Activity: Workshop on Government Procurement Modernization in the Caribbean
Topic: Digital Signature, E-Government Procurement
Title: Demystifying Authentication & Digital Signatures, PKI, ETA
Speaker: Dainsworth Richard
Country: Jamaica
Date: May 13th, 2008
Demystifying Authentication & Digital Signatures, PKI & ETA

Dainsworth Richards
CEO (Actg.)

Modernizing Government Procurement in the Caribbean
May 15, 2008
Gran Bahia Principe, Runaway Bay, Jamaica
Vision & Mandate of CITO

To lead in establishing a world-class national ICT sector, with Jamaica becoming the regional leader in ICT development

Mandate Components

- Key Contributor to E- Enabling of Jamaica
- Champion of the
  - National ICT Strategy
  - National e-Readiness Programme
- GoJ ICT Standards Body
- ICT Best Practices Repository
Core Mission

Cabinet Decision 2001

- The Cabinet approved that proposals for the procurement of computer hardware, software and services should be submitted to the Central Information Technology Office (CITO).

- The Cabinet approved the establishment of CITO to coordinate the implementation of the National Information Technology Strategic Plan and assist Government Ministries in the development and monitoring of sectoral information technology plans, among other things.
Research & Reference Analysis
  • Local Situational Analysis
  • Global References – 9 countries
  • International Development Programmes
Extensive stakeholder consultations
Flagship Initiatives and timelines
Inclusive Enabling Operational Framework
Master Implementation Plan
Integration into Jamaica 2030 plan
Electronic Transactions Act (ETA)

- Effective since April 2, 2007
- Affects ALL Jamaican legislation which refers to “writing”:
  
  \[E\text{-information} = \text{written information}\]

- E-Information admissible in court
- Applies to all e-transactions
- Key consumer protection provisions
- Secure confidence for in e-commerce in the Jamaican jurisdiction
Electronic Transactions Act (ETA)

- Act confirms legal basis for:
  - Purchase of goods and services online
  - Privacy and security of our E-transactions
  - Transacting E-business and E-Filing with Government departments

- We have been conducting such transactions for years but the ETA now establishes legal basis
E-Signatures – ETA

- Clear method to identify signatory
- Method is reliable
- Uniquely linked to signatory
- Capable of identifying signatory
- Signature-creation under sole control of signatory
- Subsequent alteration is detectable
The ‘PAIN’ of Online Transactions

(P)rivacy / Confidentiality

Interception

Is my communication private?

(I)ntegrity

Modification

Has my communication been altered?

(A)uthentication

Fabrication

Who am I dealing with?

(N)on-repudiation

Not Sent

Claims

Not Received

Who sent/received it and when?
Where do Digital Signatures come in?

- Passwords are a weak method of authentication.
- Passwords do not ensure integrity.
- Passwords can be broken, guessed, leaked, extracted, etc.
- A Digital Signature cannot be duplicated, guessed, broken, etc.
- No legal protection for disputes in case of other authentication methods.

*Digital Signatures are an effective remedy against ‘PAIN’ of e-Transactions.*
Digital Signing

Electronic Data

Hash Function → Hash Result → Signing Function

Electronic Data → Signed Data

Only Private Key holder can sign
Digital Signature Verification

Anyone can verify identity of sender

Electronic Data

Hash Function

Hash Result

Digital Signature

Verify Function

Hash Result

Signed Data

Public of A

Valid compare Yes / No ?

So the receiver can compare hashes to verify the signature

www.cito.gov.jm

Enabling a World-Class National ICT Sector
The ‘PAIN’ of Online Transactions

(P)rivacy / Confidentiality:
- Interception
- Is my communication private?

(I)ntegrity:
- Modification
- Has my communication been altered?

(A)uthentication:
- Fabrication
- Who am I dealing with?

(N)on-repudiation:
- Not Sent → Claims → Not Received
- Who sent/received it and when?
ETA, PKI & The Trade Board

- Public Key Infrastructure (PKI): is a system that enables secure e-government and e-transactions by allowing an individual/entity to identify themselves once to a Certification Service Provider (CSP), which will then vouch for that person/entity’s identity when they interact with other entities over the internet.
ETA, PKI & The Trade Board

- Digital Certificate: A digital/electronic document issued by a CSP that verifies a person/entity’s identity. Similar to a passport or drivers licence which ties personal details to a photograph. The digital certificate ties personal details to a public key – hence associated private key.

- Certification Service Providers (CSP), as defined in the ETA, are the trusted third party in an online transaction.
Role of the Trade Board Jamaica

- Be the Certifying Authority for CSPs
  - Registration and Regulation of CSPs
  - Authorise and regulate the issue of certificates by CSPs.
  - Authenticate certificates issued by any local or overseas CSP
- Issue Certificates – Act as CSP for government primarily
- Co-operate with overseas CAs in establishing a system of mutual certification
Components of PKI

- Certification Authorities (CAs) / Certification Service Providers (Issuers)
- Registration Authorities (RAs) / Certifying Authority (Authorize the binding between Public Key & Certificate Holder)
- Certificate Holders (Subscribers)
- Relying Parties (Validate signatures & certificate paths)
- Repositories (Store & distribute certificates & status: expired, revoked, etc.)
Digital Signatures, PKI and E-Procurement
Where does Buyer use PKI?

- Secure Login
- Tender floating
- Corrigendum
- Secure communications with vendors
- Tender opening
- Clarifications and negotiations
- Digitally signed PO/WO
- Digitally Signed Archives
Where does Vendor use PKI?

- Secure Login
- Secure storage of content
- Tender submission
- Encryption using buyer’s public key
- Clarifications and negotiations
Dainsworth Richards
CITO
Thank You

drichards@cito.gov.jm