






**SYNAPTIC**  
LABORATORIES LTD.

## Technologies for our Quantum Future (2007)



Emerging technologies will enable Smart Cards to meet new identity theft challenges with post quantum security, anonymous authentication and hardware validation of tokens in a Federated System

# Presentation outline

**Part 1:** Government Directions to prevent Identity Theft

**Part 2:** New Challenges

**Part 3:** New Technologies

**Part 4:** Comprehensive Solution





# Part 1:

## Government Directions to Prevent Identity Theft

# EC Directions on Identity Management

- Increasing corporate responsibility for data security
- Stakeholder control of information flow
  - Unobservability by third parties
  - Pseudonymity with accountability
- 50 to 100 year security and availability
  - Auditability

## Principle Objectives

- The authorized participants of a transaction maintain long term control over when, where and who accesses their private data
- Reduce unintended information disclosure and its proliferation
- Opportunities for choice between trusted service providers in a Federated System





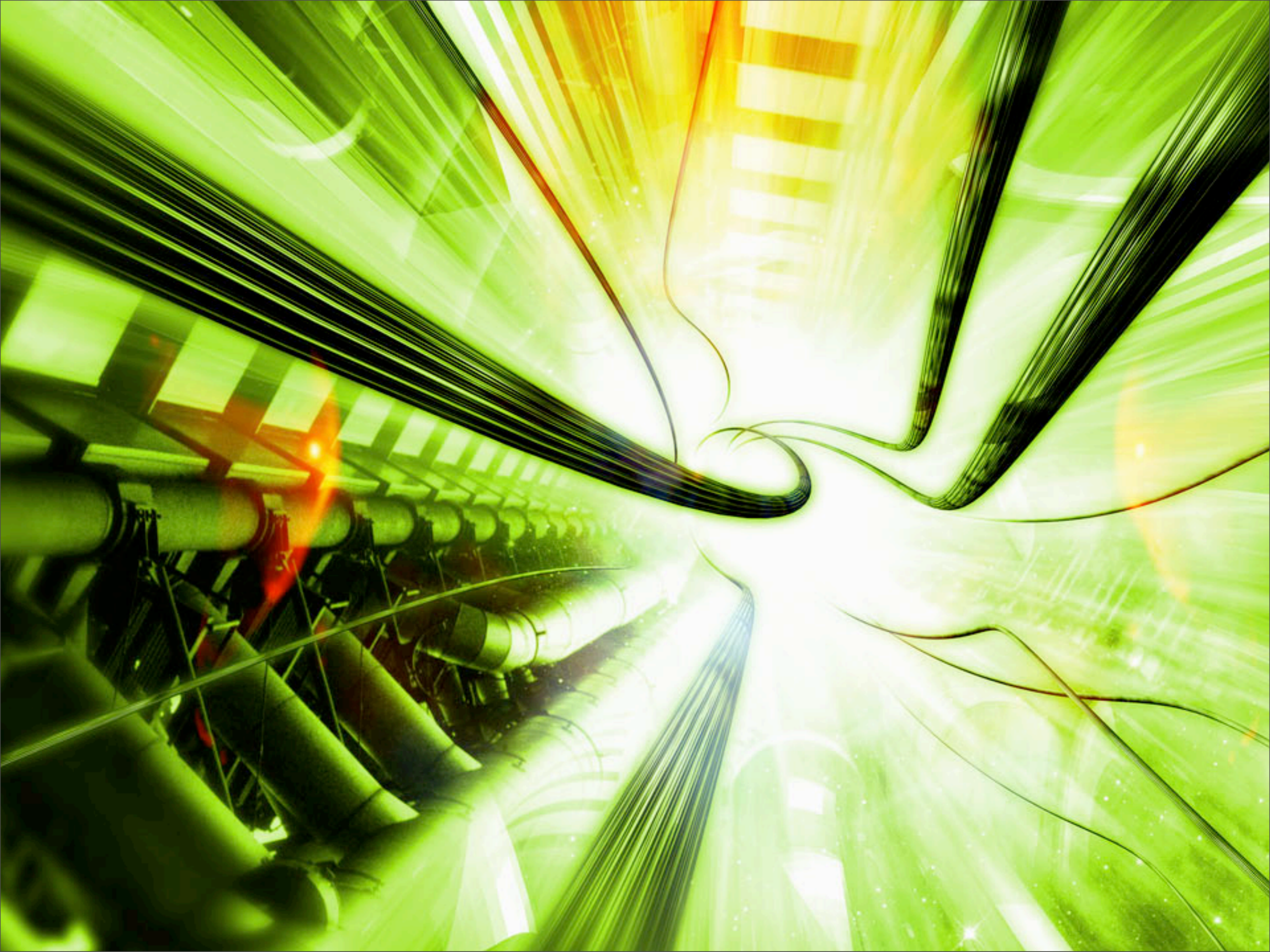
## **Part 2:**

# New Challenges

Challenge of Increased Connectivity

Challenge of Increased Monitoring

Challenge of Increased Computing power





## **Challenge of Increased Connectivity**

The existing Internet enables enormous information capture and flow

The Network of the Future greatly increases this ability by dramatically increasing the number of devices and enabling Multi-Gigabit per second traffic flow

# Network of the Future

- **Security:** Protect the Internet from technology failures
  - **Interoperability:** Enhanced interaction between devices
  - **Interconnectivity:** Support increased number of devices
  - **Speed:** Faster Broadband in Europe
- “i2010 - A EU Information Society for growth and employment”,  
Commission of the EU Communities June 2005



# Network of the Future

The major IT research groups funded by the European Commission (EC) met together at the Helsinki Network of the Future (NoF) conference in November 2006 to confirm their readiness to begin creation of a NoF



# Network of the Future

In 2007 the European Commission allocated 200 Million Euro to support research into Network of the Future (NoF) related technologies

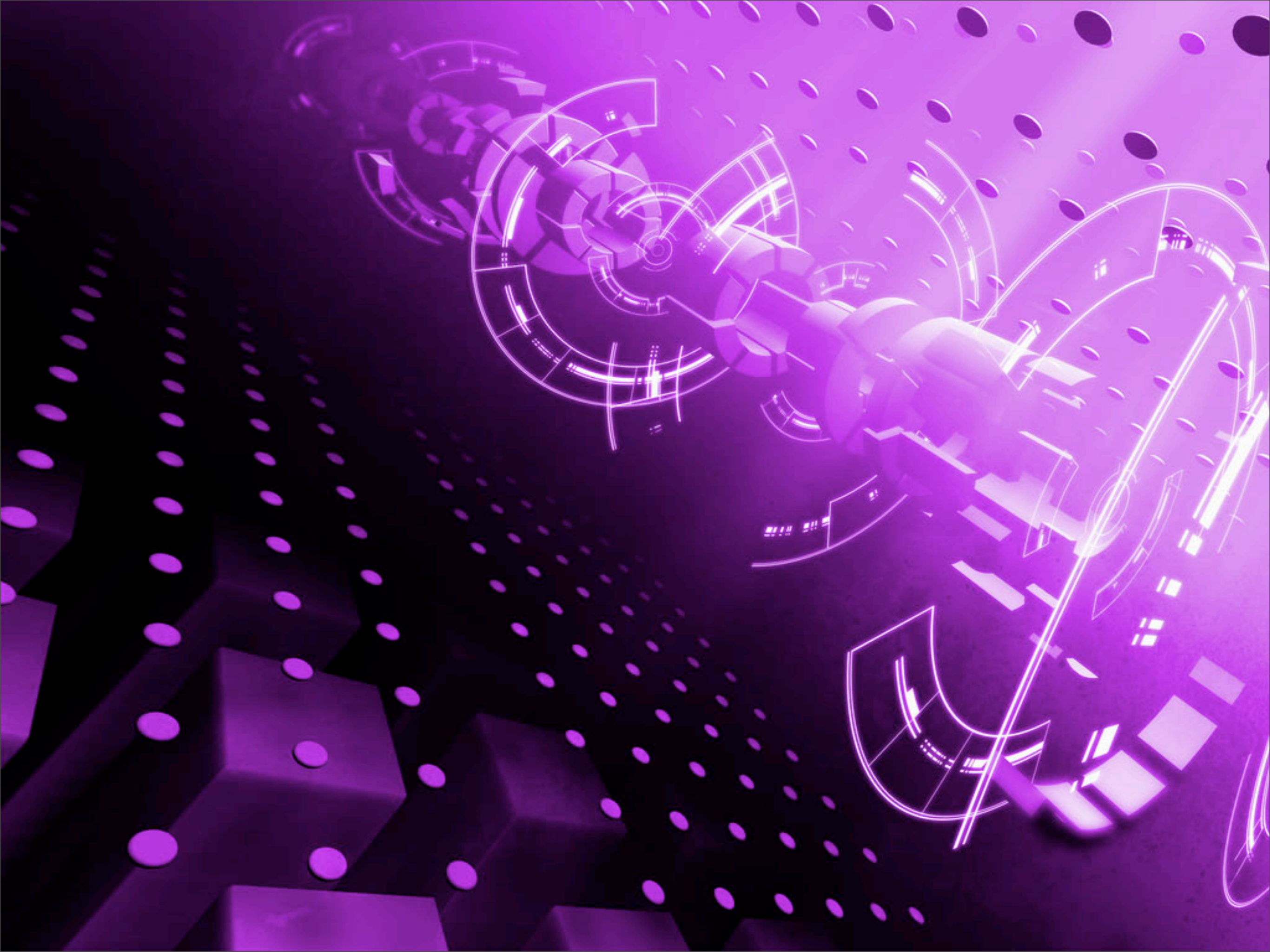
(EC FP7 ICT Work Program 2007-2008)



# Network of the Future

On August 17 2007 Japan announced it will also begin research into a replacement for the Internet

Japan hopes to have a new Super Internet ready for deployment by 2020



## Challenge of Increased Monitoring

In the EC vision of an ambient intelligence world billions of tiny devices work interactively to support people and improve every day activities

**These devices provide services, monitor and gather and distribute information**

# Ambient Intelligence Monitoring

RFID and contactless Smart Card technologies are an important part of the ambient intelligence vision

Many of the next generation technologies and services in ambient intelligence will evolve out of the Smart Card Industry (See Eurosmart)

# Ambient Intelligence Security Failure

With billions of smart objects deployed in the field a **security failure** of the core cryptographic primitives would be a nightmare to manage

It will be extremely expensive to systematically find and replace billions of low-cost smart objects owned by millions of different organisations

## Ramifications of NoF and Aml

- A large number of **virtually invisible devices** will be **monitoring physical and electronic emanations**
- **Massive bandwidth** available to support the transport of information about our environment
- **Unintended information disclosure** will likely be **monitored and rapidly proliferated**





## Challenge of Increased Computing power

If large Quantum Super Computers can be built, it is universally acknowledged that their security threat is global and catastrophic...

- 3DES and AES-128 encryption would be broken
- SHA-1 hash function could not be trusted



## Challenge of Increased Computing power

- RSA-2048 and ECC-193 Digital Signatures could not be trusted
- RSA-2048 and ECC-193 Key Exchanges would no longer ensure privacy
- **All the many-to-many key exchange and digital signature operations implemented in Smart Cards today would be broken**



# Availability of Quantum Computers

“In the **medium term**, we need to be **prepared** for the eventuality that large quantum computers could be built”

- **Secure IST**, “D3.3 – ICT Security & Dependability Research beyond 2010: Final Strategy”, January **2007**





# Availability of Quantum Computers

In **February 2007** Canadian Super Computing Company D-Wave publicly demonstrated the proof of concept for its Super Computer (16-qbit)

D-Wave declares it will have large Super Computers commercially available in **2009-2010** for commercial applications





# Availability of Quantum Computers

The risk is evidently high as Major Corporations and Government bodies have started to take action:

- Installing Quantum Key Distribution Systems that require point-to-point optical fiber connections (Banks, canton of Geneva)
- Using quantum secure Digital Signatures (BSI of Germany use Coronado-Merkle)







## Part 2:

# New Technologies

Emerging techniques that **comprehensively** address the quantum security challenges

“we need to be **prepared** for the eventuality that large quantum computers could be built:

this would require an upgrade of most symmetric cryptographic algorithms and a completely new generation of public-key algorithms.”

- **Secure IST**, “D3.3 – ICT Security & Dependability Research beyond 2010: Final Strategy”, January **2007**

# Quantum Secure Privacy and Integrity

The common ciphers on Smart Cards are insecure against large Quantum Computers:

- DES, 2DES
- AES-128
- SHA-1
- SHA-256 (marginal security)

# Quantum Secure Privacy and Integrity

Upgrading the standards based security in Smart Cards generally requires a new generation of hardware

# Quantum Secure Privacy and Integrity

Synaptic Laboratories Limited offers an emerging software technology that is an immediate solution for existing cards

The solution uses **DES-56** to create **256-bit** Quantum Secure privacy and integrity operations (512-bit key, 768-bit hash)

# Quantum Secure Digital Signatures

The RSA and ECC Digital Signature Algorithms in Smart Cards are not post quantum secure operations

Synaptic Laboratories' research concludes that the Coronado-Merkle Digital Signature scheme can be implemented in software on existing Java Cards

“a significant breakthrough in quantum computation would **spell doom** for all these (RSA, D&H, ECC) systems.”

- The European Network of Excellence for Cryptography  
**ECRYPT**, D.AZTEC.2 Alternatives to RSA  
27 July 2005

# Quantum Secure Key Exchanges

The RSA and ECC key exchange algorithms globally deployed in Smart Cards and vital protocols such as Secure Socket Layer used to protect websites are not quantum secure operations

“Public key crypto key exchanges (RSA, D&H)...  
would essentially be ‘flat-lined’ by quantum  
computing, rendering them completely broken.”

“Open Problem”

- Brian Snow,  
Retired Technical Director of the US  
National Security Agency (**NSA**),  
Public Key Cryptography 30th Anniversary  
Conference, **Dec 2006**

# Synaptic's Quantum Secure Key Exchange

Synaptic Laboratories has prototyped a post Quantum Secure Key Exchange technology that is implemented in software on existing Java Cards (Q4 2007)

This technology is currently undergoing evaluation for use in the design of new secure protocols on Smart Cards

# Synaptic's Quantum Secure Key Exchange

- Requires the use of Smart Card like technologies
- Is suitable for use on Packet Switched Networks such as the Internet and Ethernet
- Is suitable for use in area constrained Aml devices
- Is suitable for securing traffic on the NoF



## Potential for lower cost tokens

- Use of Synaptic's Post Quantum Secure Key Exchange process does not require additional hardware unlike RSA and ECC implementations
- A single post quantum secure hash function is sufficient to accelerate all essential cryptographic operations within a Smart Card

## Three options for the Hash function

- Use the Synaptic enhanced DES Solution (PQSDES is a software cipher that is accelerated using DES hardware)
- Use the SHA-256 or SHA-512 cipher (requires retooling smart cards)
- Use one of the Synaptic VEST hardware dedicated multi-purpose ciphers (requires retooling smart cards)





**Part 4:**

# **Attributes of Future Systems**



## Attributes of future systems

- Anonymous authentication (wrt. observers) to reduce the distribution of exploitable data in a NoF / Aml world
- Post quantum secure cryptographic operations based on symmetric techniques to provide long term security
- A distributed decentralised Federated System to ensure choice of service providers and no central point of security failure



## Natural Security Extensions

- Synaptic's research concludes that large scaled anonymous authentication of tokens in a Federated System is possible
- These Federated Systems naturally support extensions such as pseudonyms and fine grain auditing of transactions



## Q4 2008 Update

- Synaptic has advanced the design of the post quantum secure key exchanges and received positive independent preliminary evaluations
- Synaptic has advanced the design of high speed post quantum secure hash functions suitable for next generation digital signatures on smart cards



# Synaptic Technologies Enquiries

Ron Kelson  
Chairperson and CEO  
Synaptic Laboratories Limited

[r.kelson@synaptic-labs.com](mailto:r.kelson@synaptic-labs.com)  
+356 79 56 21 64

