Standardisation of Quantum Cryptography and Quantum Technologies

Thomas Längner, Austrian Research Centers – ARC, Vienna
Solange Ghernaouti-Hélie, Université de Lausanne

Certification and Standardisation - FP6 Integrated Project SECOQC

3rd ETSI Security Workshop
Overview

1. Project SECOQC
   – Objectives, participants, project structure
   – Advantages and problems of quantum cryptography

2. Standardisation of Quantum Cryptography
   – Applicability of standardisation
   – Standardisation Activities
   – ETSI Industry Specification Group
1. Project SECOQC
Project SECOQC

• EU-Integrated Project FP6 April ‘04 – September ’08

• General Objective:
  Development of a network for the generation and distribution of symmetrical secrets between arbitrarily remote network nodes

• Scientific and Technological Objectives:
  • Improvement of quantum key distribution technology
  • Development of a network-concept
  • Development of interfaces (customers)
  • Work towards certification and standardisation
More Facts...

• **Coordinator:**
  Austrian Research Centers GmbH – ARC, Vienna

• **41 Participants:**
  – 25 Universities
  – 4 National Research Centers
  – 8 Multinational Enterprises
  – 4 SMEs

• **From 11 European Countries**
  A, B, CH, CZ, D, DK, F, I, RU, S, UK

• **Budget:** 16,5 million €  **Funding:** 11,3 million €
Project Structure

• Quantum Part
  – Quantum Optical Components (COM)
  – Experimental Quantum Key Distribution (QKD)
  – Quantum Information Theory (QIT)

• Infrastructure Part
  – Security and Cryptography (SEC)
  – Network Architecture (NET)
  – System Integration and Requirements Analysis (SYS)
  – Certification According to Common Criteria (CCC)

• Implementation Part
  – Quantum Back-Bone (QBB)
  – Quantum Access Network (QAN)
  – Network Implementation (NI)
Quantum Cryptography...

...is actually “Quantum Key Distribution” – QKD

- A quantum link has two stations, connected by two channels
- Quantum information is encoded into single photons
- Photons are transmitted through quantum channel (optical glass fibre or free-space), other channel is a public classical channel
- Purpose: Generation and distribution of secret bit sequences
- Subsequently to be used for cryptographic tasks
Advantages

• ‘Provable Security’ (even in presence of attacker with unlimited computational power). Eavesdropping can be detected.

• Current public key cryptography systems (Diffie-Hellman key distribution) may become obsolete in the future (extremely powerful computers)
Problems

- Limitation in distance
- Limitation in secret-key-rate
- Limitation in availability
- Still expensive
SECOQC Network Paradigm: „Quantum Back Bone“

- Binary QBB-Links
- **QBB-Nodes** with multiple QBB-Links to neighbouring QBB-Nodes. Nodes must be trusted.
- Hop-by-hop distribution of secrets
QBB-Node I

QBB-Node Module interfaces with different QBB-Link technologies:

- Coherent One Way System
  (N. Gisin, Univ. Genève)
- One Way Weak Pulse System
  (A. Shields, Toshiba)
- Continuous Variables
  (P. Grangier, CNRS)
- Entangled Photons
  (A. Zeilinger, Univ. Vienna)
- Autocompensating Plug&Play
  (G. Ribordy, id Quantique, Genève)
SECOQC Demonstrator in the SIEMENS Optical Fiber Network
Vienna, Sept. 2008

- 5 QKD Technologies
- 5 QBB-Nodes / 7 QBB-Links
SECOQC Demonstrator in the SIEMENS Optical Fiber Network
Vienna, Sept. 2008
2. Standardisation of Quantum Cryptography
Standardisation in SECOQC

- Certification according to Common Criteria sub-project:
  - Need for standardisation arose gradually
  - Had to combine different links
  - Needed a basis for security evaluation

- Release SECOQC Node-Link Interface as de-facto standard
  (Creative Commons by-nc-nd license)

- Develop and promote detailed plan for standardisation activity
Standardisation On Three Levels

1. Top-level Interface (user interface)
   - Between QC Network and Application
   - ... to ensure connectivity to existing systems

2. Interfaces between macroscopic components of QC – network
   - Between links and network nodes of different vendors
   - ... to further development of components of different vendors

1. Properties of quantum optical components
   - Properties of photon sources, detectors, error rates
   - ... basis for security proofs, make products comparable
Standardisation for Quantum Cryptography

Top-level Interface (user interface)

– Shall be compatible with existing architectures and interfaces
– Shall be compatible with existing service management
– Will have to be developed with customers and vendors
Standardisation for Quantum Cryptography

Interfaces between macroscopic components of QC network

- Shall further development of interoperable components of different vendors
- Provide unified management (monitoring, performance management, fault management)
- Shall be developed with component developers
- SECOQC Link/Node Interface is about to be published as open “SECOQC standard”
Standardisation for Quantum Cryptography

Properties of quantum optical components

- Properties of photon sources and detectors
- Definition of key distillation protocols and applicable cryptographic algorithms
- Provable security of QKD relies on assumptions on components (like sources, detectors)
- Standardisation is the necessary foundation for security proofs and security evaluation
- Enables the definition of ‘Security Classes’ (metrology), makes products comparable
Three Initiatives - Pointing Out Importance

• Workshop on Quantum Information Technology at Royal Society, London, May ‘06
  – NIST, The Cambridge MIT Institute

• Japan. Initiative, ‘Updating QC’, Tokyo, Oct ‘07
  – JST (Japanese Science and Technology Initiative)
  – NICT (National Inst. for Information and Comm.)

• Telcordia Initiative (Oct. 2007)
  – Planning workshop ‘Missing Pieces and Real World Issues)
  – They are ETSI member!
Our Approach: ETSI Industry Specification Group (ISG)

- **Maintain European advantage** in quantum cryptography
- Create a forum with significant leverage effects on *coordination, cooperation, and convergence* on a European level
- **Accelerate user adoption**

  - Open for any interested parties
  - Projected start: Spring 2008
Thank You!

Thomas Längner
Quantum Technologies
Austrian Research Centers ARC, Vienna
thomas.laenger @ arcs.ac.at

Solange Ghernaouti-Hélie
Faculté des Hautes Etudes Commerciales (HEC)
Université de Lausanne
sgh @ unil.ch

www.secoqc.net
Development of a Global Network for Secure Communication based on Quantum Cryptography

www.secoqc.net