PKI, Digital Signature and e-Government

July 2011
Prof. Bae, Kyoung Yul
Sangmyung University
01 Introduction

02 Digital Bangladesh

03 Information Security

04 PKI & Digital Signature

05 PKI Services in Korea

06 Future Works & Conclusion
Introduction

• **Digital**
  - Generates, stores, and processes data in terms of two states: positive and non-positive.

  - A digital system uses discrete (discontinuous) values, usually but not always symbolized numerically (hence called "digital") to represent information for input, processing, transmission, storage.

  - Digital technology is primarily used with new physical communications media. Electronic transmission was limited to analog technology, which conveys data as electronic signals of varying frequency or amplitude that are added to carrier waves of a given frequency.
### Introduction

- **Digital Natives**

<table>
<thead>
<tr>
<th>How they <strong>handle</strong> information</th>
<th>Digital Immigrant</th>
<th>Digital Natives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow &amp; controlled from limited channels</td>
<td>Quickly from multiple sources</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How they <strong>view</strong> information</th>
<th>Digital Immigrant</th>
<th>Digital Natives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text before pictures, sounds and video</td>
<td>Pictures, sounds and video before text</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How they <strong>process</strong> information</th>
<th>Digital Immigrant</th>
<th>Digital Natives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequential, linear and logical</td>
<td>Random access to hyperlinks multimedia information</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

• **Data**
  – Raw, non-summarized and unanalyzed facts and figures

• **Information**
  – Data that have been converted into a meaningful and useful context for the receiver
Introduction

• Why Digital?
Introduction

• Digital Risky?
  – It may take a considerable processing time
  – It can be hard to reduce noise
Introduction

• IT Convergence

Convergence
IT Service, Computing Networking, Information Devices

Ubiquity
Anytime, Anyplace, Any Device, Any Platform, Mobility, Accessibility Seamless

Intelligence
Artificial Intelligence Context Awareness Service

Broadband
High Data Processing Power Real Time Information Processing
Introduction

• IT Prediction
  – Gartner Research: Hype Cycle of Emerging Technologies, July 2009
Introduction

• **Mobile App**
  – YouTube, Game, Entertainment, Fun etc
  – Location, Public Services
  – Augment Reality
  – One source - multi users
Introduction

- **Mobile Services**

  - **FUN**
  - **Social Network**
  - **INFORMATION**
Introduction

- Technology Paradigm

- Technology Improve

- Convergence

- Changing of Value Foundation

- Desiring for Healthy Life

- Convient Entertainment Mobility

- Material Industry: SIC, Embedded S/W, FPD, 2nd Batter
- Electronic Industry: Home appliance, Home networking, Telemetrics, HD DVD
- Broadcasting Industry: Video, Software, DMB
- Advanced Communication
- Medical Industry: DNA, Biomedical DB
- Service Industry: Financial, Logistics, Banking
- Cultural Contents: Entertainment, Game, Digital Contents
- Environment/Energy: Micro Cell & Fuel

Highly Customer needs
Introduction

Digital Bangladesh

Information Security

PKI & Digital Signature

PKI Services in Korea

Future Works & Conclusion
• National IT Strategy

United Kingdom
100% of Government Services Online by 2005
More than 50% as of End of 2001
74% Estimated by End of 2002

Canada
100% of Government Services Online by 2005

United States
Government Services & Documents Online by 2003

Australia
100% of Federal Government Services Online by 2001
90% Have Met This Target

Japan
Establishment of e-Government by 2003

Korea
100% of Government Services Online by 2006
### Digital Bangladesh

- **National IT index**
  - **Infrastructure index**

<table>
<thead>
<tr>
<th>Country</th>
<th>Internet Index</th>
<th>PC Index</th>
<th>Cellular Index</th>
<th>Main Telephone Lines Index</th>
<th>Broadband Index</th>
<th>Infrastructure Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>0.019</td>
<td>0.003</td>
<td>0.051</td>
<td>0.005</td>
<td>0.000</td>
<td>0.0158</td>
</tr>
<tr>
<td>Albania</td>
<td>0.169</td>
<td>0.019</td>
<td>0.321</td>
<td>0.117</td>
<td>0.000</td>
<td>0.1251</td>
</tr>
<tr>
<td>Algeria</td>
<td>0.083</td>
<td>0.012</td>
<td>0.414</td>
<td>0.088</td>
<td>0.019</td>
<td>0.1230</td>
</tr>
<tr>
<td>Andorra</td>
<td>0.367</td>
<td>...</td>
<td>0.633</td>
<td>0.547</td>
<td>0.485</td>
<td>0.4066</td>
</tr>
<tr>
<td>Angola</td>
<td>0.006</td>
<td>0.008</td>
<td>0.092</td>
<td>0.006</td>
<td>0.000</td>
<td>0.0224</td>
</tr>
<tr>
<td>Antigua and Barbuda</td>
<td>0.400</td>
<td>0.164</td>
<td>0.695</td>
<td>0.484</td>
<td>0.221</td>
<td>0.3891</td>
</tr>
<tr>
<td>Argentina</td>
<td>0.235</td>
<td>0.100</td>
<td>0.530</td>
<td>0.251</td>
<td>0.126</td>
<td>0.2484</td>
</tr>
<tr>
<td>Armenia</td>
<td>0.065</td>
<td>0.109</td>
<td>0.067</td>
<td>0.704</td>
<td>0.007</td>
<td>0.0894</td>
</tr>
<tr>
<td>Australia</td>
<td>0.845</td>
<td>0.848</td>
<td>0.639</td>
<td>0.506</td>
<td>0.604</td>
<td>0.6884</td>
</tr>
<tr>
<td>Austria</td>
<td>0.576</td>
<td>0.677</td>
<td>0.743</td>
<td>0.450</td>
<td>0.548</td>
<td>0.5989</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>0.110</td>
<td>0.025</td>
<td>0.257</td>
<td>0.145</td>
<td>0.001</td>
<td>0.1077</td>
</tr>
<tr>
<td>Bahamas</td>
<td>0.359</td>
<td>0.137</td>
<td>0.464</td>
<td>0.427</td>
<td>0.130</td>
<td>0.3033</td>
</tr>
<tr>
<td>Bahrain</td>
<td>0.240</td>
<td>0.195</td>
<td>0.802</td>
<td>0.271</td>
<td>0.165</td>
<td>0.3346</td>
</tr>
<tr>
<td>Barbados</td>
<td>0.003</td>
<td>0.027</td>
<td>0.085</td>
<td>0.008</td>
<td>0.000</td>
<td>0.0246</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>0.669</td>
<td>0.164</td>
<td>0.504</td>
<td>0.520</td>
<td>0.374</td>
<td>0.4464</td>
</tr>
<tr>
<td>Belarus</td>
<td>0.635</td>
<td>0.009</td>
<td>0.404</td>
<td>0.360</td>
<td>0.004</td>
<td>0.2823</td>
</tr>
<tr>
<td>Belgium</td>
<td>0.514</td>
<td>0.416</td>
<td>0.609</td>
<td>0.469</td>
<td>0.603</td>
<td>0.5222</td>
</tr>
<tr>
<td>Belize</td>
<td>0.139</td>
<td>0.168</td>
<td>0.282</td>
<td>0.128</td>
<td>0.064</td>
<td>0.1561</td>
</tr>
<tr>
<td>Benin</td>
<td>0.090</td>
<td>0.005</td>
<td>0.077</td>
<td>0.009</td>
<td>0.000</td>
<td>0.0363</td>
</tr>
<tr>
<td>Bhutan</td>
<td>0.035</td>
<td>0.017</td>
<td>0.028</td>
<td>0.042</td>
<td>...</td>
<td>0.0244</td>
</tr>
<tr>
<td>Bolivia</td>
<td>0.070</td>
<td>0.026</td>
<td>0.188</td>
<td>0.074</td>
<td>0.004</td>
<td>0.0725</td>
</tr>
<tr>
<td>Bosnia and Herzegovina</td>
<td>0.273</td>
<td>0.060</td>
<td>0.316</td>
<td>0.252</td>
<td>0.032</td>
<td>0.1887</td>
</tr>
<tr>
<td>Botswana</td>
<td>0.038</td>
<td>0.054</td>
<td>0.366</td>
<td>0.081</td>
<td>0.003</td>
<td>0.1082</td>
</tr>
<tr>
<td>Brazil</td>
<td>0.254</td>
<td>0.178</td>
<td>0.347</td>
<td>0.213</td>
<td>0.099</td>
<td>0.2181</td>
</tr>
<tr>
<td>Brunei Darussalam</td>
<td>0.488</td>
<td>0.097</td>
<td>0.437</td>
<td>0.218</td>
<td>0.086</td>
<td>0.2653</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>0.274</td>
<td>0.070</td>
<td>0.709</td>
<td>0.324</td>
<td>0.158</td>
<td>0.3071</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>0.007</td>
<td>0.002</td>
<td>0.047</td>
<td>0.007</td>
<td>0.000</td>
<td>0.0126</td>
</tr>
<tr>
<td>Burundi</td>
<td>0.009</td>
<td>0.008</td>
<td>0.011</td>
<td>0.004</td>
<td>0.000</td>
<td>0.0062</td>
</tr>
</tbody>
</table>

Source: UN e-government survey 2008
**Digital Bangladesh**

- **Asia IT**
  - E-participation index: one tool that enables governments to dialogue with their citizens

### Table: E-participation Index 2008

<table>
<thead>
<tr>
<th>Country</th>
<th>E-Information</th>
<th>E-Consultation</th>
<th>E-Decision-Making</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States of America</td>
<td>93.33</td>
<td>100.00</td>
<td>75.00</td>
<td>89.80</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>93.33</td>
<td>77.78</td>
<td>93.75</td>
<td>87.76</td>
</tr>
<tr>
<td>Denmark</td>
<td>80.00</td>
<td>83.33</td>
<td>87.50</td>
<td>83.67</td>
</tr>
<tr>
<td>France</td>
<td>86.67</td>
<td>77.78</td>
<td>87.50</td>
<td>83.67</td>
</tr>
<tr>
<td>Australia</td>
<td>100.00</td>
<td>61.11</td>
<td>81.25</td>
<td>79.59</td>
</tr>
<tr>
<td>New Zealand</td>
<td>53.33</td>
<td>100.00</td>
<td>56.25</td>
<td>71.43</td>
</tr>
<tr>
<td>Mexico</td>
<td>60.00</td>
<td>88.89</td>
<td>50.00</td>
<td>67.35</td>
</tr>
<tr>
<td>Estonia</td>
<td>73.33</td>
<td>66.67</td>
<td>56.25</td>
<td>65.31</td>
</tr>
<tr>
<td>Sweden</td>
<td>60.00</td>
<td>50.00</td>
<td>68.75</td>
<td>59.18</td>
</tr>
<tr>
<td>Singapore</td>
<td>66.67</td>
<td>83.33</td>
<td>18.75</td>
<td>57.14</td>
</tr>
<tr>
<td>Ukraine</td>
<td>53.33</td>
<td>61.11</td>
<td>37.50</td>
<td>51.02</td>
</tr>
<tr>
<td>Jordan</td>
<td>20.00</td>
<td>61.11</td>
<td>62.50</td>
<td>48.98</td>
</tr>
<tr>
<td>Viet Nam</td>
<td>33.33</td>
<td>44.44</td>
<td>62.50</td>
<td>46.94</td>
</tr>
<tr>
<td>Bhutan</td>
<td>20.00</td>
<td>44.44</td>
<td>68.75</td>
<td>44.90</td>
</tr>
<tr>
<td>China</td>
<td>46.67</td>
<td>27.78</td>
<td>56.25</td>
<td>42.86</td>
</tr>
<tr>
<td>Argentina</td>
<td>66.67</td>
<td>44.44</td>
<td>12.50</td>
<td>40.82</td>
</tr>
<tr>
<td>Brazil</td>
<td>40.00</td>
<td>33.33</td>
<td>50.00</td>
<td>40.82</td>
</tr>
<tr>
<td>Colombia</td>
<td>73.33</td>
<td>22.22</td>
<td>25.00</td>
<td>38.78</td>
</tr>
<tr>
<td>Mozambique</td>
<td>46.67</td>
<td>38.89</td>
<td>31.25</td>
<td>38.78</td>
</tr>
</tbody>
</table>

*Source: UN e-Government Survey 2008*
Digital Bangladesh

• Use of ICT in Governance
  – United Nations E-Government Survey 2010
  – Bangladesh is ranked 134.

Source: Bangladesh Computer Council, 2010
Digital Bangladesh

• **Use of ICT in Governance**
  – Critical factors in implementing e-government in Bangladesh

![Critical Factors](chart.png)

Source: Success and Failure Factors for e-Government projects implementation in developing countries: A study on the perception of government officials of Bangladesh, Chowdhury Golam Hossan, 2006
Digital Bangladesh

- ICT enabled connected Governance

ICT-enabled connected governance contributes to:

**Internally**
- Avoidance of duplication
- Reducing transaction costs
- Simplifying bureaucratic procedures
- Greater efficiency
- Greater coordination and communication
- Enhanced transparency
- Information sharing between agencies
- Security of information management

**Externally**
- Faster service delivery
- Greater efficacy
- Increased flexibility of service use
- Innovation in service delivery
- Greater participation
- Greater citizen empowerment
- Citizen participation

source: un e-government survey 2008
• The application of ICT in interactions between
  – Government and Citizens
  – Government and Businesses
  – Government and Employees
  – Government and Government

Publish
Interact
Transact
Integrate
Transform

Information available online
Two-way communication
Transaction handled online
Process, system and organisational integration
Entirely new services delivered cross-agency through a centralized enterprise portal
Digital Bangladesh

• Use of ICT in Governance
  – Constraints and Recommendations

**Constraints**
- Inadequate Access to ICT
- Public Awareness about ICTs
- Lack of integrated approach
- Lack of regulatory/legal framework
- Absence of processes and systems

**Recommendations**
- Create one-stop government portal
- Prioritization of Services
- Improve ICT access by citizens
- Emphasize Bangla interface for citizen services
- Need training and leadership from the government
- Awareness for the use of Open Source
- Payment Gateway

Source: Bangladesh Computer Council, 2010
Digital Bangladesh

- **Legal Infrastructure & Policy**
  - 2000: Copyright Act enacted with inclusion of Software and ICT
  - 2001: First ICT Policy drafted
  - 2002: National ICT Policy adopted
  - 2006: ICT Act enacted
  - 2008: Revised Policy Drafted
  - 2009: New ICT Policy approved
  - 2010: Rules for Digital Signature (Certifying Authority)

Source: Bangladesh Computer Council, 2010
Digital Bangladesh

• Building confidence and Security in the use of ICT
  – Network Security Policy
  – Cyber Laws: Formulated
  – Digital Signature: Law Formulated
  – Privacy Law: Approved
  – Intellectual Copyright: Approved
  – Anti Piracy Law: Approved
  – Cyber Crime unit: Established

Source: Expert Group Meeting on Regional Cooperation towards Building an Information Society in Asia and the Pacific, 2009
Digital Bangladesh

To improve Government efficiency and promote interaction between governments Ministry/Divisions, Departments, Districts and Upazillas by construction of Government network infrastructure.

To use ICT system within the public administration to improve efficiency and transparency, reduce wastage of resources, enhance planning and raise the quality of services.

To maximize the computerization of work processes and resources through integrated information management system enabling real time administration.

Source: Bangladesh Computer Council, 2010
Digital Bangladesh

- Digital Government for Services Delivery
  - Two sub-components: e-Citizen, e-Admin

Source: Bangladesh Computer Council, 2010
• **e-Citizen services**
  – Requires: Innovative service design; Suitable delivery channel
  – Leads to efficient delivery avoiding face-to-face contact;
    • Examples: Ticket info using SMS, bill pay, etc.

• **e-Administration:**
  – Encapacitate civil servants;
  – Reengineering administrative processes;
    • Examples: MPO management at BANBEIS, Custom House Automation
• **BanglaGovNet**
  - It is a Public Network to connect all the Government entities throughout the country under a single Network.
  - To ensure a Basic Infrastructure for e-Government.
  - To ensure a Secured Connectivity among all the Government entities.
  - To ensure e-Governance through an integrated common platform

Source: Bangladesh Computer Council, 2010
### Digital Bangladesh

#### BanglaGovNet

<table>
<thead>
<tr>
<th>Phase</th>
<th>Year wise Plan</th>
<th>Scope of Work</th>
<th>Estimated Budget (US Dollar)</th>
<th>Main Solutions</th>
</tr>
</thead>
</table>
| I (BanglaGovNet) | Apr 2010 ~ June 2014 | - National ICT Center (NICTC)  
- Ministries/Divisions (45)  
- Major Departments (>100)  
- District Offices (64 DICTC)  
- Upazila Offices (64 UICTC) | 40.21 Million | - E-mail  
- Security Solutions  
- E-Document  
- Government WEB  
- G2G |
| II (Info-Sarker) | July 2011 ~ Dec 2015 | - Expand Network to Upazila level  
- Interoperability between Central and Local Govt. Administration  
- Development of Bangladesh Education Network ("BanglaEduNet") => Primary & Secondary level Education  
- Connecting High level education Institutions  
- Making an ICT-driven society  
- Final preparation for Digital Bangladesh | 150 Million | - e-Education  
- e-Procurement  
- e-Financial Services  
- e-Local Government  
- e-Community  
- G2B, G2C, G2P  
- Etc |

Source: Bangladesh Computer Council, 2010
03  Information Security
Information Security

• Security
  – Freedom from risk or danger; safety.
  – Freedom from doubt, anxiety, or fear; confidence.
  – Something that gives or assures safety, as:
  – A group or department of private guards: Call building security if a visitor acts suspicious.

• Measures adopted by a government to prevent espionage, sabotage, or attack.
• Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant….etc.
Information Security

• Network and Data Security

**Network Security**
- Identity validation
- Confidentiality
- Integrity
- Non-Receive Repudiation

**Data Security**
- Identity validation
- Confidentiality
- Integrity
- Non-Sending Repudiation

- It must be developed to prevent many dangerous things (hacking, illegal forgery) from data transfer on the internet.

- It must be developed to prevent illegal forgery and validation for stored data.
Information Security

- **Internet Incident**

  **Malicious Activity**
  - 2007 1/2: 30% (USA), 9% (44%)
  - 2007 2/2: 31% (USA), 10% (42%)

  **Malicious BOT Infection**
  - 2004: 25% (UK), 9% (3%)
  - 2005: 26% (USA), 4% (8%)
  - 2006: 26% (China), 11% (12%)
  - 2007: 31% (USA), 15% (12%)

  **Attack Origin**
  - 2004: 30% (USA), 4% (4%)
  - 2005: 31% (USA), 10% (2%)
  - 2006: 33% (USA), 9% (2%)
  - 2007: 31% (USA), 10% (2%)

  **Phishing Sites Host**
  - 2004: 60% (USA), 2% (4%)
  - 2005: 56% (USA), 3% (9%)
  - 2006: 44% (USA), 6% (3%)
  - 2007: 33% (USA), 9% (3%)

Source: www.kisa.or.kr
• Security Challenge

Leakage of the personal Inf.

---

**ISP**

- Sales of 6 MM customer information to telemarketing company for 2yrs
- Sales is controlled by the board of directors

**Korean eBay Site**

- DB Server is hacked by hackers (2008.4.)
- 10 MM customers’ personal information including banking

Suspend biz for 3 months
Financial compensation

Loss customer’s trust
Financial compensation

source: www.kisa.or.kr
• Information Security
  – Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.
  – To achieve business objective
Information Security

- Information Security

Security Properties
- Confidentiality
- Integrity
- Availability

Information States
- Processing
- Storage
- Transmission

Security Measures
- Policy & Procedures
- Technology
- Education, Training & Awareness
04 PKI & Digital Signature
PKI & Digital Signature

• Personal Information Flow
• Electronic Signature
  - It is a unique information which identifies a person who made an electronic document and confirms whether the electronic document has been modified or not. The electronic document has functions such as self-identification, secret protection and prevention of tampering, forging document and denying himself.
• **Weakness of Electronic Document**
  – The 3rd party can send documents deceiving he is the transmitter.
  – The document can be modified in the middle of the transmitting process by 3rd party.
  – The receiver can be easily deceived and it is difficult for receiver to verify.
PKI & Digital Signature

- Requirement of Electronic Signature

- **Identification**
  - Person who owns the key is the one who performs electronic signature

- **Not forgeable**
  - Person who does not have key cannot create electronic signature

- **Not changeable**
  - Person who does not have key can modify electronic document

- **Not reusable**
  - Electronic signature of document A cannot be replaced by electronic signature of document B

- **Not repudiation**
  - Prevent from repudiate the act of signing for person who has the key and has performed electronic signing
- **Electronic Signature**
  - To secure the stability and the reliability of electronic documents
    - Electronic signature
  - Functions of electronic signature
    - Identification; Authentication
    - Integrity of Electronic document
    - Confidentiality
    - Non-repudiation
    - Fulfill conditions of written document and signature
  - Introduction to authentication system to secure stability and integrity of electronic signature and to activate usage of electronic documents.
PKI & Digital Signature

- **PKI**
  - A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

<table>
<thead>
<tr>
<th>Security Services</th>
<th>Threat</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticity</td>
<td>Unauthorized User</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data Leakage</td>
<td>Encryption</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data Forgery</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Repudiation</td>
<td>Digital Signature</td>
</tr>
</tbody>
</table>

![Diagram showing PKI and related concepts]

- **PKI Components**
  - **Certificate Authority (CA)**
    - Root-CA
  - **Registration Authority (RA)**
    - Certificate Management
    - Operation Management
  - **Certificate**
    - Registration
    - Issue
    - Revoke
    - Renew
  - **Corporation**
  - Individual
  - Server
  - S/MIME
PKI & Digital Signature

- **PKI**

  \[ PKI = \text{Regulations, PKI Standards} + \text{PKI System, Facility and Equipment} + \text{Operation} \]

  **Server-side software**

  **Digital Signature**

  **Client-side software**

  **PKI Client**

  (PC/Phone/PDA/Mobile Device)

  **CA (Certificate Authority)**

  **DS (Directory Server)**

  **RA (Registration Authority)**

  **PKI Server**

  **Repository**

  **Certificate**
• PKI Component

**Certificate Authority**
- Issue or distribute the certificate for other CA, End Entity, RA.
- handle revocation request from the owner of certificate or RA.
- publish certificate and CRL to directory server
- issues the cross-certificate and manages

**Registration Authority**
- identify the user and register the user information
- transmit certificate request to CA.
- search certificate and CRLs from directory server.
- request the certificate revocation

**Directory System**
- store certificates (End Entity, RA, CA) and CRLs
- support LDAP (Lightweight Directory Access Protocol)
PKI & Digital Signature

- PKI Component

  - **End Entity**
    - Manage the certificate with certificate management software published by CA.
    - Create digital signature and verify that.

  - **Online Certificate Status Protocol System (OCSP)**
    - OCSP is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
    - Can choose as an alternative to certificate revocation lists (CRL).
    - Can confirm a current status of the certificate immediately.

  - **Time Stamping Authority (TSA)**
    - TSA's role is to time-stamp a datum to establish evidence indicating that a datum existed before a particular time.
    - Verify that a digital signature was applied to a message before the corresponding certificate was revoked.
    - Indicate the time of submission when a deadline is critical, or to indicate the time of transaction for entries in a log.
### PKI & Digital Signature

**PKI Functions**

- When to apply PKI techniques in each business unit, Security functions (Authentication, Integrity, Confidentiality, Non-repudiation) are applied as follows:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Matched security method</th>
<th>Protection Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficult to verify user</td>
<td>Authentication of identity</td>
<td>Digital Signature Technology (User authentication)</td>
</tr>
<tr>
<td>Easy to make forgery or modification on contents</td>
<td>Guarantee Integrity</td>
<td>Digital Signature Technology (Message authentication)</td>
</tr>
<tr>
<td>Breach information</td>
<td>Confidentiality</td>
<td>Encryption Technology (Message authentication)</td>
</tr>
<tr>
<td>Repudiate transactions</td>
<td>Non-repudiation</td>
<td>Digital Signature Technology (Message authentication)</td>
</tr>
</tbody>
</table>
PKI & Digital Signature

• PKI Terminology
  – Hashing functions
  – Symmetric encryption and decryption
    • Session key
  – Asymmetric encryption and decryption
    • Key pair
  – Digital signature
  – Digital certificate
  – Certification Authorities (CA)
  – Registration Authorities (RA)
  – Hierarchy of trust
PKI & Digital Signature

- **Hashing Function**

  It was the best of times, it was the worst of times

  Small Difference

  Hash Function

  Examples: MD5 (128 bit), SHA-1 (160 bit)

  It was the best of thymes, it was the worst of times

  Large Difference

  Hash Function

  3au8 e43j jm8x g84w

  b6hy 8dhy w72k 5pqd

Examples: MD5 (128 bit), SHA-1 (160 bit)
• **Symmetric Key Cryptography**
  – Problems:
    • Alice and Bob must agree on the secret key without anyone else finding out
    • Anyone who intercepts the key in transit can later read, modify, and forge all messages encrypted using that key
PKI & Digital Signature

- **Asymmetric Key Cryptography**
  
  - Problems:
    - Key exchange has to be done in a secure way
    - Encryption and decryption are extremely SLOW

![Diagram of Asymmetric Key Cryptography]
PKI & Digital Signature

• Creating Digital Signature

Message or File

This is the document created by Gianni

Message Digest

(Typically 128 bits)

SHA, MD5

Signatory's private key

Digital Signature

Asymmetric Encryption

RSA

Py75c%bn

3kJfgf*£$$

Generate Hash

Calculate a short message digest from even a long input using a one-way message digest function (hash)

Signed Document

Signatory's private key
• Verifying Digital Signature

Digital Signature

Jrf843kjf
gf*£$$&Hd
if*7oUsd
*&,<CHD
FHSD(**

Asymmetric
decryption
(e.g. RSA)

Py75c%bn&*)
9|fDe^bDFaq
#xzjFr@g5=
&nmdFg$5kn
vMd’rkvegMs”

Signatory’s
public key

Everyone has
access to trusted
public key of the
signatory

Are They Same?

? == ?

Same hash function
(e.g. MD5, SHA…)

This is a really long
message about Bill’s…

Original Message
• Certificate Like

- **DN**: cn=Bob Smith, ou=MBS, c=CA
- **Serial #**: 8391037
- **Start**: 1/5/00 1:02
- **End**: 7/5/01 1:02
- **CRL**: cn=CRL2, ou=MBS, c=CA
- **Key**: Unique name of owner
- **CA DN**: ou=MBS, c=CA
- **Unique serial number**: Period of validity
- **Revocation information**: Public key
- **Name of issuing CA**: CA’s digital signature on the certificate
PKI Services in Korea
PKI Services in Korea

**Stage of PKI in Korea**

1. **Stage 1 Introduction** (1999 ~ 2001)
   - Enacted Digital Signature Law
   - Designated accredited Certification Authority
   - Promotion of Digital Signature usage
   - Interoperability among accredited CAs

2. **Stage 2 Take-off** (2002 ~ 2005)
   - Providing User-friendliness (UI Guidelines, Storages)
   - Increasing in certificates and applications rapidly
   - Mandatory use of certificates (Banking, Stock)
   - Cross Certification for NPKI and GPKI

3. **Stage 3 Maturity** (2006 ~)
   - Upgrading of PKI technologies (RFC3280, RSA 2048)
   - Addition of Root CA Certificate to Microsoft IE for secure web server
   - Providing users with secure environment (HSM)
PKI Services in Korea

• Management of PKI in Korea

- MIC
  - Arrangement of law and decree
  - Planning national authentication
  - Accredited CA management

- KISA (Root CA)
  - National authentication system operation
  - Field test for accredited CA designation
  - Issuing certificate for accredited CA

- Accredited CA
  - Operation management of CA center
  - Providing CA services
  - Certificate issuance
  - Certificate termination / renewal
PKI Services in Korea

- Government PKI & National PKI

<table>
<thead>
<tr>
<th></th>
<th>GPKI</th>
<th>NPKI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Act</strong></td>
<td>Established in 2001 pursuant to E-Government Act</td>
<td>Established in 1999 under Electronic Signature Act</td>
</tr>
<tr>
<td><strong>Ministry in Charge</strong></td>
<td>MOPAS (Ministry of Public Administration and Security)</td>
<td>KISA (<a href="http://www.rootca.or.kr">http://www.rootca.or.kr</a>)</td>
</tr>
<tr>
<td><strong>Root CA</strong></td>
<td>GCMA (<a href="http://www.gpki.go.kr">http://www.gpki.go.kr</a>)</td>
<td>KISA (<a href="http://www.rootca.or.kr">http://www.rootca.or.kr</a>)</td>
</tr>
<tr>
<td><strong>Main Customer</strong></td>
<td>Public Servants</td>
<td>Individual, Company</td>
</tr>
<tr>
<td><strong>Algorithm</strong></td>
<td>NEET (not open)</td>
<td>SEED, AES</td>
</tr>
</tbody>
</table>

- Types of Accredited Certificate and Fees

<table>
<thead>
<tr>
<th>Types</th>
<th>Entity</th>
<th>Certificate Usage Field</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td>All electronic transactions</td>
<td>US$ 4/year</td>
</tr>
<tr>
<td>Individual</td>
<td></td>
<td>All electronic transactions</td>
<td>US$ 100/year</td>
</tr>
<tr>
<td>Corporation</td>
<td></td>
<td>G2C, Bank, Insurance</td>
<td>Free</td>
</tr>
<tr>
<td>Specific</td>
<td></td>
<td>G2C, Stock, Insurance</td>
<td>Free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>G4C, Credit Card</td>
<td>Free</td>
</tr>
</tbody>
</table>
PKI Services in Korea

- Government PKI & National PKI
PKI Services in Korea

- **PKI in e-Government Applications**
  - **Regional Administration**
    - Service for counties
    - Access with certificates
  - **Taxation**
    - National Tax Agency
    - Access with certificates
  - **Petition Service**
    - Identify oneself online by certificates
  - **Personal Management inside Government**
    - All employees inside Government
  - **National Financing Information System**
    - Based on Internet banking, etc
  - **Digital Signature & Seal**
    - Distribute certificates
    - Develop and enhance system adopting certificates
  - **E-Supply (G2B)**
    - Online bidding with certificate
  - **Electric document system**
    - Interoperable with other systems
  - **Enhance computerization**
    - Sharing national resource information
  - **Education Administration System**
    - Teachers can assess with cert.
  - **4 Major Insurances data exchange**
    - Labor, Medical care, Pension, Industrial disaster
    - Internet access with certificate
PKI Services in Korea

• **PKI Services**
  
  – **Internet Banking**
    
    • 19 Banks and Post Office provide internet banking service based on accredited certificate
    
    • Internet banking users must use the accredited certificate for secure online transaction ('02. 9)
PKI Services in Korea

- **PKI Services**
  - Public Services
    - Housing subscription deposit system, Education, Medical information, e-bidding ('06)
    - Housing subscription, the year-end tax adjustment, NEIS, National health Insurance, etc.
PKI Services in Korea

- PKI Services
  - Mobile Banking
    - Mobile banking service with certificate ('07~)
    - Transferring a certificate from PC to mobile phone
    - Generating electronic signature in mobile phone
E-Procurement in Korea (KONEPS)
Characteristics of KONEPS

Integration of entire procurement work
- All business is conducted via the internet (registration, bid notice, bidding, contracting, payment); one click purchase at online shopping mall

Single Window
- Integrated provision of all bid information
- One time registration at KONEPS suffices participation in all tenders

One-stop service
- About 400 types of documents are exchanged electronically by using the linkage with 90 external systems
E-Tendering Flow for KONEPS

1) Issue encryption key
2) Tender Notice
3) Bid Opening
4) Verify decryption key

3) Record bidding time
3) Bidding (w/digital signature)

3) Submit warrantee (upon bidding)
2) Tender Notice
3) Award Notice

3) Free payment

Surety Companies
Supplier
Authentication Authority

KFTC: Korea Financial Telecommunications & Clearings Institute
NIA: National Information Society Agency
- Reliability and Stability in e-Transactions are secured through PKI and Digital Signature

- Decryption key for the Bid
- Result Opening
KONEPS Security

Network Security
- Separation of Intranet and Extranet, Dual Fire-wall, Intrusion Detection System, Security Solutions, etc
- Periodic Security Check-up

System Operation complying with ITIL
- Check and Balance between PPS and outsourced Operator, Programmers and System managers

Access control to system, program and D/B
- National Computing & Information Resources Center
- Automatic management of log access and program modification history, post-verification system
- On-line monitoring of program modification by the independent body

System Stability against accidents
- Dual operation of servers and networks, Back-up Center(Data mirroring), ITSM
Transparency of Public Procurement

Real time disclosure of entire contract process

- Bidders can have real time info on the progress of bidding and contract
- Eligibility test for successful bidder through KONEPS

Inspection/payment thru internet

- No need to visit procurement offices
KONEPS Helps to Expand e-Commerce

E-Procurement by KONEPS

- Application of digital signature authentication in e-Bidding
- Certified authentication for enterprises mainly for e-Procurement
- Gov’t & enterprises jointly used certified authentication electronically ⇒ Expanding e-Commerce base

Development of e-Authentication industry

- Promoting technological base for e-Procurement including digital signature and security
- Encouraging firm establishment of certified authentication market including internet baking and online stock trading

Graph showing growth from 1.9m to 11.9m between 2001, 2003, and 2007.
Future Works
• **Advanced Trends**

  **The major trends at a glance**

  - Advance of the Internet
  - Advance of mobile communication
  - Bandwidth evolution
  - Convergence of digital industries*
  - Advance of e-commerce

**Services are key**

*The end user is interested in services and applications only, the underlying technology is not relevant to her or him.*

**From Technology-driven, to service-driven**
• **General PKI Issues**
  
  – PKI technologies have been matured
    * However, lack of killer applications
  
  – Long term signature retention is necessary
    * Stable standards are needed for signature verification capability over long term period
  
  – PKI supports high assurance security
    * Many applications will reside on web services
  
  – Trusted validation authority
    * Out source validation service from client
Future Works

• PKI in Korea
  – Establishing a reliable u-Authentication System
  – Extending the authentication means to Biometric, OTP with PKI certificate
  – Extending the authentication object to devices
  – Developing new PKI business model
Future Works

• Considerable PKI Service in Bangladesh
  – Government Procurement System
  – Utility Bill Payment -Gas & Electricity
  – Law Web Portal
  – Process Automation –Bangladesh Bank
  – Automatic Clearing House –Bangladesh Bank
  – Bangladesh Post Office Online
  – Service Ticketing System
Thank You

You have to leave the city of your comfort and go into the wilderness of your intuition.

What you’ll discover will be wonderful.

What you’ll discover is yourself.

- Alan Alda