QUANTUM SECURE (PRE) STANDARDIZATION IN ETSI

May 2014

Presented by Gaby Lenhart

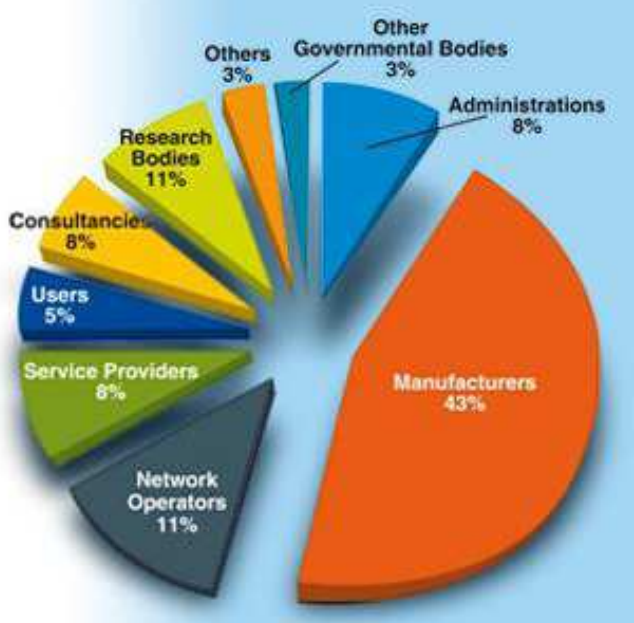
for **Post-Quantum Research - Identifying Future Challenges and Directions**

What Is ETSI?

- Globally applicable standards for Information & Communications Technologies:
  - Telecommunications
  - Radiocommunications
  - Broadcasting
  - Other related areas
- Officially recognised European Standards Organization
- Independent, Not-for-profit
- Direct member participation
- 30,000 publications available for free
- ISO 9001 : 2000 Certified

Membership

- Almost 800 companies, big and small, from more than 70 countries on 5 continents
- Manufacturers, network operators, service and content providers, national administrations, ministries, universities, research bodies, consultancies, user organizations



A powerful and dynamic mix of **resources, skills** and **ambitions**

Basic Requirements for Standards

- Standards must free for download to everybody
- IPR Policy defining obligations to inform users of standards about Essential IPRs
- FRAND IPR policy is strongly recommended
  - **F**air
  - **R**easonable
  - **A**nd
  - **N**on-
  - **D**iscriminatory
- details in SR 000 314

Why Standardization Matters

- Standardization contributes to consumer confidence
- Standardization lowers the burden of evolution and maintenance, supported by industry
- Products are commercialized faster by
  - Exploiting already existing research results
  - discovering and feeding back technical issues into research
  - avoiding full manufacturing of interim development steps
- Standardization focuses investment into research for certain issues
- Standardization improves technologies and products through multiple feed-back
- Products reach global markets
- Standardization ensures interoperability
- Standardization ensures backward compatibility

Members of ISG QKD

- Applied Communication Sciences
- Arche Finanz
- Austrian Institute of Technology
- German Bundesmisterium fuer Wirtschaft und Technologie
- Hewlett Packard
- ID Quantique
- INRiM
- MIMOS Berhad
- Mitsubishi
- NICT
- National Physical Laboratories
- NTT
- QinetiQ
- SK Telecom
- Swisscom
- Telecom Paris Tech
- Telefonica
- Thales
- Toshiba
- Tubitak Uekae
- UK Department for Business, Innovation & Skills
- Universidad Politechnica de Madrid
- University of Waterloo

Overview

- Chairman = Dr. Andrew Shields, Toshiba
- Specifications in draft
  - Integration into optical networks (http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=29100)
  - Ontology (http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=30486)
- Published specifications (http://pda.etsi.org/pda/queryform.asp)
  - Use Cases
  - Components and Internal Interfaces
  - Application Interfaces
  - QKD Module Security Specification
  - Security Specification

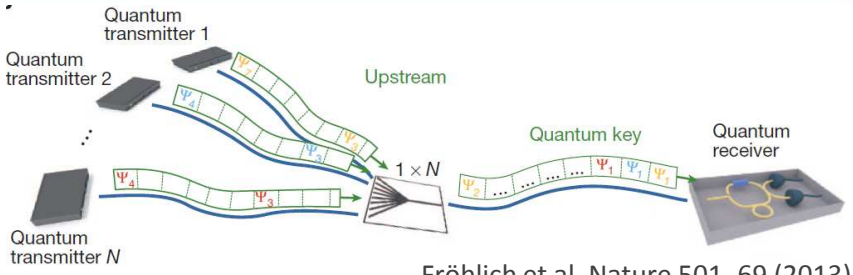
QKD Issues currently Standardized I

- Implementation Security
  - Describe the necessary system elements – without impeding innovation
  - Metrology of components and system blocks
  - Qualifying tests to quantify against modes of attack
  - Relate back to security proofs
- Channel Requirements
  - What are the requirements on fibre link?
  - How to specify
  - Enable customer to estimate performance in a network
  - Requirements when multiplexing with classical data - crosstalk etc.

Martin Ward and Andrew Shields, Toshiba Research Europe Ltd., 1st ETSI QSC workshop, 2013

QKD Issues currently Standardized II

- Quantum Networks
  - Quantum access networks
  - Quantum repeaters
  - Leading on to distributed quantum computing – quantum cloud – secure database search etc.



Fröhlich et al. Nature 501, 69 (2013)

- Interfaces
  - Enabling systems to be networked together
  - Classical interfaces: system management, network routing, how key material is used
  - Quantum interfaces: connect where technology is compatible, quantum information sharing etc. in future

Martin Ward and Andrew Shields, Toshiba Research Europe Ltd., 1st ETSI QSC workshop, 2013

ETSI QSC Workshop Series

- Quantum-Safe Cryptography workshop series
  - Conference proceedings:

  http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf
  - Aim: bringing together the conventional cryptography community and the quantum cryptography community to jointly create and standardize a quantum-safe cryptographic environment

ETSI 2nd Quantum-Safe Crypto Workshop in partnership with the IQC, 6-7 Oct. 2014, Ottawa

- Call for Presentations open until end of June
  http://www.etsi.org/news-events/events/770-etsi-crypto-workshop-2014

Who Should Write the Standards?

In all the history of standardization the
most successful standards
always were
written by those
who use them later on.

A really successful standard
is used by the vast majority of those
who offer products of the particular technology
on the market.

Contact Details:

Gaby Lenhart, Senior Research Officer

gaby.lenhart@etsi.org

Thank you!