

# QKD in ETSI

Gaby Lenhart  
Strategy and New Initiatives  
© ETSI 2009. All rights reserved

A dark blue world map with a subtle gradient, showing the continents in a slightly lighter shade of blue. The map is centered on the Atlantic Ocean.

## Current Use of QKD

# QKD already in use I

- ❑ **11. October 2007 – Swiss Federal Elections (**  
<http://www.idquantique.com/news/news-elections2008.htm>)
  - QKD used to secure a gigabit ethernet link connecting the central counting station located in downtown Geneva and the data center where all the results were stored and processed
  - following this successful pilot project, the Chancellery of the Canton of Geneva decided to on QKD for all future elections
- ❑ **2009 first metropolitan QKD network in Durban (**  
<http://www.secoqc.net/downloads/abstracts/SECOQC-Pettruccione.pdf>)
  - based on the QuantumCity project from 2005 consisting of four nodes in a Municipal Area Network star configuration linking municipal buildings in Pinetown, Westville and Cato Manor
- ❑ **2010 QKD to be used by 3 Japanese ministries**
  - this was officially announced by high ranked representants of these ministries on slide presentations during the UQC 2008 meeting organized by NICT in Tokyo, but unfortunately these slides are not publicly available
  - funding for proceedings on QKD for the next 10 years currently under government review

# QKD already in use II

### ❑ 2010 first European metropolitan QKD network in Madrid

<http://www.secoqc.net/downloads/abstracts/SECOQC-Fernandez.pdf>

- UPM project focuses on sharing as much infrastructure as possible between the quantum and conventional parts and manage services and network in an integrated way to allow for the network to grow o demand

### ❑ 2010 first metropolitan QKD network in London

[http://www.qinetiq.com/home/newsroom/news\\_releases\\_homepage/2009/2nd\\_quarter/02.html](http://www.qinetiq.com/home/newsroom/news_releases_homepage/2009/2nd_quarter/02.html)

- Operating QinetiQ's quantum-based security over AboveNet's dedicated fibre optic network in London will offer an extremely secure way for governments, financial institutions and organisations with high security requirements, to transfer confidential information and sensitive data



World Class Standards

# ETSI ISG on QKD

ECOC 2009

## Organization

- ❑ **Chair:**
  - Thomas Laenger (AIT)
- ❑ **Vice Chairs:**
  - Brian Lowens (Qinetiq)
  - Gregoire Ribordy (id Quantique)
- ❑ **Secretary:**
  - Mercedes Soto Rodriguez (Telefonica)
- ❑ **Support Coordinator:**
  - Estelle Mancini (ETSI)
- ❑ **STFs:**
  - 367 (financed by EC)

## Terms of Reference

- ☐ **Analysing the cryptographic implications of Quantum Key Distribution**
- ☐ **Securing confidentiality and privacy of communication in the future ICT**
- ☐ **Specify a system for QKD and its environment**
- ☐ **Transferring quantum cryptography out of the controlled and trusted environment of experimental laboratories into the real world with business requirements, malevolent attackers, and societal and legal norms to be respected**

### Members of ISG QKD

- ☐ AIT
- ☐ Arche Finanz
- ☐ HP
- ☐ id Quantique
- ☐ Instiut telecom
- ☐ INRiM
- ☐ MIMOS Behard
- ☐ NICT
- ☐ QinetiQ
- ☐ QuantumWorks
- ☐ Smart Quantum
- ☐ Swisscom
- ☐ Telcordia

- ☐ Telefonica
- ☐ Thales
- ☐ Toshiba
- ☐ Uni Politecnica de Madrid

there are several more candidates to signing contracts with this ISG on QKD, some contracts are currently on their way to ETSI



## Current Work Items

- ☐ **Security assurance requirements**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=28890](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=28890)
- ☐ **User requirements**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=29096](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=29096)
- ☐ **Components' interfaces**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=29099](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=29099)
- ☐ **Application interfaces**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=29097](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=29097)
- ☐ **Security proofs**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=29098](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=29098)
- ☐ **Integration within optical networks**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=29100](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=29100)
- ☐ **Ontology**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=30486](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=30486)
- ☐ **Security specification**  
[http://webapp.etsi.org/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=30487](http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=30487)

### What's next

- ❑ **Necessary steps beyond the development of QKD basic technology to transfer QKD from lab to commercial environment**
  - development of networked structures (network types): mixed networks, hierarchical networks,...
  - improve key-generation rates
  - system management
  - connectivity
  - trusted repeaters
  - access for end-users
- ❑ **ETSI's doors are wide open towards other Quantum Technologies**
  - hardware components for QKD networks
  - several groups speak about enormous bandwidth needed for future generation IPTV
  - see, if there is a need for Quantum Compression

## Degrees of success



**Real success: Specifications are used & implemented**

## Contact

□ **Gaby Lenhart, ETSI SNI Senior Research Officer**

- [gaby.lenhart@etsi.org](mailto:gaby.lenhart@etsi.org)
- **+33 6 74 40 83 76**



ECOC 2009