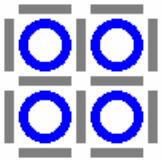
Nepal Government
Controller of Certification Authority
Ministry of Environment, Science and Technology
Singh Durbar, Kathmandu, Nepal

Government Applications and its Legal Authentication



IT Professional Forum

9 July, 2009

Presentation Outline

- General
- Government Applications in use and Authentication (not limited, but for …)
  - Inland Revenue Department Applications
  - Election Commission Applications
  - eProcurement System at Department of Roads
  - Banking System
- Authentication Technologies
- Conclusion and Feedback

General

Controller of Certification Authority (CCA)

- CCA is established under the Electronic Transaction Act 2063 (2006)
- CCA is in the process of setting up Public Key Infrastructure (PKI)

IT Professional Forum (ITPF)

- Registered professional society, team of established IT Professionals.
- ITPF members represent private, semi-government, government, academic and financial institutions in Nepal
- ITPF represents at the HLCIT and is an institutional member of CAN
- ITPF has conducted numerous policy research with respect to Electronic Transaction & Digital Signature Act, Regulations, VOIP, IPR, e-procurement, e-payments, business incubation etc.
- The Forum is also involved in academies, running M.Tech. in IT program in association with Kathmandu University

General …

This study is outcome of response to expression of interest by IT Professional Forum (ITPF) to Office of Controller of Certification (OCC) to conduct a short study on Government Applications and its Legal Authentication.

Study Objective

- 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

Overview of Study: **Content**

1.0 INTRODUCTION
1.1 Background
1.2 Study Objective and Contents
1.3 Government System Security and Authentication
1.4 Legal Framework

2.0 GOVERNMENT APPLICATION IN USE AND AUTHENTICATION
2.1 Inland Revenue Department (IRD)
2.2 Election Commission (EC)
2.3 Security System at eProcurement System of DoR
2.4 Nepalese Banking Sector
2.5 Security System at Nepal Telecom Ltd.
2.6 Nepal Police
2.7 Assessment of Authentication in Existing Applications **> Feed Back**

3.0 AUTHENTICATION TECHNOLOGIES
3.1 Digital Signature
3.2 eSignature
3.3 Hardware based Authentication Technologies
3.4 Recommendations on Authentication

4.0 CONCLUSION AND RECOMMENDATIONS

Government System Security and Authentication

- **Privacy:** Privacy is maintained while exchanging documents between government & people (G2P, G2G, G2B) over the web. No unauthorized person(s) can get access
- **Authenticity:** System must promise identity & authenticity of sender and recipient of documents and transactions.
- **Integrity:** System must guarantee on integrity of document content when exchanged across web
- **Non-repudiation:** Neither *Receiver* nor *Sender* should be in a position to deny that they had not delivered or not received

Government Applications in use

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
- 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
- Department of Transport Management
- Department of Roads
- Ministry of Environment, Science & Technology
  - National Information Technology Center (NITC)

III. Financial and Service Sector

- Nepal Rastra Bank
- Nepal Bank Limited
- Rastriya Banijya Bank
- Employment Provident Fund
- Nepal Telecom

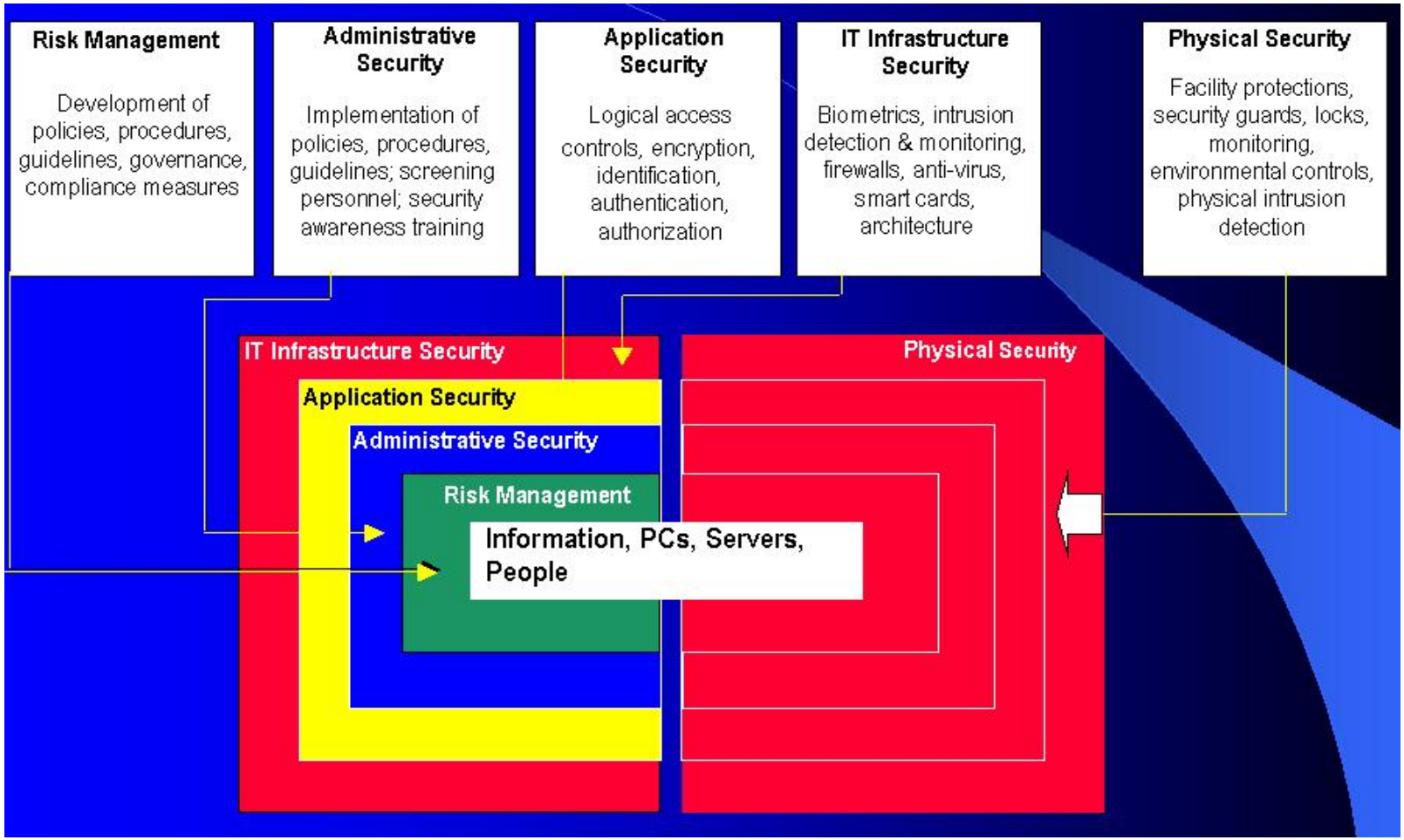
IV. Local Governments

- Municipalities

V. Judiciary

- Supreme Court / Other Courts

Security Overview



We have focused on Application & IT Infrastructure Security

Inland Revenue Department (IRD)

- The ProTax application software, which presently covers following main modules:
  - **Taxpayer registration**
  - **VAT assessment & collection**
  - **Income Tax assessment & collection**
- Revenue Administration System (RAS)
  - Revenue Collection Information System
- Some eGovernment initiatives by IRD
  - **e-PAN (Electronic Permanent Account Number) System**
  - **e-TDS (Electronic Tax Deduction at Source) System**
  - **e-Estimated Income Tax Returns System (e-IN)**
  - **e-VAT Returns**
  - **SMS System**
  - **Web Site: http://www.ird.gov.np**
- Other systems not directly related to public

Security procedure and authentication in IRD Systems

From system securities perspective, two types of system in IRD:

First: **Closed group system** which is only available within the 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 WAN

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**

Second: **New group of eGovernment** applications (**e-PAN**, **e-TDS**, **e-IN**, **e-VAT**) - annexed to closed group applications.

In order to protect central database general public is given access to a **dirty database**

Securities Levels

Applications within IRD

S. No	Product / Application	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) – *Still to be in operation*	Yes	Yes	Centralized

eProcurement System of Department of Roads (DOR)

DOR - early stage of eProcurement: without **ePayment & Certification Authority**, basically used as **eTender** system.

The eTender security features:

- **Only one** authorized **Site Administrator** shall be responsible for assigning **Buyer & Administer the site**.
- Site Administrator can not access individual buyer's & bidder's site.
- Site Administrator can not access the **bidding information** except information on home page.
- All users **must be registered with password authentication in the database** of the application for access to corresponding workspace. **Passwords are stored in encrypted form** in database. Even Site Administrator is not able to reveal password.
- Publishing of tender, amendments, viewing bids, & down loading of e-submitted bids could be done only by Buyer who creates the tender notice.
- A buyer could view list of electronically submitted bids only after dead line for submission of bid.
- A buyer could download electronically submitted bids only after dead line for opening of bid.

eProcurement System of DOR … …

- 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 eTender site to submit bid**
- Bidding documents submitted in electronic form is stored in database table in binary form and not available in web server file system.
- Bidders have to use their own password for the bidding files and separately submit their password to 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 secure with the use of Public Key Infrastructure (PKI).**

Security & Authentication in Banking System

Some of the very general security & authentication system implemented in banking industries are:

1. Network security & authentication for internal users
2. Banking application security & authentication
3. eMail security & authentication
4. Internet security & authentication
5. Back Office system security & authentication

Security and Authentication in Banking System … …

Brief assessment of security at Government owned banks:

1. Nepal Rastra Bank (NRB)

- **Cisco PIX firewall** with basic configuration & parameters
- Security in gateway is not at par with standard setup in other banks
- Anti-virus is being only in gateway, not using VPN for connectivity
- Internet access is being control against MAC address
- Most of back office application are developed in-house & hence does not complied industry standard security norms
- Only some of the general securities stated above are being implemented

The security & authentication system is still in premature state.

Security and Authentication in Banking System … …

Brief assessment of security at Government owned banks:

2. Rastria Banijaya Bank (RBB)

- General security & authentication system is 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 & Cisco PIX as firewall for internet gateway, yet to disable USB ports
- 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

Security and Authentication in Banking System … …

3. Nepal Bank Limited (NBL)

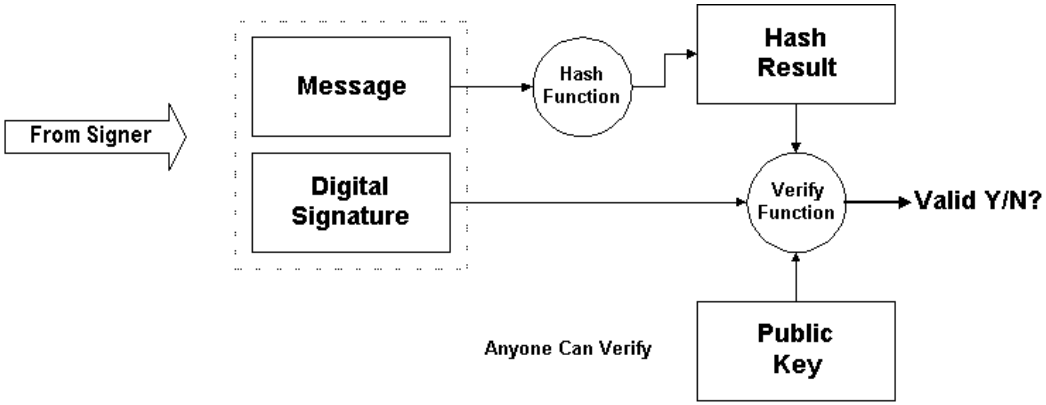
- General security measures are being implemented
- For traffic, **applications are divided into five different levels** depending upon **criticality**
- Mission critical are given highest precedence on data traffic congestion situation
- **IP level control** is being used while giving access to banking application
- **Standard IT Security Policy is in place and is being complied.**
- Access to facilities are confined to branch level.

4. Agricultural Development Bank Ltd (ADBL)

- The bank is under reform process.
- At present, do not have any security or authentication system on organization level.
- Few applications used in branch level with basic user authentication system
- The comprehensive security & authentication system will be implemented only upon completion of reform process

Authentication Technologies

1. Digital Signature



Public Key Infrastructure (PKI)

2. eSignature

- The electronic equivalent of a handwritten signature
- Electronic signature software binds a signature, or other mark, to a specific document
- An electronic signature also requires user authentication such as a digital certificate, smart card or biometric method.
- U.S. government passed the eSignature bill (June 2000), which gives electronic signatures the same legality as handwritten ones

3. Hardware based Authentication Technologies

- **Biometric Authentication**
  - USB device based on technology that scans eye before allowing access to data
  - Many devices that won't provide access to data until they check fingerprint
- **Smart Cards** and their associated personal identification numbers (PINs)
- **IPv6** authentication system to **individual device level** - dedicated IP address to devices based on their unique hardware ID.
  - eg., a PC could have its IPv6 issued based on its MAC address, while a cell phone's IPv6 could be based on its IMEI number.

Conclusion and Feedback

- Implementation of PKI or any other authentication technologies is in urgency, mainly for IRD applications and eProcurement
- There is need of in depth study for security status of systems in operation
- Industry standard security & authentication system to be implemented in banks and financial institutions
- There should be option for other security and authentication technologies like eSignature and Hardware Based (IPv6), for that initiation to amend cyber act needed
- OECD Guidelines (2007) on Electronic Authentication recommended follow, instead of creating the new one

Conclusion and Feedback … …

Government impacts digital economy in significant ways:

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

Government Applications MUST Ensure:

1. High Level Cyber Security
2. Personal Digital & Data Security
3. Content Safeguards

Conclusion and Feedback … …

Issues to resolve on Security and Authentication

- Secured Transaction
- Implementation of PKI
- Assessment of technologies (cost to users, implementation management etc.)
- … …
- … … …
- … … … … …

Thank you !

Feed back and Suggestions !

itpf@info.com.np