Public Key Infrastructure (PKI) – In Depth

26 – 30 October 2015
Port of Spain, Trinidad and Tobago

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Overview

This 5-day course is designed to provide participants with an understanding of the PKI and the issues surrounding its implementation. This training is considered essential for anyone who needs to understand the PKI-related solutions (digital signature, time stamping) that are of fundamental importance to the design and the implementation of security critical online services. It covers the issues and the technologies involved in PKI in depth and gives hands-on practical experience of setting up and maintaining a variety of PKI solutions.

For more information about this course, or to register, contact us on:
Tel: +44 (0) 208 600 3800
Fax: +44 (0) 208 600 3819
Email: h.muchando@cto.into

OBJECTIVES

The course aims to:

- Explain the modern cryptographic techniques and protocols.
- Examine the basic concepts of a PKI and its components.
- Provide the latest developments on digital identity, digital signature mechanisms, time stamping and electronic proofs to be used in the context of cyber-criminality.
- Give the latest cryptographic solutions and their potential use in protecting the critical infrastructures.
- Explain how building a trust and secure environment help in promoting the digital interactions between government and citizens (G2C), government and businesses/commerce (G2B), and also between government and governments/ agencies (G2G).

TARGET AUDIENCE

This course is ideal for telecommunications managers, executive professionals, technical officers and professional staff such as engineers, IT administrators, technical, policy, legal and regulatory officers.

COURSE OUTLINE

Building Trust in a Digital World

- Security objectives: authentication, integrity, confidentiality and non-repudiation
- Threats in real-world scenarios and security concerns in e-business
- Role of the modern cryptography in information security

Elements of PKI

- PKI Architecture
  - Root CA
  - Subordinate CAs
  - Bridge CA
  - Cross-certification and mutual recognition between CAs
  - Certification Path
- Registration authorities (RAs) responsible of identification and authentication of certificate subjects
- Digital certificates (certificate structure, basic fields, extensions and types)
- Certificate revocation lists (CRLs)
- Publishing digital certificates and CRLs
- OCSP responder (online certificate status protocol)
- Recommended cryptographic algorithms and key lengths
- Technical solutions
  - Open SSL
  - Open CA
  - EJBCA
  - Microsoft CA

Trust Models in PKI

- Rooted hierarchical trust model
- Network (cross certification) trust model
- Hybrid Trust Model

Hardware protection of (cryptographic) secrets

- Cryptographic smartcard card for end users
- Smartcard management systems
- Hardware security module (HSM) for servers

Digital Signature Mechanisms

- PKCS#7
- ASN.1/CMS
- CadES
- PAdES
- XMLDSig
- XAdES

Time Stamping Service

- Network Time Protocol (NTP) service
- Time stamp authority (TSA) and Time stamp providers (TSPs)
- Structure of Time stamp requests (TSRs) and Time stamp tokens (TSTs)
- Time stamp client tools
- ISO/IEC 18014, ANSI ASC X9.95 Standard and RFC3161
- Technical solutions
  - Open TSA
  - EJBCA TSA

Legal framework, policies and procedures

- Encryption
- Digital signature

Relevant PKI Standards and Protocols

- X.509 ITU-T standard
- RSA public-key cryptography standard PKCS
- RFC3647 «Internet X.509 Public Key Infrastructure
- Certificate Policy and Certification Practices Framework», RFC5280 «Internet X.509 PKI certificate and certificate revocation list (CRL) Profile», RFC3161 «Internet X.509 PKI time stamping protocols», RFC6277 «online certificate status protocol algorithm agility»
- European Telecommunication Standards Institute (ETSI)
  - TS 101 456: policy requirements for certification authorities issuing qualified certificates
  - TS 101 861: time-stamping profile
  - TS 102 023: policy requirements for time stamping authorities
  - TS 102 176-1 and TS 102 176-2: algorithms and parameters for secure electronic signatures

Transition to the Electronic Transactions

- Use of the cryptographic libraries to design and implement cryptographic solutions
  - IAIK, Bouncy castle
  - Oracle JCE/JCA
  - Open SSL
- Security over the Internet
  - SSL/TLS
  - Secure POP
  - Secure SMTP
  - Secure IMAP
  - S/MIME,
  - VPN SSL
- Secure mobile application through the use of mobile identity, mobile PKI, mobile signature, dual-use SIM cards etc
- Using cryptography in the context of Internet services
  - Government to Government (G2G)
  - Government to Citizens (G2C)

COURSE TRAINER

Dr Nizar Ben Neji

Dr Neji holds an engineering degree from the Tunisian National School of Computer Sciences and a PhD in Information and communication technologies (ICT) from Sup'Com of the University of Carthage in Tunisia. He has more than nine years of experience in ICT consultancy and training with comprehensive expertise in project management and security problem solving. Currently he is working as an assistant professor at University of Carthage, Tunisia. Some of Dr Neji working experience involves: Project manager at the Tunisian Government CA of the Ministry of Information and Communication Technologies, IT professional trainer at the National Centre of Training in Communication Technologies of the Ministry of ICT in Tunisia etc. In his consulting practice, Dr Neji has conducted a great number of training courses globally ranging from the Second International eID, ePasseport and PKI conference organised in Athens, Greece, the Third Arab PKI Forum organised by Arab Information and Communication Technologies Organisation and many more.

INTERNATIONAL COURSES	DATE	LOCATION	DURATION
ICT Regulation Understanding the Big Picture of ICTs for Development	October 26 - 30, 2015	London, UK	5 days
Telecommunications Finance for Non Finance	November 2 - 6, 2015	Johannesburg, South Africa	5 days
Building Consumer Advocacy in the Telecommunications	November 2 - 6, 2015	Port of Spain, Trinidad & Tobago	5 days
Licensing in a Converged Environment	November 2 - 6, 2015	Johannesburg, South Africa	5 days
Broadband Technologies and Multimedia Services	November 16 - 20, 2015	Gaborone, Botswana	5 days
Analogue to Digital Broad-casting Switchover	November 23 - 27, 2015	Johannesburg, South Africa	5 days
Introduction to IPTV	January 18 - 22, 2015	Johannesburg, South Africa	5 days

Who we are

The CTO is the oldest and largest Commonwealth organisation engaged in multilateral collaboration in the field of ICTs. Using in-house and partner experience, it supports members in integrating ICTs to deliver effective development interventions that emancipate, enrich, equalise and empower people within the Commonwealth and beyond.

What we do

The work of the CTO goes back to the Organisation's creation in 1901 as the Pacific Cable Board. Since then, the CTO has been at the centre of continuous and extensive international communications development funding, cooperation and assistance programmes. Since 1985, the Organisation has delivered to its members in Europe, the Caribbean, the Americas, Africa and Asia-Pacific over 3,760 bilateral and multilateral telecommunications and ICT capacity building projects in the form of policy, operational and regulatory training, and expert assistance. Moreover, the CTO has been at the forefront of generating cutting-edge knowledge through its research and consultancy services, as well as sharing ideas through its conferences and workshops held around the world. This long history as a development facilitator provides the Organisation with a unique and growing delivery capacity for ICT4D programmes and services.

Supporting ICT4D in the Commonwealth

The CTO seeks to work collaboratively with other Commonwealth bodies to build mutually beneficial synergies in the interests of its members. The CTO has a key role to play in leading ICT4D initiatives across the Commonwealth, and it is committed to working together with other Commonwealth entities to reduce overlap and replication of activities. The CTO welcomes the opportunity to offer secretariat support to any Commonwealth ICT initiatives that reflect the needs and interests of its members.

Registration Form

Personal Details

Event ID: 8199

Mr/Mrs/Ms/Other _____ First Name _____ Last Name _____

Job Title _____

Organisation _____

Address _____

City _____ Postcode _____ Country _____

Tel. _____ Mobile _____ Fax _____

E-mail _____

Authorising Line Manager's Name _____

Authorising Line Manager's E-mail _____

Payment Options

1. Select Delegate Rate (please refer to the list of CTO members/PDT Partners provided overleaf)

	Standard Rate	Early Registration by: 11 September 2015
CTO Members	☐ £750	☐ £650
PDT Partners	☐ £1,150	☐ £1,050

2. Payment Mode (choose from either Invoice, Bank Transfer, Cheque, or Credit Card)

☐ Invoice
Invoice me at the above address (Discounts do not apply, payment must be received by us prior to the above event's start date)

☐ Bank Transfer
To: Coutts & Co., 440 Strand, London WC2R 0QS, UK
A/c Name: CTO; A/c Number: 83675071
Reference: GB72COUT18000208367507
Sort Code: 18-00-02; Swift Code: COUT GB22

☐ Cheque
Cheque enclosed, payable to "CTO HQ"

☐ Credit Card: Visa / Mastercard (circle as appropriate)

Card Holder's Name _____

Card Holder's Billing Address (if different from above) _____

Card Number | | | | | | | | | | | | | | | | |

Valid From MM / YY Expiry Date MM / YY 3-digit security code on back of card | | |

Signature

Date _____ Name _____ Signature _____

Additional Information

To help us improve our services to you and your organisation, please tell us more about you and your organisation.

Your role in the organisation

- ☐ Strategic/executive
- ☐ Planning
- ☐ Control
- ☐ Operational

Your organisation type

- ☐ Government
- ☐ Regulator
- ☐ Operator
- ☐ Manufacturer
- ☐ Other

Your area of work in the organsnisation

- ☐ Business development
- ☐ Corporate affairs
- ☐ Customer service and care
- ☐ Engineering and technical management
- ☐ Financial, purchasing and investor relations
- ☐ IT/IP management
- ☐ Marketing and sales
- ☐ Public relations and corporate communications
- ☐ Regulatory and legal affairs
- ☐ Telecoms network management
- ☐ Human resources
- ☐ Other

Your organisation's service areas

- ☐ Fixed network/services
- ☐ Mobile/wireless network/services
- ☐ Satellite network/services
- ☐ Internet
- ☐ Broadcasting
- ☐ Value-added services
- ☐ Support
- ☐ Other services

Fax it back to +44 20 8600 3819, or return to the CTO at programmes@cto.int.

REGISTRATION DEADLINE

16 October 2015

3 SIMPLE WAYS TO REGISTER!

Fill in and fax this form back at +44 20 8600 3819

Call the programme team at +44 20 8600 3800

E-mail the programme team at programmes@cto.int, quoting the course "Event ID" above.

NEED HELP?

Call us now on +44 20 8600 3800
or e-mail the Programmes team at programmes@cto.int

Summary Terms and Conditions

The CTO will endeavour, as can be reasonably expected, to ensure that the course is delivered to meet delegates' expectations. Registration is subject to availability and payment received by the deadline where specified, or else before the course start date, whichever applies. Dates may be subject to changes. Travel, accommodation, daily transportation to venue, subsistence and other costs are the sole responsibility of the delegate and are not included in the above fees. Applicants are responsible for their visa arrangements and other formalities wherever required. Course bookings may be cancelled at the discretion of the CTO or its partners. Applicants paying by bank transfer are responsible for bank charges and any other such costs and should ensure the exact amount in GBP Sterling is credited in the CTO bank account. Applicants requiring additional information prior to their booking should ensure they provide sufficient time before the booking deadline. Cancellation rules apply, as summarised below. For a full version of our Ethical Framework or our Terms and Conditions, please visit our website at www.cto.int

Cancellations / Refunds

For delegate cancellations/withdrawals, the following refund rules apply:
- 31 days or more prior to event: the full amount less a handling charge of 10% or a minimum of £55, whichever applies
- 30 days or less prior to event: no refund

For CTO cancellations/withdrawals, delegates are entitled to a 100% refund within 60 days of the withdrawal/cancellation.
Refunds will be made by bank transfer only.

Data Protection / Privacy

The CTO does not sell, rent or lease its customer information to third parties. We may, from time to time, contact you on behalf of a third party/partner about a particular offering that may be of interest to you. In those cases, your unique personally identifiable information (e-mail, name, address, telephone number) is not transferred to the third party/partner. In addition, we may share your information with trusted partners to help us perform statistical analyses, send you by e-mail or postal mail, provide customer support, or arrange for deliveries or other such services. All such third parties are prohibited from using your personal information except to provide these services to the CTO and they are required to maintain the confidentiality of your information. For more information about our privacy policy, visit our website at www.cto.int.