only in gateway. They are not using VPN for connectivity. Internet access is being controled against MAC address. Most of back office application are developed in-house and hence does not fully comply with the industry standard security norms. Only some of the general securities stated above are being implemented. The security and authentication system is still in premature state.

2. Nepal Bank Limited (NBL)

Almost all the security measures as stated above are being implemented. For the traffic, the applications are divided into five different levels depending upon criticality. Mission critical applications are given highest precedence on data traffic congestion situation. IP level control is being used while giving access to banking application. Standard IT

Security Policy is in place and is being complied. Access to facilities is confined to branch level.

3. **Rastria Banijaya Bank (RBB)**

   Almost all the security measures as stated above are being implemented. The implementation of primary domain control is in progress whereby the end-user will not be able to change desktop background, screen saver, desktop parameters, etc. Industry standard ForeFront is being used for Anti-virus and Cisco PIX as firewall for internet gateway. RBB yet to disable USB ports. RbB have adopted more secured Level 2 layer security. Different servers are being used for each application in different logical network. User belonging to one department cannot access application of other department.

4. **Agricultural development Bank Limited (ADBL)**

   The bank is under reform process. At this time, they do not have any security or authentication system on organization level. Few applications are being used in branch level with very basic user authentication system. The comprehensive security and authentication system will be implemented only upon completion of reform process. A new banking system is going to installed across the branches of ADBL.

2.4.4 Recommendation on Banking System Security

Viewing increasing security threats from both internal and external, each of the government banks should adopt industry standard stringent security and authentication system. The security and authentication system should address possible threat from both internal and external entities. In this changing world such security and authentication system should be regularly audited and enhanced with change in technology. This should be applied right from bank's employee to bank's customer including possible threat from outsiders such as hackers and intruders.

The time has come to secure each and every document that is being produced using IT. The document should be accessible, readable, changeable, and printable and delete only by authorized person. Each data and access type should well control. With increase number of commercial bank one has to secure its intellectual property and other critical information. There is constant flow of staff from one bank to another. Hence, this is more critical.

Each bank should have at least above stated general security and authentication system. In order to compete with foreign banks after getting into WTO by 2010 the security and authentication system should be at par with any international or multinational bank in the world.

Security Audit for Banking system, IT infrastructure and users identity authentication should be scheduled as frequently as possible.

2.5 Security System at Nepal Telecom Ltd.

Public awareness about the Internet is increasing. Every second, information is being sent and received over the Internet on a local, national, and global scale. Effective network security is now more crucial over public network.

Nepal Telecom is an ISP providing Internet Services (application and traffic) to its users. Boarder of the network is defined by users and peer boundaries.

The most common form of network security on the Internet today is to closely regulate which types of packets can move between networks. If a packet which may do something malicious to a remote host never gets there, the remote host will be unaffected. Traffic regulation provides this screen between hosts and remote sites. This typically happens at three basic areas of the network: routers, firewalls and Servers.

Router traffic: Any traffic that pass through a router or server (hosts whose primary purpose is to forward the packets of other hosts) is based on packet characteristics.

Firewall traffic: Traffic regulation or filtering that is performed via application gateways or proxies.

Servers traffic regulation: Traffic regulation that is performed at the destination of a packet. Servers are playing a smaller role in traffic regulation with the advent of filtering routers and firewalls.

Nepal Telecom (NT) uses firewall and access list to regulate different types of traffic. NT has firewall from Juniper, Fortigate and Check point to protect their Internet and Intranet network.

Filters and access lists

Regulating which packets can go between two sites is a fairly simple concept on the surface- it shouldn't be and isn't difficult for any router or firewall to decide simply not to forward all packets from a particular site. Unfortunately, the reason most people connect to the Internet is so that they may exchange packets with remote sites. Developing a plan that allows the right packets through at the right time and denies the malicious packets.

- **Restricting access in, but not out**: Almost all packets (besides those at the lowest levels which deal with network reachability) are sent to destination sockets of either UDP or TCP. Typically, packets from remote hosts will attempt to reach one of what are known as the well known ports. These ports are monitored by applications which provide services such as Mail Transfer and Delivery, Domain Name Service, and various login protocols.

- **Dynamic route filters**: Is the ability to dynamically add entire sets of route filters for a remote site when a particular set of circumstances occur. With these techniques, it

is possible to have a router which automatically detects suspicious activity and deny a machine or entire site access for a short time. In many cases this will thwart any sort of automated attack on a site.

Filters and access lists are typically placed on all three types of systems, although they are most common on routers.

NT has firewall at different places of the network for different types of traffic regulation.

- Use Line Rate ACLS on router interfaces
  - − ACLs on all interfaces on all platforms
  - − Full packet match capability
- Filters and access lists on all edge and boarder routers
- Line Rate ACLS on all Routers (core)
- Label pops on MPLS

2.6 Computer Software and ICT usage in Nepal Police

2.6.1 Background

Nepal Police is one of the government organizations in the country serving people to maintain peace and security to the society. From its establishment since 1956, Nepal Police has always worked for constitutional rights of the People and to maintain law and order in the country. Since policing is a constitutional obligation on the part of the government in Nepal, Nepal Police Organization is the main administrative apparatus in the hands of the government to safeguard people's constitutional rights and to maintain law and order in the country. Maintaining Law and Order, Crime Prevention and Investigation of Crime are the three major roles of Nepal Police in the country.

Nepal Police Computer Division is mainly responsible for providing computer facility on the basis of need and priority of Departments, Secretarial Office, Directorates, Divisions and other units within the organization. Other major roles are to develop and deploy computer software for various police offices, repairing and maintaining the computer devices, researching and providing the detailed analysis about the nature of work on the demand of those units for future reference. Except this, Computer Division also provides technical training to various police offices to generate computer literate manpower from basic to skilled level according to the annual training calendar. A central data warehouse for several police software is also maintained by Computer Division.

2.6.2 List of Software being used in Nepal Police

Below is the list of software being used by Nepal Police:

S/N	Software	Being Used By	Purpose
1	Personnel Information Management System	Personnel Administration Section	To digitize the personal records of all police officers.
2	Integrated GIS Based Digital Control Room	Metropolitan Police Commissioner's Office	To increase the work efficiency and prompt response at accident site.
3	Criminal Record System	Operation Department	To store the information about criminals
4	Party Incidents Recording System	Political Research Section	To record the incidents caused by various political parties.
5	Communication Devices Information System	Communication Division	To record the information about communication devices distributed to various police units.

6	Daily Incident Reporting System	Operation Department	To store and report the daily incidents.
7	Weapons Management System	Bhandar Section	To record the information about Weapons distributed to various police units.
8	Bhandar Management System	Bhandar Section	To store the information about logistics provided to Police officers.
9	Online Examination System	Training Section, Computer Division	To take online exams of trainings conducted by NP Computer Division
10	Hardware Management System	Hardware Section, Computer Division	To store the information about various computer accessories and computer systems maintained by Hardware Section
11	Administration Management System	Administration Section, Computer Division	To replace the manual paper based system for daily administration work
12	Nepol Intranet	All networked offices OF NP	To make NP more ICT friendly organization and less paper use and publish and maintain all the daily circulation of document in Intranet for the concern of all NP staffs.

2.6.3 Situation of Software

The software being used in Nepal Police has solved many problems; that may have taken a lot of time by manual system. The software is being used within the intranet of Nepal Police. Access to the software from outer world is restricted by use of various security measures and firewall. However, despite of the efficiency of the software, there are a lot of problems that should be undertaken thoroughly to increase the productivity of this software.

Though, there are a number of software being used in Nepal Police, the reach of those software is limited to only a number of Police Offices inside the valley. For example, the DIRS software is being used by MPCO Police Ranges Kathmandu, Lalitpur and Bhaktapur and MPCO. Similarly PMIS Software is being used only by Personnel Administration section at Police Headquarters. If we can increase the reach of this software from various regions and districts, then the efficiency of the police officers will be greatly enhanced. To use this software from Regional and District level, a private network link connecting various police offices to Police Headquarters is on the process for establishment within two months time. It will be completed all through the FOC network through private service provider. Adequate data security had been kept in mind before the operation of NP national ICT network with existing technology (routers level and firewalls and separation of public network from core database server). For monitoring all network system we have NMS and EMS server .

3.0 Available Authentication Technologies and Recommendations

This section describes the technological choices available for the Authentication.

Individual authentication in an information system takes place in a client/server context, in which the individual user is the client (a "presenter") and some computer is a form of server (the "verifier"). A user is required to authenticate his or her identity to a computer, usually as a prerequisite for gaining access to resources (access control or authorization). This is typically an explicit one-way authentication process; that is, the user authenticates himself or herself to the computer. If the user is authenticating to a computer directly (for example, when sitting at a desktop or laptop computer), there is an implicit two-way authentication; the user sees the computer with which he or she is interacting and presumably knows that it is the one he or she wishes to use.

However, if the user is authenticating to a computer accessed via a communication network, there is often no way to verify that the computer at the other end of the communication path is the one that the user is trying to contact. The user typically relies on the communication infrastructure operating properly and thus connecting him or her to the intended computer. This assumption may be violated by any of a number of attacks against the communication path, starting with the computer that the user is employing locally.

This lack of explicit, secure, two-way authentication can subvert many types of individual authentication mechanisms. If a presenter provides an identifier and authenticator to the wrong verifier, both security and privacy are adversely affected. Thus, two-way authentication is preferred so that a presenter can verify the identity of the verifier to which a secret may be disclosed. Initial authentication takes place when an individual first establishes a connection of some sort to a system. This may be a direct, very local connection, such as logging in to a desktop or laptop computer, or it may be a remote connection to a computer via a communication network. In either case, there is an assumption that future communication, for some period of time, is taking place between the two parties who were initially authenticated. For a direct connection, this assumption usually relies on physical and procedural security measures; there is an assumption that the user will log out when leaving the computer unattended and in a place where others might access it. This is a form of implicit, continuous authentication.

This assumption may not always be valid, and sometimes users are required to re-authenticate themselves explicitly to the computer periodically, to verify that they are still present. This periodic re-authentication requirement is an explicit attempt at continuous authentication, although it is not really continuous. Periodic re-authentication is also burdensome for the user and thus not commonly employed. When the connection between the user and a computer is through a network, there are many more opportunities for the connection to be "hijacked" that is, for an attacker to inject traffic into the connection or to seize the connection from the legitimate user. In remote-access contexts, it is appropriate to employ explicit measures to ensure continuous authentication. Typically, this continuity is

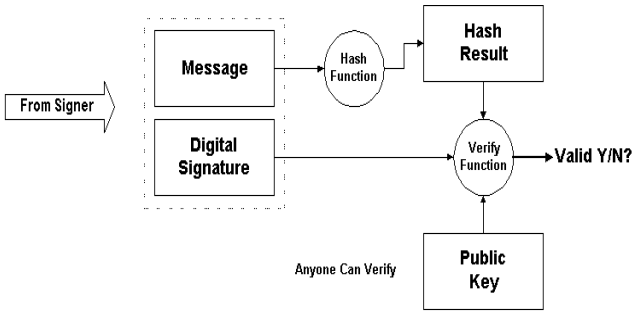
effected using cryptographic means, based on a secret (a cryptographic key) shared between a local computer employed by the user and a remote computer being accessed by the user, for the life of the connection. In this latter context, the technical term for the security service being provided is "data origin authentication." Continuous authentication is generally a result of a transition from initial, individual authentication to data origin authentication. It is the source (origin) of the data sent between two systems for example, between a user's desktop and a server that is being authenticated rather than the user per se. A further technical distinction is sometimes applied. If the authentication mechanism ensures the timeliness of the communication and thus provides protection against attacks that replay old messages, the service is referred to as "peer-entity authentication." Individual authentication increasingly takes place in the context of information systems, and thus all of the flavors of authentication described above are relevant to this discussion of individual authentication technologies.

BASIC TYPES OF AUTHENTICATION MECHANISMS

By the mid-1970s, three basic classes of authentication technologies for use with information systems had been identified. They are colloquially characterized as "something you know, something you have, and something you are". This section focuses on specific technological examples. In the first class are authentication technologies based on what an individual can memorize (know). Passwords and personal identification numbers (PINs) are the canonical examples of such technology. In the "something you have" class are physical objects that are (assumed to be) hard to forge or to alter, such as magnetic-stripe cards, smart cards, SecurID cards, and so on. The object is issued to an identified individual and retained by the individual, so that possession of the object serves to identify the individual. In the last class are biometric authentication technologies, which measure physical and behavioral characteristics of an individual. Each of these classes of authentication technologies has advantages and limitations with regard to security, usability, and cost.

3.1 Digital Signature

A digital signature is the combination of: Hash Value, Encryption (conversion) of the documents and Private Key.



The digital signature is unique and is very difficult to forge. In addition, the digital signature assures that any changes made to the document that has been signed cannot go undetected.

The person who receives your documents can use your digital signature to verify your identity, and can use your public key to send you encrypted message that only you can decrypt the message and read by using your private key.

Digital signatures are created and verified by means of cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. For digital signatures, two different keys are generally used, one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys is often termed an "asymmetric cryptosystem".

The keys of an asymmetric crypto system for digital signatures are termed the private key, which is known only to the signer and used to create the digital signature, and the public key, which is ordinarily more widely known and is used to verify the digital signature. A recipient must have the corresponding public key in order to verify that a digital signature is the signer's. If many people need to verify the signer's digital signatures, the public key must be distributed to all of them, perhaps by publication in an on-line repository or directory where they can easily obtain it.

3.2 eSignature

eSignature is the electronic equivalent of a handwritten signature. There is more to it than pasting a graphic of a signature into a text document. Electronic signature software binds a signature, or other mark, to a specific document. Just as experts can detect a paper contract that was altered after it was signed, electronic signature software can detect the alteration of an electronically signed file any time in the future.

An electronic signature is often confused with a "digital signature," because it uses digital signature technology for detection alteration. An electronic signature also requires user authentication such as a digital certificate, smart card or biometric method. In June 2000, the U.S. government passed the E-sign bill, which gives electronic signatures the same legality as handwritten ones.

3.3 Hardware based Authentication Technologies

There are many devices that won't provide access to data until they check your fingerprint. Among the best is the U.are.U Personal. Simply touching the device's fingerpad, which plugs into your USB port via a long cable, can instantly log you on to your system, decrypt data, or sign on to Web sites.

The SecurLock replaces your Windows log-on, asking you to plug in the key and type in a PIN number. Similarly, after encrypting individual pieces of data, you can require the key and PIN for decryption

Another biometric option is the Authenticam, a USB device based on technology that scans your eye before allowing access to data. This device is more expensive than the average fingerprint reader, but it can also double as a full PC video camera, able to capture both still and moving images.

Smart cards and their associated personal identification numbers (PINs) are an increasingly popular, reliable, and cost-effective form of two-factor authentication. With the right controls in place, the user must have the smart card and know the PIN to gain access to network resources. The two-factor requirement significantly reduces the likelihood of unauthorized access to an organization's network.

Smart cards provide particularly effective security control in two scenarios: to secure administrator accounts and to secure remote access.

3.4 Recommendations on Authentication

IT Policy and Electronic Transaction Act 2006 has provisioned for Public Key Infrastructure (PKI) for issuing and the security keys management, but still the Infrastructure is not in place to date. Government should amend the Electronic Transaction Act and give an open option for the users to choose from PKI and eSignature. eSignature is gaining popularity worldwide and the countries using PKI are gradually migrating to eSignature based authentication system, providing authenticity of the signature with due diligence post review.

Public Key Infrastructure (PKI), for example, is a technology which provides a high level of security through encryption and digital signatures. Authentication on the basis of digital certificates, however, requires interested suppliers to go and get the digital certificate which can put them at a competitive disadvantage with other suppliers. There is no higher security risk if the authentication during the transaction process is based on an electronic signature without certificate and verified as part of the due diligence during the post-qualification procedure.

A regulatory or legislative approach should be considered to allow e-Signature rather than digital signatures, with correspondingly greater reliance on the due diligence phase of any transaction. This latter approach would be more consistent with business practice, is less complicated and less expensive and is common in some other countries.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) has published its Guidance for Electronic Authentication in 2007.

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalization. The OECD is also at the forefront of efforts to understand and to help governments respond to new

developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organization provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organization's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

Hence it makes all sense to follow the same guidelines and recommendations instead of devising our own separate guidelines through a duplication of work:

Recognizing that trust is a key condition for many online transactions to take place, and that, within a broader system of measures and strategies, electronic authentication of persons and entities plays an important role in this respect;

Recognizing that electronic authentication, which is an essential component of the verification and management of identities online, provides a level of assurance as to whether the other party is who or what it claims to be; and thereby reduces the uncertainty inherent in domestic and cross-border electronic interactions and transactions;

Recognizing that effective electronic authentication helps to strengthen systems and network security, as well as privacy by reducing risks such as unauthorized access to personal data, identity theft and data breaches, and by providing additional means of accountability;

Recognizing that electronic authentication is an important element in the continued development of governmental and other social and individual activities online, enables the creation of new business opportunities, contributes to the development of electronic commerce, and is a key component of a viable and sustainable Internet;

Recognizing finally, that this Recommendation addresses electronic authentication of persons and entities, but does not address other aspects of electronic authentication, such as legal assurance of validity of documents or electronic signatures;

On the proposal of the Committee for Information, Computer and Communications Policy:

RECOMMENDS that Member countries:

• Work towards establishing technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities, consistent with the OECD

Guidelines for the Security of Information Systems and Networks and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

• Foster the development, provision and use of electronic authentication products and services that embody sound business practices, including technical and non technical safeguards to meet the participants' needs, in particular with respect to security and privacy of their information and identity.

• In both the private and public sectors, encourage business and legal compatibility and technical interoperability of authentication schemas, to facilitate cross-sectoral and cross-jurisdictional online interactions and transactions and to ensure that authentication products and services can be deployed at both national and international levels.

• Take steps to raise the awareness of all participants, including those in non-Member economies, on the benefits of the use of electronic authentication at national and international levels

4.0 Conclusion and Recommendations

On 26 August 1768, when Captain James Cook set sail for Australia, it took 2 years and 320 days before he returned to describe what he found there. On 15 June 2009, 20 hours of new content were posted on YouTube every minute, 494 exabytes of information were transferred seamlessly across the globe, over 2.6 billion mobile minutes were exchanged across Europe, and millions of enquiries were made using a Google algorithm.

The Digital World is a reality in all of our lives. The use of digital technology also brings about the possibility to reform governance, making it more efficient, transparent, accountable and effective. The end result is good governance with increased quality and speed of services at lesser cost. Many countries are still in their early stages of e-Governance. The Government impacts the digital economy in significant ways:

1) as a deliverer of public services;
2) as a major purchaser of ICT systems products and standards;
3) as a commissioner and controller of data and content, and gatherer, keeper and user of public and personal data; and
4) as strategic hub for development of the nation's future digital strength.

While a successful e-Government initiative means optimization in the operations and service delivery of the government, a failure in the initiative can waste a lot of money, time and effort. Hence an extremely careful e-Governance planning is important, first to design small projects that are SMART (simple, measurable, accountable, realistic and time-related), and then to be able to eventually scale and integrate all such projects so that the interaction with the government can be done through one virtual counter 24 hours a day, 7 days a week, throughout the year.

In order to consider confidence and safety of doing business online, Privacy, Authenticity, Integrity, and Non-repudiation must be ensured. Whilst ultimately, the Internet cannot be made risk-free, if it is to function effectively, governments, businesses, civil society and individual users can and must share responsibility for minimizing the risks. And due to its global nature, issues relating to governance of the Internet are often outside the jurisdiction of individual national governments and regulators. Responsibility for ensuring that Internet governance is effective therefore needs to be considered at three levels:

- at the global level, recognising the cross jurisdictional nature of today's networks;
- at the national level, on those issues where appropriate national action remains a highly effective tool; and
- at the consumer level, through appropriate action and by empowering all of us to take steps to protect themselves.

Whilst global collaboration will be increasingly important, there remains a significant and critical role for appropriate action at the National level to help shape a safer online world so that the citizens have greater confidence in public service transactions; thus yielding efficiencies and cost saving. Thus the government applications must ensure the following safeguards through a legal authentication system:

- **High Level Cyber Security:** by which we mean the approach to high level network security and to serious and organised crime and terrorism, often taking place at a supra-national level;
- **Personal Digital and Data Security:** by which we mean the approach to making consumers safer online in relation to online scams and rip-offs, identity and data privacy and personal network protection; and
- **Content Safeguards:** by which we mean protecting consumers from illegal content and protection of certain vulnerable groups from potentially harmful material, particularly children.

Besides authentication systems discussed earlier, the potential for an entirely new way of authentication can also be explored for the imminent future. Since the world will soon be moving into IPv6, another authentication system to individual device level that we are trying to conceive is assigning dedicated IP address to devices based on their unique hardware ID. For example, a PC or notebook could have its IPv6 issued based on its MAC address, while a mobile phone's IPv6 could be based on its IMEI number. Thus, individual devices will have their unique IP from which the actual hardware can be authenticated or traced. If this is managed at the national level, computer crime can be dramatically reduced, and spam and unsolicited emails can be traced back and stopped.

The following key recommendations regarding the future steps on the series of actions and studies needed:

- Next phase of detail study on Security and Authentication is necessary.
- There is need of another level of study focusing on each government applications.
- Application software and IT infrastructure security guidelines for government is utmost necessary. A basic security guideline is urgently needed.
- Security and Authentication technology assessment is needed to recommend next phase of amendment of Digital Transaction Act (Cyber Act).
- Agreed on the formulation and implementation of Security Guidelines, it may be adopted from the OECD guidelines with simple localization, without re-inventing the wheel.

References

ITPF (2003), Report on Electronic Procurement in Government, A Consultation, Documentation & Advocacy Report with the support from The Asia Foundation, Information Technology Professional Forum (ITPF), Kathmandu.

ITPF (2005), A Brochure on Digital Signature, An Awareness building brochure published with support from The Asia Foundation, Information Technology Professional Forum (ITPF), Kathmandu.

CAN (2007) Information Security Survey

Digital Britain (2009), Final Report, Presented to Parliament by The Secretary of State for Culture, Media and Sport and the Minister for Communications, Technology and Broadcasting.

OECD (2007) Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication